BEDIENUNGSANLEITUNG

Bitdefender CONSUMER SOLUTIONS

Ultimate Small Business Security

Bitdefender Ultimate Small Business Security

Bedienungsanleitung

Publication date 05/31/2024

Impressum

Bitdefender

Inhaltsverzeichnis

ÜBER DIESE ANLEITUNG

Zweck und Zielgruppe

Bitdefender Ultimate Sicherheit für kleine Unternehmen ist ein Abonnementpaket mit mehreren Abonnements, das auf die Cybersicherheitsanforderungen kleiner Unternehmen zugeschnitten ist. Mit einem umfassenden Funktionsumfang, dediziertem Onboarding und intuitiven Verwaltungstools können Kleinunternehmer ihre digitalen Assets ohne IT- oder Cybersicherheitskenntnisse schützen.

Der Plan bietet umfassenden Schutz, der speziell auf kleine Unternehmen zugeschnitten ist, einschließlich:

- **Plattformübergreifender Geräteschutz:** Schützen Sie alle Ihre Geräte, von Computern bis hin zu Mobiltelefonen und Servern.
- **Einfache Verwaltung:** Sorgen Sie mühelos für die Sicherheit Ihres Teams und Ihrer Geschäftsabläufe.
- **Schutz des Unternehmensvermögens und des Rufs:** Sorgen Sie für den größtmöglichen Schutz Ihres Unternehmens, indem Sie eine Verbindung zu betrügerischen Aktivitäten verhindern.
- **Optimiertes Setup:** Der Onboardingprozess vereinfacht die Einrichtung für technisch nicht versierte Benutzer und gewährleistet eine reibungslose und sichere Konfiguration.

So verwenden Sie dieses Handbuch

Dieses Handbuch ist um die vier Produkte herum aufgebaut, die in Bitdefender Total Security enthalten sind:

- Absolute Sicherheit für den PC (Seite 9)
  Erfahren Sie, wie Sie das Produkt auf Ihren Windows-basierten PCs und Laptops verwenden.
- Virenschutz für Mac (Seite 160)
  Erfahren Sie, wie Sie das Produkt auf Ihren Macs verwenden.
- Mobile Sicherheit für Android (Seite 194)
  Erfahren Sie, wie Sie das Produkt auf Ihren Android-basierten Smartphones und Tablets verwenden.

- Mobile Sicherheit für iOS (Seite 231)
  Erfahren Sie, wie Sie das Produkt auf Ihren iOS-basierten Smartphones und Tablets verwenden.
- VPN (Seite 247)
  Erfahren Sie, wie Sie Ihre Online-Identität mit Bitdefender VPN auf jedem Ihrer Geräte verbergen.
- Passwortmanager (Seite 270)
  Behalten Sie den Überblick und speichern Sie alle Ihre Passwörter und Anmeldeinformationen sicher mit dem Passwort-Manager.
- Schutz der digitalen Identität (Seite 297)
  Erfahren Sie, wie Sie den Schutz Ihrer digitalen Identität richtig verwalten.
- Hilfe und Support (Seite 305)
  Finden Sie heraus, wo Sie Hilfe suchen können, wenn etwas Unerwartetes auftaucht.

Konventionen in diesem Handbuch

Typografie

Um die Lesbarkeit zu fördern werden verschiedene Arten von Textstilen verwendet. Die jeweiligen Bedeutungen entnehmen Sie bitte der nachfolgenden Tabelle.

Erscheinungsbild	Beschreibung
Beispielsyntax	Syntaxbeispiele sind in Konstantschrift dargestellt.
https://www.bitdefender.com	Verweise (Links) auf externe Inhalte auf HTTP- oder FTP-Servern.
documentation@bitdefender.com	Verweise auf E-Mail-Adressen, z. B. zur Kontaktaufnahme.
<link xlink:href="urn:resource:component:28104">Über diese Anleitung</link>	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
Dateiname	Dateien und Verzeichnisse sind in Konstantschrift dargestellt.
Optionen	Alle Produktoptionen sing **fett** gedruckt.
Stichwort	Wichtige Stichwörter oder Ausdrücke werden durch **fett** hervorgehoben.

Zusätzliche Hinweise

Zusätzliche Hinweise sind im Text grafisch markiert und liefern ergänzende Informationen zum aktuellen Absatz, die Sie unbedingt beachten sollten.

Hinweis

Ein solcher Hinweis ist nur eine Anmerkung. Sie können ihn überspringen, dennoch können Hinweise auch nützliche Informationen z. B. zu einzelnen Funktionen oder verwandten Themen liefern.

Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es handelt sich in der Regel nicht kritische, aber dennoch wichtige Informationen.

Warnung

Hierbei handelt es sich um kritische Informationen, die besondere Vorsicht erfordern. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie müssen unbedingt gelesen und verstanden werden, weil sie auf riskante Vorgänge hinweisen.

Ihre Mithilfe

Wir laden Sie ein mit zu helfen unser Buch zu verbessern. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen. Bitte schreiben Sie uns bezüglich Fehler, die in diesem Buch finden oder auch bezüglich Dinge, die Ihrer Meinung nach verbessert werden könnten. Dies hilft uns Ihnen die beste mögliche Dokumentation zur Verfügung zu stellen.

Schicken Sie Ihre Anmerkungen an documentation@bitdefender.com. Bitte verfassen Sie bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch, damit wir sie schnellstmöglich bearbeiten können.

1. EINRICHTEN IHRES ABONNEMENTS

Mit Ihrem **Bitdefender Ultimate Small Business Security**-Abonnement können Sie sofort loslegen. Die Einrichtung ist schnell und unkompliziert und braucht keine IT- oder Cybersicherheitskenntnisse. Sie müssen lediglich:

1. **Bitdefender Ultimate Small Business Security aktivieren:**
   Befolgen Sie dazu die Anweisungen in der Bestätigungs-E-Mail, die Sie nach dem Kauf des Produkts erhalten haben.
2. **Ihr Unternehmenskonto einrichten:**
   Nach der Aktivierung werden Sie aufgefordert, Ihren Unternehmensnamen einzugeben. Dies dient lediglich der Identifizierung und wird an verschiedenen Stellen in der Benutzeroberfläche angezeigt. Sie können jeden beliebigen Namen verwenden, da keine Überprüfung erfolgt.
3. **Wählen Sie Ihre Rolle im Unternehmen:**
   - **Geschäftsinhaber:** Wählen Sie diese Option, wenn Sie der Geschäftsinhaber sind und die Käufe sowie die Einrichtung selbst vornehmen.
   - **Sicherheitsadministrator:** Wählen Sie diese Option, wenn Sie für die Sicherheitsverwaltung im Unternehmen zuständig sind.

     Hinweis
     Der Sicherheitsadministrator hat ähnliche Berechtigungen wie der Geschäftsinhaber, jedoch ohne die Möglichkeit, Einkäufe zu tätigen.

4. **Teammitglieder zur Kontoerstellung einladen:**
   Nachdem Sie Ihren Namen und Ihre Position ausgewählt haben, sehen Sie eine Übersicht Ihres Bitdefender-Abonnements. Hier können Sie das Abonnement entweder mit anderen Teammitgliedern teilen oder mit der eigenen Einrichtung fortfahren, indem Sie die Installationsanweisungen für das jeweilige Gerät befolgen.

> **Wichtig**
> Es wird empfohlen, zunächst Ihre Mitarbeiter einzuladen, bevor Sie mit den Installationsschritten beginnen.

5. **Rollen der Teammitglieder auswählen:**
   Wählen Sie die Rollen der Mitarbeiter aus, die Sie zu Ihrem Sicherheitsabonnement hinzufügen möchten. Sie können sie einladen als:

   - **Sicherheitsadministrator:** Diese Rolle umfasst das Verwalten von Mitgliedern, Geräten und Sicherheitsvorgängen. Sie ist für Mitarbeiter vorgesehen, die über ein gewisses IT-Verständnis verfügen und für die Überwachung der Cybersicherheit Ihres Unternehmens verantwortlich sind.
   - **Mitarbeiter:** Mitarbeiter haben eingeschränkte Zugriffs- und Verwaltungsmöglichkeiten. Sie benötigen ein Bitdefender Central-Konto, um ihre eigenen Geräte zu schützen. **Sicherheitsadministratoren dagegen** können ihren Schutz verwalten und die Geräte per Fernzugriff verwalten.

6. **E-Mail-Einladungen an Teammitglieder senden:**
   Geben Sie die E-Mail-Adressen der Mitarbeiter ein, mit denen Sie das Bitdefender-Abonnement teilen möchten. Es können mehrere Einladungen gleichzeitig gesendet werden.

   > **Hinweis**
   > Eingeladene Mitglieder erhalten unabhängig von ihrer Rolle eine E-Mail-Einladung. Sie müssen auf die Schaltfläche **In Bitdefender Central aktivieren** klicken und die Einladung mit derselben E-Mail-Adresse annehmen, über die sie eingeladen wurden.

7. **Zu überwachende sensible Geschäftsdaten hinzufügen:**
   Als letzter Schritt müssen Sie die Überwachung der Unternehmensressourcen auf Gefährdungen einrichten.

   > **Hinweis**
   > **Gefährdung von Unternehmenswerten** ist ein Dienst, der nur für Administratorrollen verfügbar ist (**Sicherheitsadminstrator** und **Geschäftsinhaber**).

Diese Funktion überwacht Ihre Unternehmensdaten auf mögliche Gefährdungen, um den guten Ruf Ihres Unternehmens zu schützen und gezielte Angriffe zu verhindern.

- Im linken Menü Ihres Bitdefender Central-Kontos finden Sie den Abschnitt**Unternehmensaktivitäten**.
- Klicken Sie im Abschnitt **Gefährdung von Unternehmenswerten** auf die Schaltfläche **Zur Einrichtung**.
- Geben Sie die erforderlichen Unternehmensdaten ein:
  - Geschäftliche E-Mail-Adresse
  - Firmenkreditkarte
  - Social Media-Konten
- Nachdem Sie alle vorgeschlagenen Maßnahmen ergriffen haben, klicken Sie auf die Schaltfläche **Als erledigt markieren**, um das Ergebnis zu bestätigen und Ihren Fortschritt zu verfolgen.

Wenn Sie diese Schritte abgeschlossen haben, können Sie mit der Einrichtung von **Bitdefender Ultimate Small Business Security** für sich selbst beginnen:

- Auf Windows-Geräten installieren: Installation (Seite 9)
- Auf macOS-Geräten installieren:Bitdefender Antivirus for Mac wird installiert (Seite 161)
- Auf Android-Mobilgeräten installieren: So installieren Sie Bitdefender Mobile Security (Seite 194)
- Auf iOS-Mobilgeräten installieren: Installation von Bitdefender Mobile Security for iOS (Seite 232)
- Bitdefender VPN auf Ihren Geräten installieren: Bitdefender Password Manager wird installiert (Seite 249)
- Passwort-Manager einrichten:Installation (Seite 272)
- Digital Identity Protection konfigurieren: Digital Identity Protection konfigurieren (Seite 298)

Mit diesen Schritten schließen Sie die erfolgreiche Aktivierung und Einrichtung von **Bitdefender Ultimate Small Business Security** für Ihr Unternehmen ab.

2. GEFÄHRDUNG VON UNTERNEHMENSWERTEN

Gefährdung von Unternehmenswerten ist ein Dienst von Bitdefender Ultimate Small Business Security , der von Administratoren (Geschäftsinhaber und Sicherheitsadministrator) verwaltet wird. Er bietet Einblick in die potenzielle Gefährung wichtiger Unternehmensdaten bei Datenpannen. Gefährdung von Unternehmenswerten überwacht drei Komponenten, um Datenpannen zu erkennen:

- Geschäftliche E-Mail-Adresse
- Firmenkreditkarte
- Social Media-Konten

Warum die Überwachung auf Gefährdung von Unternehmenswerten so wichtig ist:

- **Rufschutz:** Schützt den Ruf Ihres Unternehmens, indem es eine umgehende Reaktion auf Datenpannen ermöglicht.
- **Mitarbeitersicherheit:** Schützt Mitarbeiter vor Phishing und anderen Social-Engineering-Angriffen durch Überwachung und Verwaltung ihrer Daten auf potenzielle Gefährdungen.
- **Prävention gezielter Angriffe:** Minimiert die Gefahr gezielter Angriffe, indem der Schutz sensibler Informationen sichergestellt wird.

Nachdem Sie die Details für Ihre Überwachung auf **Gefährdung von Unternehmenswerten**im Rahmen des **Einrichten Ihres Abonnements (Seite 4)**Prozesses eingerichtet haben, können Sie **die Ergebnisse einsehen und auf Empfehlungen reagieren:**

Das System benachrichtigt Sie über jede Datenpanne, die diese überwachten Ressourcen betrifft, einschließlich der betroffenen Dienste und der Arten von gefährdeten Daten (z. B. E-Mail-Adressen, Benutzernamen, Passwörter, geografische Standorte). Es werden nur die Kategorien der gefährdeten Daten angezeigt, keine spezifischen Details.

Für jede überwachte Komponente (geschäftliche E-Mail-Adresse, Firmenkreditkarte, Social-Media-Konten) sollten die empfohlenen Sicherheitsmaßnahmen umgesetzt werden. Vorgeschlagene Maßnahmen umfassen:

- Mitarbeiter dazu auffordern, ihre geschäftliche E-Mail-Adresse mit Bitdefender Digital Identity Protection zu überwachen.
- Passwörter auf betroffenen Webseiten ändern und Mitarbeiter dazu anhalten, den Bitdefender Password Manager zu nutzen.
- Sicherstellen, dass Mitarbeiter Bitdefender-Sicherheitslösungen auf ihren Geräten installieren, um Cyberangriffe zu verhindern.
- Mitarbeitern empfehlen, den Scam Copilot zu nutzen, um sich über Betrugsmaschen und Betrugspräventionsmaßnahmen zu informieren.
- Transaktionen überwachen und Kreditkarten mit Unterstützung des Aussteller ersetzen.
- Aktivierung der Zwei-Faktor-Authentifizierung für betroffene Social-Media-Plattformen, um nicht autorisierte Anmeldungen zu verhindern.

> **Hinweis**
> Nachdem Sie die empfohlenen Maßnahmen ergriffen haben, müssen Sie auf die Schaltfläche **Als erledigt markieren** klicken, um die Erledigung zu bestätigen und Ihren Fortschritt zu verfolgen.

Indem sie diese Schritte befolgen, können Administratoren die Ressourcen ihres Unternehmens mithilfe des Dienstes zur Überwachung auf die**Gefährdung von Unternehmenswerten**einfach überwachen und vor möglicher Offenlegung schützen.

3. ABSOLUTE SICHERHEIT FÜR DEN PC

3.1. Installation

3.1.1. Vor der Installation

Bevor Sie Bitdefender Ultimate Small Business Security installieren, sollten Sie für eine reibungslose Installation sicherstellen, dass folgende Schritte durchgeführt wurden:

- Stellen Sie sicher, dass das Zielgerät für die Bitdefender-Installation die Systemvoraussetzungen erfüllt. Wenn das Gerät die Systemvoraussetzungen nicht erfüllt, kann Bitdefender nicht installiert werden. Falls es doch installiert wird, kann es zu Leistungseinbußen und Stabilitätsproblemen kommen. Eine vollständige Liste der Systemanforderungen finden Sie im Kapitel Systemanforderungen (Seite 10).
- Melden Sie sich mit einem Administrator-Konto am Gerät an.
- Entfernen Sie alle anderen Sicherheitslösungen von Ihrem Gerät. Sollte während des Bitdefender-Installationsvorgangs welche gefunden werden, werden Sie aufgefordert, sie zu deinstallieren. Die gleichzeitige Nutzung mehrerer Sicherheitsprogramme kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen. Windows Defender wird während der Installation deaktiviert.
- Deaktivieren oder entfernen Sie jegliche Firewall-Programme, die auf dem Gerät installiert sind. Die gleichzeitige Nutzung mehreren Sicherheitsprogrammen kann die jeweilige Funktion stören und massive Probleme auf Ihrem Computer verursachen. Die Windows-Firewall wird während der Installation deaktiviert.
- Ihr Gerät sollte während der Installation mit dem Internet verbunden sein, auch wenn Sie von CD oder DVD installieren. Falls neuere Versionen der Anwendungsdateien aus dem Installationspaket verfügbar sind, kann Bitdefender diese dann herunterladen und installieren.

3.1.2. Systemanforderungen

Sie können Bitdefender Ultimate Small Business Security nur auf Geräten mit den folgenden Betriebssystemen installieren:

- Windows 7 mit Service Pack 1
- Windows 8.1
- Windows 10
- 2,5 GB verfügbarer Festplattenspeicher (davon mindestens 800 MB auf dem Systemlaufwerk)
- 2 GB Arbeitsspeicher (RAM)

Sie können Bitdefender Ultimate Small Business Security auch auf Folgendem installieren und ausführen:

- Windows Server 2016 (mit Desktop Experience):
  - Standard/RTM
  - Grundausstattung
  - Rechenzentrum
- Windows Server 2019 (mit Desktop Experience):
  - Standard/RTM
  - Essentiell
  - Rechenzentrum
- Windows Server 2022 (mit Desktop Experience):
  - Standard/RTM
  - Rechenzentrum

Wichtig

Die Systemleistung kann auf Geräten mit CPUs der alten Generation beeinträchtigt werden.

Notiz

So können Sie Informationen zu Ihrem Windows-Betriebssystem und Ihrer Hardware finden:

- Klicken Sie unter **Windows 7** auf Ihrem Desktop mit der rechten Maustaste auf **Arbeitsplatz** und wählen Sie im Menü **Eigenschaften** aus.
- Unter **Windows 8** finden Sie auf der Windows-Startseite den Eintrag **Computer** (z. B. durch Eingabe von "Computer" auf der Startseite). Rechtsklicken Sie auf das entsprechende Symbol. Suchen Sie unter **Windows 8.1** den Menüpunkt **Dieser PC**.
  Wählen Sie im Menü unten **Eigenschaften**. Im Bereich **System** finden Sie Informationen zu Ihrem Systemtyp.
- Geben Sie unter **Windows 10 System** in das Suchfeld in der Taskleiste ein und klicken Sie auf das Symbol. Im Abschnitt **System** finden Sie Informationen zu Ihrem Systemtyp.

3.1.3. Software-Anforderungen

Um Bitdefender und alle Funktionen nutzen zu können, muss Ihr Gerät die folgenden Software-Anforderungen erfüllen:

- Ab Microsoft Edge 40
- Internet Explorer 10 und höher
- Mozilla Firefox 51 und höher
- Google Chrome 34 und höher
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Ab Mozilla Thunderbird 14

3.1.4. Installieren Ihres Bitdefender-Produkts

Sie können Bitdefender vom Installationsdatenträger installieren oder den Web-Installer verwenden, der über **Bitdefender Central** auf Ihr Gerät heruntergeladen wird.

Falls Ihr Einkauf mehr als ein Gerät umfasst, wiederholen Sie den Installationsvorgang und nutzen Sie das gleiche Benutzerkonto, um Ihr Produkt auf den einzelnen Geräten zu aktivieren. Dabei müssen Sie das Benutzerkonto verwenden, das Ihr aktives Bitdefender-Abonnement enthält.

Installation über Bitdefender Central

Über Bitdefender Central können Sie das richtige Installationspaket für das von Ihnen erworbene Abonnement herunterladen. Nach Abschluss des Installationsvorgangs wird Bitdefender Ultimate Small Business Security aktiviert.

So laden Sie Bitdefender Ultimate Small Business Security über Bitdefender Central herunter:

1. Rufen Sie **Bitdefender Central** auf.
2. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **SCHUTZ INSTALLIEREN**.
3. Wählen Sie eine der beiden verfügbaren Optionen:
   - **Dieses Gerät schützen**
     a. Wählen Sie diese Option und danach den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
     b. Speichern Sie die Installationsdatei.
   - **Andere Geräte schützen**
     a. Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
     b. Klicken Sie auf **DOWNLOAD-LINK SENDEN**.
     c. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **E-MAIL VERSENDEN**.
     Bitte beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Nach Ablauf des Links müssen Sie einen neuen Link generieren. Führen Sie dazu die bereits beschriebenen Schritte erneut aus.
     d. Rufen Sie auf dem Gerät, auf dem Bitdefender installiert werden soll, das angegebene E-Mail-Konto auf und klicken Sie in der E-Mail auf die Download-Schaltfläche.
4. Warten Sie, bis der Download abgeschlossen ist, und führen Sie das Installationsprogramm aus.

Validierung der Installation

Bitdefender überprüft zunächst Ihr System, um die Installation zu bestätigen.

Wenn Ihr System die Systemvoraussetzungen zur Installation von Bitdefender nicht erfüllt, werden Sie darüber informiert, welche Bereiche aufgerüstet werden müssen, damit Sie fortfahren können.

Wenn eine inkompatible Sicherheitslösung oder eine ältere Version von Bitdefender erkannt wird, werden Sie aufgefordert, diese von Ihrem System zu entfernen. Bitte folgen Sie den Anweisungen, um die Software von Ihrem System zu entfernen und so spätere Probleme zu vermeiden. Unter Umständen müssen Sie Ihr Gerät neu starten, um die Entfernung der erkannten Sicherheitslösungen abzuschließen.

Das Installationspaket für Bitdefender Total Security wird regelmäßig aktualisiert.

> **Notiz**
> Das Herunterladen der Installationsdateien kann eine Weile dauern, besonders bei langsameren Internetverbindungen.

Sobald die Installation bestätigt ist, wird der Einrichtungsassistent angezeigt. Folgen Sie den Schritten zur Installation von Bitdefender Ultimate Small Business Security.

Schritt 1 - Bitdefender-Installation

Bevor Sie mit Installation fortfahren können, müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Ultimate Small Business Security nutzen dürfen.

Sollten Sie diesen Nutzungsbedingungen nicht zustimmen, schließen Sie das Fenster. Der Installationsprozess wird abgebrochen uns Sie verlassen den Assistenten.

In diesem Schritt können Sie zwei zusätzliche Dinge tun:

- Lassen Sie die Option **Produktberichte senden** aktiviert. Bleibt diese Option aktiviert, werden Berichte mit Informationen über Ihre Nutzung des Produkts an die Bitdefender-Server übertragen. Diese Information ist wichtig für die Verbesserung des Produktes. Wir möchten Sie darauf

hinweisen, dass diese Berichte keine vertraulichen Daten wie Ihren Namen oder Ihre IP-Adresse enthalten und dass diese Daten nicht für kommerzielle Zwecke verwendet werden.

- Wählen Sie die Sprache aus, in der das Produkt installiert werden soll.

Klicken Sie auf **INSTALLIEREN**, um den Installationsvorgang für Ihr Bitdefender-Produkt zu starten.

Schritt 2 - Installation wird durchgeführt

Bitte warten Sie, bis der Installationsvorgang abgeschlossen ist. Sie erhalten detaillierte Informationen über den Fortschritt der Installation.

Schritt 3 - Installation ist abgeschlossen

Ihr Bitdefender-Produkt wurde erfolgreich installiert.

Eine Zusammenfassung der Installation wird angezeigt. Sollte während der Installation aktive Bedrohungen erkannt und entfernt werden, könnte ein Neustart des Systems erforderlich werden.

Schritt 4 - Geräteanalyse

Sie werden jetzt gefragt, ob Sie eine Analyse Ihres Geräts durchführen möchten, um sicherzustellen, dass es nicht gefährdet ist. In diesem Schritt wird Bitdefender kritische Systembereiche scannen. Klicken Sie zum Starten auf **Geräteanalyse starten**.

Sie können die Scan-Oberfläche ausblenden, indem Sie auf **Scan im Hintergrund ausführen** klicken. Legen Sie danach fest, ob Sie informiert werden möchten, wenn der Scan abgeschlossen ist.

Klicken Sie nach Abschluss des Scans auf **Bitdefender-Benutzeroberfläche öffnen**.

> **Notiz**
> Alternativ können Sie, wenn Sie den Scan nicht durchführen möchten, einfach auf **Überspringen** klicken.

Schritt 5 - Erste Schritte

Im Fenster **Erste Schritte** finden Sie weitere Einzelheiten zu Ihrem aktivem Abonnement.

Klicken Sie auf **ABSCHLIEßEN**, um die Benutzeroberfläche Bitdefender Ultimate Small Business Security aufzurufen.

Installation vom Installationsdatenträger

Um Bitdefender vom Installationsdatenträger aus zu installieren, legen Sie den Datenträger in das optische Laufwerk ein.

Ein Installationsbildschirm sollte nach wenigen Augenblicken angezeigt werden. Folgen Sie den Anweisungen, um die Installation zu starten.

Wenn der Installationsbildschirm nicht angezeigt wird, öffnen Sie im Windows Explorer das Root-Verzeichnis des Datenträgers und doppelklicken Sie auf **autorun.exe**.

Bei langsamen Internetverbindungen oder falls Sie über keine Internetverbindungen verfügen, klicken Sie auf **Von CD/DVD installieren**. In diesem Fall wird das auf dem Datenträger befindliche Bitdefender-Produkt installiert. Eine neuere Version wird dann im Zuge des Produktupdates zu einem späteren Zeitpunkt von den Bitdefender-Servern heruntergeladen.

Validierung der Installation

Bitdefender überprüft zunächst Ihr System, um die Installation zu bestätigen.

Wenn Ihr System die Systemvoraussetzungen zur Installation von Bitdefender nicht erfüllt, werden Sie darüber informiert, welche Bereiche aufgerüstet werden müssen, damit Sie fortfahren können.

Wenn eine inkompatible Sicherheitslösung oder eine ältere Version von Bitdefender erkannt wird, werden Sie aufgefordert, diese von Ihrem System zu entfernen. Bitte folgen Sie den Anweisungen, um die Software von Ihrem System zu entfernen und so spätere Probleme zu vermeiden. Unter Umständen müssen Sie Ihr Gerät neu starten, um die Entfernung der erkannten Sicherheitslösungen abzuschließen.

Das Installationspaket für Bitdefender Total Security wird regelmäßig aktualisiert.

> **Notiz**
> Das Herunterladen der Installationsdateien kann eine Weile dauern, besonders bei langsameren Internetverbindungen.

Sobald die Installation bestätigt ist, wird der Einrichtungsassistent angezeigt. Folgen Sie den Schritten zur Installation von Bitdefender Ultimate Small Business Security.

Schritt 1 - Bitdefender-Installation

Bevor Sie mit der Installation fortfahren, müssen Sie dem Abonnementvertrag zustimmen. Bitte nehmen Sie sich etwas Zeit, um den Abonnementvertrag zu lesen, da er die Bedingungen enthält, unter denen Sie ihn verwenden dürfen Bitdefender Ultimate Small Business Security.

Wenn Sie diesen Bedingungen nicht zustimmen, schließen Sie das Fenster. Der Installationsvorgang wird abgebrochen und Sie beenden das Setup.

In diesem Schritt können zwei zusätzliche Aufgaben ausgeführt werden:

- Behalte das **Produktberichte versenden** Option aktiviert. Wenn Sie diese Option zulassen, werden Berichte mit Informationen darüber, wie Sie das Produkt verwenden, an die Bitdefender-Server gesendet. Diese Informationen sind für die Verbesserung des Produkts unerlässlich und können uns helfen, in Zukunft ein besseres Erlebnis zu bieten. Beachten Sie, dass diese Berichte keine vertraulichen Daten wie Ihren Namen oder Ihre IP-Adresse enthalten und nicht für kommerzielle Zwecke verwendet werden.
- Wählen Sie die Sprache aus, in der Sie das Produkt installieren möchten.

Klicken **INSTALLIEREN** um den Installationsprozess Ihres Bitdefender-Produkts zu starten.

Schritt 2 - Installation läuft

Warten Sie, bis die Installation abgeschlossen ist. Detaillierte Informationen zum Fortschritt werden angezeigt.

Schritt 3 - Installation abgeschlossen

Eine Zusammenfassung der Installation wird angezeigt. Wenn während der Installation eine aktive Bedrohung erkannt und entfernt wurde, ist möglicherweise ein Systemneustart erforderlich.

Schritt 4 – Geräteanalyse

Sie werden nun gefragt, ob Sie eine Analyse Ihres Geräts durchführen möchten, um sicherzustellen, dass es sicher ist. Während dieses Schritts scannt Bitdefender kritische Systembereiche. Klicken **Geräteanalyse starten** es zu initiieren.

Sie können die Scanoberfläche ausblenden, indem Sie auf klicken **Scan im Hintergrund ausführen**. Wählen Sie danach, ob Sie benachrichtigt werden möchten, wenn der Scan abgeschlossen ist, oder nicht.

Klicken Sie nach Abschluss des Scans auf **Weiter mit Konto erstellen**.

> **Notiz**
> Wenn Sie den Scan nicht durchführen möchten, können Sie alternativ einfach auf klicken **Überspringen**.

Schritt 5 - Bitdefender-Benutzerkonto

Nach Abschluss der ersten Einrichtung wird das Bitdefender Account-Fenster angezeigt. Zur Aktivierung des Produktes und zur Nutzung seiner Online-Funktionen wird ein Bitdefender-Benutzerkonto benötigt. Weitere Informationen finden Sie im Kapitel Bitdefender-Zentrale.

Fahren Sie entsprechend Ihrer Situation fort.

❍ **Ich möchte ein Bitdefender-Benutzerkonto anlegen**

1. Geben Sie die Daten in die entsprechenden Felder ein. Die hier eingetragenen Daten bleiben vertraulich. Das Passwort muss mindestens 8 Zeichen enthalten, davon mindestens eine Ziffer, ein Sonderzeichen, einen Kleinbuchstaben und einen Großbuchstaben.
2. Bevor Sie fortfahren können, müssen Sie zunächst den Nutzungsbedingungen zustimmen. Rufen Sie die Nutzungsbedingungen auf und lesen Sie sie aufmerksam durch, da Sie hier die Bedingungen zur Nutzung von Bitdefender finden.
   Darüber hinaus können Sie auch die Datenschutzrichtlinie aufrufen und lesen.
3. Klicken Sie auf **BENUTZERKONTO ERSTELLEN**.

> **Notiz**
> Sobald das Benutzerkonto erstellt wurde, können Sie sich mit der angegebenen E-Mail-Adresse und dem Passwort unter https://central.bitdefender.com bei Ihrem Konto anmelden. Alternativ ist dies auch über die Bitdefender Central-App möglich, falls Sie diese auf einem Ihrer Android- oder iOS-Geräten installiert haben. Rufen Sie zur Installation der Bitdefender Central-App auf Ihrem Android-Gerät Google Play auf, suchen Sie Bitdefender Central und tippen Sie auf Installieren. Rufen Sie zur Installation der Bitdefender Central-App auf Ihrem iOS-Gerät den App Store auf, suchen Sie Bitdefender Central und tippen Sie auf Installieren.

- **Ich habe bereits ein Bitdefender-Benutzerkonto**

  1. Klicken Sie auf **Anmelden**.
  2. Geben Sie die E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **WEITER**.
  3. Geben Sie Ihr Passwort ein und klicken Sie auf **ANMELDEN**.
     Wenn Sie das Passwort vergessen haben oder aus anderen Gründen zurücksetzen möchten, gehen Sie bitte wie folgt vor:
     a. Klicken Sie auf **Passwort vergessen?**.
     b. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **WEITER**.
     c. Rufen Sie Ihre E-Mails ab, geben Sie den Sicherheitscode ein, den Sie per E-Mail bekommen haben, und klicken Sie auf **WEITER**.
        Oder Sie klicken in der E-Mail, die Sie von uns bekommen haben, auf **Passwort ändern**.
     d. Geben Sie das neue Passwort ein, das Sie festlegen möchten, und wiederholen Sie die Eingabe. Klicken Sie auf **SPEICHERN**.

     > **Notiz**
     > Wenn Sie bereits ein MyBitdefender-Konto haben, können Sie sich damit bei Ihrem Bitdefender-Konto anmelden. Wenn Sie Ihr Passwort vergessen haben, müssen Sie es zunächst unter https://my.bitdefender.com zurücksetzen. Verwenden Sie dann die aktualisierten Anmeldedaten, um sich bei Ihrem Bitdefender-Konto anzumelden.

- **Ich möchte mich über mein Microsoft-, Facebook- oder Google-Konto anmelden**
  So können Sie sich mit Ihrem Microsoft-, Facebook- oder Google-Konto anmelden:

  1. Wählen Sie, worüber Sie sich anmelden möchten. Sie werden auf die Anmeldeseite dieses Dienstes weitergeleitet.
  2. Folgen Sie den Anweisungen des ausgewählten Dienstes, um Ihr Benutzerkonto mit Bitdefender zu verknüpfen.

  > **Notiz**
  > Bitdefender hat keinen Zugriff auf Ihre vertraulichen Informationen, so zum Beispiel das Passwort, das Sie zur Anmeldung in Ihrem Konto verwenden, oder die persönlichen Informationen Ihrer Freunde und Kontakte.

Schritt 6 - Produkt aktivieren

> **Notiz**
> Dieser Schritt muss durchgeführt werden, falls Sie sich im vorausgegangenem Schritt für die Anlage eines neuen Bitdefender-Konto entschieden haben oder sich mit einem Benutzerkonto angemeldet haben, für das das Abonnement bereits abgelaufen ist.

Zum Abschluss der Produktaktivierung wird eine aktive Internet-Verbindung benötigt.

Gehen Sie abhängig von Ihrer persönlichen Situation folgendermaßen vor:

- Ich habe einen Aktivierungscode
  In diesem Fall aktivieren Sie das Produkt, indem Sie die folgenden Schritte durchführen:

  1. Geben Sie den Aktivierungscode in das Feld "Ich habe einen Aktivierungscode" ein und klicken Sie auf **FORTFAHREN**.

  > **Notiz**
  > Hier finden Sie Ihren Aktivierungscode:
  >
  > - auf dem Label der CD/DVD.
  > - Auf der Registrierungskarte des Produktes.
  > - In der E-Mail-Bestätigung des Online-Kaufs.

2. **Ich möchte Bitdefender testen**
   In diesem Fall können Sie das Produkt 30 Tage lang nutzen. Um die Testphase zu beginnen, wählen Sie **Ich habe kein Abonnement, ich möchte das Produkt kostenlos testen**, und klicken Sie dann auf **FORTFAHREN**.

Schritt 7 - Erste Schritte

Im Fenster **Erste Schritte** erhalten Sie erweiterte Informationen zu Ihrem aktivem Abonnement.

Klicken **BEENDEN** um auf die zuzugreifen Bitdefender Ultimate Small Business Security Schnittstelle.

3.2. Verwalten Ihrer Sicherheit

3.2.1. Virenschutz

Bitdefender schützt Ihr Gerät vor allen Arten von Bedrohungen (Malware, Trojaner, Spyware, Rootkits etc.). Der Virenschutz ist in zwei Kategorien aufgeteilt:

- **Zugriff-Scan** - Verhindert, dass neue Bedrohungen auf Ihr System gelangen. Bitdefender wird z.B. ein Worddokument auf Malware scannen, wenn Sie es öffnen oder eine Email-Nachricht, wenn Sie diese empfangen.
  Der Zugriff-Scan stellt den Echtzeitschutz vor Bedrohungen sicher und ist damit ein grundlegender Bestandteil jedes Computer-Sicherheitsprogramms.

  Wichtig
  Um zu verhindern, dass Ihr Gerät durch Bedrohungen infiziert wird, sollte der **Zugriff-Scan** immer aktiviert bleiben.

- **On-demand Prüfung** - erkennt und entfernt die Bedrohung, die sich bereits auf dem System befindet. Hierbei handelt es sich um eine klassische , durch den Benutzer gestartete, Prüfung - Sie wählen das Laufwerk, Ordner oder Datei welche BitDefender prüfen soll, und BitDefender prüft diese.

Bitdefender scannt automatisch alle Wechselmedien, die mit dem Gerät verbunden werden, um einen sicheren Zugriff zu garantieren.

Weitere Informationen finden Sie im Kapitel Automatischer Scan von Wechselmedien (Seite 35).

Erfahrene Benutzer können Scan-Ausnahmen konfigurieren, wenn Sie nicht möchten, dass bestimmte Dateien oder Dateitypen gescannt werden. Weitere Informationen finden Sie im Kapitel Konfigurieren der Scan-Ausnahmen (Seite 38).

Wenn Bitdefender eine Bedrohung erkennt, versucht das Programm automatisch den Schad-Code der infizierten Datei zu entfernen und die Originaldatei wiederherzustellen. Diese Operation bezeichnet man als Desinfektion. Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Weitere Informationen finden Sie im Kapitel Verwalten von Dateien in Quarantäne (Seite 40).

Wenn Ihr Gerät durch Bedrohungen infiziert wurde, siehe Entfernung von Bedrohungen (Seite 152). Um Ihnen bei der Entfernung von Bedrohungen zu helfen, die nicht von innerhalb des Windows-Betriebssystems entfernt werden können, erhalten Sie mit Bitdefender eine Rettungsumgebung (Seite 153). Dabei handelt es sich um eine vertrauenswürdige Umgebung, die speziell der Entfernung von Bedrohungen dient und es Ihnen ermöglicht, Ihr Gerät unabhängig von Windows zu starten. Wenn das Gerät in der Rettungsumgebung ausgeführt wird, sind die Windows-Bedrohungen inaktiv, so dass sie leicht entfernt werden können.

Zugriff-Scans (Echtzeitschutz)

Bitdefender bietet durch die Prüfung aller aufgerufenen Dateien und E-Mail-Nachrichten Echtzeitschutz vor einer Vielzahl von Bedrohungen.

Aktivieren / Deaktivieren des Echtzeitschutzes

So können Sie den Echtzeitschutz vor Bedrohungen aktivieren oder deaktivieren:

1. Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf **Schutz**.
2. Klicken Sie im Bereich **VIRENSCHUTZ** auf **Öffnen**.
3. Aktivieren oder deaktivieren Sie im Fenster **Erweitert** die Option **Bitdefender-Schild**.
4. Wenn Sie den Echtzeitschutz deaktivieren, wird ein Warnfenster angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im

Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll. Sie können den Echtzeitschutz für 5, 15 oder 30 Minuten, 1 Stunde, dauerhaft oder bis zum Neustart des Systems deaktivieren. Der Echtzeitschutz wird automatisch nach Ablauf des festgelegten Zeitraums aktiviert.

Warnung

Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen den Echtzeitschutz so kurz wie möglich zu deaktivieren. Während der Echtzeitschutz deaktiviert ist, sind Sie nicht vor Bedrohungen geschützt.

Erweiterte Einstellungen des Echtzeitschutzes konfigurieren

Erfahrene Benutzer können die Scan-Einstellungen von Bitdefender nutzen. Sie können die Einstellungen für den Echtzeitschutz im Detail konfigurieren, indem Sie eine benutzerdefinierte Sicherheitsstufe festlegen.

So können Sie die erweiterten Einstellungen für den Echtzeitschutz konfigurieren:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Im Fenster **Erweitert** können Sie die Scan-Einstellungen nach Bedarf konfigurieren.

Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- **Nur Anwendungen scannen.** Sie können Bitdefender so einrichten, dass nur aufgerufene Anwendungen gescannt werden.
- **Auf potenziell unerwünschte Anwendungen prüfen**. Aktivieren Sie diese Option, um nach nicht erwünschten Anwendungen zu suchen. Bei einer potenziell unerwünschten Anwendung (PUA) oder einem potenziell unerwünschten Programm (PUP) handelt es sich um Software, die meist in Verbindung mit kostenloser Software installiert wird und danach Pop-up-Nachrichten anzeigt oder eine Symbolleiste im Standard-Browser installiert. Einige dieser Anwendungen und Programme verändern die Homepage oder die Suchmaschine, andere führen Hintergrundprozesse aus, die den PC verlangsamen, oder

zeigen immer wieder Werbung an. Diese Programme können ohne Ihre Zustimmung installiert werden (wird auch als Adware bezeichnet) oder werden standardmäßig bei der Express-Installation mitinstalliert (werbeunterstützt).

- **Auf Skripte scannen**. Die Funktion Auf Skripte scannen erlaubt es Bitdefender, PowerShell-Skripte und Office-Dokumente zu scannen, die skriptbasierte Malware enthalten können.
- **Netzwerkfreigaben scannen**. Um von Ihrem Gerät aus sicher auf Remotenetzwerke zugreifen zu können, empfehlen wir die Option Netzwerkfreigaben scannen aktiviert zu lassen.
- **Prozessspeicher scannen.** Sucht nach schädlichen Aktivitäten im Speicher von laufenden Prozessen.
- **Befehlszeile scannen.** Scannt die Befehlszeile von neu gestarteten Anwendungen, um dateilose Angriffe zu verhindern.
- **Archive scannen**. Das Scannen von Archiven ist ein langsamer und ressourcenintensiver Prozess und wird daher nicht für den Echtzeitschutz empfohlen. Archive, die infizierte Dateien enthalten, stellen keine unmittelbare Bedrohung für die Sicherheit Ihres Systems dar. Die Bedrohung kann Ihr System nur dann beeinträchtigen, wenn die infizierte Datei aus dem Archiv extrahiert und dann ohne aktivierten Echtzeitschutz ausgeführt wird.
  Wenn Sie sich für diese Option entscheiden, aktivieren Sie sie und ziehen Sie den Regler dann entlang der Skala, um Archive, die größer als ein bestimmter Wert in MB (Megabyte) sind, vom Scan auszuschließen.
- **Boot-Sektoren scannen**. Sie können Bitdefender so einrichten, dass die Boot-Sektoren Ihrer Festplatte gescannt werden. Dieser Sektor der Festplatte enthält den notwendigen Computercode, um den Boot-Vorgang zu starten. Wenn eine Bedrohung den Boot-Sektor infiziert, kann das Laufwerk unzugänglich werden und Sie können Ihr System nicht mehr starten und auf Ihre Daten zugreifen.
- **Nur neue und veränderte Dateien scannen**. Indem Sie nur neue und geänderte Dateien scannen, können Sie die allgemeine Reaktionsfähigkeit Ihres Systems mit minimalen Einbußen bei der Sicherheit erheblich verbessern.
- **Auf Keylogger prüfen**. Wählen Sie diese Option, um Ihr System auf Keylogger zu prüfen. Keylogger zeichnen auf, was Sie über Ihre

Tastatur eingeben, und schicken dann via Internet Berichte an Hacker. Hacker können über diese gestohlenen Daten sensible Informationen erfahren, so wie Kontonummern und Passwörter und Sie zu ihrem eigenen Profit verwenden.

- **Früher Boot-Scan**. Wählen Sie die Option **Füher Boot-Scan**, um Ihr System beim Start zu scannen, sobald alle kritischen Dienste geladen sind. Diese Funktion verbessert die Erkennung von Bedrohungen beim Systemstart und lässt Ihr System schneller starten.

Für gefundene Bedrohungen durchgeführte Aktionen

So können Sie einstellen welche Aktionen der Echtzeitschutz durchführen soll:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Scrollen Sie im Fenster **Erweitert** nach unten, bis Sie die Option **Bedrohungsaktionen** sehen.
4. Konfigurieren Sie die Scan-Einstellungen nach Ihren Wünschen.

Der Echtzeitschutz in Bitdefender kann die folgenden Aktionen durchführen:

Aktionen ausführen

Bitdefender wird je nach Art der infizierten Datei die empfohlenen Aktionen ausführen:

- **Infizierte Dateien**. Dateien, die als infiziert erkannt werden, stimmen mit in der Bitdefender-Datenbank gefundenen Bedrohungsinformationen überein. Bitdefender wird automatisch versuchen, den Schadcode aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren. Diesen Vorgang bezeichnet man als Desinfektion.

  Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Weitere Informationen finden Sie im Kapitel Verwalten von Dateien in Quarantäne (Seite 40).

Wichtig

Bestimmte Bedrohungsarten können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien**. Dateien werden von der heuristischen Analyse als verdächtig klassifiziert. Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne verschoben, um eine mögliche Infektion zu verhindern.
- **Archive mit infizierten Dateien**.
  - Archive, die nur infizierte Dateien enthalten, werden automatisch gelöscht.
  - Wenn ein Archiv sowohl infizierte als auch nicht infizierte Dateien enthält, wird Bitdefender versuchen, die infizierten Dateien zu löschen, vorausgesetzt, dass das Archiv mit den nicht infizierten Dateien wieder rekonstruiert werden kann. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

In Quarantäne verschieben

Verschiebt die entdeckten Dateien in die Quarantäne. Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko. Weitere Informationen finden Sie im Kapitel Verwalten von Dateien in Quarantäne (Seite 40).

Zugriff verweigern

Im Falle eines Virenfundes wird der Zugriff auf die Datei verhindert.

Wiederherstellen der Standardeinstellungen

Die vorgegebenen Einstellungen zum Echtzeitschutz stellen einen guten Schutz gegen Bedrohungen bei nur minimaler Beeinträchtigung der Systemleistung sicher.

Um die vorgegebenen Echzeitschutz-Einstellungen wiederherzustellen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.

3. Scrollen Sie im Fenster **Erweitert** nach unten, bis Sie die Option **Erweiterte Einstellungen zurücksetzen** sehen. Wählen Sie diese Option aus, um die Virenschutzeinstellungen auf die Standardeinstellungen zurückzusetzen.

Bedarf-Scan

Die Aufgabe der Bitdefender-Software ist es sicherzustellen, dass es keine Bedrohungen auf Ihrem Gerät gibt. Dies wird erreicht, indem neue Bedrohungen ferngehalten und Ihre E-Mail-Nachrichten sowie alle heruntergeladenen oder auf Ihr Gerät kopierten Dateien sorgfältig gescannt werden.

Es besteht aber die Gefahr, dass eine Bedrohung bereits in Ihrem System lauert, bevor Sie Bitdefender installieren. Deshalb sollten Sie Ihr Gerät nach der Installation von Bitdefender auf bereits vorhandene Bedrohungen prüfen. Übrigens sollten Sie Ihr Gerät auch in Zukunft regelmäßig auf Bedrohungen prüfen.

Bedarf-Scans werden über Scan-Aufgaben ausgeführt. Die Scan-Aufgaben beinhalten die Scan-Optionen und die Objekte, die gescannt werden sollen. Sie können das Gerät jederzeit scannen, indem Sie die Standard-Aufgaben oder Ihre eigenen Scan-Aufgaben (benutzerdefinierte Aufgaben) ausführen. Wenn Sie bestimmte Bereiche Ihres Geräts scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.

Eine Datei oder einen Ordner auf Bedrohungen prüfen

Wenn Sie den Verdacht hegen, dass Dateien und Verzeichnisse infiziert sein könnten, sollten Sie einen Scan durchführen. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, die/den Sie scannen möchten, wählen Sie **Bitdefender** und dann **Mit Bitdefender scannen**. Der **Viren-Scan-Assistent** wird angezeigt und führt Sie durch den Scan-Vorgang. Nach Abschluss des Scans werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

Durchführen von Quick Scans

Quick Scan setzt auf In-the-Cloud-Scans, um auf Ihrem System laufende Bedrohungen aufzuspüren. Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil

der Systemressourcen, die ein normaler Virenschutz-Scan in Anspruch nehmen würde.

So können Sie eine Quick Scan durchführen:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf Schutz.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Scans** neben **Quick Scan** auf die Schaltfläche **Scan starten**.
4. Folgen Sie den Anweisungen des **Viren-Scan-Assistenten**, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Durchführen von System-Scans

Der System-Scan prüft das gesamte Gerät auf alle Bedrohungsarten, die ein Sicherheitsrisiko darstellen, so zum Beispiel Malware, Spyware, Adware, Rootkits usw.

> **Notiz**
> Da ein **System-Scan** das gesamte System scannt, kann er eine Weile dauern. Es empfiehlt sich daher, diese Aufgabe durchzuführen, wenn Sie das Gerät gerade nicht benötigen.

Bevor Sie einen System-Scan ausführen, sollten Sie Folgendes beachten:

- Stellen Sie sicher, dass die Datenbank mit den Bedrohungsinformationen in Bitdefender jederzeit auf dem neuesten Stand ist. Wenn die Bedrohungsprüfung auf Grundlage einer Datenbank mit veralteten Bedrohungsinformationen erfolgt, kann dies verhindern, dass Bitdefender neue Bedrohungen erkennt, die seit dem letzten Update gefunden wurden. Weitere Informationen finden Sie im Kapitel Bitdefender auf dem neuesten Stand halten.
- Schließen Sie alle geöffneten Programme.

Wenn Sie bestimmte Bereiche Ihres Geräts scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen. Weitere Informationen finden Sie im Kapitel Benutzerdefinierte Scans durchführen (Seite 28).

So können Sie einen System-Scan durchführen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Scans** neben **System-Scan** auf die Schaltfläche **Scan starten**.
4. Bei der ersten Durchführung eines System-Scans werden Sie mit der Funktion vertraut gemacht. Klicken zum Fortfahren auf **OK, verstanden**.
5. Folge dem Antivirus-Scan-Assistent um den Scan abzuschließen. Bitdefender ergreift automatisch die empfohlenen Maßnahmen für erkannte Dateien. Wenn es weiterhin ungelöste Bedrohungen gibt, werden Sie aufgefordert, die Maßnahmen auszuwählen, die für sie ergriffen werden sollen.

Benutzerdefinierte Scans durchführen

Im Fenster **Scans verwalten** können Sie Bitdefender so einrichten, dass Scans ausgeführt werden, wenn Sie glauben, dass Ihr Gerät eine Überprüfung auf mögliche Bedrohungen benötigt. Sie können wählen, ob Sie einen **System-Scan** oder einen **Quick-Scan** planen möchten, oder ob Sie einen benutzerdefinierten Scan nach Ihren Anforderungen erstellen möchten.

So können Sie einen benutzerdefinierten Scan im Detail konfigurieren:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Scans** auf **+Scan erstellen**.
4. Geben Sie im Feld **Aufgabenname** einen Namen für den Scan ein, wählen Sie die Bereiche aus, die Sie scannen möchten, und klicken Sie auf **Weiter**.
5. Konfigurieren Sie diese allgemeinen Optionen:
   - **Nur Anwendungen scannen.** Sie können Bitdefender so einstellen, dass nur aufgerufene Apps gescannt werden.
   - **Priorität der Scan-Aufgabe**. Sie können festlegen, wie sich ein Scan-Vorgang auf die Systemleistung auswirkt.

- Auto - Die Priorität des Scan-Vorgangs hängt von der Systemaktivität ab. Um sicherzustellen, dass der Scan-Vorgang die Systemaktivität nicht beeinträchtigt, entscheidet Bitdefender, ob der Scan-Vorgang mit hoher oder niedriger Priorität ausgeführt wird.
- Hoch - Die Priorität des Scan-Vorgangs wird als hoch festgelegt. Wenn Sie diese Option wählen, können andere Programme langsamer ausgeführt werden. So kann der Scan-Vorgang schneller abgeschlossen werden.
- Niedrig - Die Priorität des Scan-Vorgangs wird als niedrig festgelegt. Wenn Sie diese Option wählen, können andere Programme schneller ausgeführt werden. So dauert es länger, bis der Scan-Vorgang abgeschlossen wird.

- **Aktionen nach dem Scan**. Wählen Sie die Aktion, die von Bitdefender durchgeführt werden soll, wenn keine Bedrohungen gefunden wurden:
  - Übersichtsfenster anzeigen
  - Gerät herunterfahren
  - Scan-Fenster schließen

6. Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Erweiterte Optionen anzeigen**. Informationen zu den aufgeführten Scans finden Sie am Ende dieses Abschnitts.
   Klicken Sie auf **Weiter**.
7. Sie können bei Bedarf die Option **Scan-Aufgabe planen** aktivieren und dann festlegen, wann der von Ihnen erstellte benutzerdefinierte Scan gestartet werden soll.
   - Beim Systemstart
   - Täglich
   - Monatlich
   - Wöchentlich

   Wenn Sie Täglich, Monatlich oder Wöchentlich wählen, ziehen Sie den Regler entlang der Skala, um den gewünschten Zeitraum festzulegen, in dem der geplante Scan beginnen soll.

8. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Konfigurationsfenster zu schließen.
   Abhängig von den Bereichen, die gescannt werden sollen, kann der Scan einige Zeit in Anspruch nehmen. Wenn während des Scan-Vorgangs Bedrohungen gefunden werden, werden Sie aufgefordert, die Aktionen auszuwählen, die für die erkannten Dateien durchgeführt werden sollen.

Informationen zu den Scanoptionen

Sie können diese Informationen nützlich finden:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im **Glossar** nach. Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Scannen Sie potenziell unerwünschte Anwendungen.** Wählen Sie diese Option, um nach unerwünschten Anwendungen zu suchen. Eine potenziell unerwünschte Anwendung (PUA) oder ein potenziell unerwünschtes Programm (PUP) ist eine Software, die normalerweise mit Freeware-Software gebündelt geliefert wird und im Standardbrowser Popups anzeigt oder eine Symbolleiste installiert. Einige von ihnen ändern die Startseite oder die Suchmaschine, andere führen mehrere Prozesse im Hintergrund aus, die den PC verlangsamen, oder zeigen zahlreiche Anzeigen an. Diese Programme können ohne Ihre Zustimmung installiert werden (auch als Adware bezeichnet) oder sind standardmäßig im Express-Installationskit enthalten (werbefinanziert).
- **Archive scannen**. Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit. Archive, die infizierte Dateien enthalten, stellen keine unmittelbare Bedrohung für die Sicherheit Ihres Systems dar. Die Bedrohung kann Ihr System nur dann beeinträchtigen, wenn die infizierte Datei aus dem Archiv extrahiert und dann ohne aktivierten Echtzeitschutz ausgeführt wird. Wir empfehlen jedoch, diese Option zu nutzen, um potenzielle Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.
  Ziehen Sie den Regler entlang der Skala, um Archive, die größer als ein bestimmter Wert in MB (Megabyte) sind, vom Scan auszuschließen.

> **Notiz**
> Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Scannen Sie nur neue und geänderte Dateien.** Indem Sie nur neue und geänderte Dateien scannen, können Sie die Reaktionsfähigkeit des Gesamtsystems mit einem minimalen Kompromiss bei der Sicherheit erheblich verbessern.
- **Bootsektoren scannen.** Sie können Bitdefender so einstellen, dass es die Bootsektoren Ihrer Festplatte scannt. Dieser Sektor der Festplatte enthält den notwendigen Computercode, um den Startvorgang zu starten. Wenn eine Bedrohung den Bootsektor infiziert, kann das Laufwerk unzugänglich werden und Sie können Ihr System möglicherweise nicht starten und nicht auf Ihre Daten zugreifen.
- **Speicher scannen**. Wählen Sie diese Option, um Programme zu scannen, die im Speicher Ihres Systems laufen.
- **Registrierung scannen**. Wählen Sie diese Option, um die Registrierungsschlüssel zu scannen. Die Windows-Registrierung ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.
- **Cookies scannen**. Wählen Sie diese Option, um die Cookies zu scannen, die von Browsern auf Ihrem Gerät gespeichert werden.
- **Keylogger scannen.** Wählen Sie diese Option, um Ihr System nach Keylogger-Apps zu durchsuchen. Keylogger zeichnen auf, was Sie auf Ihrer Tastatur eingeben, und senden Berichte über das Internet an eine böswillige Person (Hacker). Der Hacker kann aus den gestohlenen Daten sensible Informationen wie Bankkontonummern und Passwörter herausfinden und daraus persönliche Vorteile ziehen.

Viren-Scan-Assistent

Wenn Sie einen Bedarf-Scan starten (z. B. indem Sie mit der rechten Maustaste auf einen Ordner klicken, dann Bitdefender und anschließend **Mit Bitdefender scannen** wählen), wird der Bitdefender-Viren-Scan-Assistent eingeblendet. Folgen Sie den Anweisungen des Assistenten, um den Scan-Vorgang abzuschließen.

Notiz

Falls der Scan-Assistent nicht erscheint, ist der Scan möglicherweise als Hintergrund-Scan konfiguriert. Suchen Sie nach dem Symbo für den Scan-Fortschritt in der **Taskleiste**. Klicken Sie auf das Symbol, um das Scan-Fenster zu öffnen und so den Scan-Fortschritt zu sehen.

Schritt 1 - Führen Sie den Scan durch

BitDefender prüft die gewählten Dateien und Ordner. Sie erhalten Echtzeitinformationen über den Scan-Status sowie Scan-Statistiken (einschließlich der bisherigen Laufzeit, einer Einschätzung der verbleibenden Laufzeit und der Anzahl der erkannten Bedrohungen).

Bitte warten Sie bis Bitdefender den Prüfvorgang beendet hat. Der Scan-Vorgang kann, abhängig von der Größe Ihrer Festplatte, eine Weile dauern.

Einen Scan anhalten oder unterbrechen. Sie können den Scan-Vorgang jederzeit unterbrechen, indem Sie auf **STOPP** klicken. Sie gelangen dann direkt zum letzten Schritt des Assistenten. Um den Scan-Vorgang nur vorübergehend anzuhalten, klicken Sie einfach auf **PAUSE**. Klicken Sie auf **FORTSETZEN**, um den Scan-Vorgang fortzusetzen.

Passwortgeschützte Archive. Wird ein passwortgeschütztes Archiv gefunden, werden Sie abhängig von den Scan-Einstellungen zur Eingabe des Passworts aufgefordert. Passwortgeschützte Archive können nur nach Eingabe des Passworts gescannt werden. Die folgenden Optionen sind verfügbar:

- **Passwort**. Wenn Sie möchten, dass Bitdefender Archive scannt, wählen Sie diese Option aus und geben das Passwort an. Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.
- **Nicht nach einem Passwort fragen und dieses Objekt beim Scan überspringen.** Wählen Sie diese Option, um das Scannen dieses Archivs zu überspringen.
- **Alle passwortgeschützten Dateien beim Scan überspringen.** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten. Bitdefender kann diese dann nicht scannen, erstellt aber einen Eintrag im Scan-Protokoll.

Wählen Sie die gewünschte Option aus und klicken Sie auf **OK**, um den Scan fortzusetzen.

Schritt 2 - Wählen Sie entsprechende Aktionen aus

Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

> **Notiz**
> Wenn Sie einen Quick Scan oder einen System-Scan durchführen, wird Bitdefender während des Scans automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen. Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Die infizierten Objekte werden nach Bedrohung sortiert in Gruppen angezeigt. Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine umfassende Aktion für alle Probleme auswählen oder Sie können einzelne Aktionen für Problemgruppen auswählen. Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

Aktionen ausführen

Bitdefender ergreift je nach Typ der erkannten Datei die empfohlenen Maßnahmen:

- **Infizierte Dateien.** Als infiziert erkannte Dateien stimmen mit Bedrohungsinformationen überein, die in der Bitdefender-Datenbank für Bedrohungsinformationen gefunden wurden. Bitdefender versucht automatisch, den Schadcode aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren. Dieser Vorgang wird als Desinfektion bezeichnet.

  Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um die Infektion einzudämmen. Quarantänedateien können nicht ausgeführt oder geöffnet werden; daher verschwindet das Risiko, sich zu infizieren. Weitere Informationen finden Sie unter Verwalten von Dateien in Quarantäne (Seite 40).

> **Wichtig**
> Bei bestimmten Arten von Bedrohungen ist eine Desinfektion nicht möglich, da die erkannte Datei vollständig bösartig ist. In solchen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig erkannt. Verdächtige Dateien können nicht desinfiziert werden, da keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne gebracht, um eine mögliche Ansteckung zu verhindern.
- **Archive mit infizierten Dateien.**
  - Archive, die nur infizierte Dateien enthalten, werden automatisch gelöscht.
  - Wenn ein Archiv sowohl infizierte als auch saubere Dateien enthält, versucht Bitdefender, die infizierten Dateien zu löschen, sofern es das Archiv mit den sauberen Dateien rekonstruieren kann. Wenn die Wiederherstellung des Archivs nicht möglich ist, werden Sie darüber informiert, dass keine Maßnahmen ergriffen werden können, um den Verlust sauberer Dateien zu vermeiden.

Löschen

Infizierte Dateien werden von der Festplatte entfernt.

Falls infizierte Dateien zusammen mit nicht infizierten Dateien in einem Archiv gespeichert sind, wird Bitdefender versuchen, die infizierten Dateien zu löschen und das Archiv mit den nicht infizierten Dateien zu rekonstruieren. Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Keine Aktion durchführen

Es wird keine Aktion für die infizierte Dateien ausgeführt. Nachdem der Scan-Vorgang beendet wurde, können Sie das Scan-Protokoll öffnen um Informationen über diese Dateien anzuzeigen.

Klicken Sie auf **Fortfahren** um die festgelegten Aktionen anzuwenden.

Schritt 3 - Zusammenfassung

Wenn BitDefender das Beheben der Risiken beendet hat wird eine Zusammenfassung in einem neuen Fenster geöffnet. Falls Sie umfangreichere Informationen zum Scan-Prozess möchten, klicken Sie auf **LOGDATEI ANZEIGEN**.

Wichtig
In den meisten Fällen desinfiziert BitDefender erfolgreich die infizierten Dateien, die er entdeckt hat, oder er isoliert die Infektion. Dennoch gibt es Probleme, die nicht automatisch gelöst werden können. Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Bereinigungsprozess abgeschlossen werden kann. Weitere Informationen und eine Anleitung, wie Sie eine Bedrohung manuell entfernen können, finden Sie im Kapitel Entfernung von Bedrohungen (Seite 152).

Scan-Protokolle lesen

Bei jedem Scan wird ein Scan-Protokoll erstellt, und Bitdefender zeichnet die gefundenen Probleme im Fenster Virenschutz auf. Der Bericht enthält detaillierte Informationen über den Scan-Vorgang, so wie Scan-Optionen, das Scan-Ziel, die gefundenen Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **PROTOKOLL ANZEIGEN** klicken.

So können Sie ein Scan-Protokoll oder gefundene Infektionen auch später anzeigen:

1. Klicken **Benachrichtigungen** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Wählen Sie unter dem Reiter **Alle** die Benachrichtigung bezüglich des neuesten Scans aus.
   Hier können Sie alle Ereignisse des Bedrohungs-Scans finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.
3. In der Benachrichtigungsliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden. Klicken Sie auf eine Benachrichtigung, um mehr darüber zu erfahren.
4. Um das Scan-Protokoll zu öffnen, klicken Sie auf **Protokoll anzeigen**.

Automatischer Scan von Wechselmedien

Bitdefender erkennt automatisch, wenn Sie Wechselmedien mit Ihrem Gerät verbinden und scannt diese im Hintergrund, wenn die Auto-Scan-

Option aktiviert wurde. Dies ist empfohlen, um die Infizierung Ihres Geräts durch Bedrohungen zu verhindern.

Entdeckte Geräte fallen in eine dieser Kategorien:

- CDs/DVDs
- Speichersticks, wie z. B. Flash Pens oder externe Festplatten
- verbundene (entfernte) Netzlaufwerke

Sie können den automatischen Scan der Speichermedien eigens für jede Kategorie konfigurieren. Der automatische Scan der abgebildeten Netzlaufwerke ist standardmäßig deaktiviert.

Wie funktioniert es?

Wenn ein Wechseldatenträger erkannt wird, beginnt Bitdefender diesen auf Bedrohungen zu prüfen (vorausgesetzt, dass der automatische Scan für diesen Gerätetyp aktiviert ist). Ein Pop-up-Fenster wird Sie darüber informieren, dass ein neues Gerät erkannt wurde und dass es derzeit gescannt wird.

Das Bitdefender-Scan-Symbol erscheint in der **Task-Leiste**. Sie können dieses Objekt anklicken, um das Scan-Fenster zu öffnen und so den Scan-Fortschritt zu sehen.

Sobald der Scan abgeschlossen ist, wird das Fenster mit den Scan-Ergebnissen angezeigt, um Sie darüber zu informieren, ob Sie die Dateien auf dem Wechselmedium gefahrlos aufrufen können.

In den meisten Fällen entfernt Bitdefender erkannte Bedrohungen automatisch oder isoliert infizierte Dateien in der Quarantäne. Sollte es nach dem Scan noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

> **Notiz**
> Bitte beachten Sie, dass für infizierte oder verdächtige Dateien auf CDs oder DVDs keine Aktionen durchgeführt werden können. Ebenso können für infizierte oder verdächtige Dateien auf abgebildeten Netzlaufwerken keine Aktionen durchgeführt werden, wenn Sie nicht die über die entsprechenden Rechte verfügen.

Diese Informationen könnten sich als hilfreich erweisen:

- Bitte gehen Sie vorsichtig vor, wenn Sie eine CD oder DVD nutzen, die mit Bedrohungen infiziert ist, da diese nicht von dem Datenträger

entfernt werden kann (diese Medien sind schreibgeschützt). Stellen Sie sicher, dass der Echtzeitschutz aktiviert ist, um zu verhindern, dass Bedrohungen auf Ihr System gelangen. Es empfiehlt sich, wichtige Daten vom Datenträger auf Ihr System zu kopieren und den Datenträger dann zu entsorgen.

- Es kann vorkommen, dass Bitdefender nicht in der Lage ist, Bedrohungen aus juristischen oder technischen Gründen aus bestimmten Dateien zu entfernen. Ein Beispiel hierfür sind Dateien, die mithilfe von proprietären Technologien archiviert wurden (der Grund dafür ist, dass das Archiv nicht korrekt wiederhergestellt werden kann).

  Eine Anleitung zum Umgang mit Bedrohungen finden Sie im Kapitel Entfernung von Bedrohungen (Seite 152).

Verwalten des Scans für Wechselmedien

So können Sie Wechselmedien automatisch scannen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Rufen Sie das Fenster **Einstellungen** auf.

Die Prüfoptionen sind für bestmögliche Enteckungsraten vorkonfiguriert. Wenn infizierte Dateien erkannt werden, wird Bitdefender versuchen, diese zu desinfizieren (d. h. den Schad-Code zu entfernen) oder in die Quarantäne zu verschieben. Sollten beide Maßnahmen fehlschlagen, können Sie im Assistenten für den Virenschutz-Scan andere Aktionen für die infizierten Dateien festlegen. Die Prüfoptionen sind standartisiert, sie können daher nicht geändert werden.

Um den bestmöglichen Schutz zu garantieren, empfiehlt es sich, die **Auto-Scan-Option** für alle Arten von Wechselmedien zu aktivieren.

Host-Datei scannen

Die Host-Datei ist standardmäßig Teil der Betriebssysteminstallation und dient der Zuordnung von Hostnamen zu IP-Adressen, wenn Sie neue Webseiten aufrufen oder Verbindungen mit FTP- und anderen Internet-Servern aufbauen. Dabei handelt es sich um eine reine Textdatei, die von Schadprogrammen verändert werden kann. Erfahrene Nutzer wissen, wie man damit lästige Werbeanzeigen, Banner, Cookies von Drittanbietern oder Datenjäger blockiert.

So können Sie die Option Host-Datei scannen konfigurieren:

1. Klicken **Einstellungen** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Wähle aus **Fortschrittlich** Tab.
3. Aktivieren oder deaktivieren Sie die Option **Host-Datei scannen**.

Konfigurieren der Scan-Ausnahmen

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateiendungen vom Scan ausnehmen. Diese Funktion soll verhindern, dass Sie bei Ihrer Arbeit gestört werden und kann zudem dabei helfen, die Systemleistung zu verbessern. Ausnahmen sollten nur von Benutzern eingesetzt werden, die erfahren im Umgang mit Computern sind oder wenn dies von einem Bitdefender-Mitarbeiter empfohlen wurde.

Sie können Ausnahmen so konfigurieren, dass sie für Zugriff-Scans, Bedarf-Scans oder beide Arten von Scans gelten. Die ausgenommenen Objekte werden nicht geprüft, egal ob der Zugriff von Ihnen oder von einem Programm erfolgt.

> **Notiz**
> Ausnahmen werden bei Kontext-Scans NICHT berücksichtigt. Kontextprüfung ist eine Art von On-Demand-Prüfung: rechtsklicken Sie die zu prüfende Datei oder den Ordner und wählen Sie **Prüfe mit BitDefender** aus.

Dateien und Ordner vom Scan ausnehmen

So können Sie bestimmte Dateien und Ordner vom Scan ausnehmen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Einstellungen** auf **Ausnahmen verwalten**.
4. Klicken Sie auf **+Ausnahme hinzufügen**.
5. Geben Sie den Pfad des Ordners, den Sie vom Scan ausnehmen möchten, in das entsprechende Feld ein.
   Alternativ können Sie zu dem Ordner navigieren, indem Sie rechts in der Benutzeroberfläche auf die Schaltfläche "Durchsuchen" klicken, ihn auswählen und dann auf **OK** klicken.

6. Aktivieren Sie den Schalter neben der Schutzfunktion, durch die der Ordner nicht gescannt werden soll. Sie haben drei Optionen:
   - Virenschutz
   - Online-Gefahrenabwehr
   - Erweiterte Gefahrenabwehr
7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und das Fenster zu schließen.

Dateiendungen vom Scan ausnehmen

Wenn Sie eine Dateiendung vom Scan ausnehmen, wird Bitdefender Dateien mit dieser Endung unabhängig von ihrem Speicherort nicht mehr scannen. Die Ausnahme bezieht sich auch auf Dateien auf Wechselmedien, wie zum Beispiel CDs, DVDs, USB-Sticks oder Netzlaufwerke.

> **Wichtig**
> Lassen Sie Vorsichtig walten, wenn Sie Dateiendung vom Scan ausnehmen, da solche Ausnahmen Ihr Gerät anfällig für Bedrohungen machen können.

So können Sie Dateierweiterungen vom Scan ausnehmen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Im **Einstellungen** Fenster, klicken **Ausnahmen verwalten**.
4. Klicken **+Fügen Sie eine Ausnahme hinzu**.
5. Geben Sie die Dateiendungen, die vom Scannen ausgenommen werden sollen, mit einem Punkt davor ein. Trennen Sie einzelne Endungen mit einem Semikolon (;).
   txt;avi;jpg
6. Aktivieren Sie den Schalter neben der Schutzfunktion, durch die die Dateiendung nicht gescannt werden soll.
7. Klicken Sie auf **Speichern**.

Verwalten der Scan-Ausnahmen

Werden die konfigurierten Scan-Ausnahmen nicht mehr benötigt, empfehlen wir, diese zu löschen oder die Scan-Ausnahmen zu deaktivieren.

So können Sie die Scan-Ausnahmen verwalten:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Einstellungen** auf **Ausnahmen verwalten**. Es wird eine Liste mit allen von Ihnen festgelegten Ausnahmen angezeigt.
4. Um Scan-Ausnahmen zu entfernen oder zu bearbeiten, klicken Sie auf die jeweiligen Schaltflächen. Gehen Sie wie folgt vor:
   - Entfernen Sie einen Eintrag aus der Liste, indem Sie auf die entsprechende -Schaltfläche klicken.
   - Klicken Sie zum Bearbeiten eines Eintrags aus der Tabelle auf die Schaltfläche **Bearbeiten** neben dem Eintrag. Ein neues Fenster wird angezeigt. Hier können Sie nach Bedarf festlegen, welche Dateiendungen oder -pfade von welcher Schutzfunktion ausgeschlossen werden sollen. Führen Sie die notwendigen Änderungen durch und klicken Sie dann auf **Ändern**.

Verwalten von Dateien in Quarantäne

Mit Bedrohungen infizierte Dateien, die nicht desinfiziert werden können, sowie verdächtige Dateien werden von Bitdefender in einem sicheren Bereich isoliert, der sogenannten Quarantäne. Bedrohungen in Quarantäne können keinen Schaden anrichten, da sie dort nicht geöffnet oder ausgeführt werden können.

Zudem werden nach jedem Update der Datenbank mit den Bedrohungsinformationen die Dateien in der Quarantäne von Bitdefender gescannt. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.

So können Sie die Dateien in der Quarantäne einsehen und verwalten:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.

3. Rufen Sie das Fenster **Einstellungen** auf.
   Hier finden Sie den Namen der Dateien in Quarantäne, ihren ursprünglichen Speicherort sowie den Namen der gefundenen Bedrohungen.
4. Dateien in Quarantäne werden von Bitdefender in Übereinstimmung mit den Standardeinstellungen für die Quarantäne automatisch verwaltet.
   Sie können die Quarantäneeinstellungen nach einem Klick auf **Einstellungen anzeigen** an Ihre Anforderungen anpassen, dies wird aber nicht empfohlen.
   Klicken Sie auf die Schalter, um das Folgende zu aktivieren oder deaktivieren:
   Quarantäne nach Update der Bedrohungsinformationen erneut scannen
   Lassen Sie diese Option aktiviert, um Dateien in Quarantäne automatisch nach jedem Update der Bedrohungsinformationen zu scannen. Gesäuberte Dateien werden automatisch an ihren Ursprungsort zurück gelegt.
   Inhalte löschen, die älter als 30 Tage sind
   Dateien in Quarantäne, die älter als 30 Tage sind, werden automatisch gelöscht.
   Ausnahmen für wiederhergestellte Dateien erstellen
   Dateien, die Sie aus der Quarantäne wiederherstellen, werden ohne Reparatur an Ihren ursprünglichen Speicherort verschoben und bei zukünftigen Scans automatisch übersprungen.
5. Um eine Quarantäne-Datei zu löschen, markieren Sie diese und klicken dann auf den Button **Löschen**. Wenn Sie eine Quarantäne-Datei am ursprünglichen Speicherort wiederherstellen möchten, klicken Sie zuerst auf die Datei und dann auf **Wiederherstellen**.

3.2.2. Erweiterte Bedrohungsabwehr

Die Erweiterte Gefahrenabwehr von Bitdefender ist eine innovative und vorbeugende Erkennungstechnologie, die hoch entwickelte heuristische Methoden nutzt, um Ransomware und mögliche neue Bedrohungen in Echtzeit zu erkennen.

Die Erweiterte Gefahrenabwehr überwacht durchgehend alle auf Ihrem Gerät laufenden Anwendungen auf Aktionen, die auf Bedrohungen

hindeuten. Jede einzelne dieser Aktionen erhält einen Wert, und jeder Prozess erhält so einen aggregierten Gesamtwert.

Als Sicherheitsmaßnahme werden Sie jedes Mal benachrichtigt, wenn Bedrohungen und potenziell gefährliche Prozesse erkannt und blockiert werden.

Aktivieren oder Deaktivieren der Advanced Threat Defense

So aktivieren oder deaktivieren Sie die Advanced Threat Defense:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Klicken Sie im Bereich **ERWEITERTE GEFAHRENABWEHR** auf **Öffnen**.
3. Rufen Sie das Fenster **Einstellungen** auf und klicken Sie auf den Schalter neben **Bitdefender Erweiterte Gefahrenabwehr**.

> **Notiz**
> Zum Schutz Ihrer Systeme vor Ransomware und anderen Bedrohungen empfehlen wir Ihnen, die Erweiterte Gefahrenabwehr nicht über einen längeren Zeitraum zu deaktivieren.

Einsehen von erkannten schädlichen Angriffen

Werden Bedrohungen oder potenziell schädliche Angriffe erkannt, werden diese von Bitdefender umgehend blockiert, um eine Infektion Ihres Geräts durch Ransomware oder andere Malware zu verhindern. Gehen Sie wie folgt vor, um eine Liste der erkannten schädlichen Angriffe einzusehen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **ERWEITERTE BEDROHUNGSABWEHR** Bereich, klicken Sie auf **Offen**.
3. Rufen Sie das Fenster **Threat Defense** auf.
   Alle in den vergangenen 90 Tagen erkannten Angriffe werden angezeigt. Klicken Sie auf den entsprechenden Eintrag, um weitere Details zum erkannten Ransomware-Typ und den Dateipfad des schädlichen Prozesses anzuzeigen. Hier können Sie auch einsehen, ob die Desinfektion erfolgreich war.

Hinzufügen von Prozessen zu den Ausnahmen

Sie können Ausnahmeregeln für vertrauenswürdige Anwendungen festlegen, damit die Erweiterte Gefahrenabwehr diese nicht blockiert, wenn ihr Verhalten auf eine Bedrohung hindeutet.

So können Sie Prozesse zur Ausnahmeliste der Erweiterten Gefahrenabwehr hinzufügen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **ERWEITERTE BEDROHUNGSABWEHR** Bereich, klicken Sie auf **Offen**.
3. Im **Einstellungen** Fenster, klicken **Ausnahmen verwalten**.
4. Klicken **+Fügen Sie eine Ausnahme hinzu**.
5. Geben Sie den Pfad des Ordners, den Sie vom Scannen ausnehmen möchten, in das entsprechende Feld ein.
   Alternativ können Sie zu der ausführbaren Datei navigieren, indem Sie rechts in der Benutzeroberfläche auf die Schaltfläche "Durchsuchen" klicken, sie auswählen und dann auf **OK** klicken.
6. Aktivieren Sie den Schalter neben **Erweiterte Gefahrenabwehr**.
7. Klicken **Speichern**.

Exploits gefunden

Hacker nutzen zum Eindringen in Systeme häufig bestimmte Fehler oder Schwachstellen in Computersoftware (Anwendungen oder Plug-ins) und Hardware aus. Um Ihr Gerät von derartigen Angriffen zu schützen, die sich in aller Regel sehr schnell ausbreiten, verwendet Bitdefender die neuesten Technologien zur Abwehr von Exploits.

Aktivieren oder Deaktivieren der Exploit-Erkennung

So können Sie die Exploit-Erkennung aktivieren oder deaktivieren:

- Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
- Im **ERWEITERTE BEDROHUNGSABWEHR** Bereich, klicken Sie auf **Offen**.
- Rufen Sie das Fenster **Einstellungen** auf und klicken Sie auf den Schalter neben **Exploit-Erkennung**, um die Funktion zu aktivieren oder deaktivieren.

Notiz
Die Option zur Exploit-Erkennung ist standardmäßig aktiviert.

3.2.3. Abwehr von Online-Bedrohungen

Die Online-Gefahrenabwehr von Bitdefender lässt Sie sicher im Netz surfen, indem sie Sie vor potenziell schädlichen Seiten warnt.

Bitdefender bietet Echtzeit-Online-Gefahrenabwehr für:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

So können Sie die Einstellungen der Online-Gefahrenabwehr konfigurieren:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Klicken Sie im Bereich **ONLINE-GEFAHRENABWEHR** auf **Einstellungen**.

Klicken Sie im Bereich **Internet-Schutz** zur Aktivierung oder Deaktivierung auf die entsprechenden Schalter:

- Die Prävention von Internetangriffen blockiert Bedrohungen aus dem Internet, so zum Beispiel auch Drive-by-Downloads.
- Suchberater, eine Komponente, die Ihre Suchmaschinentreffer und Links auf Seiten sozialer Netzwerke analysiert und bewertet. Die Bewertung wird durch ein Symbol neben dem Link oder Treffer angezeigt:

  Sie sollten diese Webseite nicht aufrufen.

  Diese Webseite könnte gefährliche Inhalte haben. Lassen Sie Vorsicht walten, wenn Sie sie dennoch aufrufen möchten.

  Diese Seite ist sicher und kann aufgerufen werden.

Der Suchberater anaylsiert die Treffer der folgenden Internet-Suchmaschinen:

- Google
- Yahoo!
- Bing
- Baidu

Der Suchberater bewertet Links, die auf den folgenden sozialen Netzwerken im Internet veröffentlicht werden:

- Facebook
- 109

- Verschlüsselter Web-Scan.
  Gute durchdachte Angriffsversuche könnten den sicheren Datenverkehr für sich zu nutzen, um ihre Opfer zu täuschen. Wir empfehlen daher, die Option Verschlüsselter Web-Scan aktiviert zu lassen.
- Betrugsschutz.
- Phishing-Schutz.

Scrollen Sie nach unten, um zum Abschnitt **Netzwerk-Gefahrenabwehr** zu gelangen. Hier finden Sie die Option **Netzwerk-Gefahrenabwehr**. Um Ihr Gerät vor Angriffen durch komplexe Malware-Bedrohungen (so z. B. Ransomware) zu schützen, die sich Schwachstellen im System zu Nutze machen, sollten Sie diese Option aktiviert lassen.

Sie können eine Liste mit Websites, Domains und IP-Adressen anlegen, die von den Bitdefender-Engines für den Bedrohungs-, Phishing- und Betrugsschutz nicht gescannt werden sollen. Die Liste sollte nur Websites, Domänen und IP-Adressen enthalten, denen Sie uneingeschränkt vertrauen.

So können Sie mit der Online-Gefahrenabwehr in Bitdefender Websites, Domains und IP-Adressen konfigurieren und verwalten:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **VORBEUGUNG VON ONLINE-BEDROHUNGEN** Bereich, klicken Sie auf **Einstellungen**.

3. Klicken Sie auf **Ausnahmen verwalten**.
4. Klicken **+Fügen Sie eine Ausnahme hinzu**.
5. Geben Sie in das entsprechende Feld den Namen der Website, den Namen der Domain oder die IP-Adresse ein, die Sie zu den Ausnahmen hinzufügen möchten.
6. Klicken Sie auf den Schalter neben **Online-Gefahrenabwehr**.
7. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf Schaltfläche daneben.
   Klicken **Speichern** um die Änderungen zu speichern und das Fenster zu schließen.

Bitdefender-Benachrichtigungen im Browser

Wenn Sie versuchen eine Website aufzurufen, die als unsicher eingestuft wurde, wird die entsprechende Website blockiert und eine Warnseite wird in Ihrem Browser angezeigt.

Die Seite enthält Informationen wie zum Beispiel die URL der Website und die erkannte Bedrohung.

Sie müssen entscheiden, wie Sie fortfahren möchten. Die folgenden Optionen stehen Ihnen zur Auswahl:

- Verlassen Sie die Website mit einem Klick auf **ICH GEHE LIEBER AUF NUMMER SICHER**.
- Rufen Sie die Website trotz der Warnung auf, indem Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken.
- Wenn Sie sich sicher sind, dass die erkannte Website sicher ist, klicken Sie auf **SENDEN**, um Sie zu den Ausnahmen hinzuzufügen. Wir empfehlen Ihnen, nur Websites hinzuzufügen, denen Sie uneingeschränkt vertrauen.

3.2.4. E-Mail-Schutz

Ihre E-Mail ist ein wichtiger Teil Ihres digitalen Lebens und aufgrund ihrer vielfältigen Anwendungen im wirklichen Leben ist sie zu einem bevorzugten Angriffsvektor für böswillige Akteure und zu einem der Hauptanliegen der Cybersicherheit für den alltäglichen Benutzer geworden.

E-Mail-Schutz ist eine Sicherheitsfunktion, mit der Sie potenziell gefährliche Inhalte in E-Mails, die Sie in Ihrem Posteingang erhalten, scannen und identifizieren können. Bei dieser Funktion handelt es sich um ein Paket verschiedener Technologien, die unter demselben Schutzmodul zusammengefasst sind, z. B. Anti-Phishing-, Anti-Malware-, Anti-Spam-, Anti-Betrugs- und Anti-Scam-Software.

Indem Sie eine direkte Verbindung zwischen Bitdefender und Ihrem E-Mail-Dienstanbieter herstellen, ermöglichen Sie dem Antivirenprogramm, Ihre E-Mails direkt zu scannen und beseitigen die Einschränkungen, die durch die Verwendung verschiedener Geräte oder E-Mail-Clients entstehen.

Notiz
Sie können bis zu 5 verschiedene E-Mail-Konten schützen.

Konfigurieren Sie Ihr Konto

Diese Funktion ist nahtlos in die Benutzeroberfläche integriert. So beginnen Sie mit der Verwendung des E-Mail-Schutzes:

1. Unter **Schutz**, klicken **Offen** im **E-Mail-Schutz** Karte.
2. Wählen Sie Ihren E-Mail-Anbieter für das E-Mail-Konto, das Sie schützen möchten.

   Notiz
   Der E-Mail-Schutz ist derzeit für Google-Konten, Outlook-Konten und in Kürze auch für Yahoo Mail verfügbar.

3. Klick auf das **anmelden** Taste.
   Der Vorgang wird dann in Ihrem Browser fortgesetzt.
4. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **Nächste** Taste
5. Um fortzufahren, geben Sie Ihr Passwort ein und klicken Sie auf **Nächste** Taste.
6. Überprüfen Sie die auf dem Bildschirm angeforderten Berechtigungen und erlauben Sie Bitdefender, Ihr E-Mail-Konto zu schützen.

Ihr E-Mail-Konto ist jetzt geschützt und alle neu eingehenden E-Mails werden auf Bedrohungen überprüft.

Notiz

Jede gescannte E-Mail wird mit einem Etikett versehen, um den Sicherheitsgrad anzugeben.

Armaturenbrett

Das Dashboard zeigt Ihre geschützten E-Mails an, unter denen Sie Folgendes finden:

- Konfigurationsdatum (das Datum, an dem das Konto für den E-Mail-Schutz eingerichtet wurde)
- Status (aktiv oder inaktiv)
- Anzahl der gefilterten E-Mails in den letzten 30 Tagen.
  Hier sehen Sie ein Diagramm, das die Anzahl der empfangenen sicheren und gefährlichen E-Mails anzeigt.

Um mehrere E-Mail-Konten hinzuzufügen Klick auf das **Fügen Sie ein weiteres Konto hinzu** und führen Sie für jeden von ihnen den oben genannten Konfigurationsprozess durch.

Um den Scanvorgang anzuhalten oder ein Konto zu entfernen Klicken Sie in dieser Funktion auf die drei Punkte neben dem betreffenden Konto und dann auf „ **Konto verwalten**.

3.2.5. Spam-Schutz

Spam ist ein Begriff, den man für unaufgeforderte Emails verwendet. Spam ist ein wachsendes Problem für Heimanwender wie auch für Organisationen. Sie wollen wahrscheinlich nicht, dass Ihre Kinder die meisten dieser Spam-Mails mit häufig pornographischem Inhalt lesen oder dass Sie deswegen sogar in Unannehmlichkeiten geraten. Spam wird immer mehr zum Ärgernis. Daher ist es das Beste, diese Mails gar nicht mehr zu erhalten.

BitDefender Antispam verwendet aussergewöhnliche Technologische Innovationen und Standard-Antispam Filter um Spam auszusortieren bevor dieser im Posteingang landet. Weitere Informationen finden Sie im Kapitel Wie funktioniert der Spam-Schutz? (Seite 49).

Der Bitdefender Spam-Schutz ist nur für E-Mail-Clients verfügbar, die für den Empfang von E-Mail-Nachrichten über das POP3-Protokoll konfiguriert sind. POP3 ist eines der gängigsten Protokolle zum Herunterladen von E-Mail-Nachrichten von einem Mail-Server.

Notiz

Bitdefender bietet keinen Antispam-Schutz für Email-Konten, auf die Sie über einen web-basierten Email-Service zugreifen.

Die von Bitdefender erkannten Spam-Nachrichten sind mit dem Präfix [Spam] in der Betreffzeile gekennzeichnet. Bitdefender verschiebt Spam-Nachrichten automatisch in einen bestimmten Ordner:

- In Microsoft Outlook, Spams werden verschoben in den **Spam** Ordner, zu finden unter **gelöschte Objekte**. Der **Spam**-Ordner wird erstellt, wenn eine E-Mail als Spam markiert wurde.
- In Mozilla Thunderbird werden Spam-Nachrichten in den Ordner **Spam** verschoben, der sich im Ordner **Papierkorb** befindet. Der Ordner **Spam** wird erstellt, wenn eine E-Mail als Spam gekennzeichnet wird.

Wenn Sie andere E-Mail-Clients verwenden, müssen Sie eine Regel erstellen, um die von Bitdefender als [Spam] markierten E-Mails in einen benutzerdefinierten Quarantäneordner zu verschieben. Wenn die Ordner "Gelöschte Objekte" oder "Papierkorb" gelöscht werden, wird auch der Spam-Ordner gelöscht. Es wird jedoch ein neuer Spam-Ordner erstellt, sobald eine neue E-Mail als Spam gekennzeichnet wird.

Wie funktioniert der Spam-Schutz?

Die Spam-Schutz-Funktion umfasst die folgenden Funktionen und Einstellungen:

AntiSpam Filter

Die Bitdefender Antispam Engine nutzt Cloud-Schutz und verschiedene Filter, um Ihren Posteingang frei von Spam zu halten, darunter **Liste der Freunde**, **Liste der Spammer** und **Zeichensatzfilter**.

Freundesliste/ Spammer-Liste

Viele Menschen kommunizieren normalerweise mit einer bestimmten Gruppe von Menschen oder aber erhalten Nachrichten von Firmen oder Organisationen mit derselben Domain. Wird eine **Freunde-/Spammerliste** geführt, so können Sie festlegen, welche Emails Sie erhalten wollen (die von Freunden) und welche Sie nicht erhalten möchten (die von Spammern).

Notiz

Wir empfehlen, dass Sie die Namen Ihrer Freunde und deren Email-Adressen der **Freundesliste** hinzufügen, damit sichergestellt wird, dass nur solche Emails an Sie weitergeleitet werden. BitDefender blockiert keine Nachrichten dieser Absender. Somit stellt die Liste der Freunde sicher, dass alle legitimen Nachrichten auch ankommen.

Zeichensatz-Filter

Viele Spam-E-Mails sind in Kyrillisch und/oder Asiatisch geschrieben. Der Zeichensatzfilter erkannt diese Art von Nachrichten und kennzeichnet sie als Spam.

Spam-Schutz

Die Bitdefender Antispam Engine kombiniert alle Spam-Schutz-Filter, um zu entscheiden, ob eine bestimmte E-Mail-Nachricht Ihren **Posteingang** erreichen soll oder nicht.

Jede E-Mail aus dem Internet wird zunächst mit dem Filter **Liste der Freunde**/**Liste der Spammer** geprüft. Wenn die Adresse des Absenders in der **Liste der Freunde** gefunden wird, wird die E-Mail direkt in Ihren **Posteingang** verschoben.

Wenn nicht, überprüft der Filter **Spammerliste**, ob der Absender der E-Mail auf der Liste der Spammer steht. Falls dem so ist, wird die E-Mail als Spam markiert und in den **Spam**-Ordner verschoben.

Der **Zeichensatz-Filter** überprüft, ob die E-Mail in kyrillischen oder asiatischen Zeichen geschrieben wurde. Falls dem so ist, wird die E-Mail als Spam markiert und in den **Spam**-Ordner verschoben.

Notiz

Wenn die Email in der Betreffzeile als „ausdrücklich sexuell“ gekennzeichnet wurde, stuft Bitdefender die Email als Spam ein.

Unterstützte E-Mail-Clients und Protokolle

Der Antispam-Schutz steht für alle POP3/SMTP E-Mail-Clients zur Verfügung. Die BitDefender Antispam Toolbar ist integriert in:

- Microsoft Outlook 2007 / 2010 / 2013 / 2016 / 2019
- Mozilla Thunderbird 14 und höher

Aktivieren / Deaktivieren des Spam-Schutzes

Der Spam-Schutz ist standardmäßig aktiviert.

So können Sie die Spam-Schutz-Funktion deaktivieren:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Aktivieren oder deaktivieren Sie den Schalter im Bereich **SPAM-SCHUTZ**

Verwenden der Spam-Schutz-Symbolleiste in Ihrem Mail-Client-Fenstr

Im oberen Teil Ihres Mail Client Fensters können Sie die Antispamleiste sehen. Diese hilft Ihnen beim Verwalten des Antispamschutzes direkt vom E-Mail Client aus. Sie können BitDefender ganz einfach korrigieren falls eine reguläre Mail als Spam markiert wurde.

> **Wichtig**
> BitDefender integriert sich in die gebräuchlichsten Mail Clients durch eine einfach zu verwendende Antispam Toolbar. Um die komplette Liste der unterstützen E-Mail Clients zu erhalten, lesen Sie bitte: Unterstützte E-Mail-Clients und Protokolle (Seite 50).

Jede Schaltfläche wird unten beschrieben:

Einstellungen - öffnet ein Fenster, in dem Sie die Spam-Schutz-Filter und die Einstellungen der Symbolleiste konfigurieren können.

Ist Spam - zeigt an, dass es sich bei der ausgewählten E-Mail um Spam handelt. Die E-Mail wird sofort in den Ordner **Spam** verschoben. Wenn die Spam-Schutz-Cloud-Dienste aktiviert sind, wird die Nachricht zur weiteren Analyse an die Bitdefender Cloud gesendet.

Kein Spam - zeigt an, dass die ausgewählte E-Mail kein Spam ist und Bitdefender sie nicht hätte kennzeichnen sollen. Die E-Mail wird vom Ordner **Spam** in den **Posteingang** verschoben. Wenn die Spam-Schutz-Cloud-Dienste aktiviert sind, wird die Nachricht zur weiteren Analyse an die Bitdefender Cloud gesendet.

> **Wichtig**
> Die Schaltfläche **Kein Spam** wird aktiv, wenn Sie eine von Bitdefender als Spam markierte Nachricht auswählen (üblicherweise befinden sich diese Nachrichten im Ordner **Spam**).

Neuer Spammer - fügt den Absender der ausgewählten E-Mail zur Liste der Spammer hinzu. Möglicherweise müssen Sie zur Bestätigung auf **OK** klicken. Die von Adressen in der Liste der Spammer empfangenen E-Mails werden automatisch als [Spam] gekennzeichnet.

Neuer Freund - fügt den Absender der ausgewählten E-Mail zur Liste der Freunde hinzu. Möglicherweise müssen Sie zur Bestätigung auf **OK** klicken. E-Mail-Nachrichten von dieser Adresse werden Ihnen unabhängig von Ihrem Inhalt immer zugestellt.

Spammer - öffnet die **Liste der Spammer**, die alle E-Mail-Adressen enthält, von denen Sie keine Nachrichten erhalten möchten, unabhängig von deren Inhalt. Weitere Informationen finden Sie unter Konfigurieren der Spammerliste (Seite 55).

Freunde - öffnet die **Liste der Freunde**, die alle E-Mail-Adressen enthält, von denen Sie immer E-Mail-Nachrichten erhalten möchten, unabhängig von deren Inhalt. Weitere Informationen finden Sie unter Konfigurieren der Freundesliste (Seite 53).

Anzeigen von Erkennungsfehlern

Wenn Sie einen unterstützten E-Mail-Client verwenden, können Sie den Spam-Filter einfach korrigieren (indem Sie angeben, welche E-Mails nicht als [Spam] hätten markiert werden sollen). Dadurch wird die Effizienz des Spam-Filters verbessert. Gehen Sie wie folgt vor:

1. Öffnen Sie den Mail Client.
2. Gehen Sie zu dem Junk Mail Ordner, wo die Spam Nachrichten hin verschoben werden.
3. Wählen Sie die Nachricht aus, die von Bitdefender fälschlicherweise als [Spam] markiert wurde.
4. Klicken Sie auf die Schaltfläche **Neuer Freund** in der Bitdefender Spam-Schutz-Symbolleiste, um den Absender zur Liste der Freunde hinzuzufügen. Möglicherweise müssen Sie zur Bestätigung auf **OK** klicken. E-Mail-Nachrichten von dieser Adresse werden Ihnen unabhängig von Ihrem Inhalt immer zugestellt.
5. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die

Schaltfläche **Kein Spam**. Die E-Mail wird in den Posteingangsordner verschoben.

Hinweisen auf unerkannte Spam-Nachrichten

Wenn Sie einen unterstützten E-Mail-Client verwenden, können Sie einfach angeben, welche E-Mails als Spam hätten markiert werden sollen. Dadurch wird die Effizienz des Spam-Filters verbessert. Folgen Sie diesen Schritten:

1. Öffnen Sie Ihren E-Mail-Client.
2. Begeben Sie sich zum Inbox Ordner.
3. Wählen Sie die unentdeckte Spam-Nachricht.
4. Klicken Sie in der Bitdefender Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die Schaltfläche **Ist Spam**. Sie werden sofort als [Spam] markiert und in den Junk-Mail-Ordner verschoben.

Konfigurieren der Symbolleisteneinstellungen

Um die Einstellungen für die Spam-Schutz-Symbolleiste in Ihrem E-Mail-Client zu konfigurieren, klicken Sie in der Symbolleiste auf die Schaltfläche **Einstellungen** und danach auf den Reiter **Symbolleisteneinstellungen**.

Dabei haben Sie die folgenden Möglichkeiten:

- **Markieren Sie Spam-E-Mail Nachrichten als 'gelesen'** - Markiert die Spam-Nachrichten automatisch als gelesen, so dass sie Sie nicht stören, wenn diese ankommen.
- Sie können festlegen, ob Bestätigungsfenster angezeigt werden sollen, wenn Sie auf die Schaltflächen **Neuer Spammer** und **Neuer Freund** in der Spam-Schutz-Symbolleiste klicken.
  Bestätigungsfenster verhindern, dass Sie die Absender von E-Mail-Nachrichten versehentlich zu Ihrer Freundes- bzw. Spam-Liste hinzufügen.

Konfigurieren der Freundesliste

Die **Liste der Freunde** ist eine Liste, die alle E-Mail-Adressen enthält, von denen Sie immer Nachrichten erhalten möchten, egal, welchen Inhalt sie

haben. Nachrichten Ihrer Freunde werden nicht als Spam markiert, auch wenn der Inhalt dem von Spam ähnlich sein sollte.

> **Notiz**
> Jede Mail von einer Adresse Ihrer **Freundesliste** wird automatisch in Ihren Posteingang verschoben.

Konfigurierung und Verwaltung der Freundesliste:

- Wenn Sie Microsoft Outlook oder Thunderbird verwenden, klicken Sie in der **Bitdefender Spam-Schutz-Symbolleiste** auf die Schaltfläche Freunde.
- Alternativ:
  1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
  2. Klicken Sie im Bereich **SPAM-SCHUTZ** auf **Einstellungen**.
  3. Rufen Sie das Fenster **Freunde verwalten** auf.

Um eine E-Mail-Adresse hinzuzufügen, wählen Sie die Option **E-Mail-Adresse**, geben die Adresse ein und klicken dann auf **HINZUFÜGEN**. Syntax: name@domain.com.

Um alle E-Mail-Adressen einer bestimmten Domain hinzuzufügen, wählen Sie die Option **Domain-Name**, geben Sie den Namen der Domain ein, und klicken Sie dann auf **HINZUFÜGEN**. Syntax.

- @domain.com und domain.com - alle eingehenden Mails von domain.com werden in Ihren **Posteingang** verschoben, gleich welchen Inhalts;
- domain - alle eingehenden Mails von domain (egal welcher Endung) werden als Spam markiert;
- com - alle Mails mit dieser Endung com werden als Spam markiert;

Wir empfehlen, keine kompletten Domains hinzuzufügen, in einigen Situationen kann dies jedoch sinnvoll sein. Sie können beispielsweise die Email-Domain der Firma, für die Sie arbeiten, oder die von vertrauenswürdigen Partnern hinzufügen.

Um einen Eintrag aus der Liste zu löschen, klicken Sie auf die entsprechende Schaltfläche daneben. Um alle Einträge aus der Liste zu löschen, klicken Sie auf **Liste löschen**.

Sie können die Freundesliste speichern, so dass diese auf einem anderen Gerät oder nach einer Neuinstallation genutzt werden kann. Um die Freundesliste aufzunehmen, klicken Sie auf Speichern und wählen Sie den gewünschten Ort. Die Datei wird .bwl als Erweiterung haben.

Um eine zuvor gespeicherte Freundesliste zu laden, klicken Sie **Laden** und öffnen die entsprechende .bwl Datei. Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie **Liste überschreiben**.

Konfigurieren der Spammerliste

Liste der Spammer - Liste die alle E-Mail-Adressen enthält, von denen Sie keine Nachrichten erhalten wollen, gleich welchen Inhalts. Jede Mail von einer Adresse Ihrer **Spammerliste** wird automatisch als Spam markiert.

Konfigurierung und Verwaltung der Spammer-Liste:

- Wenn Sie Microsoft Outlook oder Thunderbird nutzen, klicken Sie auf **Spammer** auf der **Bitdefender Spam-Schutz-Symbolleiste**, die in Ihr E-Mail-Programm integriert ist.
- Alternative:
  1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
  2. Im **SPAMSCHUTZ** Bereich, klicken Sie auf **Einstellungen**.
  3. Rufen Sie das Fenster **Spammer verwalten** auf.

Um eine E-Mail-Adresse hinzuzufügen, wählen Sie die aus **E-Mail-Addresse** Option, geben Sie die Adresse ein und klicken Sie dann auf **HINZUFÜGEN**. Syntax: name@domain.com.

Um alle E-Mail-Adressen einer bestimmten Domäne hinzuzufügen, wählen Sie die aus **Domänenname** Option, geben Sie den Domänennamen ein und klicken Sie dann auf **HINZUFÜGEN**. Syntax:

- @domain.com und domain.com - alle eingehenden Mails von domain.com werden unabhängig von ihrem Inhalt in Ihren **Posteingang** verschoben;
- Domäne - alle empfangenen E-Mail-Nachrichten von der Domäne (unabhängig von den Domänensuffixen) werden als SPAM gekennzeichnet;

- com - alle Mails mit dieser Endung com werden als Spam markiert.

Wir empfehlen, keine kompletten Domains hinzuzufügen, in einigen Situationen kann dies jedoch sinnvoll sein.

> **Warnung**
> Fügen Sie keine Domänen seriöser webbasierter E-Mail-Anbieter (wie Yahoo, Gmail, Hotmail etc.) zur Liste der Spammer hinzu. Andernfalls werden die E-Mail-Nachrichten, die von einem registrierten Benutzer eines solchen Dienstes eingehen, als Spam erkannt. Wenn Sie beispielsweise **yahoo.com** zur Liste der Spammer hinzufügen, werden alle E-Mail-Nachrichten, die von **yahoo.com**-Adressen kommen, als [Spam] markiert.

Um ein Element aus der Liste zu löschen, klicken Sie auf das entsprechende Element Schaltfläche daneben. Um alle Einträge aus der Liste zu löschen, klicken Sie auf **Liste leeren**.

Sie können die Spammerliste speichern, so dass diese auf einem anderen Gerät oder nach einer Neuinstallation genutzt werden kann. Um die Spammerliste aufzunehmen, klicken Sie auf **Speichern** und wählen Sie den gewünschten Ort. Die Datei wird .bwl als Erweiterung haben.

Um eine zuvor gespeicherte Spammerliste zu laden, klicken Sie **LADEN** und öffnen die entsprechende .bwl Datei. Um den Inhalt einer aktuellen Liste zurückzusetzen während der Inhalt einer zuvor gespeicherten Liste geladen wird, wählen Sie Liste überschreiben.

Konfigurieren der lokalen Spam-Schutz-Filter

Wie in Wie funktioniert der Spam-Schutz? (Seite 49) beschrieben, nutzt Bitdefender eine Kombination aus unterschiedlichen Spam-Filtern, um Spam zu identifizieren. Die Spam-Filter sind für den effizienten Schutz vorkonfiguriert.

> **Wichtig**
> Abhängig davon, ob Sie legitime Emails mit asiatischen oder kyrillischen Zeichen erhalten, aktivieren oder deaktivieren Sie die Einstellung, die solche Emails automatisch abblockt. Die entsprechende Einstellung ist in den lokalisierten Programmversion deaktiviert, die solche Zeichensätze verwendet (wie z. B. in der russischen oder chinesischen Programmversion).

So können Sie die lokalen Spam-Schutz-Filter konfigurieren:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **SPAMSCHUTZ** Bereich, klicken Sie auf **Einstellungen**.
3. Rufen Sie das Fenster **Einstellungen** auf und klicken Sie auf den entsprechenden Ein- oder Ausschalter.

Wenn Sie Microsoft Outlook oder Thunderbird nutzen, können Sie die lokalen Spam-Schutz-Filter direkt in Ihrem E-Mail-Client konfigurieren. Klicken Sie auf die Schaltfläche ⚙ **Einstellungen** in der Bitdefender Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des E-Mail-Client-Fensters befindet) und dann auf den Reiter **Antispam-Filter**.

Konfigurieren der Cloud-Einstellungen

Die Cloud-Erkennung nutzt die Bitdefender Cloud-Dienste, um Ihnen effizienten und stets aktuellen Spam-Schutz bieten zu können.

Der Cloud-Schutz funktioniert, solange der Bitdefender Spam-Schutz aktiviert ist.

Beispiele von legitimen E-Mails und Spam-Nachrichten können in die Bitdefender Cloud übermittelt werden, wenn Sie auf Erkennungsfehler oder unerkannte Spam-Nachrichten hinweisen möchten. Dies trägt dazu bei, die Spam-Erkennung von Bitdefender zu verbessern.

Konfigurieren Sie die Übermittlung der E-Mail-Beispiele an die Bitdefender Cloud, indem Sie die gewünschten Optionen wie folgt auswählen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **SPAMSCHUTZ** Bereich, klicken Sie auf **Einstellungen**.
3. Gehen Sie zum **Einstellungen** Fenster und klicken Sie auf die entsprechenden Schalter zum Ein- oder Ausschalten.

Wenn Sie Microsoft Outlook oder Thunderbird nutzen, können Sie die Cloud-Erkennung direkt in Ihrem E-Mail-Client konfigurieren. Klicken Sie auf die Schaltfläche ⚙ **Einstellungen** in der Bitdefender Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des E-Mail-Client-Fensters befindet) und dann auf den Reiter **Cloud-Einstellungen**.

3.2.6. Firewall

> **Hinweis**
> Das Firewall-Modul in Bitdefender Ultimate Small Business Security ist standardmäßig deaktiviert. Sie müssen es manuell aktivieren.
>
> Falls die**Windows Defender Firewall** während dieses Vorgangs aktiviert ist, werden Sie aufgefordert, diese zunächst zu deaktivieren.

Die Firewall schützt Ihr Gerät vor unerwünschten Verbindungen von innen und außen sowohl im lokalen Netzwerk als auch im Internet. Sie funktioniert im Prinzip wie ein Wächter an Ihrem Tor - sie überwacht alle Verbindungsversuche und entscheidet, welche Verbindungen zugelassen und welche blockiert werden.

Die Bitdefender-Firewall nutzt eine Regelwerk, um den eingehenden und ausgehenden Datenverkehr auf Ihrem System zu filtern.

Unter normalen Umständen legt Bitdefender automatisch eine Regel an, sobald eine Anwendung versucht, auf das Internet zuzugreifen. Sie können Anwendungsregeln zudem manuell hinzufügen oder bearbeiten.

Als Sicherheitsmaßnahme werden Sie jedes Mal benachrichtigt, wenn eine potenziell gefährliche Anwendung am Zugriff auf das Internet gehindert wird.

Bitdefender ordnet automatisch jeder erkannten Netzwerkverbindung den entsprechenden Netzwerktyp zu. Je nach Netzwerktyp wird der Firewall-Schutz für jede Verbindung auf die angemessene Stufe eingestellt.

Um mehr über die Firewall-Einstellungen für jeden Netzwerktyp und die Bearbeitung der Netzwerkeinstellungen zu erfahren, lesen Sie bitte das Kapitel Verbindungseinstellungen verwalten (Seite 62).

Aktivieren / Deaktivieren des Firewall-Schutzes

So können Sie den Firewall-Schutz aktivieren oder deaktivieren:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Aktivieren oder deaktivieren Sie den Schalter im Bereich **FIREWALL**.

> **Warnung**
> Die Deaktivierung der Firewall sollte immer nur von kurzer Dauer sein, da Ihr Gerät so der Gefahr durch nicht autorisierte Verbindungen ausgesetzt wird. Aktivieren Sie die Firewall so schnell wie möglich wieder.

Verwalten von App-Regeln

So können Sie die Firewall-Regeln anzeigen und verwalten, die den Zugang von Anwendungen zu Netzwerkressourcen und dem Internet steuern:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Klicken Sie im Bereich **FIREWALL** auf **Einstellungen**.
3. Rufen Sie das Fenster **Anwendungszugriff** auf.

Sie können die neuesten Programme (Prozesse) sehen, die Bitdefender Firewall und das Internet-Netzwerk, mit dem Sie verbunden sind, durchlaufen haben. Um die für eine bestimmte Anwendung erstellten Regeln zu sehen, klicken Sie einfach auf die Anwendung und dann auf den Link **Anwendungsregeln anzeigen**. Das Fenster **Regeln** wird geöffnet.

Für jede Regel werden die folgenden Informationen angezeigt:

- **NETZWERK** - Der Prozess und die Netzwerkadaptertypen (Heim / Büro, Öffentlich oder Alle), auf die die Regel angewendet wird. Regeln werden automatisch erstellt um den Netzwerk- oder Internetzugriff jedes Adapters zu filtern. Die Regeln werden standardmäßig auf jedes Netzwerk angewendet. Sie können manuell Regeln erstellen oder bestehende Regeln bearbeiten um den Zugriff einer Anwendung auf das Netzwerk/Internet über einen speziellen Adapter zu filtern (zum Beispiel ein drahtloser Netzwerkadapter).
- **PROTOKOLL** - Das IP-Protokoll, auf das die Regel angewendet wird. Die Regeln werden standardmäßig auf jedes Protokoll angewendet.
- **DATENVERKEHR** - Die Regel wird in beide Richtungen angewendet, eingehend und ausgehend.
- **PORTS** - Das PORT-Protokoll, auf das die Regel angewendet wird. Die Regeln werden standardmäßig auf alle Ports angewendet.
- **PORTS** - Das Internet-Protokoll (IP), auf das die Regel angewendet wird. Die Regeln werden standardmäßig auf alle IP-Adressen angewendet.
- **ZUGRIFF** - Gibt an, ob der Zugriff der Anwendung auf das Netzwerk oder das Internet unter den festgelegten Umständen zugelassen oder verweigert wird.

Um die Regeln für die ausgewählte Anwendung zu bearbeiten oder zu löschen, klicken Sie auf das Symbol ⋯ .

- **Regel bearbeiten** - Öffnet ein Fenster, in dem die aktuelle Regel bearbeitet werden kann.
- **Regel löschen** - Hiermit können Sie den vorhandenen Regeln für die ausgewählte App löschen.

Hinzufügen von App-Regeln

Gehen Sie zum Hinzufügen einer App-Regel folgendermaßen vor:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **FIREWALL** Bereich, klicken Sie auf **Einstellungen**.
3. Klicken Sie im Fenster **Regeln** auf **Regel hinzufügen**.

Hier können Sie die folgenden Änderungen vornehmen:

- **Diese Regel auf alle Anwendungen anwenden.** Aktivieren Sie diesen Schalter, um die erstellte Regel auf alle Anwendungen anzuwenden.
- **Programmpfad**. Klicken Sie auf **DURCHSUCHEN** und wählen Sie die Anwendung, auf die die Regel angewendet werden soll.
- **Berechtigung**. Wählen Sie eine der verfügbaren Berechtigungen:

Berechtigung	Beschreibung
Zulassen	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen erlaubt.
Verweigern	Der eingestellten Anwendung wird die Verbindung unter den angegebenen Umständen verweigert.

- **Netzwerktyp**. Wählen Sie den Netzwerktyp, für den die Regel gelten soll. Sie können den Typ ändern, indem Sie das Dropdown-Menü **Netzwerktyp** öffnen und einen der verfügbaren Typen aus der Liste auswählen.

Netzwerktyp	Beschreibung
Alle Netzwerk	Unabhängig vom Netzwerktyp sämtlichen Datenverkehr zwischen Ihrem Gerät und anderen Geräten zulassen.
Heim/Büro	Datenverkehr zwischen Geräten im lokalen Netzwerk in beide Richtungen zulassen.
Öffentlich	Sämtlicher Datenverkehr wird gefiltert.

- **Protokoll**. Wählen Sie aus dem Menü das IP-Protokoll aus, für das die Regel angewendet werden soll.

- Wenn Sie möchten, dass die Regel für alle Protokolle angewendet wird, wählen Sie **Alle**.
- Wenn Sie möchten, dass die Regel für TCP-Protokolle angewendet wird, wählen Sie **TCP**.
- Wenn Sie möchten, dass die Regel für UDP-Protokolle angewendet wird, wählen Sie **UDP**.
- Wenn Sie möchten, dass die Regel für ICMP angewendet wird, wählen Sie **ICMP** aus.
- Wenn Sie möchten, dass die Regel für IGMP angewendet wird, wählen Sie **IGMP** aus.
- Wenn Sie möchten, dass die Regel auf GRE angewendet wird, wählen Sie **GRE** aus.
- Wenn Sie möchten, dass die Regel auf ein bestimmtes Protokoll angewendet wird, geben Sie die Nummer des Protokolls, das Sie filtern möchten, in das leere Feld ein.

> **Notiz**
> IP-Protokollnummern werden von der Internet Assigned Numbers Authority (IANA) vergeben. Die vollständige Liste der vergebenen IP-Protokollnummern finden Sie unter http://www.iana.org/assignments/protocol-numbers.

- **Richtung**. Wählen Sie aus dem Menü die Richtung des Datenverkehrs, auf den die Regel angewendet werden soll.

Richtung	Beschreibung
Ausgehend	Die Regel bezieht sich nur auf den ausgehenden Datenverkehr.
Eingehend	Die Regel bezieht sich nur auf den eingehenden Datenverkehr.
Beides	Die Regel findet in beiden Richtungen Anwendung.

Klicken Sie auf die Schaltfläche **Erweiterte Einstellungen** unten im Fenster, um die folgenden Einstellungen vorzunehmen:

- **Benutzerdefinierte lokale Adresse**. Geben Sie die lokale IP-Adresse und den Port an, auf die/den die Regel anwendet werden soll.
- **Benutzerdefinierte Remoteadresse**. Geben Sie die Remote-IP-Adresse und den Port an, auf die/den die Regel anwendet werden soll.

Klicken Sie zum Entfernen des aktuellen Regelsatzes und Wiederherstellen der Standardregeln im Fenster **Regeln** auf **Regeln zurücksetzen**.

Verbindungseinstellungen verwalten

Je nachdem, ob Sie Ihre Internetverbindung per WLAN oder Ethernet-Adapter herstellen, können Sie die entsprechenden Einstellungen für ein sicheres Surfvergnügen konfigurieren. Ihnen stehen die folgenden Optionen zur Auswahl:

- **Dynamisch** – Legt den Netzwerktyp automatisch anhand des Profils des Netzwerks fest, mit dem Sie verbunden sind (Heim/Büro oder öffentlich). Tritt dies ein, werden nur die Firewall-Regeln angewendet, die für diesen Netzwerktyp bzw. für alle Netzwerktypen konfiguriert wurden.
- **Heim/Büro** – Der Netzwerktyp wird immer als Heim/Büro festgelegt, unabhängig von Profil des Netzwerks, mit dem Sie verbunden sind. Tritt dies ein, werden nur die Firewall-Regeln angewendet, die für Heim/Büro bzw. für alle Netzwerktypen konfiguriert wurden.
- **Öffentlich** – Der Netzwerktyp wird immer als öffentlich festgelegt, unabhängig von Profil des Netzwerks, mit dem Sie verbunden sind. Tritt dies ein, werden nur die Firewall-Regeln angewendet, die für öffentliche Netzwerke bzw. für alle Netzwerktypen konfiguriert wurden.

So konfigurieren Sie Ihre Netzwerkadapter:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **FIREWALL** Bereich, klicken Sie auf **Einstellungen**.
3. Rufen Sie das Fenster **Netzwerkadapter** auf.
4. Wählen Sie die Einstellungen aus, die bei Verbindungen mit den folgenden Adaptern angewendet werden sollen:
   - WLAN
   - Ethernet

Konfigurieren der erweiterten Einstellungen

So können Sie die erweiterten Firewall-Einstellungen konfigurieren:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **FIREWALL** Bereich, klicken Sie auf **Einstellungen**.
3. Wähle aus **Einstellungen** Fenster.

Die folgenden Funktionen können konfiguriert werden:

- **Port-Scan-Schutz** - Erkennt und blockiert Versuche, offene Ports zu finden.
  Portscans werden von Hackern verwendet, um herauszufinden, welche Ports auf Ihrem Gerät offen sind. Wenn Sie dann einen ungesicherten Port finden, können Sie in Ihr Gerät eindringen.
- **Benachrichtigungsmodus** - es wird jedes Mal eine Benachrichtigung angezeigt, wenn eine Anwendung versucht, sich mit dem Internet zu verbinden. Wählen Sie **Zulassen** oder **Blockieren**. Wenn der Benachrichtigungsmodus aktiviert ist, wird die Funktion **Profile** automatisch ausgeschaltet. Der Benachrichtigungsmodus kann gleichzeitig mit dem Modus **Akkubetrieb** verwendet werden.
- **Zugriff auf Domänennetzwerk zulassen** - Den Zugriff auf Ressourcen und Freigaben, die von Ihren Domänencontrollern definiert wurden, erlauben oder verweigern.
- **Tarnkappe** - legt fest, ob Sie von anderen Geräten gefunden werden können. Klicken Sie auf **Tarneinstellungen bearbeiten**, um festzulegen, wann Ihr Gerät für andere Geräte sichtbar sein soll und wann nicht.
- **Standardmäßiges Anwendungsverhalten** - Erlaubt, dass Bitdefender automatische Einstellungen auf Anwendungen ohne festgelegte Regel anwendet. Klicken Sie auf **Standardregeln bearbeiten**, um festzulegen, ob automatische Einstellungen angewendet werden sollen oder nicht.
  - Automatisch - Der Anwendungszugriff wird anhand der automatischen Firewall-Regeln und der benutzerdefinierten Regeln zugelassen oder verweigert.
  - Zulassen - Anwendungen ohne festgelegte Firewall-Regeln werden automatisch zugelassen.
  - Blockieren - Anwendungen ohne festgelegte Firewall-Regeln werden automatisch blockiert.

3.2.7. Schwachstellen

Ein wichtiger Schritt für den Schutz Ihres Geräts gegen Angriffe und schädliche Anwendungen besteht darin, das Betriebssystem und regelmäßig genutzte Programme stets auf dem neusten Stand zu halten. Darüber hinaus müssen für jedes Windows-Benutzerkonto und die genutzten WLAN-Netzwerke sichere Passwörter vergeben werden, um zu verhindern, dass ein nicht autorisierter physischer Zugriff auf Ihr Gerät erfolgt.

Bitdefender bietet Ihnen zwei einfache Möglichkeiten, die Schwachstellen Ihres Systems zu beheben:

- Sie können Ihr System nach Schwachstellen durchsuchen und diese Schritt für Schritt mit dem **Schwachstellen-Scan** beheben.
- Mithilfe der automatischen Schwachstellenüberwachung können Sie im **Benachrichtigungen**-Fenster erkannte Schwachstellen überprüfen und beheben.

Sie sollten Ihr System alle ein bis zwei Wochen nach Schwachstellen durchsuchen und diese beheben.

Scannen des Computers nach Schwachstellen

Bitdefender benötigt eine aktive Internetverbindung, um Systemschwachstellen zu erkennen.

So können Sie Ihr System auf Schwachstellen überprüfen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Klicken Sie im Fenster **SCHWACHSTELLE** auf **Öffnen**.
3. Klicken Sie im Reiter **Schwachstellen-Scan** auf **Scan starten**, und warten Sie dann, bis Bitdefender Ihr System auf Schwachstellen überprüft hat. Die gefundenen Schwachstellen werden in drei Kategorien unterteilt:
   - **BETRIEBSSYSTEM**
     - **Betriebssystemsicherheit**
       Geänderte Systemeinstellungen, die Ihr Gerät und Ihre Daten gefährden können, z. B. die Nichtanzeige von Warnungen, wenn ausgeführte Dateien ohne Ihre Erlaubnis Änderungen an Ihrem System vornehmen oder wenn MTP-Geräte wie Telefone

oder Kameras ohne Ihr Wissen angeschlossen werden und verschiedene Operationen ausführen.

- **Kritische Windows-Updates**
  Es wird eine Liste aller kritischen Windows-Updates angezeigt, die nicht auf Ihrem Computer installiert sind. Ein Neustart des Systems kann erforderlich sein, damit Bitdefender die Installation abschließen kann. Bitte beachten Sie, dass die Installation der Updates einige Zeit in Anspruch nehmen kann.
- **Unsichere Windows-Konten**
  Sie können die Liste der auf Ihrem Gerät konfigurierten Windows-Benutzerkonten sehen und die Sicherheit, die das jeweilige Passwort bietet. Sie können den jeweiligen Benutzer auffordern, das Passwort bei der nächsten Anmeldung zu ändern oder das Passwort sofort selbst ändern. Klicken Sie auf **Ändern Sie jetzt das Passwort**, um ein neues Passwort für Ihr System festzulegen.
  Um ein sicheres Passwort festzulegen, empfehlen wir Ihnen, eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (z. B. #, $ oder @) zu verwenden.

- **ANWENDUNGEN**
  - **Browser-Sicherheit**
    Änderungen an den Einstellungen Ihres Geräts, die die Ausführung von Dateien und Programmen ermöglichen, die über den Internet Explorer ohne Integritätsprüfung heruntergeladen wurden, was zu einer Gefährdung Ihres Geräts führen kann.
  - **Anwendungsupdates**
    Um Informationen über die zu aktualisierende App zu erhalten, klicken Sie auf den Namen in der Liste.
    Wenn eine Anwendung nicht auf dem neuesten Stand ist, klicken Sie auf **Neue Version herunterladen**, um die neueste Version herunterzuladen.

- **NETZWERK**
  - **Netzwerk & Anmeldedaten**
    Geänderte Systemeinstellungen, wie z. B. der automatische Verbindungsaufbau mit offenen Hotspot-Netzwerken ohne

Ihr Wissen oder keine erzwungene Verschlüsselung des ausgehenden Datenverkehrs über einen sicheren Kanal.

- **WLAN-Netzwerke und Router**
  Um weitere Informationen über das gerade verwendete Drahtlosnetzwerk und den Router zu erhalten, klicken Sie auf den entsprechenden Namen in der Liste. Wenn Ihnen empfohlen wird, ein sichereres Passwort für Ihr Heimnetzwerk festzulegen, sollten Sie unsere Anleitung unbedingt befolgen, damit Sie auch weiterhin vernetzt bleiben können, ohne Ihre Privatsphäre zu gefährden.
  Falls weitere Empfehlungen vorliegen, können Sie den Anweisungen folgen, um Ihr Heimnetzwerk vor Hackern zu schützen.

Automatische Schwachstellensuche

Bitdefender scannt Ihr System im Hintergrund regelmäßig nach Schwachstellen und erfasst alle erkannten Probleme im Fenster **Benachrichtigungen**.

So können Sie erkannte Probleme prüfen und beheben:

1. Klicken **Benachrichtigungen** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Wählen Sie unter dem Reiter **Alle** die Benachrichtigung bezüglich des neuesten Schwachstellen-Scans aus.
3. Sie erhalten detaillierte Informationen zu den erkannten Systemschwachstellen. Abhängig vom Problem, um eine spezifische Schwachstelle zu beheben, gehen Sie folgendermaßen vor:
   - Klicken Sie auf **Installieren**, falls Windows-Updates verfügbar sind.
   - Klicken Sie auf **Aktivieren**, falls automatische Windows-Updates deaktiviert wurden.
   - Falls eine Anwendung nicht mehr auf dem neuesten Stand ist, klicken Sie auf **Jetzt aktualisieren**, um einen Link zur Website des Anbieters zu finden, von der aus Sie die neueste Version der Anwendung installieren können.
   - Wenn ein Windows-Benutzerkonto mit einem schwachen Passwort gesichert ist, klicken Sie auf **Passwort ändern**, um den Benutzer

dazu zu zwingen, das Passwort bei der nächsten Anmeldung zu ändern oder es selbst zu ändern. Verwenden Sie für ein sicheres Passwort eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen (z.B. #, $ or @).

- Sollte die Autorun-Funktion in Windows aktiviert sein, klicken Sie auf **Beheben**, um sie zu deaktivieren.
- Falls für den von Ihnen konfigurierten Router ein unsicheres Passwort vergeben wurde, klicken Sie auf **Passwort ändern**, um auf seine Benutzeroberfläche zuzugreifen und das Passwort entsprechend anzupassen.
- Falls das Netzwerk, mit dem Sie verbunden sind, Schwachstellen aufweist, die Ihr System gefährden könnten, klicken Sie auf **WLAN-Einstellungen ändern**.

So können Sie die Einstellungen für die Schwachstellensuche konfigurieren:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **VERLETZLICHKEIT** Bereich, klicken Sie auf **Offen**.

   Wichtig
   Um automatisch über System- oder Anwendungsschwachstellen benachrichtigt zu werden, lassen Sie die Option **Schwachstellen** aktiviert.

3. Wechseln Sie zum Reiter **Einstellungen**.
4. Nutzen Sie die entsprechenden Schalter, um die Systemschwachstellen auszuwählen, die Sie regelmäßig überprüfen möchten.

   Windows-Updates
   Überprüfen Sie, ob die neuesten kritischen Microsoft-Sicherheits-Updates auf Ihrem Windows-Betriebssystem installiert sind.

   Anwendungsaktualisierungen
   Prüfen Sie, ob die auf Ihren System installierten Anwendungen aktuell sind. Veraltete Anwendungen können von schädlicher Software ausgenutzt werden und Ihren PC so anfällig für Angriffe von außen machen.

   Benutzerpasswörter

Überprüfen Sie, ob die Passwörter Ihrer Windows-Benutzerkonten und Router leicht zu erraten sind oder nicht. Passwörter, die schwer zu erraten sind (starke Passwörter), mache es sehr schwierig für Hacker, in Ihr System einzudringen. Ein starkes Passwort sollte aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen (z.B. #, $ oder @) bestehen.

Autoplay

Überprüfen Sie den Status der Windows-Autorun-Funktion. Mit dieser Funktion lassen sich Anwendungen automatisch direkt von CD, DVD, USB-Stick oder anderen externen Speichermedien starten.

Manche Bedrohungsarten verbreiten sich über den Autostart von Wechselmedien auf Ihrem PC. Aus diesem Grund sollten Sie diese Windows-Funktion deaktivieren.

WLAN-Sicherheitsberater

Prüfen Sie, ob das Heim-WLAN, mit dem Sie verbunden sind, sicher ist und ob Schwachstellen vorliegen. Überprüfen Sie zudem, ob das Passwort für Ihren Heim-Router ausreichend sicher ist und wie Sie es bei Bedarf sicherer machen können.

Die Mehrzahl der ungeschützten Drahtlosnetzwerke sind nicht sicher und erlauben Hackern ohne Weiteres, an Ihren privaten Aktivitäten teilzuhaben.

Notiz

Wenn Sie die Überwachung einer bestimmten Schwachstelle deaktivieren, werden damit zusammenhängende Probleme nicht mehr im Benachrichtigungsfenster erfasst.

WLAN-Sicherheitsberater

Egal ob unterwegs, bei der Arbeit in einem Café oder beim Warten am Flughafen: Oftmals ist es am bequemsten, sich mit einem öffentlichen WLAN zu verbinden, um Zahlungen anzuweisen, E-Mails abzurufen oder einen schnellen Blick in soziale Netzwerke zu werfen. Aber hier können auch Datenjäger lauern, die nur darauf warten, dass Ihre persönlichen Daten durch das Netzwerk wandern.

Persönliche Daten wie Ihre Passwörter und Benutzernamen, die Sie zur Anmeldung bei Ihren Online-Konten für E-Mail, Bankgeschäfte, und Social Media nutzen, aber auch die Nachrichten die Sie verschicken.

Öffentliche WLAN-Netzwerke sind in aller Regel nicht besonders sicher, da sie bei der Anmeldung kein Passwort anfordern. Und falls doch, wird

dieses Passwort allen zur Verfügung gestellt, die sich dort anmelden möchten. Darüber hinaus könnten Sie in betrügerischer Absicht oder als Honeypot eingerichtet worden sein und sind damit ein Ziel für Cyberkriminelle.

Der WLAN-Sicherheitsberater von Bitdefender liefert Informationen zu:

- **WLAN-Heimnetzwerk**
- **WLAN-Büronetzwerk**
- **Öffentliches WLAN-Netzwerk**

Aktivieren und Deaktivieren der Benachrichtigungen des WLAN-Sicherheitsberaters

So können Sie die Benachrichtigungen des WLAN-Sicherheitsberaters aktivieren oder deaktivieren:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **VERLETZLICHKEIT** Bereich, klicken Sie auf **Offen**.
3. Rufen Sie das Fenster **Einstellungen** auf und aktivieren oder deaktivieren Sie die Option **WLAN-Sicherheitsberater**.

Konfigurieren eines WLAN-Heimnetzwerks

So beginnen Sie mit der Konfiguration Ihres Heimnetzwerks:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **VERLETZLICHKEIT** Bereich, klicken Sie auf **Offen**.
3. Rufen Sie das Fenster **WLAN-Sicherheitsberater** auf und klicken Sie auf **Heim-WLAN**.
4. Klicken Sie im Reiter **Heim-WLAN** auf **WLAN-HEIMNETZWERK AUSWÄHLEN**.
   Eine Liste der bisher genutzten WLAN-Netzwerke wird angezeigt.
5. Bewegen Sie den Mauszeiger auf Ihr Heim-WLAN und klicken Sie auf **AUSWÄHLEN**.

Falls Ihr Heimnetzwerk als ungesichert oder unsicher eingestuft wurde, werden Konfigurationsempfehlungen zur Verbesserung der Sicherheit eingeblendet.

Um ein WLAN-Netzwerk zu entfernen, das Sie als Heimnetzwerk festgelegt haben, klicken Sie auf **ENTFERNEN**.

Klicken Sie auf **Neues WLAN-Heimnetzwerk auswählen**, um ein neues Drahtlosnetzwerk als Heimnetzwerk hinzuzufügen.

Konfigurieren eines WLAN-Büronetzwerks

So beginnen Sie mit der Konfiguration Ihres Büronetzwerks:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **VERLETZLICHKEIT** Bereich, klicken Sie auf **Offen**.
3. Rufen Sie das Fenster **WLAN-Sicherheitsberater** auf und klicken Sie auf **Büro-WLAN**.
4. Klicken Sie im Reiter **Büro-WLAN** auf **WLAN-BÜRONETZWERK AUSWÄHLEN**.
   Eine Liste mit den drahtlosen Netzwerken, mit denen Sie bisher verbunden waren, wird angezeigt.
5. Bewegen Sie den Mauszeiger auf Ihr Büronetzwerk und klicken Sie auf **AUSWÄHLEN**.

Falls Ihr Büronetzwerk als ungesichert oder unsicher eingestuft wurde, werden Konfigurationsempfehlungen zur Verbesserung der Sicherheit eingeblendet.

Um ein WLAN-Netzwerk zu entfernen, das Sie als Büronetzwerk festgelegt haben, klicken Sie auf {**ENTFERNEN**.

Klicken Sie auf **Neues WLAN-Büronetzwerk auswählen**, um ein neues Drahtlosnetzwerk als Büronetzwerk hinzuzufügen.

Öffentliches WLAN

Bei Verbindungen mit einem ungesicherten oder unsicheren WLAN-Netzwerk wird das Öffentliche WiFi-Profil aktiviert. Bei Aktivierung dieses Profils werden von Bitdefender Ultimate Small Business Security automatisch die folgenden Programmeinstellungen vorgenommen:

- Die Erweiterte Gefahrenabwehr ist aktiviert
- Die Bitdefender-Firewall ist aktiviert, und die folgenden Einstellungen werden auf Ihren Drahtlosadapter angewandt.
  - Tarnkappe - AKTIVIERT

- Netzwerktyp - Öffentlich

- Die folgenden Einstellungen der Online-Gefahrenabwehr sind aktiviert:
  - Verschlüsselter Web-Scan
  - Schutz gegen Betrug
  - Schutz vor Phishing-Attacken

- Eine Schaltfläche, die Bitdefender Safepay™ öffnet, wird angezeigt. In diesem Fall ist der Hotspot-Schutz für ungesicherte Netzwerke standardmäßig aktiviert.

Abrufen von Informationen zu WLAN-Netzwerken

So können Sie Informationen zu den WLAN-Netzwerken abrufen, zu denen Sie regelmäßig Verbindungen herstellen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **VERLETZLICHKEIT** Bereich, klicken Sie auf **Offen**.
3. Rufen Sie das Fenster **WLAN-Sicherheitsberater** auf.
4. Wählen Sie je nach benötigter Information einen der drei Reiter **Heim-WLAN**, **Büro-WLAN** oder **Öffentliches WLAN** aus.
5. Klicken Sie neben dem Netzwerk, über das Sie sich informieren möchten, auf **Details anzeigen**.

Es gibt drei Arten von WLAN-Netzwerken, die nach ihrer Wichtigkeit sortiert werden. Diese werden durch verschiedene Symbole unterschieden:

WLAN ist nicht sicher - zeigt an, dass das Netzwerk eine niedrige Sicherheitsstufe hat. Das bedeutet, dass ein hohes Risiko bei der Nutzung besteht. Es wird nicht empfohlen, ohne zusätzlichen Schutz Zahlungen zu tätigen oder Bankkonten einzusehen. In solchen Situationen empfehlen wir Ihnen, Bitdefender Safepay™ mit aktiviertem Hotspot-Schutz für ungesicherte Netzwerke zu verwenden.

WLAN ist nicht sicher - zeigt an, dass das Netzwerk eine mittlere Sicherheitsstufe hat. Das bedeutet, dass es Schwachstellen aufweisen kann. Es wird nicht empfohlen, ohne zusätzlichen Schutz Zahlungen zu tätigen oder Bankkonten einzusehen. In solchen Situationen empfehlen

wir Ihnen, Bitdefender Safepay™ mit aktiviertem Hotspot-Schutz für ungesicherte Netzwerke zu verwenden.

WLAN ist sicher - zeigt an, dass das von Ihnen verwendete Netzwerk sicher ist. In diesem Fall können Sie sensible Daten für Online-Vorgänge übermitteln.

Mit einem Klick auf **Details anzeigen ...** im Bereich der einzelnen Netzwerke werden die folgenden Details angezeigt:

- **Gesichert** - Hier sehen Sie, ob das ausgewählte Netzwerk sicher ist oder nicht. Unverschlüsselte Netzwerke können eine Gefahr für Ihre Daten darstellen.
- **Verschlüsselungstyp** - Hier sehen Sie, welcher Verschlüsselungstyp von dem ausgewählten Netzwerk verwendet wird. Manche Verschlüsselungstypen sind unter Umständen nicht sicher. Wir möchten Ihnen daher nachdrücklich empfehlen, die Informationen über den Verschlüsselungstyp einzusehen, um sicherzustellen, dass Sie sicher im Netz surfen.
- **Kanal/Frequenz** - Hier können Sie die Kanalfrequenz des ausgewählten Netzwerks einsehen.
- **Passwortsicherheit** - Hier sehen Sie, wie sicher das Passwort ist. Bitte beachten Sie, dass Netzwerke mit unsicheren Passwörtern für Cyberkriminelle besonders attraktiv sind.
- **Art der Anmeldung** - Hier können Sie sehen, ob das ausgewählte Netzwerk mit einem Passwort geschützt ist oder nicht. Wir empfehlen Ihnen dringend, ausschließlich Verbindungen mit Netzwerken herzustellen, die mit sicheren Passwörtern geschützt sind.
- **Authentifizierungstyp** - Hier sehen Sie, welcher Authentifizierungstyp von dem ausgewählten Netzwerk verwendet wird.

3.2.8. Video- & Audioschutz

Immer mehr Bedrohungen richten sich gegen integrierte Webcams und Mikrofone. Um den unbefugten Zugriff auf Ihre Webcam zu verhindern und Sie darüber zu informieren, welche nicht vertrauenswürdigen Anwendungen wann auf das Mikrofon Ihres Geräts zugreifen, verfügt Bitdefender Video und Audio über:

- **Webcam-Schutz**

- **Mikrofonüberwachung**

Webcam-Schutz

Dass Hacker Ihre Webcam übernehmen können, um Sie auszuspionieren, ist längst nichts Neues mehr. Mögliche Lösungen zum Schutz Ihrer Webcam, wie das Entziehen von App-Berechtigungen und das Deaktivieren oder Abkleben der integrierten Kamera, sind nicht sehr praktisch. Um zu verhindern, dass Unbefugte Ihre Privatsphäre verletzen, überwacht der Bitdefender Webcam-Schutz kontinuierlich Apps, die versuchen, auf Ihre Kamera zuzugreifen, und blockiert alle Apps, die nicht als vertrauenswürdig eingestuft sind.

Als Sicherheitsmaßnahme werden Sie jedes Mal benachrichtigt, wenn eine nicht vertrauenswürdige App versucht, auf Ihre Kamera zuzugreifen.

Aktivieren und Deaktivieren des Webcam-Schutzes

1. Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf **Privatsphäre**.
2. Klicken Sie im Bereich **VIDEO- & AUDIO-SCHUTZ** auf **Einstellungen**.
3. Rufen Sie jetzt das Fenster **Einstellungen** auf und aktivieren oder deaktivieren Sie den entsprechenden Schalter.

Konfigurieren des Webcam-Schutzes

So legen Sie fest, welche Regeln angewendet werden sollen, wenn eine App versucht, auf Ihre Kamera zuzugreifen:

1. Klicken **Privatsphäre** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **VIDEO- UND AUDIOSCHUTZ** Bereich, klicken Sie auf **Einstellungen**.
3. Gehen Sie zum **Einstellungen** Tab.

Die folgenden Optionen stehen zur Verfügung:

Blockierungsregeln für Anwendungen

- **Jeglichen Zugriff auf die Webcam blockieren** - Der Zugriff auf Ihre Webcam wird für alle Anwendungen unterbunden.
- **Webcam-Zugriff für Browser blockieren** - keinem Webbrowser außer Internet Explorer und Microsoft Edge wird der Zugriff auf Ihre Webcam

gestattet. Weil die Windows Store-Apps in einem einzigen Prozess ausgeführt werden, können Internet Explorer und Microsoft Edge von Bitdefender nicht als Webbrowser erkannt werden und sind daher von dieser Einstellung ausgenommen.

- **Anwendungsberechtigungen anhand der Auswahl anderer Benutzer festlegen** - Wird eine beliebte App von der Mehrzahl der Bitdefender-Benutzer als harmlos eingestuft, wird der Webcam-Zugriff für diese App automatisch zugelassen. Wird eine beliebte App von der Mehrheit als gefährlich eingestuft, wird der Zugriff für diese App automatisch blockiert.

Benachrichtigungen

- **Benachrichtigen, wenn zugelassene Anwendungen eine Webcam-Verbindung herstellen** - Sie werden jedes Mal benachrichtigt, wenn eine zugelassene App auf Ihre Webcam zugreift.

Hinzufügen von Apps zur Liste für den Webcam-Schutz

Zugriffsversuche von Apps werden automatisch erkannt. Abhängig von App-Verhalten und der Auswahl anderer Benutzer, wird der Zugriff zugelassen oder verweigert. Sie können darüber hinaus auch selbst festlegen, welche Aktionen ausgeführt werden soll, indem Sie folgendermaßen vorgehen:

1. Klicken **Privatsphäre** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **VIDEO- UND AUDIOSCHUTZ** Bereich, klicken Sie auf **Einstellungen**.
3. Rufen Sie das Fenster **Webcam-Schutz** auf.
4. Klicken Sie auf das Fenster **Anwendung hinzufügen**.
5. Klicken Sie auf den gewünschten Link:
   - **Aus dem Windows Store** - Eine Liste mit allen gefundenen Windows Store-Anwendungen wird angezeigt. Aktivieren Sie die Schalter neben den Apps, die Sie zur Liste hinzufügen möchten.
   - **Aus Ihren Apps** - rufen Sie die .exe-Datei auf, die Sie zur Liste hinzufügen möchten, und klicken Sie auf **OK**.

Um anzuzeigen, welche Auswahl andere Bitdefender-Anwender für eine ausgewählte App getroffen haben, bewegen Sie den Mauszeiger über das -Symbol.

In diesem Fenster werden neben dem Zeitpunkt der letzten Aktivität alle Apps angezeigt, die den Zugriff auf Ihre Kamera angefordert haben.

Sie werden jedes Mal benachrichtigt, wenn eine der zugelassenen Apps von den Bitdefender-Anwendern blockiert wurde.

Um den Zugriff einer hinzugefügten Anwendung auf Ihre Webcam zu stoppen, klicken Sie auf das -Symbol.

Das Symbol ändert sich zu . Das bedeutet, dass diese App keinen Zugriff mehr auf die Webcam hat.

Mikrofonüberwachung

Malware-Apps könnten unbemerkt im Hintergrund auf Ihr Mikrofon zugreifen. Um Sie auf potenzielle bösartige Angriffe aufmerksam zu machen, informiert Sie die Bitdefender-Mikrofonüberwachung über derartige Ereignisse. So ist sichergestellt, dass keine App auf Ihr Mikrofon zugreifen kann, ohne dass Sie es ausdrücklich erlauben.

Mikrofonüberwachung ein- und ausschalten

1. Klicken **Privatsphäre** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **VIDEO- UND AUDIOSCHUTZ** Bereich, klicken Sie auf **Einstellungen**.
3. Wähle aus **Einstellungen** Fenster.
4. Aktivieren oder deaktivieren Sie im Fenster **Einstellungen** den Schalter **Mikrofonüberwachung**.

Benachrichtigungen für die Mikrofonüberwachung konfigurieren

Wenn Sie die Benachrichtigungen konfigurieren möchten, die ausgegeben werden, wenn eine App versucht, auf Ihr Mikrofon zuzugreifen, gehen Sie wie folgt vor:

1. Klicken **Privatsphäre** im Navigationsmenü auf der Bitdefender-Oberfläche.

2. Im **VIDEO- UND AUDIOSCHUTZ** Bereich, klicken Sie auf **Einstellungen**.
3. Gehen Sie zum **Einstellungen** Fenster.

Benachrichtigungen

- **Benachrichtigen, wenn eine Anwendung versucht, auf das Mikrofon zuzugreifen**
- **Benachrichtigen, wenn Browser auf das Mikrofon zugreifen**
- **Benachrichtigen, wenn nicht vertrauenswürdige Apps auf das Mikrofon zugreifen**
- **Benachrichtigung anhand der Bitdefender-Benutzerauswahl anzeigen**

Apps zur Mikrofonüberwachungsliste hinzufügen

Apps, die versuchen, auf Ihr Mikrofon zuzugreifen, werden automatisch erkannt und dieser Liste hinzugefügt. Sie können aber auch manuell einstellen, ob Benachrichtigungen angezeigt werden oder nicht. Gehen Sie dazu wie folgt vor:

1. Klicken **Privatsphäre** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **VIDEO- UND AUDIOSCHUTZ** Bereich, klicken Sie auf **Einstellungen**.
3. Rufen Sie das Fenster **Audioschutz** auf.
4. Klicken **Anwendung hinzufügen** Fenster.
5. Klicken Sie auf den gewünschten Link:
   - **Aus dem Windows-Store** - Eine Liste mit den erkannten Windows Store-Apps wird angezeigt. Aktivieren Sie die Schalter neben den Apps, die Sie der Liste hinzufügen möchten.
   - **Von Ihren Apps** - Gehen Sie zu der .exe-Datei, die Sie der Liste hinzufügen möchten, und klicken Sie dann auf **OK**.

Um anzuzeigen, was die Bitdefender-Benutzer mit der ausgewählten App machen möchten, klicken Sie auf Symbol.

In diesem Fenster werden alle Apps angezeigt, die versucht haben auf Ihr Mikrofon zuzugreifen, sowie der Zeitpunkt der letzten Aktivität.

Um keine weiteren Benachrichtigungen zur Aktivität einer hinzugefügten App zu erhalten, klicken Sie auf das -Symbol.

Das Symbol ändert sich zu . Das bedeutet, dass keine Bitdefender-Benachrichtigung mehr angezeigt wird, wenn diese App versucht auf Ihr Mikrofon zuzugreifen.

3.2.9. Ransomware-Bereinigung

Die Ransomware-Bereinigung von Bitdefender sichert Ihre Dateien wie Dokumente, Bilder, Videos oder Musik, um sicherzustellen, dass sie im Falle einer Ransomware-Verschlüsselung nicht beschädigt werden oder verloren gehen. Jedes Mal, wenn ein Ransomware-Angriff erkannt wird, blockiert Bitdefender alle Prozesse, die an dem Angriff beteiligt sind, und startet den Bereinigungsprozess. Auf diese Weise können Sie den Inhalt Ihrer gesamten Dateien wiederherstellen, ohne ein Lösegeld bezahlen zu müssen.

Aktivieren und Deaktivieren der Ransomware-Bereinigung

So können Sie die Ransomware-Bereinigung aktivieren oder deaktivieren:

1. Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf **Schutz**.
2. Aktivieren oder deaktivieren Sie im Bereich **RANSOMWARE-BEREINIGUNG** den entsprechenden Schalter.

> **Notiz**
> Wie empfehlen, die Ransomware-Bereinigung zum Schutz Ihrer Dateien vor Ransomware aktiviert zu lassen.

Aktivieren oder Deaktivieren der automatischen Wiederherstellung

Die automatische Wiederherstellung stellt Ihre Dateien im Falle der Verschlüsselung durch Ransomware automatisch wieder her.

So können Sie die automatische Wiederherstellung aktivieren oder deaktivieren:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Klicken Sie im Fenster **RANSOMWARE-BEREINIGUNG** auf **Verwalten**.

3. Aktivieren oder deaktivieren Sie im Fenster Einstellungen den Schalter **Automatische Wiederherstellung**.

Anzeigen von automatisch wiederhergestellten Dateien

Wurde die Option **Automatisches Wiederherstellen** aktiviert, stellt Bitdefender automatisch Dateien wieder her, die durch Ransomware verschlüsselt wurden. So können Sie Ihr Gerät ganz unbeschwert genießen, ohne sich Sorgen um die Sicherheit Ihrer Dateien machen zu müssen.

So können Sie automatisch wiederhergestellte Dateien anzeigen:

1. Klicken **Benachrichtigungen** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Wechseln Sie zum Reiter **Alle** und wählen Sie die Benachrichtigung zu dem neuesten bereinigten Ransomware-Verhalten aus. Klicken Sie danach auf **Wiederhergestellte Dateien**.
   Eine Liste mit allen wiederhergestellten Dateien wird angezeigt. Hier können Sie auch einsehen, an welchem Speicherort die Dateien wiederhergestellt worden sind.

Manuelles Wiederherstellen von verschlüsselten Dateien

Gehen Sie folgendermaßen vor, um durch Ransomware verschlüsselte Dateien manuell wiederherzustellen:

1. Klicken **Benachrichtigungen** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Wechseln Sie zum Reiter **Alle** und wählen Sie die Benachrichtigung zu dem neuesten bereinigten Ransomware-Verhalten aus. Klicken Sie danach auf **Verschlüsselte Dateien**.
3. Eine Liste mit allen verschlüsselten Dateien wird angezeigt.
   Klicken Sie zum Fortfahren auf **Dateien wiederherstellen**.
4. Sollte der Wiederherstellungsprozess vollständig oder teilweise fehlschlagen, müssen Sie den Speicherort auswählen, an dem die entschlüsselten Dateien gespeichert werden sollen. Klicken Sie auf **Wiederherstellungsort** und wählen Sie einen Speicherort auf Ihrem PC aus.
5. Ein Bestätigungsfenster wird angezeigt.

Klicken Sie zum Abschluss des Wiederherstellungsprozesses auf **Beenden**.

Dateien mit den folgenden Dateiendungen können im Falle einer Verschlüsselung wiederhergestellt werden:

.3g2;.3gp;.7z;.ai;.aif;.arj;.asp;.aspx;.avi;.bat;.bin;.bmp;.c;.cda;.cgi;.class;.com;.cpp;.cs;.css;.csv;.dat;.db;.dbf;.deb;.doc;.docx;.gif;.gz;.h264;.h;.flv;.htm;.html;.ico;.jar;.java;.jpeg;.jpg;.js;.jsp;.key;.m4v;.mdb;.mid;.midi;.mkv;.mp3;.mp4;.mov;.mpg;.mpeg;.ods;.odp;.odt;.ogg;.pdf;.pkg;.php;.pl;.png;.pps;.ppt;.pptx;.ps;.psd;.py;.rar;.rm;.rtf;.sav;.sql;.sh;.svg;.swift;.swf;.tar;.tex;.tif;.tiff;.txt;.xlr;.xls;.xlsx;.xml;.wmv;.vb;.vob;.wav;.wks;.wma;.wpl;.wps;.wpd;.wsf;.z;.zip;

Anwendungen zu Ausnahmen hinzufügen

Sie können Ausnahmeregeln für vertrauenswürdige Anwendungen festlegen, damit die Ransomware-Bereinigung diese nicht blockiert, wenn ihr Verhalten auf Ransomware hindeutet.

So können Sie Apps zur Ausnahmeliste für die Ransomware-Bereinigung hinzufügen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **RANSOMWARE-BEHEBUNG** Bereich, klicken Sie auf **Verwalten**.
3. Rufen Sie das Fenster **Ausnahmen** auf und klicken Sie auf **+Ausnahme hinzufügen**.

3.2.10. Cryptomining Protection

Was ist Kryptomining-Schutz?

Durch den Einsatz von Kryptomining können Angreifer finanziell profitieren, ohne die damit verbundenen Kosten und rechtlichen Konsequenzen tragen zu müssen.

Die Cryptomining-Schutzfunktion von Bitdefender schützt Windows-Computer vor der wachsenden Bedrohung durch nicht autorisierte Crypto-Mining-Aktivitäten, eine böswillige Praxis, die die Ressourcen und den Strom eines Benutzers ausnutzt, um Einnahmen für Angreifer zu generieren.

Notiz

Der Kryptomining-Schutz basiert auf:

- Bitdefender-Schild
- Verhinderung von Web-Angriffen

Damit der Cryptomining-Schutz ausgeführt werden kann, müssen auch diese beiden Funktionen aktiviert sein.

Aktivieren des Kryptomining-Schutzes

Die Funktion „Cryptomining-Schutz“ befindet sich auf der Registerkarte „Schutz“.

Um es zu aktivieren, schalten Sie einfach den entsprechenden Schalter um.

Notiz

Der Cryptomining-Schutz ist standardmäßig deaktiviert, um sicherzustellen, dass Benutzer die Kontrolle über seine Aktivierung haben.

Betriebsarten

Nach der Aktivierung arbeitet die Funktion „Cryptomining-Schutz“ in zwei verschiedenen Zuständen, die jeweils auf die Vorlieben des Benutzers zugeschnitten sind:

1. **Blockieren Sie alle Cryptomining-Aktivitäten.** (blockiert automatisch alle Krypto-Mining-Aktivitäten und ergreift die notwendigen Maßnahmen, um weitere unbefugte Versuche zu verhindern)
   Dieser Modus ist ideal für Benutzer, die nicht die Absicht haben, sich an Krypto-Mining-Aktivitäten zu beteiligen.
2. **Erkennen Sie Cryptomining-Aktivitäten.** (gibt Warnungen aus, wenn eine Krypto-Mining-Aktivität erkannt wird, und erfordert Benutzereingaben, um die entsprechende Aktion zu bestimmen)
   Dieser Modus eignet sich für Benutzer, die aktiv an ihren eigenen Krypto-Mining-Aktivitäten beteiligt sind, aber alle unbefugten Versuche überwachen und kontrollieren möchten.

Ausnahmen verwalten

Für Anwendungen können Ausnahmen angegeben werden, mit der zusätzlichen Möglichkeit, bestimmte Befehlszeilen zu definieren. Es

können jedoch auch Ausnahmen festgelegt werden, ohne dass solch detaillierte Parameter bereitgestellt werden müssen, was ein Gleichgewicht zwischen Anpassung und Einfachheit bietet.

So fügen Sie eine Ausnahme hinzu:

1. Klicken**Schutz**im Menü auf der linken Seite der Bitdefender-Benutzeroberfläche.
2. Im**Kryptomining-Schutz**Bereich, klicken Sie**Einstellungen**.
3. Drücke den**Ausnahmen verwalten**Möglichkeit.
4. Klicken Sie anschließend auf**Fügen Sie eine Ausnahme hinzu**Taste.
5. Es öffnet sich ein neues Fenster. Sie können Anwendungen, URLs und IP-Adressen manuell ausschließen.
6. Klicken Sie abschließend**Speichern**. Die neue Regel wird zur Ausnahmeliste für den Cryptomining-Schutz hinzugefügt.

> **Notiz**
> Um eine Ausnahme zu entfernen, klicken Sie einfach auf das Papierkorbsymbol daneben.

3.2.11. Anti-Tracker

Viele der von Ihnen aufgerufenen Websites verwenden Tracker, um Informationen über Ihr Surf-Verhalten zu sammeln, entweder um sie mit anderen Unternehmen zu teilen oder um Werbeanzeigen einzublenden, die für Sie relevanter sind. Website-Betreiber verwenden die hierdurch erzielten Einnahmen, um Ihnen kostenlose Inhalte anzubieten oder den eigenen Betrieb aufrechtzuerhalten. Das Sammeln dieser Informationen kann sich auch auf Ihre Surf-Geschwindigkeit auswirken und übermäßig Bandbreite in Anspruch nehmen.

Durch Aktivierung der Bitdefender Anti-Tracker-Erweiterung in Ihrem Browser verhindern Sie Tracking, sodass Ihre Daten während des Surfens im Netz privat bleiben. Darüber hinaus können Websites schneller geladen werden.

Die Bitdefender-Erweiterung ist mit den folgenden Web-Browsern kompatibel:

- Internet Explorer

- Google Chrome
- Mozilla-Firefox

Die von uns erkannten Tracker sind in die folgenden Kategorien unterteilt:

- **Werbung** - Dient der Analyse von Website-Verkehr, von Nutzerverhalten oder von Datenverkehrsmustern von Website-Besuchern.
- **Kundeninteraktion** - Dient der Messung der Benutzerinteraktion mit verschiedenen Eingabemöglichkeiten wie Chat oder Support.
- **Wesentlich** - Dient der Überwachung kritischer Webseiten-Funktionen.
- **Site Analytics** - Dient der Sammlung von Daten über die Nutzung von Webseiten.
- **Social Media** - Dient der Überwachung von Social-Media-Zielgruppen sowie der Aktivitäten und Nutzerbindung über verschiedene Social-Media-Plattformen.

Anti-Tracker-Benutzeroberfläche

Nach Aktivierung der Bitdefender Anti-Tracker-Erweiterung erscheint das Symbol neben der Suchleiste in Ihrem Webbrowser. Jedes Mal, wenn Sie eine Website besuchen, wird auf dem Symbol ein Zähler angezeigt, der Aufschluss über erkannte und blockierte Tracker gibt. Um weitere Details zu den blockierten Trackern anzuzeigen, klicken Sie auf das Symbol, um die Benutzeroberfläche zu öffnen. Neben der Anzahl der blockierten Tracker können Sie die Ladezeit der Seite und die Kategorien der erkannten Tracker einsehen. Klicken Sie auf die gewünschte Kategorie, um die Liste der Websites anzuzeigen, die Sie tracken.

Um Bitdefender davon abzuhalten, Tracker auf der aktuell von Ihnen besuchten Website zu blockieren, klicken Sie auf **Schutz für diese Website anhalten**. Diese Einstellung gilt nur, solange die Website geöffnet ist und wird beim Schließen der Website in den Ausgangszustand zurückgesetzt.

Um Trackern aus einer bestimmten Kategorie die Überwachung Ihrer Aktivität zu erlauben, klicken Sie auf die gewünschte Aktivität, und klicken Sie dann auf die entsprechende Schaltfläche. Klicken Sie erneut auf die gleiche Schaltfläche, falls Sie Ihre Meinung ändern.

Deaktivieren von Bitdefender Anti-Tracker

So deaktivieren Sie den Bitdefender Anti-Tracker:

- Von Ihrem Webbrowser:
  1. Öffnen Sie Ihren Internet-Browser.
  2. Klicken Sie auf das -Symbol neben der Adressleiste in Ihrem Webbrowser.
  3. Klicken Sie rechts oben auf das -Symbol.
  4. Verwenden Sie zum Deaktivieren den entsprechenden Schalter. Das Bitdefender-Symbol wird grau.
- Über die Bitdefender-Oberfläche:
  1. Klicken **Privatsphäre** im Navigationsmenü auf der Bitdefender-Oberfläche.
  2. Klicken Sie im Bereich **ANTI-TRACKER** auf **Einstellungen**.
  3. Deaktivieren Sie neben dem Web-Browser, für den Sie die Erweiterung deaktivieren möchten, den entsprechenden Schalter.

Erlauben von Tracking auf einer Website

Wenn Sie beim Besuch einer bestimmten Website das Tracking erlauben möchten, können Sie die entsprechende Adresse wie folgt zu den Ausnahmen hinzufügen:

1. Öffnen Sie Ihren Webbrowser.
2. Klicken Sie auf das -Symbol neben der Suchleiste.
3. Drücke den Symbol in der oberen rechten Ecke.
4. Wenn Sie die Website, die Sie zu den Ausnahmen hinzufügen möchten, bereits aufgerufen haben, klicken Sie auf **Aktuelle Website zur Liste hinzufügen**.
   Wenn Sie eine weitere Website hinzufügen möchten, geben Sie deren Adresse in das entsprechende Feld ein und klicken Sie auf .

3.2.12. Sichere Online-Transaktionen mit Safepay

Immer mehr Menschen nutzen ihren Computer regelmäßig für ihre Einkäufe und Bankgeschäfte. Rechnungen bezahlen, Überweisungen tätigen und einkaufen war noch nie schneller und einfacher.

Bei diesen Transaktionen werden personenbezogene Daten, Konto- und Kreditkartennummern, Passwörter und andere vertrauliche Informationen über das Internet übermittelt. Und das sind genau die Daten, die Online-Kriminelle so gerne in die Finger kriegen würden. Hacker lassen nichts unversucht, an diese Daten zu gelangen. Sie können also bei der Absicherung Ihrer Online-Transaktionen gar nicht vorsichtig genug sein.

Bitdefender Safepay™ ist in erster Linie ein abgesicherter Browser, d. h. ein abgeschottetes System, das speziell entwickelt wurde, damit Online-Transaktionen wie Einkäufe und Bankgeschäfte sicher und privat abgewickelt werden können.

Bitdefender Safepay™ umfasst die folgenden Funktionen:

- Es blockiert den Zugriff auf Ihren Desktop sowie sämtliche Versuche, Bildschirmfotos zu machen.
- Es hat eine eingebaute virtuelle Tastatur, die es Hackern unmöglich macht, Ihre Tastenanschläge aufzuzeichnen.
- Es ist völlig unabhängig von Ihren anderen Browsern.
- Es enthält den Hotspot-Schutz für Situationen, in denen Ihr Gerät mit ungesicherten WLAN-Netzwerken verbunden ist.
- Es hat eine Lesezeichenfunktion, mit der Sie mühelos auf Ihre Lieblings-Banking/Shopping-Seiten zugreifen können.
- Es ist jedoch nicht nur auf Online-Banking und -Shopping beschränkt. Sie können mit Bitdefender Safepay™ auch jede andere Website öffnen.

Nutzen von Bitdefender Safepay™

Bitdefender erkennt standardmäßig, wenn Sie auf Ihrem Computer über einen Browser eine Online-Banking-Seite oder einen Online-Shop aufrufen und fordert Sie auf, diese Seite in Bitdefender Safepay™ zu öffnen.

Es gibt verschiedene Möglichkeiten™, das Bitdefender Safepay-Hauptfenster zu öffnen:

- Über die **Bitdefender-Benutzeroberfläche**:
  1. Klicken **Privatsphäre** im Navigationsmenü auf der Bitdefender-Oberfläche.
  2. Klicken Sie im Bereich **SAFEPAY** auf **Einstellungen**.
  3. Klicken Sie im Fenster **Safepay** auf **Safepay starten**.
- In Windows:
  - Unter **Windows 7**:
    1. Klicken Sie auf **Start** und gehen Sie zu **Alle Programme**.
    2. Klicken Sie auf **Bitdefender**.
    3. Klicken Sie auf **Bitdefender Safepay™**.
  - Unter **Windows 8** und **Windows 8.1**:
    Finden Sie Bitdefender Safepay™ auf der Windows-Startseite (z.B. durch die Eingabe von "Bitdefender Safepay™" auf der Startseite) und rechtsklicken Sie auf das Symbol.
  - Unter **Windows 10** und **Windows 11**:
    Geben Sie "Bitdefender Safepay™" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.

Wer schon einmal einen Internet-Browser benutzt hat, wird mit Bitdefender Safepay keinerlei Probleme haben ™- es sieht aus wie ein Browser und verhält sich auch so:

- Sie können URLs in die Adressleiste eingeben, um auf die entsprechende Seite zu gelangen.
- fügen Sie Reiter hinzu, um mehrere Websites im Bitdefender Safepay™-Fenster aufzurufen, indem Sie auf ✚ klicken.
- gehen Sie Seiten vor und zurück und laden Sie sie neu, indem Sie jeweils auf ← → und ↻ klicken.
- auf Bitdefender Safepay™ zugreifen Einstellungen durch Anklicken und Auswählen **Einstellungen**.
- verwalten Sie Ihre **Lesezeichen**, indem Sie neben der Adressleiste auf ☆ klicken.

- öffnen Sie die virtuelle Tastatur, indem Sie auf klicken.
- passen Sie die Größe des Browser-Fensters durch gleichzeitiges Drücken von **Strg** und den **+/-** -Tasten im numerischen Tastenblock an.
- rufen Sie Informationen über Ihr Bitdefender-Produkt auf, indem Sie auf ··· klicken und dann **Über** wählen.
- drucken Sie wichtige Informationen, indem Sie auf ··· klicken und dann **Drucken** wählen.

> **Notiz**
> Um zwischen Bitdefender Safepay™ und dem Windows-Desktop zu wechseln, drücken Sie die Tasten **Alt+Tab**, oder klicken Sie auf die Option **Zum Desktop wechseln** oben links im Fenster.

Einstellungen verändern

Klicken Sie auf ··· und wählen Sie **Einstellungen**, um Bitdefender Safepay™ zu konfigurieren.

Bitdefender Safepay™-Regeln auf aufgerufene Domains anwenden

Hier werden die Websites angezeigt, die Sie mit aktivierter Option **Automatisch in Safepay öffnen** zu den **Lesezeichen** hinzugefügt haben. Wenn Sie das automatische Öffnen einer Website aus der Liste mit Bitdefender Safepay™ beenden möchten, klicken Sie neben dem gewünschten Eintrag in der Spalte **Entfernen** auf ×.

Pop-ups blockieren

Pop-ups können Sie mit einem Klick auf den entsprechenden Schalter blockieren.

Sie können auch eine Liste mit Websites anlegen, die Pop-ups anzeigen dürfen. Diese Liste sollte nur Websites enthalten, denen Sie uneingeschränkt vertrauen.

Um eine Website zu der Liste hinzuzufügen, geben Sie die Adresse in das entsprechende Feld ein und klicken Sie dann auf **Domain hinzufügen**.

Um eine Website aus der Liste zu löschen, klicken Sie auf das X für den jeweiligen Eintrag.

Plug-ins verwalten

Sie können selbst entscheiden, welche Plug-ins Sie in Bitdefender Safepay™ aktivieren oder deaktivieren möchten.

Zertifikate verwalten

Sie können Zertifikate von Ihrem System in einen Zertifikatspeicher importieren.

Klicken Sie auf **IMPORTIEREN** und folgen Sie den Anweisungen des Assistenten, um Zertifikate in Bitdefender Safepay™ zu nutzen.

Virtuelle Tastatur verwenden

Die virtuelle Tastatur wird automatisch angezeigt, wenn ein Passwortfeld angewählt wird.

Über den entsprechenden Schalter können Sie die Funktion aktivieren oder deaktivieren.

Druckbestätigung

Aktivieren Sie diese Option, wenn Sie eine Bestätigung geben möchten, bevor der Druckvorgang startet.

Lesezeichen verwalten

Wenn Sie die automatische Erkennung einiger oder aller Websites deaktiviert haben oder Bitdefender einfach bestimmte Websites nicht korrekt erkennt, können Sie in Bitdefender Safepay™ Lesezeichen anlegen und so in Zukunft häufig besuchte Seiten schneller aufrufen.

So fügen Sie eine URL zu den Lesezeichen von Bitdefender Safepay™ hinzu:

1. Klicken Sie auf ⋯ und wählen Sie **Lesezeichen**, um eine Seite mit Ihren Lesezeichen zu öffnen.

   > **Notiz**
   > Die Lesezeichenliste wird standardmäßig geöffnet, wenn Sie Bitdefender Safepay™ starten.

2. Klicken Sie auf das **+** um ein neues Lesezeichen hinzuzufügen.
3. Geben Sie die URL und den Namen für das Lesezeichen ein, und klicken Sie anschließend auf **ERSTELLEN**. Aktivieren Sie die Option **Automatisch in Safepay öffnen**, wenn die in den Lesezeichen gespeicherte Seite bei jedem Besuch mit Bitdefender Safepay™

geöffnet werden soll. Die URL wird auch in der Domain-Liste auf der Seite Einstellungen hinzugefügt.

Deaktivieren der Safepay-Benachrichtigungen

Wird eine Online-Banking-Seite erkannt, wird von Ihrem Bitdefender-Produkt standardmäßig eine entsprechende Pop-up-Benachrichtigung angezeigt.

So können Sie die Safepay-Benachrichtigungen deaktivieren:

1. Klicken **Privatsphäre** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **SICHERE BEZAHLUNG** Bereich, klicken Sie auf **Einstellungen**.
3. Deaktivieren Sie im Fenster **Einstellungen** den Schalter neben **Safepay-Benachrichtigungen**.

3.2.13. Diebstahlschutz für Geräte

Laptop-Diebstahl ist ein großes Problem, das Einzelpersonen und Organisationen gleichermaßen betrifft. Noch mehr als der Verlust der Hardware selbst können die damit verlorenen Daten sowohl finanziell als auch emotional erheblichen Schaden anrichten.

Doch nur wenige Menschen unternehmen die richtigen Schritte, um ihre wichtigen persönlichen, geschäftlichen und finanziellen Daten im Falle von Diebstahl oder Verlust zu sichern.

Bitdefender Anti-Theft hilft Ihnen, besser auf ein solches Ereignis vorbereitet zu sein, indem es Ihnen ermöglicht, Ihren Laptop aus der Ferne zu lokalisieren oder zu sperren und sogar alle Daten darauf zu löschen, falls Sie sich jemals gegen Ihren Willen von Ihrem Laptop trennen sollten.

Um die Anti-Theft-Funktionen nutzen zu können, müssen folgende Voraussetzungen erfüllt sein:

- Die Befehle können nur vom Bitdefender-Konto gesendet werden.
- Der Laptop muss mit dem Internet verbunden sein, um die Befehle zu empfangen.

Anti-Diebstahl-Funktionen funktionieren wie folgt:

Lokalisieren

Zeigen Sie den Standort Ihres Geräts auf Google Maps an.

Die Genauigkeit des Standorts hängt davon ab, wie Bitdefender ihn bestimmen kann. Der Standort wird auf zehn Meter genau bestimmt, wenn Wi-Fi auf Ihrem Laptop aktiviert ist und sich drahtlose Netzwerke in Reichweite befinden.

Wenn der Laptop mit einem kabelgebundenen LAN ohne WLAN-basierten Standort verbunden ist, wird der Standort anhand der IP-Adresse bestimmt, die erheblich ungenauer ist.

Alarm

Senden Sie eine Fernwarnung auf dem Gerät.

Die Funktion ist nur auf Mobilgeräten verfügbar.

Sperren

Sperren Sie Ihren Laptop und legen Sie eine 4-stellige PIN zum Entsperren fest. Beim Versenden der **Sperren** Befehl startet das System neu und eine erneute Anmeldung bei Windows ist nur nach Eingabe der von Ihnen festgelegten PIN möglich.

Wenn Sie möchten, dass Bitdefender Fotos von demjenigen macht, der versucht, sich Zugang zu Ihrem Laptop zu verschaffen, aktivieren Sie das entsprechende Kontrollkästchen. Die aufgenommenen Fotos werden mit der Frontkamera aufgenommen und zusammen mit dem Zeitstempel im Anti-Theft-Dashboard angezeigt. Nur die beiden neuesten Fotos werden gespeichert.

Diese Aktion ist nur für Laptops mit Frontkamera verfügbar.

Wischen

Entfernen Sie alle Daten von Ihrem System. Beim Versenden der **Wischen** Befehl startet der Laptop neu und die Daten auf allen Festplattenpartitionen werden gelöscht.

IP anzeigen

Zeigt die letzte IP-Adresse für das ausgewählte Gerät an. Klicken **IP ZEIGEN** sichtbar zu machen.

Anti-Theft wird nach der Installation aktiviert und kann ausschließlich über Ihr Bitdefender-Konto von jedem mit dem Internet verbundenen Gerät und überall aufgerufen werden.

Verwenden von Anti-Theft-Funktionen

Um auf die Anti-Theft-Funktionen zuzugreifen, verwenden Sie eine der folgenden Möglichkeiten:

- Über die Hauptoberfläche von Bitdefender:
  1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
  2. Klicken **ZUR ZENTRALE GEHEN**.
     Sie werden zur Bitdefender Central-Seite weitergeleitet. Stellen Sie sicher, dass Sie mit Ihren Anmeldeinformationen angemeldet sind.
  3. Klicken Sie im sich öffnenden Bitdefender Central-Fenster auf die gewünschte Gerätekarte und wählen Sie sie aus **Diebstahlschutz**.

- Auf jedem Gerät mit Internetzugang:
  1. Öffnen Sie einen Webbrowser und gehen Sie zu: https://central.bitdefender.com.
  2. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
  3. Wähle aus **Meine Geräte** Tafel.
  4. Klicken Sie auf die gewünschte Gerätekarte und wählen Sie sie aus **Diebstahlschutz**.
  5. Wählen Sie die Funktion aus, die Sie verwenden möchten:
     Lokalisieren - Zeigen Sie den Standort Ihres Geräts auf Google Maps an.
     IP anzeigen - Anzeige der letzten IP-Adresse Ihres Geräts.
     Alarm - Senden Sie eine Benachrichtigung auf dem Gerät.
     Sperren - Sperren Sie Ihren Laptop und legen Sie einen PIN-Code zum Entsperren fest.
     Wischen - Löschen Sie alle Daten von Ihrem Laptop.

> **Wichtig**
> Nachdem Sie ein Gerät gelöscht haben, funktionieren alle Anti-Theft-Funktionen nicht mehr.

3.3. Dienstprogramme

3.3.1. Profile

Das Arbeiten, Filme schauen oder Spielen am Computer kann das System verlangsamen, ganz besonders dann, wenn diese Aktivitäten mit Windows-Update-Vorgängen oder Wartungsaufgaben einhergehen. Mit Bitdefender können Sie jetzt ein bevorzugtes Profil auswählen und anwenden und damit Ihr System so anpassen, dass die jeweils benötigten Anwendungen optimal laufen.

Bitdefender bietet die folgenden Profile:

- Arbeitsprofil
- Filmprofil
- Spielprofil
- **Öffentliches WLAN-Profil**
- Batteriemodusprofil

Wenn Sie sich entscheiden, die **Profile** nicht zu nutzen, wird ein voreingestelltes Profil mit dem Namen **Standard** aktiviert, das Ihr System nicht optimiert.

In Übereinstimmung mit Ihrer Aktivität werden die folgenden Produkteinstellungen vorgenommen, wenn ein Arbeits-, Film- oder Spielprofil aktiviert wird:

- Alle BitDefender Alarme und Pop-ups werden deaktiviert.
- Automatische Updates werden verschoben.
- Geplante Scans werden verschoben.
- Das Spam-Schutz-Funktion ist aktiviert.
- **Suchberater** ist deaktiviert.
- Benachrichtigungen zu Sonderangeboten sind deaktiviert.

In Übereinstimmung mit Ihrer Aktivität werden die folgenden Systemeinstellungen vorgenommen, wenn ein Arbeits-, Film- oder Spielprofil aktiviert wird:

- Automatische Windows-Updates werden verschoben.

- Windows-Benachrichtigungen und Pop-ups sind deaktiviert.
- Nicht benötigte Hintergrundprogramme werden angehalten.
- Die visuellen Effekte werden für maximale Leistung optimiert.
- Wartungsaufgaben werden verschoben.
- Die Energiespareinstellungen werden angepasst.

Bei Aktivierung das Öffentlichen-WLAN-Profils werden von Bitdefender Ultimate Small Business Security automatisch die folgenden Programmeinstellungen vorgenommen:

- Advanced Threat Defense ist aktiviert
- Die Bitdefender-Firewall ist aktiviert und die folgenden Einstellungen werden auf Ihren WLAN-Adapter angewendet:
  - Stealth-Modus - EIN
  - Netzwerktyp - Öffentlich
- Die folgenden Einstellungen des Online-Bedrohungsschutzes sind aktiviert:
  - Verschlüsselter Web-Scan
  - Schutz vor Betrug
  - Schutz vor Phishing

Arbeitsprofil

Das gleichzeitige Ausführen von verschiedenen Aufgaben bei der Arbeit am PC, so zum Beispiel das Versenden von E-Mails, das Abhalten von Videokonferenzen mit Kollegen oder das Arbeiten mit Grafikprogrammen, können die Leistung Ihres Systems beeinträchtigen. Das Arbeitsprofil wurde entwickelt, um Sie effizienter arbeiten zu lassen. Dafür werden einige Hintergrunddienste und Wartungsaufgaben deaktiviert.

Konfigurieren des Arbeitsprofils

So konfigurieren Sie die durchzuführenden Aktionen für das Arbeitsprofil:

1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Profile** Registerkarte, klicken Sie auf **Einstellungen**.

3. Klicken Sie im Bereich Arbeitsprofil auf **KONFIGURIEREN**.
4. Wählen Sie die Systemanpassungen aus, die Sie durchführen möchten, indem Sie die folgenden Optionen auswählen:
   - Die Systemleistung für Arbeitsanwendungen steigern
   - Produkteinstellungen für das Arbeitsprofil optimieren
   - Hintergrundprogramme und Wartungsaufgaben verschieben
   - Automatische Windows-Updates später durchführen
5. Klicken Sie auf **SPEICHERN**, um die Änderungen zu speichern und das Fenster zu schließen.

Manuelles Hinzufügen von Anwendungen zur Arbeitsprofilliste

Wenn Bitdefender das Arbeitsprofil beim Aufrufen einer Arbeitsanwendung nicht automatisch aktiviert, können Sie die Anwendung manuell zu der **Liste der Arbeitsanwendungen** hinzufügen.

So fügen Sie Anwendungen manuell zur Liste der Arbeitsanwendungen im Arbeitsprofil hinzu:

1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Profile** Registerkarte, klicken Sie auf **Einstellungen**.
3. Drücke den **KONFIGURIEREN** Schaltfläche aus dem Bereich Arbeitsprofil.
4. Klicken Sie im Fenster **Einstellungen Arbeitsprofil** auf **Anwendungsliste**.
5. Klicken Sie auf **HINZUFÜGEN**.
   Ein neues Fenster wird angezeigt. Scrollen Sie bitte bis zu der ausführbaren Datei der Anwendung, wählen Sie diese aus und klicken Sie auf **OK**, um diese zu der Liste hinzuzufügen.

Filmprofil

Das Abspielen von Videos mit hoher Qualität, so zum Beispiel HD-Filme, nimmt viele Systemressourcen in Anspruch. Mit dem Filmprofil werden die System- und Produkteinstellungen so angepasst, dass Sie Ihre Filme ungestört genießen können.

Konfigurieren des Filmprofils

So konfigurieren Sie die durchzuführenden Aktionen für das Filmprofil:

1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Profile** Registerkarte, klicken Sie auf **Einstellungen**.
3. Klicken Sie im Bereich Filmprofil auf **KONFIGURIEREN**.
4. Wählen Sie die Systemanpassungen aus, die angewendet werden sollen, indem Sie die folgenden Optionen aktivieren:
   - Die Systemleistung für das Abspielen von Videos steigern
   - Produkteinstellungen für das Filmprofil optimieren
   - Verschieben Sie Hintergrundprogramme und Wartungsaufgaben
   - Verschieben Sie automatische Windows-Updates
   - Energiesparplaneinstellungen für den Filmbetrieb anpassen
5. Klicken **SPEICHERN** um die Änderungen zu speichern und das Fenster zu schließen.

Manuelles Hinzufügen von Video-Playern zur Filmprofilliste

Wenn Bitdefender das Filmprofil beim Aufrufen einer Video-Anwendung nicht automatisch aktiviert, können Sie die Anwendung manuell zu der **Liste der Filmanwendungen** hinzufügen.

So fügen Sie Video-Anwendungen manuell zur Liste der Filmanwendungen im Filmprofil hinzu:

1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Profile** Registerkarte, klicken Sie auf **Einstellungen**.
3. Drücke den **KONFIGURIEREN** Schaltfläche aus dem Bereich Filmprofil.
4. Klicken Sie im Fenster **Einstellungen Filmprofil** auf **Player-Liste**.
5. Klicken **HINZUFÜGEN**.

Ein neues Fenster erscheint. Navigieren Sie zur ausführbaren Datei der App, wählen Sie sie aus und klicken Sie darauf **OK** um es der Liste hinzuzufügen.

Spielprofil

Um Ihre Spiele ohne Unterbrechungen genießen zu können, müssen die Systemlast und Leistungseinbußen unbedingt minimiert werden. Durch die Kombination von verhaltensbasierten Heuristiken und einer Liste bekannter Spiele kann Bitdefender automatisch erkennen, ob ein Spiel ausgeführt wird, und Ihre Systemressourcen so optimieren, dass Sie in Ruhe spielen können.

Konfigurieren des Spielprofils

So können Sie die durchzuführenden Aktionen für das Spielprofil konfigurieren:

1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Profile** Registerkarte, klicken Sie auf **Einstellungen**.
3. Klicken Sie im Bereich Spielprofil auf **Konfigurieren**.
4. Wählen Sie die Systemanpassungen aus, die angewendet werden sollen, indem Sie die folgenden Optionen aktivieren:
   - Die Systemleistung für Spiele steigern
   - Produkteinstellungen für das Spielprofil optimieren
   - Verschieben Sie Hintergrundprogramme und Wartungsaufgaben
   - Verschieben Sie automatische Windows-Updates
   - Energiesparplaneinstellungen für den Spielbetrieb anpassen
5. Klicken **SPEICHERN** um die Änderungen zu speichern und das Fenster zu schließen.

Spiele manuell zu der Spielliste hinzufügen

Wenn Bitdefender das Spielprofil beim Aufrufen einer eines Spiels oder einer Anwendung nicht automatisch aktiviert, können Sie die Anwendung manuell zu der **Liste der Spieleanwendungen** hinzufügen.

So fügen Sie Spiele manuell zur Liste der Spieleanwendungen im Spielprofil hinzu:

1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Profile** Registerkarte, klicken Sie auf **Einstellungen**.
3. Drücke den **Konfigurieren** Schaltfläche aus dem Spielprofilbereich.
4. Klicken Sie im Fenster **Einstellungen Spielprofil** auf **Spieleliste**.
5. Klicken **HINZUFÜGEN**.
   Ein neues Fenster wird angezeigt. Öffnen Sie den Ordner, in dem sich die ausführbare Datei des Spiels befindet, markieren Sie sie und klicken Sie auf **OK**, um das Spiel zur Liste hinzuzufügen.

Öffentliches WLAN-Profil

Bei Verbindungen mit unsicheren WLAN-Netzwerken kann der Versand von E-Mails, die Eingabe von sensiblen Anmeldedaten oder das Einkaufen im Internet die Vertraulichkeit Ihrer Daten gefährden. Das Öffentliche-WLAN-Profil passt die Produkteinstellungen entsprechend an, um Ihnen eine geschützte Umgebung für Online-Zahlungen und die Eingabe von sensiblen Daten zu ermöglichen.

Konfiguration des Öffentlichen-WLAN-Profils

Konfigurieren Sie Bitdefender wie folgt, um die entsprechenden Produkteinstellungen bei Verbindungen mit unsicheren Drahtlosnetzwerken anzuwenden:

1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Profile** Registerkarte, klicken Sie auf **Einstellungen**.
3. Klicken Sie im Bereich Öffentliches-WLAN-Profil auf **KONFIGURIEREN**.
4. Lassen Sie das Kästchen **Passt Produkteinstellungen so an, dass bei Einwahl in ein ungeschütztes WLAN-Netzwerk der Schutz erhöht wird** aktiviert.
5. Klicken **Speichern**.

Akkubetriebsprofil

Das Profil für den Akkubetrieb wurde speziell für Laptop- und Tablet-Nutzer entwickelt. Er minimiert die Auswirkungen des System- und Bitdefender-Betriebs auf die Akkulaufzeit, sobald der von Ihnen oder standardmäßig festgelegte Akkuladestand unterschritten wird.

Konfiguration des Profils für den Akkubetrieb

So konfigurieren Sie das Profil für den Akkubetrieb:

1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Profile** Registerkarte, klicken Sie auf **Einstellungen**.
3. Klicken Sie im Bereich Akkubetriebsprofil auf **Konfigurieren**.
4. Wählen Sie die durchzuführenden Systemanpassungen aus, indem Sie die folgenden Optionen auswählen:
   - Produkteinstellungen für den Akkubetrieb optimieren.
   - Hintergrundprogramme und Wartungsaufgaben verschieben.
   - Automatische Windows-Updates später durchführen.
   - Energiesparplaneinstellungen für den Akkubetrieb anpassen.
   - Externe Geräte und Netzwerk-Ports deaktivieren.
5. Klicken **SPEICHERN** um die Änderungen zu speichern und das Fenster zu schließen.

Geben Sie einen gültigen Wert in das Drehfeld ein oder wählen Sie ihn über die Pfeiltasten aus, um festzulegen, wann das System in den Akkubetrieb wechseln soll. Standardmäßig wird der Akkubetrieb aktiviert, sobald der Akkuladestand unter 30 % sinkt.

Die folgenden Produkteinstellungen werden angewendet, wenn Bitdefender in das Akkubetriebsprofil versetzt wird:

- Automatische Bitdefender-Updates werden verschoben
- Geplante Scans werden verschoben.

Bitdefender erkennt, wenn Ihr Laptop vom Stromnetz getrennt wird und startet den Akkubetrieb automatisch je nach festgelegten Akkuladestand. Ebenso beendet Bitdefender automatisch den Akkubetrieb, wenn der Laptop nicht mehr über den Akku betrieben wird.

Echtzeitoptimierung

Die Echtzeitoptimierung von Bitdefender ist ein Plug-in, das Ihre Systemleistung im Hintergrund verbessert und dafür sorgt, dass Sie nicht unterbrochen werden, während Sie sich in einem Profilmodus befinden. Je nach CPU-Last überwacht das Plug-in alle Prozesse und konzentriert sich dabei auf besonders CPU-intensive Prozesse, um sie an Ihre Bedürfnisse anzupassen.

So können Sie die Echtzeitoptimierung aktivieren oder deaktivieren:

1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Profile** Registerkarte, klicken Sie auf **Einstellungen**.
3. Scrollen Sie nach unten bis zur Option Echtzeitoptimierung und klicken Sie zur Aktivierung oder Deaktivierung auf den entsprechenden Schalter.

3.3.2. OneClick-Optimierer

Probleme wie Festplattenausfälle, übrig gebliebene Registrierungsdateien und der Browserverlauf können Ihre Arbeit verlangsamen, was für Sie lästig werden kann. All dies kann jetzt mit einem einzigen Klick auf eine Schaltfläche behoben werden.

Mit OneClick Optimizer können Sie nutzlose Dateien identifizieren und entfernen, indem Sie mehrere Reinigungsaufgaben gleichzeitig ausführen.

So starten Sie den OneClick Optimizer-Prozess:

1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Drücke den **Optimieren** Taste.
   a. **Analysieren**
   Warten Sie, bis Bitdefender die Suche nach Systemproblemen abgeschlossen hat.
      - Datenträgerbereinigung - identifiziert unnötige Dateien und Ordner.
      - Registry Cleanup – identifiziert ungültige oder veraltete Verweise in der Windows-Registrierung.

- Datenschutzbereinigung - identifiziert temporäre Internetdateien und Cookies, Browser-Cache und Verlauf.

Die Anzahl der gefundenen Probleme wird angezeigt. Klicken Sie auf den Link Details anzeigen, um sie zu überprüfen, bevor Sie mit dem Reinigungsprozess fortfahren. Klicken Sie auf Optimieren, um fortzufahren.

b. **Optimierung**
Warten Sie, bis Bitdefender die Optimierung Ihres Systems abgeschlossen hat.

c. **Themen**
Hier können Sie das Operationsergebnis einsehen.
Wenn Sie umfassende Informationen zum Optimierungsprozess wünschen, klicken Sie auf die **Detaillierten Bericht anzeigen** Taste.

3.3.3. Datenschutz

Endgültiges Löschen von Dateien

Wenn Sie eine Datei löschen, kann auf diese nicht mehr auf normalem Wege zugegriffen werden. Die Datei bleibt aber weiterhin auf der Festplatte gespeichert, bis Sie durch eine neue Datei überschrieben wird.

Der Bitdefender File Shredder hilft Ihnen dabei, Daten dauerhaft zu löschen, indem er sie physisch von Ihrer Festplatte entfernt.

Gehen Sie wie folgt vor, um Dateien oder Ordner auf Ihrem Gerät schnell und einfach über das Windows-Kontextmenü zu schreddern:

1. Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, den Sie unwiderruflich löschen möchten.
2. Wählen Sie im angezeigten Kontextmenü **Bitdefender > Dateischredder**.
3. Klicken Sie auf **Dauerhaft löschen** und bestätigen Sie, dass Sie mit dem Vorgang fortfahren möchten.
Bitte warten Sie, bis Bitdefender die Dateien dauerhaft gelöscht hat
4. Die Ergebnisse werden angezeigt. Klicken Sie auf **Beenden**, um den Assistenten zu schließen.

Alternativ können Sie Dateien auch von innerhalb der Bitdefender-Oberfläche schreddern. Das geht so:

1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Klicken Sie im Bereich **Datenschutz** auf **Dateischredder**.
3. Befolgen Sie die Anweisungen des Dateischredderassistenten:
   a. Klicken Sie auf die Schaltfläche **Ordner hinzufügen**, um die Dateien oder Ordner hinzuzufügen, die Sie dauerhaft löschen möchten.
   Alternativ können Sie diese Dateien oder Ordner mit der Maus auf dieses Fenster ziehen.
   b. Klicken Sie auf **Dauerhaft löschen** und bestätigen Sie, dass Sie mit dem Vorgang fortfahren möchten.
   Warten Sie, bis Bitdefender das Schreddern der Dateien abgeschlossen hat.
   c. **Ergebnisübersicht**
   Die Ergebnisse werden angezeigt. Klicken **Beenden** um den Assistenten zu beenden.

3.4. Gewusst wie

3.4.1. Installation

Wie kann ich Bitdefender auf einem zweiten Gerät installieren?

Falls Ihr erworbenes Abonnement für mehrere Geräte gültig ist, können Sie über Ihr Bitdefender-Konto einen zweiten PC aktivieren.

So können Sie Bitdefender auf einem zweiten Gerät installieren:

1. Klinken Sie unten rechts in der **Bitdefender-Benutzeroberfläche** auf **Auf weiterem Gerät installieren**.
   Ein neues Fenster erscheint auf Ihrem Bildschirm.
2. Klicken **DOWNLOAD-LINK TEILEN**.
3. Folgen Sie den angezeigten Anleitung, um Bitdefender zu installieren.

Das neue Gerät, auf dem Sie das Bitdefender-Produkt installiert haben, wird ab sofort im Bitdefender Central-Dashboard angezeigt.

Wie kann ich Bitdefender erneut installieren?

Die Folgenden sind typische Situationen, in denen Sie Bitdefender erneut installieren müssen:

- Sie haben das Betriebssystem neu installiert..
- Sie möchten Probleme beheben, die das System verlangsamt oder zum Absturz gebracht haben könnten.
- Ihr Bitdefender-Produkt startet nicht oder funktioniert nicht ordnungsgemäß.

Falls eine der genannten Situationen auf Sie zutrifft, gehen Sie bitte wie folgt vor:

- In **Windows 7**:
  1. Klicken **Start** und gehe zu **Alle Programme**.
  2. Suchen Sie nach *Bitdefender Ultimate Small Business Security* und wählen Sie **Deinstallieren**.
  3. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**.
  4. Sie müssen das Gerät neu starten, um den Vorgang abzuschließen.

- In **Windows 8** Und **Windows 8.1**:
  1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
  3. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
  4. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.
  5. Sie müssen das Gerät neu starten, um den Vorgang abzuschließen.

- In **Windows 10** Und **Windows11**:
  1. Klicken Sie auf **Start** und danach auf **Einstellungen**.
  2. Klicken Sie in den Einstellungen auf das **System**-Symbol und wählen Sie dann **Apps & Funktionen**.

3. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
5. Klicken Sie auf **ERNEUT INSTALLIEREN**.
6. Sie müssen das Gerät neu starten, um den Vorgang abzuschließen.

> **Notiz**
> Wenn Sie bei der Neuinstallation wie hier beschrieben vorgehen, werden Ihre benutzerdefinierte Einstellungen gespeichert und sind im neu installierten Produkt wieder verfügbar. Weitere Einstellungen werden unter Umständen wieder auf die Standardkonfiguration zurückgesetzt.

Woher kann ich mein Bitdefender-Produkt herunterladen?

Sie können Bitdefender vom Installationsdatenträger installieren oder den Web-Installer verwenden, der über die Bitdefender Central-Plattform auf Ihr Gerät heruntergeladen werden kann.

> **Notiz**
> Bevor Sie das Installationspaket ausführen, sollten Sie jede andere auf Ihrem System installierte Sicherheitslösung entfernen. Wenn Sie mehr als eine Sicherheitslösung auf Ihrem Gerät verwenden, wird dadurch das System instabil.

So können Sie Bitdefender über Bitdefender Central installieren:

1. Zugang Bitdefender-Zentrale.
2. Wähle aus **Meine Geräte** Panel, und klicken Sie dann auf **SCHUTZ INSTALLIEREN**.
3. Wählen Sie eine der beiden verfügbaren Optionen:
   - **Schützen Sie dieses Gerät**
     Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
   - **Schützen Sie andere Geräte**
     Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.

Klicken **DOWNLOADLINK SENDEN**. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **E-MAIL SENDEN**. Beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Wenn der Link abläuft, müssen Sie einen neuen generieren, indem Sie die gleichen Schritte ausführen.
Überprüfen Sie auf dem Gerät, auf dem Sie Ihr Bitdefender-Produkt installieren möchten, das E-Mail-Konto, das Sie eingegeben haben, und klicken Sie dann auf die entsprechende Download-Schaltfläche.

4. Führen Sie das von Ihnen heruntergeladene Bitdefender aus.

Wie verfahre ich mit meinem Bitdefender-Abonnement nach einem Windows-Upgrade?

Diese Situation tritt ein, wenn Sie Ihr Betriebssystem aktualisieren und Sie Ihren Bitdefender-Abonnement weiterhin nutzen möchten.

Wenn Sie eine frühere Bitdefender-Version verwenden, können Sie kostenlos auf die neueste Bitdefender-Version upgraden. Gehen Sie dazu wie folgt vor:

- Von einer Vorgängerversion von Bitdefender Antivirus auf die neueste verfügbare Version von Bitdefender Antivirus.
- Von einer Vorgängerversion von Bitdefender Internet Security auf die neueste verfügbare Version von Bitdefender Internet Security.
- Von einer Vorgängerversion von Bitdefender Total Security auf die neueste verfügbare Version von Bitdefender Total Security.

Es gibt zwei Fälle, die auftreten können:

- Sie haben Ihr Betriebssystem über Windows Update aktualisiert und bemerken, dass Bitdefender nicht mehr funktioniert.
  In diesem Fall müssen Sie das Produkt wie folgt neu installieren:
  - In **Windows 7**:
    1. Klicken Sie auf **Start**, rufen Sie die **Systemsteuerung** auf und doppelklicken Sie auf **Programme und Funktionen**.
    2. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.

3. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.
4. Warten Sie, bis die Deinstallation abgeschlossen ist und starten Sie Ihr System neu.
   Öffnen Sie die Benutzeroberfläche Ihres neu installierten Bitdefender-Produkts, um auf die Funktionen zugreifen zu können.

- In **Windows 8** Und **Windows 8.1**:

1. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
3. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
4. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.
5. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.
   Öffnen Sie die Benutzeroberfläche Ihres neu installierten Bitdefender-Produkts, um auf seine Funktionen zuzugreifen.

- In **Windows 10** Und **Windows11**:

1. Klicken **Start**, dann klick **Einstellungen**.
2. Klicken Sie in den Einstellungen auf das **System**-Symbol und danach auf **Apps**.
3. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
4. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.
5. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.
6. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.
   Öffnen Sie die Benutzeroberfläche Ihres neu installierten Bitdefender-Produkts, um auf seine Funktionen zuzugreifen.

> **Notiz**
> Durch Befolgen dieses Neuinstallationsverfahrens werden benutzerdefinierte Einstellungen gespeichert und stehen im neu installierten Produkt zur Verfügung. Andere Einstellungen können auf ihre Standardkonfiguration zurückgesetzt werden.

- Sie haben Ihr System gewechselt und möchten nicht auf den Bitdefender-Schutz verzichten. Deshalb müssen Sie das Produkt in der aktuellsten Version erneut installieren.
  Verfahren Sie in einer solchen Situation wie folgt:

  1. Laden Sie die Installationsdatei herunter:
     a. Zugang Bitdefender-Zentrale.
     b. Wähle aus **Meine Geräte** Panel, und klicken Sie dann auf **SCHUTZ INSTALLIEREN**.
     c. Wählen Sie eine der beiden verfügbaren Optionen:
        - **Schützen Sie dieses Gerät**
          Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
        - **Ein weiteres Gerät schützen**
          Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
          Klicken **DOWNLOADLINK SENDEN**. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **E-MAIL SENDEN**. Beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Wenn der Link abläuft, müssen Sie einen neuen generieren, indem Sie die gleichen Schritte ausführen.
          Überprüfen Sie auf dem Gerät, auf dem Sie Ihr Bitdefender-Produkt installieren möchten, das E-Mail-Konto, das Sie eingegeben haben, und klicken Sie dann auf die entsprechende Download-Schaltfläche.

  2. Führen Sie das heruntergeladene Bitdefender-Produkt aus.

Weitere Information zum Bitdefender-Installationsprozess finden Sie im Kapitel Installieren Ihres Bitdefender-Produkts (Seite 11).

Wie kann ich ein Upgrade auf die neueste Bitdefender-Version durchführen?

Ab sofort ist ein Upgrade auf die neueste Version ohne den manuellen Deinstallations- und Neuinstallationsvorgang möglich. Genauer gesagt wird das neue Produkt mit allen neuen Funktionen und wesentlichen Verbesserungen als Produktupdate ausgeliefert. Wenn Sie bereits über ein aktives Bitdefender-Abonnement verfügen, wird das Produkt automatisch aktiviert.

Als Benutzer der 2020er-Version können Sie folgendermaßen vorgehen, um ein Upgrade auf die neueste Version durchzuführen:

1. Klicken Sie in der Benachrichtigung, die mit der Upgradeinfomration einhergeht, auf **JETZT NEU STARTEN**. Sollten Sie sie verpasst haben, rufen Sie das Fenster **Benachrichtigungen** auf, bewegen Sie den Mauszeiger auf das neueste Update und klicken Sie danach auf **JETZT NEU STARTEN**. Warten Sie den Neustart des Geräts ab.

   Das Fenster **Was gibt es Neues** mit Informationen über die verbesserten und neuen Funktionen wird angezeigt.
2. Klicken Sie auf die **Lesen Sie mehr**-Links für weitere Informationen und hilfreiche Artikel.
3. Schließen Sie das Fenster **Was gibt es Neues**, um auf die Benutzeroberfläche der neu installierten Version zuzugreifen.

Benutzer, die ein kostenloses Upgrade von Bitdefender 2016 oder einer Vorgängerversion auf die neueste Bitdefender-Version durchführen möchten, müssen zunächst die aktuelle Version über die Systemsteuerung entfernen und danach die aktuellste Installationsdatei über die Bitdefener-Website herunterladen: https://www.bitdefender.com/Downloads/. Die Aktivierung ist nur mit einem gültigen Abonnement möglich.

3.4.2. Bitdefender-Zentrale

Wie kann ich mein Bitdefender-Benutzerkonto wechseln?

Sie haben ein neues Bitdefender-Konto angelegt und möchten es von nun an nutzen.

So melden Sie sich mit einem anderen Bitdefender-Konto an:

1. Klicken Sie oben im **Bitdefender-Fenster** auf Ihren Kontonamen.
2. Klicken Sie oben rechts im Bildschirm auf **Konto wechseln**, um das Gerät mit einem anderen Benutzerkonto zu verknüpfen.
3. Geben Sie die E-Mail-Adresse in das entsprechende Feld ein und klicken Sie dann auf **NÄCHSTE**.
4. Geben Sie Ihr Kennwort ein und klicken Sie dann auf **ANMELDEN**.

> **Notiz**
> Das Bitdefender-Produkt auf Ihrem Gerät wird entsprechend dem mit Ihrem Bitdefender-Konto verknüpften Abonnement automatisch umgestellt. Falls mit dem neuen Bitdefender-Konto kein verfügbares Abonnement verknüpft ist oder Sie es von einem früheren Benutzerkonto übernehmen möchten, können Sie sich wie in Abschnitt Hier wird Ihnen geholfen (Seite 305) beschrieben mit dem Bitdefender-Support in Verbindung setzen.

Wie kann ich die Bitdefender Central-Hilfemeldungen deaktivieren?

Die Hilfemeldungen werden im Dashboard angezeigt, um Ihnen zu zeigen, wie Sie die verschiedenen Optionen in Bitdefender Central nutzen können.

So können Sie diese Meldungen deaktivieren:

1. Zugang Bitdefender-Zentrale.
2. Drücke den Symbol oben rechts auf dem Bildschirm.
3. Klicken Sie im Menü auf **Mein Konto**.
4. Klicken Sie im Slide-Menü auf **Einstellungen**.
5. Deaktivieren Sie die Option **Hilfemeldungen aktivieren/deaktivieren**.

Ich habe das Passwort vergessen, das ich für mein Bitdefender-Konto festgelegt habe. Wie kann ich es zurücksetzen?

Das Passwort für Ihr Bitdefender-Konto können Sie auf eine von zwei Arten ändern:

- Von dem Bitdefender-Oberfläche:
  1. Klicken **Mein Konto** im Navigationsmenü auf der Bitdefender-Oberfläche.

2. Klicken Sie oben rechts im Bildschirm auf **Konto wechseln**.
   Ein neues Fenster wird angezeigt.
3. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **WEITER**.
   Ein neues Fenster erscheint.
4. Klicken **Passwort vergessen?**.
5. Klicken Sie auf **WEITER**.
6. Überprüfen Sie Ihr E-Mail-Konto, geben Sie den Sicherheitscode ein, den Sie erhalten haben, und klicken Sie dann auf **NÄCHSTE**.
   Alternativ können Sie auch klicken **Kennwort ändern** in der E-Mail, die wir Ihnen gesendet haben.
7. Geben Sie das neue Kennwort ein, das Sie festlegen möchten, und geben Sie es dann erneut ein. Klicken **SPEICHERN**.

❍ Von Ihrem Webbrowser:

1. Gehe zu: https://central.bitdefender.com.
2. Klicken Sie auf **ANMELDEN**.
3. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie dann auf **NÄCHSTE**.
4. Klicken **Passwort vergessen?**.
5. Klicken **NÄCHSTE**.
6. Rufen Sie Ihre E-Mails ab und folgen Sie der Anleitung, um ein neues Passwort für Ihr Bitdefender-Konto festzulegen.

Geben Sie von jetzt an Ihre E-Mail-Adresse und das neue Passwort ein, um auf Ihr Bitdefender-Konto zuzugreifen.

Wie kann ich die Benutzersitzungen in meinem Bitdefender-Konto verwalten?

In Ihrem Bitdefender-Konto können Sie die jüngsten inaktiven und aktiven Benutzersitzungen auf mit Ihrem Konto verbundenen Geräten verwalten. Außerdem können Sie sich aus der Ferne folgendermaßen abmelden:

1. Zugang Bitdefender-Zentrale.
2. Drücke den Symbol oben rechts auf dem Bildschirm.

3. Klicken Sie im Slide-Menü auf **Sitzungen**.
4. Wählen Sie im Bereich **Aktive Sitzungen** die Option **ABMELDEN** neben dem Gerät, für das Sie die Benutzersitzung beenden möchten.

3.4.3. Prüfen mit BitDefender

Wie kann ich eine Datei oder einen Ordner scannen?

Um eine Datei oder einen Ordner einfach und schnell zu scannen, klicken Sie mit der rechten Maustaste auf das Objekt, das Sie scannen möchten, bewegen Sie den Mauszeiger auf Bitdefender und klicken Sie im Menü auf **Mit Bitdefender scannen**.

Um den Scan abzuschließen, folgen Sie den Anweisungen des Scan-Assistenten. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.

Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Typische Situationen, für die diese Scan-Methode geeignet ist:

- Sie vermuten, dass eine bestimmte Datei oder ein Ordner infiziert ist.
- Immer dann, wenn Sie aus dem Internet Dateien herunterladen, von deren Ungefährlichkeit Sie nicht überzeugt sind.
- Scannen Sie einen freigegebenen Ordner, bevor Sie die enthaltenen Dateien auf Ihr Gerät kopieren.

Wie scanne ich mein System

So können Sie einen vollständigen System-Scan durchführen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie neben **System-Scan** auf die Schaltfläche **Scan starten**.
4. Folgen Sie den Anweisungen des Scan-Assistenten, um den Scan abzuschließen. Bitdefender wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.
   Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen. Weitere Informationen finden Sie im Kapitel .

Wie plane ich einen Scan?

Sie können Ihr Bitdefender-Produkt so konfigurieren, dass es wichtige Systembereiche nur dann scannt, wenn Sie Ihr Gerät nicht benötigen.

So können Sie einen Scan planen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie unten in der Benutzeroberfläche auf ··· neben dem Scan-Typ, den Sie planen möchten, System-Scan oder Quick Scan, und wählen Sie dann **Bearbeiten**.
   Alternativ können Sie auch einen individuellen Scan-Typ erstellen, indem Sie neben **Scans verwalten** auf **+Scan erstellen** klicken.
4. Richten Sie den Scan entsprechend Ihrer Anforderungen ein und klicken Sie auf **Weiter**.
5. Markieren Sie das Kästchen neben **Legen Sie fest, für wann Sie diese Aufgabe planen möchten**.
   Wählen Sie eine der entsprechenden Optionen, um einen Zeitplan festzulegen:
   - ❍ Beim Systemstart
   - ❍ Täglich
   - ❍ Wöchentlich
   - ❍ Monatlich

   Wenn Sie „Täglich“, „Monatlich“ oder „Wöchentlich“ auswählen, ziehen Sie den Schieberegler entlang der Skala, um den gewünschten Zeitraum festzulegen, in dem der geplante Scan beginnen soll.

Wenn Sie einen neuen benutzerdefinierten Scan erstellen möchten, erscheint das Fenster **Scan-Aufgabe**. Hier können Sie die Systembereiche auswählen, die gescannt werden sollen.

Wie kann ich eine benutzerdefinierte Scan-Aufgabe anlegen?

Wenn Sie bestimmte Bereiche Ihres Geräts scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierte Scan-Aufgabe konfigurieren und ausführen.

Um eine benutzerdefinierte Scan-Aufgabe anzulegen, gehen Sie folgendermaßen vor:

1. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
2. Klicken Sie neben **Scans verwalten** auf **+Scan erstellen**.
3. Geben Sie im Namensfeld einen Namen für den Scan ein, wählen Sie die Bereiche aus, die Sie scannen möchten, und klicken Sie auf **WEITER**.
4. Konfigurieren Sie diese allgemeinen Optionen:
   - **Nur Anwendungen scannen**. Sie können Bitdefender so einrichten, dass nur aufgerufene Anwendungen gescannt werden.
   - **Priorität der Scan-Aufgabe**. Sie können festlegen, wie sich ein Scan-Vorgang auf die Systemleistung auswirkt.
     - Auto - Die Priorität des Scanvorgangs hängt von der Systemaktivität ab. Um sicherzustellen, dass der Scanprozess die Systemaktivität nicht beeinträchtigt, entscheidet Bitdefender, ob der Scanprozess mit hoher oder niedriger Priorität ausgeführt werden soll.
     - Hoch – Die Priorität des Scanvorgangs ist hoch. Indem Sie diese Option wählen, erlauben Sie anderen Programmen, langsamer zu laufen, und verkürzen die Zeit, die für den Abschluss des Scanvorgangs benötigt wird.
     - Niedrig – Die Priorität des Scanvorgangs ist niedrig. Wenn Sie diese Option auswählen, können Sie andere Programme schneller ausführen und die Zeit verlängern, die für den Abschluss des Scanvorgangs benötigt wird.
   - **Aktionen nach dem Scan**. Wählen Sie die Aktion, die von Bitdefender durchgeführt werden soll, wenn keine Bedrohungen gefunden wurden:
     - Übersichtsfenster anzeigen
     - Gerät herunterfahren
     - Schließen Sie das Scan-Fenster
5. Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Erweiterte Optionen anzeigen**.
   Klicken **Nächste**.

6. Sie können bei Bedarf die Option **Scan-Aufgabe planen** aktivieren und dann festlegen, wann der von Ihnen erstellte benutzerdefinierte Scan gestartet werden soll.
   - ❍ Beim Systemstart
   - ❍ Täglich
   - ❍ Monatlich
   - ❍ Wöchentlich

   Wenn Sie „Täglich“, „Monatlich“ oder „Wöchentlich“ auswählen, ziehen Sie den Schieberegler entlang der Skala, um den gewünschten Zeitraum festzulegen, in dem der geplante Scan beginnen soll.
7. Klicken **Speichern** um die Einstellungen zu speichern und das Konfigurationsfenster zu schließen.
   Abhängig von den zu scannenden Orten kann der Scan eine Weile dauern. Wenn während des Scanvorgangs Bedrohungen gefunden werden, werden Sie aufgefordert, die Aktionen auszuwählen, die für die erkannten Dateien durchgeführt werden sollen.

Bei Bedarf können Sie einen bereits durchgeführten benutzerdefinierten Scan einfach erneut ausführen, indem Sie auf den entsprechenden Eintrag in der Liste klicken.

Wie kann ich einen Ordner vom Scan ausnehmen?

Mit Bitdefender können Sie bestimmte Dateien, Ordner oder Dateiendungen vom Scan ausnehmen.

Ausnahmen sollten nur von Benutzern genutzt werden, die erfahren im Umgang mit Computern sind und nur in den folgenden Situationen:

- ❍ Sie haben einen großen Ordner mit Filmen und Musik auf Ihrem System gespeichert.
- ❍ Sie haben ein großes Archiv mit verschiedenen Daten auf Ihrem System gespeichert.
- ❍ Sie haben einen Ordner, in dem Sie verschiedene Software-Typen und Anwendungen zu Testzwecken installieren. Ein Scan des Ordners könnte zum Verlust einiger der Daten führen.

So können Sie einen Ordner Ausschlussliste hinzufügen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.

2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie auf den Reiter **Einstellungen**.
4. Klicken Sie auf **Ausnahmen verwalten**.
5. Klicken **+Fügen Sie eine Ausnahme hinzu**.
6. Geben Sie den Pfad des Ordners, den Sie vom Scannen ausnehmen möchten, in das entsprechende Feld ein.
   Alternativ können Sie zu dem Ordner navigieren, indem Sie auf die Schaltfläche „Durchsuchen“ auf der rechten Seite der Benutzeroberfläche klicken, ihn auswählen und auf klicken **OK**.
7. Aktivieren Sie den Schalter neben der Schutzfunktion, die den Ordner nicht scannen soll. Es gibt drei Optionen:
   - Virenschutz
   - Abwehr von Online-Bedrohungen
   - Erweiterte Bedrohungsabwehr
8. Klicken **Speichern** um die Änderungen zu speichern und das Fenster zu schließen.

Wie gehe ich vor, wenn Bitdefender eine saubere Datei als infiziert eingestuft hat?

Es können Situationen auftreten, in denen Bitdefender harmlose Dateien irrtümlicherweise als Bedrohung einstuft (Fehlalarm). Um diesen Fehler zu korrigieren, können Sie die Datei der Bitdefender-Ausnahmeliste hinzufügen:

1. Deaktivieren Sie den Bitdefender-Echtzeit-Virenschutz:
   a. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
   b. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
   c. Deaktivieren Sie im Fenster **Erweitert** die Option **Bitdefender-Schild**.
      Ein Warnung wird angezeigt. Sie müssen Ihre Auswahl bestätigen, indem Sie im Menü wählen, wie lange der Echtzeitschutz deaktiviert bleiben soll. Sie können den Echtzeitschutz für 5, 15

oder 30 Minuten, 1 Stunde, dauerhaft oder bis zum Neustart des Systems deaktivieren.

2. Verborgene Objekte in Windows anzeigen. Eine Anleitung hierzu finden Sie unter Wie kann ich in Windows versteckte Objekte anzeigen? (Seite 126).
3. Stellen Sie die Datei aus der Quarantäne wieder her:
   a. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
   b. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
   c. Klicken Sie im Fenster **Einstellungen** auf **Quarantäne verwalten**.
   d. Wählen Sie die Datei aus und klicken Sie auf **Wiederherstellen**.
4. Fügen Sie die Datei zur Ausnahmeliste hinzu. Eine Anleitung hierzu finden Sie unter Wie kann ich einen Ordner vom Scan ausnehmen? (Seite 112).
5. Aktivieren Sie den Bitdefender-Echtzeit-Virenschutz.
6. Setzten Sie sich mit unserem Support in Verbindung, damit wir die Erkennung beim Update der Bedrohungsinformationen entfernen können. Eine Anleitung hierzu finden Sie unter Hier wird Ihnen geholfen (Seite 305).

Wo sehe ich, welche Bedrohungen Bitdefender gefunden hat?

Nach jedem durchgeführten Scan wird ein Protokoll erstellt, in dem Bitdefender alle gefundenen Probleme aufzeichnet.

Der Bericht enthält detaillierte Informationen über den Scan-Vorgang, so wie Scan-Optionen, das Scan-Ziel, die gefundenen Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sie können das Scan-Protokoll direkt aus dem Scan-Assistenten öffnen, sobald der Scan abgeschlossen ist, indem Sie auf klicken **PROTOKOLL ANZEIGEN**.

So überprüfen Sie ein Scan-Protokoll oder eine erkannte Infektion zu einem späteren Zeitpunkt:

1. Klicken **Benachrichtigungen** im Navigationsmenü auf der Bitdefender-Oberfläche.

2. Im **Alle** Wählen Sie auf der Registerkarte die Benachrichtigung über den letzten Scan aus.
   Hier finden Sie alle Bedrohungsscan-Ereignisse, einschließlich Bedrohungen, die durch On-Access-Scans, benutzerinitiierte Scans und Statusänderungen für automatische Scans erkannt wurden.
3. In der Benachrichtigungsliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden. Klicken Sie auf eine Benachrichtigung, um Details dazu anzuzeigen.
4. Um ein Scan-Protokoll zu öffnen, klicken Sie auf **Protokoll anzeigen**.

3.4.4. Privatsphärenschutz

Wie sichere ich meine Online-Transaktionen ab?

Um Ihre Online-Transaktionen wie Online-Banking noch sicherer zu machen, können Sie den Browser von Bitdefender verwenden.

Bitdefender Safepay™ ist ein abgesicherter Browser, der Ihre Kreditkartennummern, Kontonummern und andere sensible Daten, die Sie im Internet eingeben, zuverlässig schützt.

So können Sie Ihre Online-Aktivitäten absichern und vor neugierigen Augen schützen:

1. Klicken **Privatsphäre** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **SICHERE BEZAHLUNG** Bereich, klicken Sie auf **Einstellungen**.
3. Im **SafePay** Fenster, klicken **Starten Sie Safepay**.
4. Klicken Sie auf die -Schaltfläche, um die **Virtuelle Tastatur** zu öffnen.
   Verwenden Sie die **Virtuelle Tastatur** immer dann, wenn Sie sensible Informationen wie Passwörter eingeben.

Was kann ich tun, wenn mein Gerät gestohlen wurde?

Der Diebstahl von Mobilgeräten, egal ob Smartphone, Tablet oder Laptop, ist heute ein weit verbreitetes Problem, von dem Privatpersonen und Unternehmen in der ganzen Welt betroffen sind.

Mit dem Bitdefender-Diebstahlschutz können Sie das gestohlene Gerät nicht nur orten und sperren, sondern im Ernstfall auch alle darauf

gespeicherten Daten löschen, damit Sie dem Dieb nicht in die Hände fallen.

So können Sie über Ihr Benutzerkonto auf die Diebstahlschutzfunktionen zugreifen:

1. Zugang Bitdefender-Zentrale.
2. Wähle aus **Meine Geräte** Tafel.
3. Klicken Sie auf die entsprechende Gerätekarte und wählen Sie {1}Diebstahlschutz{2} aus.
4. Wählen Sie die Funktion, die Sie verwenden möchten:
   - **ORTEN** - Zeigt den Standort Ihres Geräts auf Google Maps an.
     IP anzeigen - Zeigt die letzte IP-Adresse für das ausgewählte Gerät an.
   - **Alarm** - lassen Sie auf dem Gerät einen Alarmton erklingen.
   - **Sperren** - sperren Sie Ihr Gerät und legen einen numerischen PIN-Code zum Entsperren fest. Sie können auch eine entsprechende Option aktivieren, damit Bitdefender Aufnahmen von Personen machen kann, die versuchen, Ihr Gerät zu entsperren.
   - **Daten löschen** - alle Daten von Ihrem Gerät löschen.

     Wichtig
     Nach einer Löschung funktionieren die Diebstahlschutz-Funktionen nicht mehr.

Wie lösche ich mit Bitdefender eine Datei unwiderruflich?

Wenn Sie eine Datei unwiderruflich von Ihrem System löschen möchten, müssen Sie die Datei physisch von Ihrer Festplatte entfernen.

Mit dem Bitdefender-Dateischredder können Sie über das Windows-Kontextmenü Dateien und Ordner auf Ihrem Computer schnell und einfach schreddern. Gehen Sie dazu wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf die Datei bzw. den Ordner, die/den Sie dauerhaft löschen möchten, und wählen Sie unter Bitdefender den Punkt **Dateischredder**.

2. Klicken **Dauerhaft löschen**, und bestätigen Sie dann, dass Sie mit dem Vorgang fortfahren möchten.
   Warten Sie, bis Bitdefender das Schreddern der Dateien abgeschlossen hat.
3. Die Ergebnisse werden angezeigt. Klicken Sie auf **BEENDEN** um den Assistenten zu schließen.

Wie schütze ich meine Webcam vor Hackern?

So können Sie Ihr Bitdefender so konfigurieren dass es den Zugriff installierter Anwendungen auf Ihre Webcam zulässt oder verweigert:

1. Klicken **Privatsphäre** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **VIDEO- UND AUDIOSCHUTZ** Bereich, klicken Sie auf **Einstellungen**.
3. Rufen Sie das Fenster **Webcam-Schutz** auf, um eine Liste mit allen Anwendungen, die Zugriff auf Ihre Kamera angefordert haben, anzuzeigen.
4. Bewegen Sie den Mauszeiger auf die Anwendung, der Sie den Zugriff erlauben oder verbieten möchten, und klicken Sie daneben auf den Schalter, der durch eine Videokamera dargestellt wird.
   Um zu sehen, was andere Bitdefender-Benutzer mit der ausgewählten App gemacht haben, klicken Sie auf das -Symbol. Sie werden jedes Mal benachrichtigt, wenn eine der aufgelisteten Apps von den Bitdefender-Benutzern blockiert wird.

Klicken Sie auf den Link **Anwendung hinzufügen**, um Anwendungen manuell zu der Liste hinzuzufügen.

- Aus dem Windows Store
- Aus Ihren Apps

Wie kann ich verschlüsselte Dateien manuell wiederherstellen, wenn der Wiederherstellungsprozess fehlschlägt?

Gehen Sie folgendermaßen vor, um Dateien manuell wiederherzustellen, die nicht automatisch wiederhergestellt werden konnten:

1. Klicken **Benachrichtigungen** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Alle** Wählen Sie auf der Registerkarte die Benachrichtigung über das zuletzt erkannte Ransomware-Verhalten aus und klicken Sie dann auf **Verschlüsselte Dateien**.
3. Die Liste mit den verschlüsselten Dateien wird angezeigt.
   Klicken Sie zum Fortfahren auf **Dateien wiederherstellen**.
4. Falls der gesamte oder ein Teil des Wiederherstellungsprozesses fehlschlägt, müssen Sie den Speicherort auswählen, an dem die entschlüsselten Dateien gespeichert werden sollen. Klicken **Speicherort wiederherstellen**, und wählen Sie dann einen Speicherort auf Ihrem PC aus.
5. Ein Bestätigungsfenster wird angezeigt.
   Klicken **Beenden** um den Wiederherstellungsvorgang zu beenden.

Dateien mit den folgenden Erweiterungen können wiederhergestellt werden, falls sie verschlüsselt werden:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com ; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

3.4.5. Optimierungstools

Wie verbessere ich meine Systemleistung?

Die Systemleistung hängt nicht nur von der Hardwarekonfiguration, wie CPU-Auslastung, Speicherauslastung und Festplattenspeicher ab. Es ist auch direkt mit Ihrer Softwarekonfiguration und Ihrem Datenmanagement verbunden.

Dies sind die wichtigsten Maßnahmen, die Sie mit Bitdefender ergreifen können, um die Geschwindigkeit und Leistung Ihres Systems zu verbessern:

- ❍ Optimieren Sie Ihre Systemleistung mit einem einzigen Klick (Seite 119)
- ❍ Scannen Sie Ihr System regelmäßig (Seite 119)

Optimieren Sie Ihre Systemleistung mit einem einzigen Klick

Die OneClick Optimizer-Option spart Ihnen wertvolle Zeit, wenn Sie Ihre Systemleistung schnell verbessern möchten, indem Sie nutzlose Dateien schnell scannen, erkennen und bereinigen.

So starten Sie den OneClick Optimizer-Prozess:

1. Klicken **Dienstprogramme** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Drücke den **Optimieren** Taste.
3. Lassen Sie Bitdefender nach Dateien suchen, die gelöscht werden können, und klicken Sie dann auf **Optimieren** Schaltfläche, um den Vorgang abzuschließen.

Scannen Sie Ihr System regelmäßig

Ihre Systemgeschwindigkeit und ihr allgemeines Verhalten können ebenfalls durch Bedrohungen beeinträchtigt werden.

Stellen Sie sicher, dass Sie Ihr System regelmäßig scannen, mindestens einmal pro Woche.

Es wird empfohlen, den System-Scan zu verwenden, da er nach allen Arten von Bedrohungen sucht, die die Sicherheit Ihres Systems gefährden, und auch in Archiven scannt.

So starten Sie den System-Scan:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken **Scannen ausführen** neben **Systemscan**.
4. Folgen Sie den Schritten des Assistenten.

3.4.6. Nützliche Informationen

Wie kann ich meine Sicherheitslösung selbst testen?

Um die ordnungsgemäße Funktion Ihres Bitdefender-Produkts zu überprüfen, empfehlen wir den EICAR-Test.

Dabei testen Sie mithilfe der speziell für diesen Zweck entwickelten EICAR-Testdatei Ihre Sicherheitslösung.

Gehen Sie folgendermaßen vor, um Ihre Sicherheitslösung zu testen:

1. Laden Sie die Testdatei von der offiziellen EICAR-Website unter http://www.eicar.org/ herunter.
2. Wechseln Sie zum Reiter **Anti-Malware Testfile**.
3. Klicken Sie im Menü links auf **Download**.
4. Klicken Sie unter **Download area using the standard protocol http** auf die **eicar.com**-Testdatei.
5. Sie werden informiert, dass die von Ihnen aufgerufene Seite die EICAR-Testdatei (keine Bedrohung) enthält.
   Wenn Sie auf **Ich bin mir der Risiken bewusst und möchte trotzdem fortfahren** klicken, beginnt der Download der Testdatei und ein Bitdefender-Fenster informiert Sie, dass eine Bedrohung erkannt wurde.
   Klicken Sie auf **Mehr...** für weitere Informationen.

Falls Sie keine Bitdefender-Benachrichtigung erhalten, empfehlen wir Ihnen, sich wie in Kapitel Hier wird Ihnen geholfen (Seite 305) beschrieben an Bitdefender zu wenden.

Wie kann ich Bitdefender deinstallieren?

So können Sie Ihr Bitdefender Ultimate Small Business Security entfernen:

- In **Windows 7**:
  1. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
  2. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.

3. Klicken Sie im angezeigten Fenster auf **Entfernen**.
4. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

- In **Windows 8** Und **Windows 8.1**:
  1. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
  2. Klicken **Ein Programm deinstallieren** oder **Programme und Funktionen**.
  3. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
  4. Klicken **ENTFERNEN** im erscheinenden Fenster.
  5. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

- In **Windows 10** Und **Windows11**:
  1. Klicken Sie auf **Start** und danach auf Einstellungen.
  2. Drücke den **System** Symbol im Bereich Einstellungen und wählen Sie dann aus **Anwendungen**.
  3. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
  4. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.
  5. Klicken **ENTFERNEN** im erscheinenden Fenster.
  6. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

  Notiz
  Wenn Sie bei der Neuinstallation so vorgehen, werden die benutzerdefinierten Einstellungen endgültig gelöscht.

Wie kann ich Bitdefender VPN deinstallieren?

Bei der Entfernung von Bitdefender VPN von Ihrem Gerät gehen Sie ganz ähnlich vor wie bei der Entfernung anderer Programme:

- In **Windows 7**:
  1. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
  2. Suchen Sie **Bitdefender VPN** und wählen Sie **Deinstallieren**.
     Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.

- In **Windows 8** Und **Windows 8.1**:
  1. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
  2. Klicken **Deinstallieren** ein Programm bzw **Programme und Funktionen**.
  3. Finden **Bitdefender-VPN** und auswählen **Deinstallieren**.
     Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.

- In **Windows 10** Und **Windows11**:
  1. Klicken **Start**, und klicken Sie dann auf Einstellungen.
  2. Klicken Sie in den Einstellungen auf das **System**-Symbol und wählen Sie **Installierte Anwendungen**.
  3. Finden **Bitdefender-VPN** und auswählen **Deinstallieren**.
  4. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.
     Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.

Wie kann ich die Bitdefender Anti-Tracker-Erweiterung entfernen?

Gehen Sie je nach verwendetem Web-Browser wie folgt vor, um die Bitdefender Anti-Tracker-Erweiterung zu deinstallieren:

- Internet Explorer
  1. Klicken Sie neben der Suchleiste auf  und wählen Sie dann Add-ons verwalten. Es wird eine Liste mit den installierten Erweiterungen angezeigt.
  2. Klicken Sie auf Bitdefender Anti-Tracker.
  3. Klicken Sie unten rechts auf **Deaktivieren**.

- Google Chrome
  1. Klicken Sie neben der Suchleiste auf ⋮.
  2. Wählen Sie **Weitere Tools** und danach **Erweiterungen**.
     Eine Liste mit allen installierten Erweiterungen wird angezeigt.
  3. Klicken Sie in der Bitdefender Anti-Tracker-Karte auf **Entfernen**.
  4. Klicken Sie im angezeigten Pop-up-Fenster auf **Entfernen**.
- Mozilla-Firefox
  1. Klicken ≡ neben der Suchleiste.
  2. Wählen Sie **Add-ons** und danach **Erweiterungen**.
     Es erscheint eine Liste mit den installierten Erweiterungen.
  3. Klicken Sie auf ··· und wählen Sie dann **Entfernen**.

Wie fahre ich das Gerät automatisch herunter, nachdem der Scan beendet wurde?

Bitdefender bietet unterschiedliche Scan-Aufgaben, mithilfe derer Sie sicherstellen können, dass Ihr System nicht durch Bedrohungen infiziert wurde. Je nach Software- und Hardwarekonfiguration kann ein Scan des gesamten Systems längere Zeit in Anspruch nehmen.

Deshalb können Sie Bitdefender so konfigurieren, dass Ihr Produkt den Computer herunterfährt, sobald der Scan abgeschlossen ist.

Stellen Sie sich folgende Situation vor: Sie sind mit der Arbeit fertig und möchten ins Bett gehen. Sie möchten aber nun noch Ihr System durch Bitdefender auf Bedrohungen prüfen lassen.

Gehen Sie folgt vor, um das Gerät herunterzufahren, sobald ein Quick-Scan oder System-Scan beendet wurde:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Scans** neben Quick Scan oder System-Scan auf ··· und wählen Sie **Bearbeiten**.
4. Richten Sie den Scan entsprechend Ihrer Anforderungen ein und klicken Sie auf **Weiter**.

5. Markieren Sie das Kästchen neben **Legen Sie fest, für wann Sie diese Aufgabe planen möchten**, und legen Sie fest, wann die Aufgabe beginnen soll.
   Wenn Sie „Täglich“, „Monatlich“ oder „Wöchentlich“ auswählen, ziehen Sie den Schieberegler entlang der Skala, um den gewünschten Zeitraum festzulegen, in dem der geplante Scan beginnen soll.
6. Klicken **Speichern**.

Gehen Sie wie folgt vor, um das Gerät nach Abschluss eines benutzerdefinierten Scans herunterzufahren:

1. Klicken Sie neben dem von Ihnen erstellten benutzerdefinierten Scan auf ⋯.
2. Klicken Sie auf **Weiter** und dann erneut auf **Weiter**.
3. Markieren Sie das Kästchen neben **Legen Sie fest, für wann Sie diese Aufgabe planen möchten** und legen Sie fest, wann die Aufgabe beginnen soll.
4. Klicken **Speichern**.

Wenn keine Bedrohungen gefunden wurden, wird das Gerät heruntergefahren.

Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen. Weitere Informationen finden Sie im Kapitel Viren-Scan-Assistent (Seite 31).

Wie konfiguriere ich Bitdefender für die Verwendung einer Proxy-Internetverbindung?

Wenn sich Ihr Gerät über einen Proxy-Server mit dem Internet verbindet, müssen Sie Bitdefender mit den Proxy-Einstellungen konfigurieren. Normalerweise findet und importiert Bitdefender automatisch die Proxy-Einstellungen Ihres Systems.

> **Wichtig**
> Internet-Verbindungen in Privathaushalten nutzen üblicherweise keine Proxy-Server. Als Faustregel gilt, dass Sie die Einstellungen der Proxy-Verbindung Ihrer Bitdefender-Anwendung prüfen und konfigurieren sollten, falls Updates nicht funktionieren. Wenn Bitdefender sich aktualisieren kann, dann ist es richtig konfiguriert, um eine Verbindung mit dem Internet aufzubauen.

So können Sie Ihre Proxy-Einstellungen verwalten:

1. Klicken **Einstellungen** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Wähle aus **Fortschrittlich** Tab.
3. Aktivieren Sie **Proxy-Server**.
4. Klicken Sie auf **Proxy-Änderung**.
5. Sie haben zwei Möglichkeiten, die Proxy-Einstellungen vorzunehmen:
   - **Proxy-Einstellungen aus Standard-Browser importieren** - Proxy-Einstellungen des aktuellen Benutzers, aus dem Standard-Browser importiert. Sollten der Proxy-Server einen Benutzernamen und ein Passwort erfordern, müssen Sie diese in den entsprechenden Feldern angeben.

     Notiz
     Bitdefender kann die Proxy-Einstellungen aus den gängigsten Browsern importieren, einschließlich der neuesten Versionen von Internet Explorer, Mozilla Firefox und Google Chrome.

   - **Benutzerdefinierte Proxy-Einstellungen** - Proxy-Einstellungen, die Sie selbst konfigurieren können.
     Die folgenden Einstellungen müssen angegeben werden:
     - **Adresse** - geben Sie die IP-Adresse des Proxy-Servers ein.
     - **Port** - geben Sie den Port ein, über den Bitdefender die Verbindung zum Proxy-Server herstellt.
     - **Benutzername** - geben Sie einen für den Proxy-Server gültigen Benutzernamen ein.
     - **Passwort** - geben Sie das Passwort des zuvor angegebenen Benutzers ein.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Bitdefender wird die verfügbaren Proxy-Einstellungen verwenden, bis die Lösung eine Verbindung mit dem Internet aufbauen kann.

Ist auf meinem System die 32- oder 64-Bit-Version von Windows installiert?

So können Sie ermitteln, ob Sie über ein 32-Bit- oder 64-Bit-Betriebssystem verfügen:

- In **Windows 7**:
  1. Klicken Sie auf **Start**.
  2. Suchen Sie im **Startmenü** nach **Computer**.
  3. Klicken Sie mit der rechten Maustaste auf **Computer** und wählen Sie **Eigenschaften**.
  4. Unter **System** können Sie die Systeminformationen einsehen.
- Unter **Windows 8**:
  1. Finden Sie auf der Windows-Startseite den Eintrag **Computer** (z.B. durch die Eingabe von "Computer" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
  2. Wählen Sie im Menü unten **Eigenschaften**.
  3. Im Bereich System finden Sie Ihren Systemtyp.
- In **Windows 10** Und **Windows11**:
  1. Geben Sie "System" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.
  2. Im Bereich System finden Sie Informationen zu Ihrem Systemtyp.

Wie kann ich in Windows versteckte Objekte anzeigen?

Diese Schritte sind sinnvoll in den Fällen, in denen Sie es mit einer Bedrohungssituation zu tun haben und Sie infizierte Dateien, die eventuell verborgen sind, finden und entfernen müssen.

Gehen Sie folgendermaßen vor, um versteckte Objekte in Windows anzuzeigen:

1. Klicken Sie auf **Start** und rufen Sie die**Systemsteuerung** auf.
   Unter **Windows 8** und **Windows 8.1**: Suchen Sie im Windows-Startmenü die **Systemsteuerung** (z. B. durch die Eingabe von

"Systemsteuerung") und klicken Sie dann auf das entsprechende Symbol.

2. Wählen Sie **Ordneroptionen**.
3. Wechseln Sie zum Reiter **Ansicht**.
4. Wählen Sie **Verborgene Dateien und Verzeichnisse anzeigen**.
5. Entfernen Sie den Haken bei **Erweiterungen bei bekannten Dateitypen ausblenden**.
6. Deaktivieren Sie **Geschützte Betriebssystemdateien verbergen**.
7. Klicken Sie auf **Anwenden** und danach auf **OK**.

In **Windows 10** Und **Windows11**:

1. Geben Sie "Alle Dateien und Ordner anzeigen" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.
2. Wählen Sie **Ausgeblendete Dateien, Ordner und Laufwerke anzeigen** aus.
3. Klar **Erweiterungen für bekannte Dateitypen verbergen**.
4. Klar **Geschützte Betriebssystemdateien ausblenden**.
5. Klicken **Anwenden**, dann klick **OK**.

Wie entferne ich andere Sicherheitslösungen?

Der Hauptgrund für den Einsatz einer Sicherheitslösung ist der Schutz und die Sicherheit Ihrer Daten. Aber was geschieht, wenn mehr als ein Sicherheitsprogramm auf demselben System läuft?

Wenn Sie mehr als eine Sicherheitslösung auf Ihrem Gerät verwenden, wird dadurch das System instabil. Das Bitdefender Ultimate Small Business Security-Installationsprogramm findet automatisch andere auf dem System installierte Sicherheits-Software und bietet an, diese zu deinstallieren.

Falls Sie weitere bereits auf dem PC installierte Sicherheitslösungen nicht während der Installation entfernt haben:

- In **Windows 7**:

  1. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.

2. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
4. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

- In **Windows 8** Und **Windows 8.1**:
  1. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
  2. Klicken **Ein Programm deinstallieren** oder **Programme und Funktionen**.
  3. Warten Sie einen Moment, bis die Liste der installierten Software angezeigt wird.
  4. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie es aus **Deinstallieren**.
  5. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

- In **Windows 10** Und **Windows11**:
  1. Klicken **Start**, und klicken Sie dann auf Einstellungen.
  2. Drücke den **System** Symbol im Bereich Einstellungen und wählen Sie dann aus **Anwendungen**.
  3. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie es aus **Deinstallieren**.
  4. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.
  5. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

Wenn es Ihnen nicht gelingt, weitere auf Ihrem Rechner installierte Sicherheits-Software zu entfernen, laden Sie sich das Deinstallations-Tool von der Website des entsprechenden Herstellers herunter oder wenden Sie sich direkt an den Hersteller für eine Deinstallationsanleitung.

Wie führe ich einen Neustart im abgesicherten Modus durch?

Der abgesicherte Modus ist ein diagnostischer Betriebsmodus, der hauptsächlich bei der Suche nach Fehlern zum Einsatz kommt, die den normalen Windows-Betrieb beeinträchtigen. Solche Probleme reichen von in Konflikt stehenden Treibern bis hin zu Bedrohungen, die Windows daran hindern, normal hochzufahren. Im abgesicherten Modus funktionieren nur einige wenige Anwendungen und Windows lädt nur die wichtigsten Treiber und ein Minimum an Betriebssystemkomponenten. Deshalb sind bei einer Verwendung von Windows im abgesicherten Modus die meisten Bedrohungen inaktiv und können einfach entfernt werden.

Start von Windows im abgesicherten Modus:

- In **Windows 7**:
  1. Starten Sie das Gerät neu.
  2. Drücken Sie wiederholt die **F8**-Taste, bevor Windows startet, um so Zugriff auf das Boot-Menü zu erhalten.
  3. Wählen Sie **Abgesicherter Modus** im Boot-Menü oder **Abgesicherter Modus mit Netzwerktreibern**, wenn Sie Zugang zum Internet haben möchten.
  4. Drücken Sie die **Eingabetaste** und warten Sie, während Windows im abgesicherten Modus startet.
  5. Der Vorgang endet mit einer Bestätigungsmeldung. Klicken Sie zur Bestätigung auf **OK**.
  6. Um Windows normal zu starten, starten Sie einfach Ihr System neu.

- Unter **Windows 8**, **Windows 8.1**, **Windows 10** und **Windows 11**:
  1. Rufen Sie die **Systemkonfiguration** in Windows auf, indem Sie auf Ihrer Tastatur gleichzeitig die Tasten **Windows + R** drücken.
  2. Geben Sie **msconfig** in das Dialogfeld hinter **Öffnen:** ein und klicken Sie dann auf **OK**.
  3. Wechseln Sie zum Reiter **Start**.
  4. Aktivieren Sie im Bereich **Startoptionen** das Kontrollkästchen **Abgesicherter Start**.
  5. Klicken Sie auf **Netzwerk** und danach auf **OK**.

6. Im Fenster **Systemkonfiguration** werden Sie darüber informiert, dass Ihr System zur Übernahme der Änderungen neu gestartet werden muss. Klicken Sie auf **OK**.
   Ihr System wird im Abgesicherten Modus mit Netzwerktreibern neu gestartet.

Setzen Sie die Einstellungen wieder zurück, um Ihr System im normalen Modus neu zu starten. Kehren Sie dazu zur **Systemkonfiguration** zurück und deaktivieren Sie das Kästchen **Abgesicherter Start**. Klicken Sie auf **OK** und danach auf **Neustart**. Warten Sie, bis die neuen Einstellungen übernommen werden.

3.5. Problemlösung

3.5.1. Verbreitete Probleme beheben

Dieses Kapitel zeigt einige Probleme bei der Benutzung von BitDefender auf und bietet mögliche Lösungen dazu. Die meisten dieser Probleme können durch die geeigneten Einstellungen im Produkt behoben werden.

- Mein System scheint langsamer zu sein (Seite 131)
- Der Scan startet nicht (Seite 132)
- Ich kann eine App nicht mehr verwenden (Seite 135)
- Was können Sie tun, wenn Bitdefender eigentlich sichere Websites, Domains, IP-Adressen oder Online-Anwendungen blockiert? (Seite 136)
- Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann (Seite 141)
- Bitdefender-Dienste antworten nicht (Seite 142)
- Der Spam-Schutz-Filter funktioniert nicht richtig (Seite 142)
- Entfernen von Bitdefender fehlgeschlagen (Seite 147)
- Mein System fährt nach der Installation von Bitdefender nicht mehr hoch (Seite 149)

Wenn Sie Ihr Problem hier nicht finden oder dieser weiterhin besteht, können Sie kontakt zu unserem BitDefender Technischen Support aufnehmen, wie beschrieben in {1}{2}.

Mein System scheint langsamer zu sein

Nach der Installation einer Sicherheitssoftware ist eine geringfügige Verlangsamung des Systems bis zu einem gewissen Grad normal.

Wenn Sie eine erhebliche Systemverlangsamung feststellen, kann dies folgende Ursachen haben:

- **Bitdefender ist nicht die einzige auf Ihrem System installierte Sicherheits-Software**.
  Obwohl Bitdefender bereits auf Ihrem System installierte Sicherheitsprogramme während der Installation sucht und entfernt, empfehlen wir dennoch, jede andere Sicherheitslösung von Ihrem Rechner zu entfernen, bevor Sie die Installation von Bitdefender starten. Weitere Informationen finden Sie im Kapitel Wie entferne ich andere Sicherheitslösungen? (Seite 127).
- **Die Systemvoraussetzungen für die Ausführung von Bitdefender sind nicht erfüllt.**
  Wenn Ihr Gerät die Systemvoraussetzungen nicht erfüllt, verlangsamt dies Ihr System, insbesondere dann, wenn mehrere Anwendungen gleichzeitig laufen. Weitere Informationen finden Sie im Kapitel Systemanforderungen (Seite 10).
- **Sie haben Apps installiert, die Sie nicht verwenden.**
  Auf jedem Gerät sind Programme oder Anwendungen installiert, die Sie nicht verwenden. Im Hintergrund laufen viele unerwünschte Programme, die Speicherplatz und Arbeitsspeicher beanspruchen. Wenn Sie ein Programm nicht nutzen, deinstallieren Sie es. Das gilt auch für vorinstallierte Software oder Testversionen, die Sie nicht wieder entfernt haben.

  > **Wichtig**
  > Wenn Sie glauben, dass ein Programm oder eine Anwendung ein wichtiger Bestandteil Ihres Betriebssystems ist, entfernen Sie es nicht und wenden Sie sich an den Bitdefender-Kundendienst.

- **Ihr System ist vielleicht infiziert.**
  Die Geschwindigkeit und das allgemeine Verhalten Ihres Systems kann auch durch Bedrohungen beeinträchtigt werden. Spyware, Malware, Trojaner und Adware wirken sich negativ auf Ihre Geräteleistung aus. Stellen Sie sicher, dass Ihr System regelmäßig gescannt wird, mindestens einmal pro Woche. Wir empfehlen, einen Bitdefender-

System-Scan durchzuführen, da so nach allen Bedrohungsarten gesucht wird, die die Sicherheit Ihres Systems gefährden.
So können Sie einen System-Scan starten:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie im Fenster **Scans** neben **System-Scan** auf die Schaltfläche **Scan starten**.
4. Befolgen Sie die Anweisungen des Assistenten.

Der Scan startet nicht

Dieses Problem kann folgende Ursachen haben:

- **Eine vorherige Installation von Bitdefender wurde nicht vollständig entfernt oder es handelt sich um eine fehlerhafte Bitdefender-Installation.**
  Installieren Sie Bitdefender in diesem Fall neu:
  - In **Windows 7**:
    1. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
    2. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
    3. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.
    4. Warten Sie, bis die Neuinstallation abgeschlossen ist und starten Sie Ihr System neu.
  - In **Windows 8** Und **Windows 8.1**:
    1. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
    2. Klicken **Deinstallieren** ein Programm bzw **Programme und Funktionen**.
    3. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.

4. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.
5. Warten Sie, bis der Neuinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

- In **Windows 10** Und **Windows11**:
  1. Klicken **Start**, dann klick **Einstellungen**.
  2. Drücke den **System** Symbol im Bereich Einstellungen und wählen Sie dann aus **Installierte Anwendungen**.
  3. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
  4. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.
  5. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.
  6. Warten Sie, bis der Neuinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

> **Notiz**
> Durch Befolgen dieses Neuinstallationsverfahrens werden benutzerdefinierte Einstellungen gespeichert und stehen im neu installierten Produkt zur Verfügung. Andere Einstellungen können auf ihre Standardkonfiguration zurückgesetzt werden.

- **Bitdefender ist nicht die einzige auf Ihrem System installierte Sicherheits-Software**.
  In diesem Fall:
  1. Entfernen Sie die andere Sicherheitslösung. Weitere Informationen finden Sie im Kapitel Wie entferne ich andere Sicherheitslösungen? (Seite 127).
  2. Bitdefender erneut installieren:
     - In **Windows 7**:
       a. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
       b. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
       c. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.

d. Warten Sie, bis der Neuinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

- In **Windows 8** Und **Windows 8.1**:

  a. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.

  b. Klicken **Deinstallieren** ein Programm bzw **Programme und Funktionen**.

  c. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.

  d. Klicken **NEU INSTALLIEREN** im erscheinenden Fenster.

  e. Warten Sie, bis der Neuinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

- In **Windows 10** Und **Windows11**:

  a. Klicken **Start**, dann klick **Einstellungen**.

  b. Drücke den **System** Symbol im Bereich Einstellungen und wählen Sie dann aus **Installierte Anwendungen**.

  c. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.

  d. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.

  e. Klicken Sie im angezeigten Fenster auf **NEU INSTALLIEREN**

  f. Warten Sie, bis der Neuinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

> **Notiz**
> Durch Befolgen dieses Neuinstallationsverfahrens werden benutzerdefinierte Einstellungen gespeichert und stehen im neu installierten Produkt zur Verfügung. Andere Einstellungen können auf ihre Standardkonfiguration zurückgesetzt werden.

Wenn Sie weitere Hilfe benötigen, kontaktieren Sie den BitDefender Support wie in folgendem Abschnitt beschrieben: Hier wird Ihnen geholfen (Seite 305).

Ich kann eine App nicht mehr verwenden

Dieses Problem tritt auf, wenn Sie versuchen, ein Programm zu verwenden, das vor der Installation von Bitdefender einwandfrei funktioniert hatte.

Nach der Installation von Bitdefender könnten folgende Situationen eintreten:

- Sie könnten einen Benachrichtigung von Bitdefender erhalten, dass das Programm versucht, Veränderungen am System durchzuführen.
- Es ist möglich, dass Sie von dem Programm, das Sie starten möchten, eine Fehlermeldung erhalten.

Diese Situation tritt ein, wenn die Erweiterte Gefahrenabwehr eine Anwendung fälschlicherweise als Malware einstuft.

Die Erweiterte Gefahrenabwehr ist ein Bitdefender-Modul, das alle laufenden Anwendungen auf Ihren Systemen durchgehend überwacht und einen Bericht über jene sendet, die sich potenziell gefährlich verhalten. Da diese Funktion auf einem heuristischen System basiert, kann es dazu kommen, dass auch seriöse Anwendungen im Bericht der Erweiterten Gefahrenabwehr aufgelistet werden.

In solchen Fällen können Sie die entsprechende Anwendung von der Überwachung durch die Erweiterte Gefahrenabwehr ausnehmen.

So können Sie das Programm zur Ausnahmeliste hinzufügen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **ERWEITERTE BEDROHUNGSABWEHR** Bereich, klicken Sie auf **Offen**.
3. Im **Einstellungen** Fenster, klicken **Ausnahmen verwalten**.
4. Klicken **+Fügen Sie eine Ausnahme hinzu**.
5. Geben Sie den Pfad der ausführbaren Datei, die Sie vom Scan ausnehmen möchten, in das entsprechende Feld ein.

Alternativ können Sie zur ausführbaren Datei navigieren, indem Sie auf die Schaltfläche „Durchsuchen“ auf der rechten Seite der Benutzeroberfläche klicken, sie auswählen und auf klicken **OK**.

6. Schalten Sie den Schalter daneben ein **Erweiterte Bedrohungsabwehr**.
7. Klicken **Speichern**.

Wenn diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten Hier wird Ihnen geholfen (Seite 305).

Was können Sie tun, wenn Bitdefender eigentlich sichere Websites, Domains, IP-Adressen oder Online-Anwendungen blockiert?

Bitdefender ermöglicht Ihnen sicheres Surfen im Netz, indem es Ihren Internet-Datenverkehr filtert und schädliche Inhalte blockiert. Es kann jedoch vorkommen, dass Bitdefender eigentlich sichere Websites, Domains, IP-Adressen oder Online-Anwendungen als unsicher einstuft, wodurch diese dann durch den Bitdefender-Scan des HTTP-Datenverkehrs irrtümlich blockiert werden.

Sollte die gleiche Seite, Domain, IP-Adresse oder Online-Anwendung wiederholt blockiert werden, können Sie diese zu den Ausnahmen hinzufügen, damit sie von den Bitdefender-Engines nicht mehr gescannt werden. So können Sie ungestört im Internet surfen.

So können Sie eine Website zu den **Ausnahmen** hinzufügen:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **VORBEUGUNG VON ONLINE-BEDROHUNGEN** Bereich, klicken Sie auf **Einstellungen**.
3. Klicken **Ausnahmen verwalten**.
4. Klicken **+Fügen Sie eine Ausnahme hinzu**.
5. Geben Sie in das entsprechende Feld den Namen der Website, den Namen der Domain oder die IP-Adresse ein, die Sie zu Ausnahmen hinzufügen möchten.
6. Klicken Sie auf den Schalter neben **Abwehr von Online-Bedrohungen**.
7. Klicken **Speichern** um die Änderungen zu speichern und das Fenster zu schließen.

Nur Websites, Domains, IP-Adressen und Anwendungen, denen Sie uneingeschränkt vertrauen, sollten dieser Liste hinzugefügt werden. Diese werden dann von den folgenden Engines vom Scan ausgenommen: Bedrohung, Phishing und Betrug.

Wenn diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten Hier wird Ihnen geholfen (Seite 305).

Ich kann keine Verbindung zum Internet herstellen

Nach der Installation von Bitdefender werden Sie unter Umständen bemerken, dass ein Programm oder ein Browser keine Verbindung mehr zum Internet herstellen oder auf Netzwerkdienste zugreifen kann.

In diesem Fall ist es die beste Lösung, Bitdefender so zu konfigurieren, dass Verbindungen von und zu der jeweiligen Software-Anwendung automatisch zugelassen werden:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **FIREWALL** Bereich, klicken Sie auf **Einstellungen**.
3. Im **Regeln** Fenster, klicken **Regel hinzufügen**.
4. Es wird ein neues Fenster angezeigt, in dem Sie die Details eingeben können. Stellen Sie sicher, dass Sie alle verfügbaren Netzwerktypen auswählen und im Abschnitt **Berechtigung** die Option **Zulassen** wählen.

Schließen Sie Bitdefender, öffnen Sie die Software-Anwendung und versuchen Sie erneut, eine Verbindung mit dem Internet aufzubauen.

Wenn diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten Hier wird Ihnen geholfen (Seite 305).

Ich kann auf ein Gerät in meinem Netzwerk nicht zugreifen

Abhängig von dem Netzwerk mit dem Sie verbunden sind, könnte die Bitdefender-Firewall die Verbindung zwischen Ihrem System und einem anderen Gerät (zum Beispiel einem anderen Gerät oder Drucker) blockieren. Dadurch sind Sie vielleicht nicht mehr in der Lage, Dateien auszutauschen oder zu drucken.

In diesem Fall konfigurieren Sie Bitdefender am besten so, dass Verbindungen von und zu dem jeweiligen Gerät automatisch zugelassen werden. Gehen Sie dazu wie folgt vor:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **FIREWALL** Bereich, klicken Sie auf **Einstellungen**.
3. Im **Regeln** Fenster, klicken **Regel hinzufügen**.
4. Aktivieren die Option **Diese Regel auf alle Anwendungen anwenden**.
5. Klicken Sie auf die Schaltfläche **Weitere Einstellungen**.
6. Geben Sie im Feld **Benutzerdefinierte Remoteadresse** die IP-Adresse des PCs oder Druckers ein, auf den Sie uneingeschränkten Zugriff haben möchten.

Wenn eine Verbindung mit dem Gerät immer noch nicht möglich ist, wird das Problem vielleicht nicht durch Bitdefender hervorgerufen.

Überprüfen Sie andere mögliche Ursachen, wie z.B:

- Die Firewall auf dem anderen Gerät blockiert möglicherweise die Datei- und Druckerfreigabe mit Ihrem PC.
  - Wenn die Windows Firewall genutzt wird, kann diese wie folgt zum Zulassen von Datei- und Druckerfreigabe konfiguriert werden:
    - In **Windows 7**:
      1. Klicken Sie auf **Start**, öffnen Sie die **Systemsteuerung** und wählen Sie **System und Sicherheit**.
      2. Öffnen Sie die **Windows-Firewall** und klicken Sie dann auf **Programm durch die Windows-Firewall kommunizieren lassen**.
      3. Wählen Sie die Option **Datei- und Druckerfreigabe**.
    - In **Windows 8** Und **Windows 8.1**:
      1. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.

2. Klicken Sie auf **System und Sicherheit**, öffnen Sie die **Windows-Firewall** und klicken Sie dann auf **Apps über die Windows-Firewall kommunizieren lassen**.
3. Wählen Sie die Option **Datei- und Druckerfreigabe** aus und klicken Sie **OK**.

- In **Windows 10** Und **Windows11**:
  1. Geben Sie "Apps über die Windows-Firewall kommunizieren lassen" in das Suchfeld in der Taskleiste ein und klicken Sie auf das entsprechende Symbol.
  2. Klicken Sie auf **Einstellungen ändern**.
  3. Markieren Sie in der Liste **Zugelassene Apps und Funktionen** das Kontrollkästchen für **Datei- und Druckerfreigabe** und klicken Sie dann auf **OK**.

- Wenn eine andere Firewall verwendet wird, greifen Sie bitte auf die entsprechende Dokumentation oder Hilfedatei zurück.

- Allgemeine Umstände, die eine Benutzung des oder Verbindung mit dem freigegebenen Drucker verhindern könnten:
  - Möglicherweise müssen Sie sich als Windows-Administrator anmelden, um auf den freigegebenen Drucker zugreifen zu können.
  - Für den gemeinsam genutzten Drucker werden Rechte vergeben, so dass dieser nur bestimmten Geräten und Benutzern den Zugriff erlaubt. Falls Sie Ihren Drucker zur gemeinsamen Nutzung freigegeben haben, überprüfen Sie die Rechte, die für den Drucker vergeben wurden, um festzustellen, ob der Nutzer des anderen Geräts Zugriffsrechte erhalten hat. Wenn Sie versuchen, eine Verbindung zu einem freigegebenen Drucker aufzubauen, sollten Sie mit Benutzer des anderen Geräts abklären, ob Sie die benötigten Rechte haben.
  - Der an Ihr Gerät oder an das andere Gerät angeschlossene Drucker ist nicht freigegeben.
  - Der freigegebene Drucker wurde dem Gerät nicht hinzugefügt.

> **Notiz**
> Um mehr darüber zu erfahren, wie Sie die Druckerfreigabe verwalten können (Drucker freigeben, Rechte vergeben oder entziehen, Verbindungen mit einen freigegebenen Drucker herstellen), klicken sie im Windows-Startmenü auf **Hilfe und Support**).

- Der Zugriff auf einen Netzwerk-Drucker könnte auf bestimmte Geräte oder Benutzer beschränkt sein. Fragen Sie Ihren Netzwerk-Administrator, ob Sie die notwendigen Rechte besitzen, um auf diesen Drucker zuzugreifen.

Wenn diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten Hier wird Ihnen geholfen (Seite 305).

Meine Internetverbindung ist langsam

Diese Situation könnte nach der Installation von Bitdefender eintreten. Das Problem könnte aufgrund von Konfigurationsfehlern der Bitdefender-Firewall auftreten.

So können Sie das Problem behandeln:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Deaktivieren Sie im Bereich **FIREWALL** den Schalter, um die Funktion zu deaktivieren.
3. Überprüfen Sie, ob Sie nach der Deaktivierung der Bitdefender-Firewall eine Verbesserung der Internet-Verbindung feststellen können.

   - Wenn die Internetverbindung immer noch langsam ist, wird das Problem vielleicht nicht durch Bitdefender hervorgerufen. Sie sollten Ihren Internet-Provider kontaktieren, um abzuklären, dass es von seiner Seite aus keine Verbindungsprobleme gibt.

     Wenn Sie von Ihrem Internet-Anbieter die Bestätigung erhalten, dass es auf Anbieterseite keine Probleme gibt und das Problem besteht weiterhin, kontaktieren Sie Bitdefender wie im Abschnitt Hier wird Ihnen geholfen (Seite 305) beschrieben.

   - Falls Sie nach der Deaktivierung der Bitdefender-Firewall eine Verbesserung der Internet-Verbindung feststellen können:

a. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.

b. Im **FIREWALL** Bereich, klicken Sie auf **Einstellungen**.

c. Wechseln Sie zum Reiter **Netzwerkadapter** und legen Sie Ihre Internetverbindung als **Heim/Büro** fest.

d. Deaktivieren Sie im Reiter **Einstellungen** den **Port-Scan-Schutz**.
Klicken Sie im Abschnitt **Tarnkappe** auf **Tarneinstellungen bearbeiten**. Aktivieren Sie den Tarnkappen-Modus für den Netzwerkadapter, mit dem Sie verbunden sind.

e. Schließen Sie Bitdefender, starten Sie das System neu und überprüfen Sie die Internet-Verbindungsgeschwindigkeit.

Wenn diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten Hier wird Ihnen geholfen (Seite 305).

Wie man Bitdefender-Updates auch mit einer langsamen Internet-Verbindung durchführen kann

Falls Sie über eine langsame Internet-Verbindung (wie z. B. ein Modem) verfügen, können während des Updates Fehler auftreten.

So stellen Sie sicher, dass die Datenbank mit den Bedrohungsinformationen in Bitdefender jederzeit auf dem neuesten Stand ist:

1. Klicken **Einstellungen** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Wähle aus **Aktualisieren** Tab.
3. Deaktivieren Sie den Schalter **Update im Hintergrund**.
4. Beim nächsten Update werden Sie aufgefordert, das Update auszuwählen, das Sie herunterladen möchten. Wählen Sie nur **Virensignatur-Update**.
5. Bitdefender wird nur die Datenbank mit den Bedrohungsinformationen herunterladen und installieren.

Bitdefender-Dienste antworten nicht

Dieser Artikel hilft Ihnen bei der Lösung des **BitDefender Dienste antworten nicht** Problems. Sie könnten folgende Fehlermeldung erhalten:

- Das Bitdefender-Symbol im der **Task-Leiste** ist grau hinterlegt und Sie erhalten eine Meldung, dass die Bitdefender-Dienste nicht reagieren.
- Das BitDefender Fenster zeigt an, dass die BitDefender Dienste nicht Antworten.

Der Fehler kann durch einen der folgenden Umstände verursacht werden:

- temporäre Kommunikationsstörungen zwischen den BitDefender Dienste.
- einige der BitDefender Dienste sind gestoppt.
- andere Sicherheitslösungen werden gleichzeitig mit Bitdefender auf Ihrem Gerät ausgeführt.

Um diesen Fehler zu beheben, versuchen Sie folgenden Lösungen:

1. Warten Sie einen Moment und beobachten Sie, ob sich etwas ändert. Der Fehler könnte vorübergehend sein.
2. Starten Sie das Gerät neu und warten Sie einige Momente, bis Bitdefender geladen ist. Öffnen Sie BitDefender und überprüffen Sie ob das Problem immernoch besteht. Durch einen Neustart des Geräts wird das Problem üblicherweise behoben.
3. Überprüfen Sie, ob Sie irgendeine andere Sicherheitslösung installiert haben, weil diese den Normalbetrieb von BitDefender stören könnte. Wenn dies der Fall ist, empfehlen wir Ihnen alle anderen Sicherheitslösungen zu entfernen und BitDefender wieder neu zu installieren.
   Weitere Informationen finden Sie im Kapitel Wie entferne ich andere Sicherheitslösungen? (Seite 127).

Sollte der Fehler weiterhin auftreten, wenden Sie sich bitte an unsere Support-Mitarbeiter, wie in Abschnitt Hier wird Ihnen geholfen (Seite 305) beschrieben.

Der Spam-Schutz-Filter funktioniert nicht richtig

Dieser Artikel hilft Ihnen, die folgenden Probleme mit der BitDefender Antispafilter lösen:

- **Eine Anzahl von seriösen E-Mails werden markiert als [spam].**
- **Viele Spams werden entsprechend nicht durch den Antispam Filter markiert.**
- **Der Antispam-Filter entdeckt keine Spamnachrichten.**

Legitime Nachrichten werden als [spam] markiert

Legitime Nachrichten werden als [Spam] markiert, weil sie für den Bitdefender Spam-Schutz-Filter wie Spam aussehen. Dieses Problem können Sie normalerweise durch eine geeignete Konfiguration des Spam-Schutz-Filters lösen.

Bitdefender fügt die Empfänger Ihrer E-Mail-Nachrichten automatisch zu einer Freundesliste hinzu. Alles von den Kontakten in dieser Freundesliste an Sie geschickten E-Mail-Nachrichten werden als harmlos eingestuft. Sie werden nicht vom Spam-Schutz-Filter überprüft und daher nicht als [Spam] markiert.

Die automatische Konfiguration der Freundesliste verhindert nicht die entdeckte Störungen, die in dieser Situationen auftreten können:

- Sie empfangen viele angeforderte Werb-E-Mails resultierend aus der Anmeldung auf verschiedene Webseiten. In diesem Fall ist die Lösung, die E-Mail Adressen, von denen Sie solche E-Mails bekommen, auf die Freunde Liste zu setzen.
- Ein erheblicher Teil Ihrer legitimen Email ist von Leuten, die bisher nie E-Mails von Ihnen erhalten haben. bspw. Kunden, potentielle Geschäftspartner und andere. Andere Lösungen sind in diesem Fall erforderlich.

Wenn Sie einen der Mail-Clients nutzen, in die sich Bitdefender integrieren lässt, sollten Sie **auf Erkennungsfehler hinweisen**.

> **Notiz**
> Bitdefender lässt sich über eine benutzerfreundliche Antispam-Symbolleiste in die am häufigsten verwendeten E-Mail-Clients integrieren. Eine vollständige Liste der unterstützten E-Mail-Clients finden Sie unter Unterstützte E-Mail-Clients und Protokolle (Seite 50).

Kontakte zur Freundesliste hinzufügen

Wenn Sie einen unterstützten E-Mail Client verwenden, können Sie den Absernder ganz leicht zu der Freundesliste hinzufügen. Folgen Sie diesen Schritten:

1. Wählen Sie in Ihrem Mail Client eine Mail eines Senders, den Sie der Freundesliste hinzufügen möchten.
2. Klicken Sie in der Bitdefender Spam-Schutz-Symbolleiste auf die Schaltfläche **Neuer Freund**.
3. Es kann sein das Sie die Adressen, die zur Freundesliste hinzugefügt wurden, bestätigen müssen. Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie **OK**.

Sie werden jetzt immer E-Mails von diesem Absender erhalten, egal welchen Inhalts.

Falls Sie einen anderen Mail Client verwenden, können Sie von der BitDefender Oberfläche aus Kontakte der Freundesliste hinzufügen. Folgen Sie diesen Schritten:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Klicken Sie im Bereich **SPAM-SCHUTZ** auf **Freunde verwalten**.
   Ein Konfigurationsfenster wird geöffnet.
3. Geben Sie die E-Mail-Adresse ein, von der Sie immer E-Mails empfangen wollen und klicken Sie auf **HINZUFÜGEN**. Sie können beliebig viele E-Mail-Adressen hinzufügen.
4. Klicken **OK** um die Änderungen zu speichern und das Fenster zu schließen.

Auf Erkennungsfehler hinweisen

Wenn Sie einen unterstützten E-Mail-Client verwenden, können Sie den Spam-Filter einfach korrigieren (indem Sie angeben, welche E-Mails nicht als [spam] hätten markiert werden sollen). Dadurch wird die Effizienz des Spam-Filters verbessert. Folgen Sie diesen Schritten:

1. Öffnen Sie Ihren E-Mail-Client.
2. Wechseln Sie in den Junk-Mail-Ordner, in den Spam-Nachrichten verschoben werden.
3. Wählen Sie die Nachricht, die von Bitdefender fälschlicherweise als [spam] markiert wurde, aus.
4. Klicken Sie auf die Schaltfläche **Neuer Freund** in der Bitdefender Spam-Schutz-Symbolleiste, um den Absender zur Liste der Freunde hinzuzufügen. Möglicherweise müssen Sie zur Bestätigung auf

OK klicken. E-Mail-Nachrichten von dieser Adresse werden Ihnen unabhängig von Ihrem Inhalt immer zugestellt.

5. Drücke den **Kein spam** Schaltfläche in der Bitdefender-Antispam-Symbolleiste (normalerweise im oberen Teil des E-Mail-Client-Fensters). Die E-Mail-Nachricht wird in den Posteingangsordner verschoben.

Eine Vielzahl von Spam-Nachrichten wird nicht erkannt

Wenn Sie viele Nachrichten erhalten, die nicht als [spam] markiert sind, konfigurieren Sie den BitDefender Antispam Filter, um seine Effektivität zu erhöhen.

Versuchen Sie die folgenden Lösungsansätze:

1. Wenn Sie einen der Mail-Clients nutzen, in die sich Bitdefender integrieren lässt, sollten Sie **auf unerkannte Spam-Nachrichten hinweisen**.

> **Notiz**
> Bitdefender lässt sich über eine benutzerfreundliche Antispam-Symbolleiste in die am häufigsten verwendeten E-Mail-Clients integrieren. Eine vollständige Liste der unterstützten E-Mail-Clients finden Sie unter Unterstützte E-Mail-Clients und Protokolle (Seite 50).

2. **Spammer zur Liste der Spammer hinzufügen**. E-Mails von Absendern auf der Liste der Spammer werden in Zukunft automatisch als [Spam]markiert.

Auf unerkannte Spam-Nachrichten hinweisen

Wenn Sie einen unterstützten E-Mail-Client verwenden, können Sie einfach angeben, welche E-Mail-Nachrichten als Spam hätten erkannt werden sollen. Dadurch wird die Effizienz des Antispam-Filters verbessert. Folge diesen Schritten:

1. Öffnen Sie Ihren E-Mail-Client.
2. Wechseln Sie zum Ordner Posteingang.
3. Wählen Sie die unerkannten Spam-Nachrichten aus.
4. Klicken Sie in der Bitdefender-Spam-Schutz-Symbolleiste (die sich üblicherweise im oberen Teil des Mail-Client-Fensters befindet) auf die

Schaltfläche **Ist Spam**. Sie werden sofort als [spam] markiert und in den Junk-Mail-Ordner verschoben.

Neue Spammer zur Liste der Spammer hinzufügen

Wenn Sie einen unterstützten E-Mail Client verwenden, können Sie den Absernder der Spamnachricht ganz leicht zu der Spammerliste hinzufügen. Folgen Sie diesen Schritten:

1. Öffnen Sie Ihren E-Mail-Client.
2. Wechseln Sie in den Junk-Mail-Ordner, in den Spam-Nachrichten verschoben werden.
3. Wählen Sie die Nachricht die von BitDefender als [spam] markiert wurde.
4. Klicken Sie in der Bitdefender Spam-Schutz-Symbolleiste auf die Schaltfläche **Neuer Spammer**.
5. Es kann sein das Sie die Adresse bestätigen müssen, die in der Spammerliste hinzugefügt wurde. Wählen Sie **Diese Nachricht nicht mehr anzeigen** und klicken Sie **OK**.

Falls Sie einen anderen E-Mail-Client verwenden, können Sie von der Bitdefender-Oberfläche aus manuell Spammer der Liste der Spammer hinzufügen. Dies sollten Sie nur dann tun, wenn Sie bereits mehrere Spam-Nachrichten vom selben Absender erhalten haben. Folgen Sie diesen Schritten:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **SPAMSCHUTZ** Bereich, klicken Sie auf **Einstellungen**.
3. Rufen Sie das Fenster **Spammer verwalten** auf.
4. Geben Sie die E-Mail-Adresse des Spammers ein und klicken Sie auf **Hinzufügen**. Sie können beliebig viele E-Mail-Adressen hinzufügen.
5. Klicken **OK** um die Änderungen zu speichern und das Fenster zu schließen.

Der Spam-Schutz-Filter erkennt keine Spam-Nachrichten

Wenn keine Nachrichten als [spam], könnte es möglicherweise ein Problem mit dem Bitdefender Antispam Fileter sein. Vor der Fehlersuche dieses Problems, sollten Sie sicherstellen , dass es nicht durch einen der folgenden Bedingungen verursacht wird:

- Der Spam-Schutz ist unter Umständen deaktiviert. Klicken Sie im Navigationsbereich der **Bitdefender-Benutzeroberfläche** auf **Schutz**, um den Status des Spam-Schutzes zu prüfen. Rufen Sie den Bereich **Spam-Schutz** auf, um zu überprüfen, ob die Funktion aktiviert ist.

  Falls der Spam-Schutz deaktiviert ist, so liegt hier die Ursache Ihres Problems. Klicken Sie auf den entsprechenden Schalter, um Ihren Spam-Schutz zu aktivieren.

- Der Bitdefender Spam-Schutz ist nur für E-Mail-Clients verfügbar, die für den Empfang von E-Mail-Nachrichten über das POP3-Protokoll konfiguriert sind. Bitte beachten Sie deshalb Folgendes:

  - Die Email-Nachrichten, die über web-basierte Email-Dienstleistungen empfangen werden (wie Yahoo, Gmail, Hotmail oder andere) gehen nichtdurch den Bitdefender Spam-Filter.

  - Wenn Ihr E-Mail-Client für den Empfang von E-Mail-Nachrichten über andere Protokolle als POP3 konfiguriert ist (z. B. IMAP4), überprüft der Bitdefender Spam-Schutz-Filter diese nicht auf Spam.

    Notiz
    POP3 ist eines der am meisten benutzten Protokolle für das Downloaden der E-Mail-Nachrichten vom Mail-Server. Falls Sie das Protokoll nicht kennen, das von Ihrem E-Mail Client benutzt wird, um E-Mail Nachrichten herunterzuladen, fragen Sie die Person, die Ihren E-Mail Client konfiguriert hat.

- Bitdefender Ultimate Small Business Security scannt nicht den Lotus Notws POP3-Datenverkehr.

Eine Lösung wäre es das Produkt zu reparieren oder erneut zu installieren. Falls Sie dennoch den BitDefender Support kontaktieren möchten, folgen Sie der Beschreibung wie im Abschnitt Hier wird Ihnen geholfen (Seite 305) beschrieben.

Entfernen von Bitdefender fehlgeschlagen

Wenn Sie Ihr Bitdefender-Produkt deinstallieren möchten und Sie bemerken, dass der Prozess hängen bleibt oder das System einfriert, klicken Sie auf **Abbrechen**. Sollte dies nicht zum Erfolg führen, starten Sie den Computer neu.

Falls die Deinstallation fehlschlägt, bleiben unter Umständen einige Bitdefender-Registry-Schlüssel und Dateien in Ihrem System. Solche Überbleibsel können eine erneute Installation von Bitdefender verhindern. Ebenso kann die Systemleistung und Stabilität leiden.

So können Sie Bitdefender vollständig von Ihrem System entfernen:

- In **Windows 7**:
  1. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
  2. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
  3. Klicken **ENTFERNEN** im erscheinenden Fenster.
  4. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

- In **Windows 8** Und **Windows 8.1**:
  1. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
  2. Klicken **Ein Programm deinstallieren** oder **Programme und Funktionen**.
  3. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
  4. Klicken **ENTFERNEN** im erscheinenden Fenster.
  5. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

- In **Windows 10** Und **Windows11**:
  1. Klicken **Start**, und klicken Sie dann auf Einstellungen.
  2. Drücke den **System** Symbol im Bereich Einstellungen und wählen Sie dann aus **Installierte Anwendungen**.
  3. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
  4. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.

5. Klicken **ENTFERNEN** im erscheinenden Fenster.
6. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

Mein System fährt nach der Installation von Bitdefender nicht mehr hoch

Wenn Sie Bitdefender gerade installiert haben und Ihr System nicht mehr im Normalmodus starten können, kann es verschiedene Ursachen für dieses Problem geben.

Höchstwahrscheinlich wird es durch eine vorherige Bitdefender-Installation hervorgerufen, die nicht vollständig entfernt wurde. Eine weitere Möglichkeit ist eine andere Sicherheitslösung, die noch auf dem System installiert ist.

Im Folgenden finden Sie Herangehensweisen für die verschiedenen Situationen:

- **Sie hatten Bitdefender schon einmal installiert und danach nicht vollständig von Ihrem System entfernt.**
  So können Sie das Problem lösen:

  1. Starten Sie Ihren Computer im abgesicherten Modus neu. Eine Anleitung hierzu finden Sie unter Wie führe ich einen Neustart im abgesicherten Modus durch? (Seite 129).
  2. Entfernen Sie Bitdefender von Ihrem System:
     - In **Windows 7**:
       a. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
       b. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.
       c. Klicken **ENTFERNEN** im erscheinenden Fenster.
       d. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.
       e. Starten Sie Ihren Computer im Normalmodus neu.
     - In **Windows 8** Und **Windows 8.1**:

a. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.

b. Klicken **Ein Programm deinstallieren** oder **Programme und Funktionen**.

c. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.

d. Klicken **ENTFERNEN** im erscheinenden Fenster.

e. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

f. Starten Sie Ihr System im normalen Modus neu.

❍ In **Windows 10** Und **Windows11**:

a. Klicken **Start**, und klicken Sie dann auf Einstellungen.

b. Drücke den **System** Symbol im Bereich Einstellungen und wählen Sie dann aus **Installierte Anwendungen**.

c. Finden **Bitdefender Ultimate Small Business Security** und auswählen **Deinstallieren**.

d. Klicken **Deinstallieren** erneut, um Ihre Auswahl zu bestätigen.

e. Klicken **ENTFERNEN** im erscheinenden Fenster.

f. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

g. Starten Sie Ihr System im normalen Modus neu.

3. Installieren Sie Ihr Bitdefender-Produkt neu.

❍ **Sie hatten zuvor eine andere Sicherheitslösung im Einsatz und haben diese nicht vollständig entfernt.**
Um dies zu lösen:

1. Starten Sie Ihr System neu und wechseln Sie in den abgesicherten Modus. Wie das geht, erfahren Sie unter Wie führe ich einen Neustart im abgesicherten Modus durch? (Seite 129).

2. Entfernen Sie die andere Sicherheitslösung von Ihrem System:
   - In **Windows 7**:
     a. Klicken **Start**, gehe zu **Schalttafel** und doppelklicken **Programme und Funktionen**.
     b. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie **Deinstallieren**.
     c. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.
   - In **Windows 8** Und **Windows 8.1**:
     a. Suchen Sie auf dem Windows-Startbildschirm **Schalttafel** (z. B. können Sie „Systemsteuerung“ direkt auf dem Startbildschirm eingeben) und dann auf das entsprechende Symbol klicken.
     b. Klicken **Ein Programm deinstallieren** oder **Programme und Funktionen**.
     c. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie es aus **Entfernen**.
     d. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.
   - In **Windows 10** Und **Windows11**:
     a. Klicken **Start**, und klicken Sie dann auf Einstellungen.
     b. Drücke den **System** Symbol im Bereich Einstellungen und wählen Sie dann aus **Installierte Anwendungen**.
     c. Suchen Sie den Namen des Programms, das Sie entfernen möchten, und wählen Sie es aus **Deinstallieren**.
     d. Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist, und starten Sie dann Ihr System neu.

   Um die andere Software vollständig zu deinstallieren, rufen Sie die Hersteller-Website auf und führen Sie das entsprechende Deinstallations-Tool aus oder wenden Sie sich direkt an den Hersteller, um eine Deinstallationsanleitung zu erhalten.

3. Starten Sie Ihr System im Normalmodus neu und installieren Sie Bitdefender erneut.

Sie haben die oben beschriebenen Schritte bereits durchgeführt und das Problem besteht weiterhin.

Um dies zu lösen:

1. Starten Sie Ihr System neu und wechseln Sie in den abgesicherten Modus. Wie das geht, erfahren Sie unter Wie führe ich einen Neustart im abgesicherten Modus durch? (Seite 129).
2. Nutzen Sie die Systemwiederherstellung von Windows, um das Gerät zu einem früheren Zeitpunkt wiederherzustellen, bevor das Bitdefender-Produkt installiert wurde.
3. Starten Sie das System im Normalmodus neu und wenden Sie sich an unsere Support-Mitarbeiter, wie in Abschnitt Hier wird Ihnen geholfen (Seite 305) beschrieben.

3.5.2. Entfernung von Bedrohungen

Bedrohungen können Ihr System auf vielfältige Art und Weise beeinträchtigen. Wie Bitdefender auf diese Malware darauf reagiert, hängt von der Art der Bedrohung ab. Da Bedrohungen ihr Verhalten ständig ändern, ist es schwierig ein Muster für ihr Verhalten und ihre Aktionen festzulegen.

Es gibt Situationen, in denen Bitdefender eine Bedrohung Ihres Systems nicht automatisch entfernen kann. In solch einem Fall ist Ihre Intervention nötig.

- Rettungsumgebung (Seite 153)
- Was ist zu tun, wenn Bitdefender Bedrohungen auf Ihrem Gerät findet? (Seite 154)
- Wie entferne ich eine Bedrohung aus einem Archiv? (Seite 155)
- Wie entferne ich eine Bedrohung aus einem E-Mail-Archiv? (Seite 156)
- Wie gehe ich vor, wenn ich eine Datei für gefährlich halte? (Seite 158)
- Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll? (Seite 158)

- Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll? (Seite 158)
- Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll? (Seite 159)
- Warum hat Bitdefender eine infizierte Datei automatisch gelöscht? (Seite 159)

Wenn Sie Ihr Problem hier nicht finden können oder die vorgestellten Lösungen es nicht lösen, können Sie sich wie in Kapitel beschrieben an die Vertreter des technischen Supports von Bitdefender wenden Hier wird Ihnen geholfen (Seite 305).

Rettungsumgebung

Die **Rettungsumgebung** ist eine Bitdefender-Funktion, mit der Sie alle bestehenden Festplattenpartitionen innerhalb und außerhalb Ihres Betriebssystems scannen und desinfizieren können.

Die Bitdefender-Rettungsumgebung ist mit Windows RE integriert.

Starten Ihres Systems in der Rettungsumgebung

Sie können den Rettungsmodus ausschließlich über Ihr Bitdefender-Produkt aufrufen. Gehen Sie dazu folgendermaßen vor:

1. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
2. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
3. Klicken Sie neben **Rettungsumgebung** auf **Öffnen**.
4. Klicken Sie im angezeigten Fenster auf **NEUSTART**.
   Die Bitdefender-Rettungsumgebung wird innerhalb weniger Augenblicke geladen.

Scannen Ihres Systems in der Rettungsumgebung

So können Sie Ihr System in der Rettungsumgebung scannen:

1. Starten Sie die Rettungsumgebung, wie beschrieben in Starten Ihres Systems in der Rettungsumgebung (Seite 153).
2. Der Bitdefender-Scan-Prozess wird automatisch gestartet, sobald das System in der Rettungsumgebung geladen wird.

3. Warten Sie, bis der Scan abgeschlossen ist. Befolgen Sie die Anweisungen, um gefundene Bedrohungen zu entfernen.
4. Klicken Sie zum Beenden der Rettungsumgebung im Fenster mit den Scan-Ergebnissen auf Schließen.

Was ist zu tun, wenn Bitdefender Bedrohungen auf Ihrem Gerät findet?

Es gibt verschiedene Möglichkeiten, wie Sie von einer Bedrohung auf Ihrem Gerät erfahren:

- Sie haben einen Scan Ihres Geräts durchgeführt und Bitdefender hat infizierte Objekte gefunden.
- Eine Bedrohungswarnung informiert Sie, dass Bitdefender einen oder mehrere Bedrohungen auf Ihrem Gerät blockiert hat.

In solchen Situationen sollten Sie Bitdefender aktualisieren, um sicherzustellen, dass Sie über die neuesten Bedrohungsinformationen verfügen und einen System-Scan durchführen, um das System zu prüfen.

Sobald der System-Scan abgeschlossen ist, wählen Sie die gewünschte Aktion für die infizierten Objekte aus (Desinfizieren, Löschen, In Quarantäne verschieben).

> **Warnung**
> Wenn Sie den Verdacht haben, dass die Datei Teil des Windows-Betriebssystems ist oder dass es sich nicht um eine infizierte Datei handelt, folgen Sie NICHT diesen Schritten und kontaktieren Sie so bald wie möglich den Bitdefender-Kundendienst.

Falls die ausgewählte Aktion nicht durchgeführt werden konnte und im Scan-Protokoll ersichtlich ist, dass Ihr PC mit einer Bedrohung infiziert ist, die nicht gelöscht werden kann, müssen Sie die Datei(en) manuell entfernen.

Die erste Methode kann im Normalmodus eingesetzt werden:

1. Deaktivieren Sie den Echtzeit-Virenschutz von Bitdefender:
   a. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
   b. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
   c. Im **Fortschrittlich** Fenster, ausschalten **Bitdefender-Schild**.

2. Zeigen Sie versteckte Objekte in Windows an. Wie das geht, erfahren Sie unter Wie kann ich in Windows versteckte Objekte anzeigen? (Seite 126).
3. Blättern Sie zum Laufwerk, in dem die infizierte Datei gespeichert ist (siehe Scan-Protokoll) und löschen Sie sie.
4. Schalten Sie den Echtzeit-Virenschutz von Bitdefender ein.

Falls die Infektion mit der ersten Methode nicht entfernt werden konnte:

1. Starten Sie Ihr System neu und wechseln Sie in den abgesicherten Modus. Wie das geht, erfahren Sie unter Wie führe ich einen Neustart im abgesicherten Modus durch? (Seite 129).
2. Zeigen Sie versteckte Objekte in Windows an. Wie das geht, erfahren Sie unter Wie kann ich in Windows versteckte Objekte anzeigen? (Seite 126).
3. Navigieren Sie zum Speicherort der infizierten Datei (überprüfen Sie das Scan-Protokoll) und löschen Sie sie.
4. Starten Sie Ihren Computer neu und starten Sie den Normalmodus.

Wenn diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten Hier wird Ihnen geholfen (Seite 305).

Wie entferne ich eine Bedrohung aus einem Archiv?

Bei einem Archiv handelt es sich um eine Datei oder eine Dateisammlung, die mit einem speziellen Format komprimiert wurde, um so den benötigten Festplattenplatz zu reduzieren.

Einige dieser Formate sind offene Formate und bieten Bitdefender die Möglichkeit, diese zu scannen und die entsprechenden Aktionen durchzuführen, um sie zu entfernen.

Andere Archivformate sind teilweise oder komplett geschlossen und Bitdefender kann nur das Vorhandensein von Bedrohungen innerhalb dieser Archive feststellen, nicht jedoch andere Aktionen ausführen.

Wenn Bitdefender Sie darüber informiert, dass eine Bedrohung innerhalb eines Archivs gefunden wurde und keine Aktion verfügbar ist, bedeutet dies, dass die Bedrohung aufgrund möglicher Restriktionen der Zugriffseinstellungen des Archivs nicht entfernt werden kann.

So können Sie eine in einem Archiv gespeicherte Bedrohung entfernen.

1. Führen Sie einen System-Scan durch, um das Archiv zu finden, in dem sich die Bedrohung befindet.
2. Deaktivieren Sie den Echtzeit-Virenschutz von Bitdefender:
   a. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
   b. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
   c. Im **Fortschrittlich** Fenster, ausschalten **Bitdefender-Schild**.
3. Gehen Sie zum Speicherort des Archivs und dekomprimieren Sie es mit einem Archivierungsprogramm wie beispielsweise WinZip.
4. Identifizieren Sie die infizierte Datei und löschen Sie sie.
5. Löschen Sie das Originalarchiv, um sicherzugehen, dass die Infizierung vollständig entfernt ist.
6. Komprimieren Sie die Dateien erneut in einem neuen Verzeichnis und verwenden Sie dafür ein Komprimierprogramm wie WinZip.
7. Aktivieren Sie den Bitdefender-Echtzeit-Virenschutz und führen Sie einen System-Scan durch, um so sicherzustellen, dass Ihr System nicht anderweitig infiziert ist.

> **Notiz**
> Es ist wichtig zu beachten, dass eine in einem Archiv gespeicherte Bedrohung für Ihr System keine unmittelbare Bedrohung darstellt, da die Bedrohung dekomprimiert und ausgeführt werden muss, bevor sie Ihr System infizieren kann.

Wenn diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten Hier wird Ihnen geholfen (Seite 305).

Wie entferne ich eine Bedrohung aus einem E-Mail-Archiv?

Bitdefender kann auch Bedrohungen in E-Mail-Datenbanken und auf Festplatten gespeicherten E-Mail-Archiven aufspüren.

Manchmal ist es notwendig, die infizierte Nachricht über die im Scan-Bericht zur Verfügung gestellten Informationen zu identifizieren und sie dann manuell zu löschen.

So können Sie in einem E-Mail-Archiv gespeicherte Bedrohungen entfernen:

1. Scannen Sie die E-Mail-Datenbank mit Bitdefender.
2. Deaktivieren Sie den Echtzeit-Virenschutz von Bitdefender:
   a. Klicken **Schutz** im Navigationsmenü auf der Bitdefender-Oberfläche.
   b. Im **Virenschutz** Bereich, klicken Sie auf **Offen**.
   c. Im **Fortschrittlich** Fenster, ausschalten **Bitdefender-Schild**.
3. Öffnen Sie den Scan-Bericht und nutzen Sie die Identifikationsinformation (Betreff, Von, An) der infizierten Nachricht, um den dazugehörigen E-Mail-Client zu finden.
4. Löschen Sie die infizierte Nachricht. Die meisten E-Mail-Clients verschieben gelöschte Nachrichten in ein Wiederherstellungsordner, von dem aus sie wiederhergestellt werden können. Sie sollten sicherstellen, dass die Nachricht auch aus diesem Recovery-Verzeichnis gelöscht ist.
5. Komprimieren Sie das Verzeichnis, in dem die infizierte Nachricht gespeichert wird.
   - In Microsoft Outlook 2007: Klicken Sie im Dateimenü auf "Datendateiverwaltung". Markieren Sie die persönlichen Ordner (.pst), die Sie komprimieren möchten, und klicken Sie auf "Einstellungen". Klicken Sie auf "Jetzt komprimieren".
   - In Microsoft Outlook 2010 / 2013/ 2016: Klicken Sie im Dateimenü auf "Info" und dann "Kontoeinstellungen" (Konten hinzufügen oder entfernen bzw. vorhandene Verbindungseinstellungen ändern). Klicken Sie danach auf "Datendatei", markieren Sie die persönlichen Ordner (.pst), die Sie komprimieren wollen, und klicken Sie auf "Einstellungen". Klicken Sie auf "Jetzt komprimieren".
6. Schalten Sie den Echtzeit-Virenschutz von Bitdefender ein.

Wenn diese Informationen nicht hilfreich waren, können Sie sich wie im Abschnitt beschrieben an Bitdefender wenden, um Support zu erhalten Hier wird Ihnen geholfen (Seite 305).

Wie gehe ich vor, wenn ich eine Datei für gefährlich halte?

Möglicherweise halten Sie eine Datei auf Ihrem System für gefährlich, obwohl Ihr Bitdefender-Produkt keine Gefahr erkannt hat.

So können Sie sicherstellen, dass Ihr System geschützt ist:

1. Führen Sie einen **System-Scan** mit Bitdefender durch. Eine Anleitung hierzu finden Sie unter How do I scan my system? .
2. Wenn der Scan ein sauberes Ergebnis liefert, Sie aber weiterhin Zweifel an der Sicherheit der Datei hegen und ganz sicher gehen möchten, wenden Sie sich bitte an unsere Support-Mitarbeiter, damit wir Ihnen helfen können.
   Eine Anleitung hierzu finden Sie unter Hier wird Ihnen geholfen (Seite 305).

Wobei handelt es sich bei den passwortgeschützten Dateien im Scan-Protokoll?

Dies ist nur eine Benachrichtigung, dass die von Bitdefender gefundenen Dateien entweder passwortgeschützt oder anderweitig verschlüsselt sind.

Am häufigsten sind passwortgeschützte Objekte:

- Dateien, die zu einer anderen Sicherheitslösung gehören.
- Dateien, die zum Betriebssystem gehören.

Um die Inhalte tatsächlich zu scannen, müssen diese Dateien entweder extrahiert oder anderweitig entschlüsselt werden.

Sollten diese Inhalte extrahiert werden, wird der Echtzeit-Scanner von Bitdefender diese automatisch scannen, um so den Schutz Ihres Geräts zu gewährleisten. Wenn Sie diese Dateien mit Bitdefender scannen möchten, müssen Sie den Produkthersteller kontaktieren, um nähere Details zu diesen Dateien zu erhalten.

Unsere Empfehlung ist, diese Dateien zu ignorieren, da Sie für Ihr System keine Bedrohung darstellen.

Wobei handelt es sich bei den übersprungenen Objekten im Scan-Protokoll?

Alle Dateien, die im Scan-Protokoll als "Übersprungen" ausgewiesen werden, sind sauber.

Für eine bessere Leistung scannt Bitdefender keine Dateien, die seit dem letzten Scan nicht verändert wurden.

Wobei handelt es sich bei den zu stark komprimierten Dateien im Scan-Protokoll?

Die zu stark komprimierten Objekte sind Elemente, die durch die Scan-Engine nicht extrahiert werden konnten oder Elemente, für die eine Entschlüsselung zu viel Zeit in Anspruch genommen hätte und die dadurch das System instabil machen würden.

Überkomprimiert bedeutet, dass Bitdefender das Scannen von Archiven übersprungen hat, da das Entpacken dieser zu viele Systemressourcen in Anspruch genommen hätte. Der Inhalt wird, wenn nötig, in Echtzeit gescannt.

Warum hat Bitdefender eine infizierte Datei automatisch gelöscht?

Wird eine infizierte Datei gefunden, versucht Bitdefender automatisch, diese zu desinfizieren. Falls die Desinfizierung fehlschlägt, wird die Datei in die Quarantäne verschoben, um dort die Infizierung einzudämmen.

Bei bestimmten Arten von Bedrohungen ist eine Desinfektion nicht möglich, da die erkannte Datei vollständig bösartig ist. In solchen Fällen wird die infizierte Datei von der Festplatte gelöscht.

Dies geschieht normalerweise bei Installationsdateien, die von nicht vertrauenswürdigen Seiten heruntergeladen werden. Wenn Sie auf ein solches Problem stoßen, laden Sie die Installationsdatei von der Website des Herstellers oder einer anderen vertrauenswürdigen Website herunter.

4. VIRENSCHUTZ FÜR MAC

4.1. Was ist Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac ist ein leistungsstarker Virenscanner, der alle Arten von Schad-Software („Bedrohungen“) erkennen und entfernen kann:

- Ransomware
- Adware
- Viren
- Spyware
- Trojaner
- Keylogger
- Computerwürmer

Diese App erkennt und entfernt nicht nur Mac-spezifische, sondern auch Windows-spezifische Bedrohungen und verhindert so, dass Sie infizierte Dateien versehentlich an die PCs Ihrer Familie, Freunde und Kollegen weiterleiten.

4.2. Installation und Deinstallation

Dieses Kapital beinhaltet die folgenden Themen:

- Systemanforderungen (Seite 160)
- Bitdefender Antivirus for Mac wird installiert (Seite 161)
- Bitdefender Antivirus for Mac deinstallieren (Seite 165)

4.2.1. Systemanforderungen

Sie können Bitdefender Antivirus for Mac auf Macintosh-Computern mit OS X Yosemite (10.10) oder höher installieren.

Sie benötigen auf Ihrem Mac zudem mindestens 1 GB verfügbaren Speicherplatz auf der Festplatte.

Für die Registrierung und Updates von Bitdefender Antivirus for Mac ist eine aktive Internetverbindung notwendig.

Notiz

Bitdefender Anti-Tracker und Bitdefender VPN können nur auf Systemen ab macOS 10.12 installiert werden.

So finden Sie heraus, welche macOS-Version und Hardware Sie nutzen

Klicken Sie auf das Apple-Symbol oben linken und wählen Sie **Über diesen Mac**. Daraufhin wird ein Fenster angezeigt, dem Sie die Version Ihres Betriebssystems und andere nützliche Informationen entnehmen können. Klicken Sie auf **Systembericht**, um detaillierte Hardwareinformationen zu erhalten.

4.2.2. Bitdefender Antivirus for Mac wird installiert

Gehen Sie wie folgt vor, um die Bitdefender Antivirus for Mac-App über Ihr Bitdefender-Konto zu installieren:

1. Als Administrator anmelden.
2. Gehen Sie zu: https://central.bitdefender.com.
3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Bitdefender-Konto an.
4. Rufen Sie den Bereich **Meine Geräte** auf und klicken Sie auf **SCHUTZ INSTALLIEREN**.
5. Wählen Sie eine der beiden verfügbaren Optionen:

   - **Dieses Gerät schützen**

     a. Wählen Sie diese Option und danach den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.

     b. Speichern Sie die Installationsdatei.

   - **Andere Geräte schützen**

     a. Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.

     b. Klicken Sie auf **DOWNLOAD LINK SENDEN**.

     c. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **E-MAIL VERSENDEN**.

Bitte beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Nach Ablauf des Links müssen Sie einen neuen Link generieren. Führen Sie dazu die bereits beschriebenen Schritte erneut aus.

d. Rufen Sie auf dem Gerät, auf dem Bitdefender installiert werden soll, das angegebene E-Mail-Konto auf und klicken Sie in der E-Mail auf die Download-Schaltfläche.

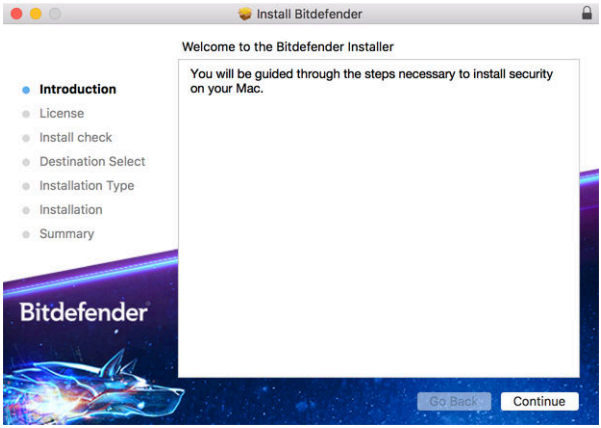
6. Führen Sie das von Ihnen heruntergeladene Bitdefender aus.
7. Führen Sie die Installationsschritte durch.

Installationsvorgang

So können Sie Bitdefender Antivirus for Mac installieren:

1. Klicken Sie auf die heruntergeladene Datei. Der Installationsassistent wird geöffnet und führt Sie durch den Installationsvorgang.
2. Folgen Sie den Anweisungen des Installationsassistenten.

Schritt 1 - Willkommensfenster



Klicken Sie auf **Fortfahren**.

Schritt 2 - Lesen Sie die Abonnementvereinbarung

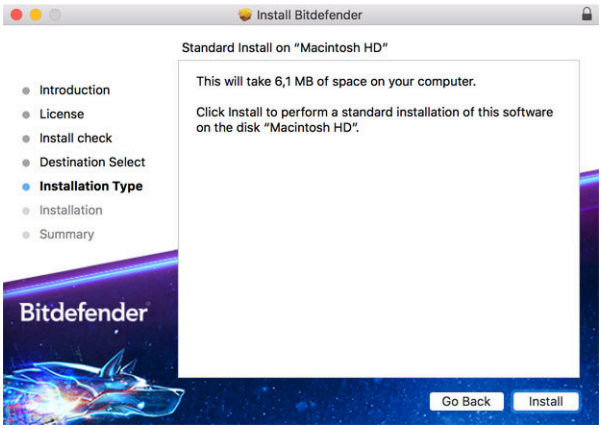
Bevor Sie mit der Installation fortfahren, müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Antivirus for Mac nutzen dürfen.

In diesem Fenster können Sie auch die Sprache auswählen, in der Sie das Produkt installieren möchten.

Klicken Sie auf **Weiter** und danach auf **Zustimmen**.

> **Wichtig**
> Falls Sie die Nutzungsbedingungen nicht akzeptieren möchten, klicken Sie auf **Weiter** und dann auf **Nicht zustimmen**. Der Installationsvorgang wird dann abgebrochen und der Installationsassistent geschlossen.

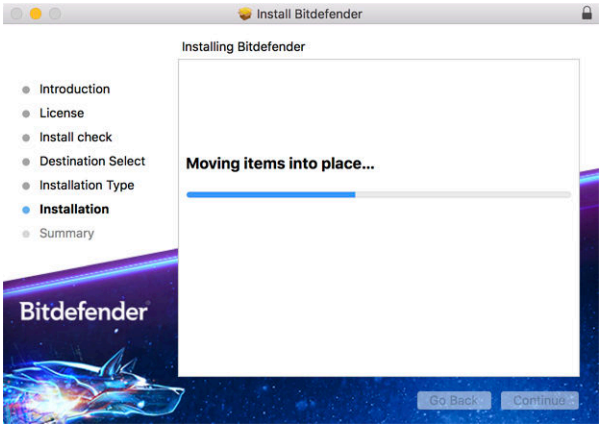
Schritt 3 - Installation starten



Die Installation von Bitdefender Antivirus for Mac erfolgt im Verzeichnis Macintosh HD/Library/Bitdefender . Diesen Installationspfad können Sie nicht ändern.

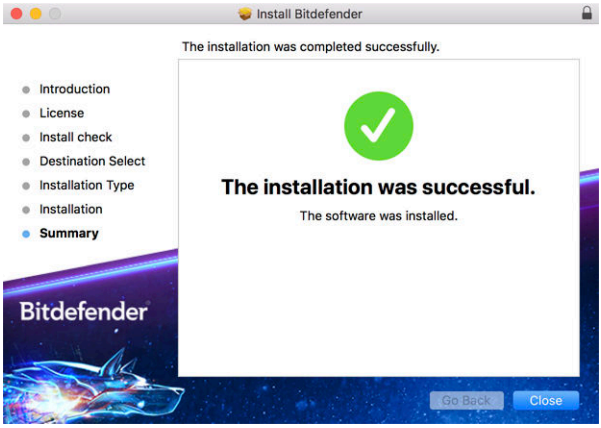
Klicken Sie auf **Installieren**, um die Installation zu starten.

Schritt 4 - Bitdefender Antivirus for Mac installieren



Warten Sie, bis die Installation abgeschlossen ist und klicken Sie auf **Weiter**.

Schritt 5 - Fertigstellung



Klicken Sie auf **Schließen**, um das Installationsfenster zu schließen.

Damit ist der Installationsvorgang abgeschlossen.

Wichtig

- Wenn Sie Bitdefender Antivirus for Mac unter macOS High Sierra 10.13.0 oder einer neueren Version installieren, erscheint die Benachrichtigung **Systemerweiterung blockiert**. Diese Benachrichtigung informiert Sie darüber, dass die von Bitdefender signierten Erweiterungen blockiert wurden und manuell aktiviert werden müssen. Klicken Sie auf OK, um fortzufahren. Klicken Sie in dem von Bitdefender Antivirus for Mac angezeigten Fenster auf den Link **Sicherheit & Datenschutz**. Klicken Sie unten im Fenster auf **Zulassen** oder wählen Sie die Bitdefender SRL aus der Liste und klicken Sie dann auf **OK**.
- Wenn Sie Bitdefender Antivirus for Mac unter macOS Mojave 10.14 oder einer neueren Version installieren, erscheint ein neues Fenster, das Sie darüber informiert, dass Sie **Bitdefender vollständigen Festplattenzugriff gewähren** und **Bitdefender das Laden erlauben** müssen. Folgen Sie den Anweisungen auf dem Bildschirm, um das Produkt ordnungsgemäß zu konfigurieren.

4.2.3. Bitdefender Antivirus for Mac deinstallieren

Bitdefender Antivirus for Mac ist eine komplexe Anwendung und kann nicht auf herkömmliche Weise deinstalliert werden, indem das Symbol

für die Anwendung aus dem Verzeichnis **Anwendungen** in den Papierkorb gezogen wird.

Gehen Sie wie folgt vor, um Bitdefender Antivirus for Mac zu entfernen:

1. Öffnen Sie **Finder** und wählen Sie den **Programme**-Ordner.
2. Öffnen Sie den Bitdefender-Ordner unter Anwendungen und doppelklicken Sie dann auf **BitdefenderUninstaller**.
3. Select the preferred uninstall option.

   Hinweis
   Wenn Sie nur die Bitdefender VPN-App entfernen möchten, klicken Sie **VPN deinstallieren**.

4. Klicken Sie auf **Deinstallieren**, und warten Sie, bis der Vorgang abgeschlossen ist.
5. Klicken Sie zum Abschluss auf **Schließen**.

   Wichtig
   Ist ein Fehler aufgetreten, so können Sie die Kundenbetreuung von Bitdefender wie in Hier wird Ihnen geholfen (Seite 305) beschrieben, kontaktieren.

4.3. Erste Schritte

Dieses Kapitel enthält die folgenden Themen:

4.3.1. Bitdefender Antivirus for Mac öffnen

Sie können Bitdefender Antivirus for Mac auf verschiedene Weisen öffnen.

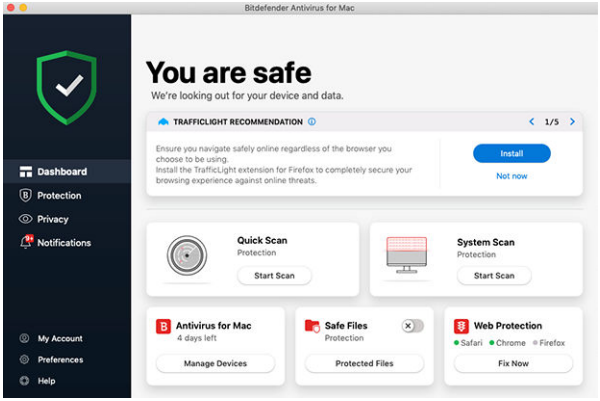
- Klicken Sie im Launchpad auf das "Bitdefender Antivirus for Mac"-Symbol.

- Klicken Sie auf das Symbol in der Menüleiste und wählen Sie **Benutzeroberfläche öffnen**.
- Öffnen Sie ein Finder-Fenster, wählen Sie Anwendungen und doppelklicken Sie auf das **Bitdefender Antivirus for Mac**-Symbol.

> **Wichtig**
> Wenn Sie Bitdefender Antivirus for Mac zum ersten Mal unter macOS Mojave 10.14 oder einer neueren Betriebssystemversion öffnen, wird eine Sicherheitsempfehlung angezeigt. Der Grund dafür ist, dass unsere Software bestimmte Berechtigungen benötigt, um Ihr System vollständig scannen zu können. Um diese Berechtigungen zu erteilen, müssen Sie als Administrator angemeldet sein. Gehen Sie dazu wie folgt vor:
>
> 1. Klicken Sie auf den Link **Systemeinstellungen**.
> 2. Klicken Sie auf das -Symbol und geben Sie dann Ihre Administratoranmeldeinformationen ein.
> 3. Ein neues Fenster wird geöffnet. Ziehen Sie die Datei **BDLDaemon** mit der Maus auf die Liste der zugelassenen Apps.

4.3.2. Das Hauptfenster

Bitdefender Antivirus for Mac entspricht den Bedürfnissen sowohl von Profis als auch von Beginnern. Die grafische Benutzeroberfläche ist so konzipiert, dass Sie für jeden Benutzer anpassbar ist.



Oben links wird ein Assistent eingeblendet, der Sie durch die Elemente der Bitdefender-Oberfläche leitet und Ihnen bei der Konfiguration zur Seite steht. Klicken Sie auf die Spitze Klammer rechts, um dem Assistenten weiter zu folgen, oder **Einführung überspringen**, um den Assistenten zu schließen.

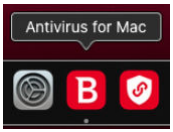
Die Statusleiste oben im Fenster informiert Sie mit eindeutigen Meldungen und aussagekräftigen Farben über den Sicherheitsstatus des Systems. Wenn Bitdefender Antivirus for Mac keine Warnmeldungen für Sie hat, bleibt die Statusleiste grün. Wenn ein Sicherheitsproblem erkannt wurde, ändert die Statusleiste ihre Farbe zu rot. Detaillierte Informationen zu Problemen und deren Behebung finden Sie unter Alle beheben (Seite 182).

Um einen wirksamen Betrieb und noch besseren Schutz bei Ihren verschiedenen Aktivitäten sicherzustellen, fungiert der **Bitdefender Autopilot** als Ihr persönlicher Sicherheitsberater. Je nachdem, was Sie gerade machen - egal, ob Sie arbeiten oder gerade Online-Zahlungen durchführen - der Bitdefender Autopilot liefert Ihnen kontextabhängige Empfehlungen, die sich an Ihrer Gerätenutzung und an Ihren Anforderungen orientieren. So lernen Sie alle Vorteile der Funktionen in Ihrer Bitdefender Antivirus for Mac-App kennen und können umfassend davon profitieren.

Über das Navigationsmenü links können Sie die Bitdefender-Abschnitte für die detaillierte Konfiguration und erweiterte Verwaltungsaufgaben (in den Reitern **Schutz** und **Privatsphäre**), Benachrichtigungen, Ihr **Bitdefender-Benutzerkonto** und den Bereich **Einstellungen** aufrufen. Außerdem können Sie sich mit uns in Verbindung setzen (im Reiter **Hilfe**), falls Sie Fragen haben oder unerwartete Probleme auftreten.

4.3.3. Dock-Symbol der App

Das Bitdefender Antivirus for Mac-Symbol wird im Dock angezeigt, sobald Sie die Anwendung öffnen. Über das Symbol im Dock können Sie Dateien und Ordner ganz einfach auf Bedrohungen scannen. Ziehen Sie einfach die Datei oder den Ordner auf das Dock-Symbol und der Scan wird sofort gestartet.



4.3.4. Navigationsmenü

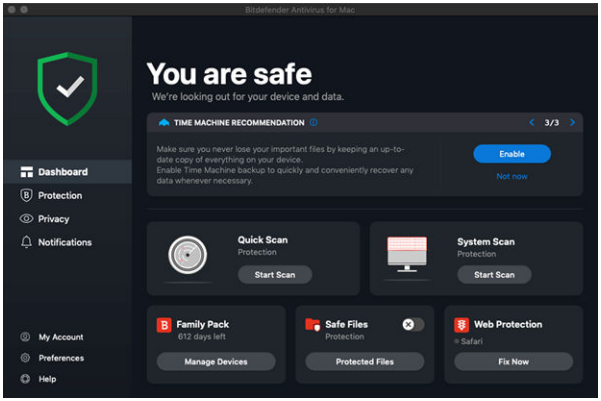
Auf der linken Seite der Bitdefender-Oberfläche finden Sie das Navigationsmenü mit Schnellzugriff auf alle Bitdefender-Funktionen, die Sie für den Umgang mit Ihrem Produkt benötigen. In diesem Bereich gibt es die folgenden Reiter:

- **Dashboard**. Von hier aus können Sie Sicherheitsprobleme schnell beheben, von Ihren Systemanforderungen und Nutzungsverhalten abgeleitete Empfehlungen anzeigen, Schnellaktionen ausführen und Ihr Bitdefender-Konto aufrufen, um die Geräte zu verwalten, die Sie Ihrem Bitdefender-Abonnement hinzugefügt haben.
- **Schuz**. Von hier aus können Sie Virenschutz-Scans starten, Dateien zur Ausnahmeliste hinzufügen, Dateien und Anwendungen vor Ransomware-Angriffen schützen, Ihre Time Machine-Backups sichern und den Schutz beim Surfen im Internet konfigurieren.
- **Privatsphäre**. Von hier aus können Sie die Bitdefender VPN-App öffnen und die Anti-Tracker-Erweiterung in Ihrem Webbrowser installieren.
- **Benachrichtigungen**. Hier finden Sie Details zu den Aktionen, die für gescannte Dateien durchgeführt wurden.
- **Mein Konto**. Hier finden Sie das Bitdefender-Konto und das Abonnement, über die Ihr Gerät geschützt ist. Hier können Sie bei Bedarf auch Ihr Konto wechseln.
- **Einstellungen**. Hier können Sie die Bitdefender-Einstellungen konfigurieren.
- **Hilfe**. Wenn Sie Unterstützung beim Umgang mit Ihrem Bitdefender-Produkt benötigen, können Sie sich von hier aus an den technischen Support wenden. Von hier aus können Sie uns zudem Ihr Feedback schicken, um uns bei der Verbesserung des Produkts zu helfen.

4.3.5. Dark Mode

Um Ihre Augen bei Nachtarbeiten oder in einer lichtarmen Umgebung vor Blendung und Licht zu schützen, unterstützt Bitdefender Antivirus for Mac den Dark Mode für Mojave 10.14 und höher. Die Farben der Benutzeroberfläche wurden so optimiert, dass Sie Ihren Mac verwenden

können, ohne Ihre Augen anzustrengen. Die Bitdefender Antivirus for Mac-Benutzeroberfläche passt sich an die Darstellungseinstellungen Ihres Geräts an.



4.4. Schutz gegen Bösartige Software

Dieses Kapitel enthält die folgenden Themen:

- Empfohlene Vorgehensweisen (Seite 171)
- Ihren Mac scannen (Seite 171)
- Scan-Assistent (Seite 173)
- Quarantäne (Seite 173)
- Bitdefender Shield (Echtzeitschutz) (Seite 174)
- Scan-Ausnahmen (Seite 175)
- Internet-Schutz (Seite 176)
- Anti-Tracker (Seite 177)
- Safe Files (Seite 180)
- Time-Machine-Schutz (Seite 182)
- Alle beheben (Seite 182)
- Benachrichtigungen (Seite 184)
- Updates (Seite 185)

4.4.1. Empfohlene Vorgehensweisen

Um Ihr System vor Bedrohungen zu schützen und eine versehentliche Infizierung anderer Systeme zu verhindern, sollten Sie folgende Empfehlungen beachten:

- Lassen Sie **Bitdefender Shield** aktiviert, damit Systemdateien automatisch von Bitdefender Antivirus for Mac gescannt werden können.
- Halten Sie Ihr Bitdefender Antivirus for Mac-Produkt mit den neusten Bedrohungsinformationen und Produktupdates immer aktuell.
- Überprüfen und beheben Sie die von Bitdefender Antivirus for Mac aufgelisteten Probleme regelmäßig. Detaillierte Informationen finden Sie im Kapitel Alle beheben (Seite 182).
- Im detaillierten Ereignisprotokoll finden Sie alle Aktionen, die Bitdefender Antivirus for Mac auf Ihrem Computer durchgeführt hat. Alle Ereignisse, die sich auf Ihr System oder Ihre Daten auswirken, werden als neue Nachricht in den Bitdefender-Benachrichtigungen angezeigt. Weitere Details finden Sie unter Benachrichtigungen (Seite 184).
- Darüber hinaus sollten Sie folgende Empfehlungen berücksichtigen:
  - Sie sollten grundsätzlich alle Dateien scannen, die Sie von externen Speichern (z.B. USB-Sticks oder CDs) herunterladen, insbesondere wenn Ihnen die Quelle nicht bekannt ist.
  - Bei DMG-Dateien sollten diese zunächst gemountet und dann ihr Inhalt (die Dateien im gemounteten Volume/Image) gescannt werden.

  Sie können Dateien, Ordner oder Volumes ganz einfach scannen, indem Sie sie per Drag & Drop auf das Anwendungsfenster oder das Dock-Symbol von Bitdefender Antivirus for Mac ziehen.

Es sind keine weitere Konfigurationen oder Aktionen erforderlich. Sie können jedoch bei Bedarf Anpassungen an den Einstellungen vornehmen. Weitere Informationen finden Sie im Kapitel Präferenzen konfigurieren (Seite 186).

4.4.2. Ihren Mac scannen

Die **Bitdefender Shield**-Funktion überwacht alle installierten Anwendungen auf Aktionen, die auf Bedrohungen hindeuten, und

verhindert, dass neue Bedrohungen auf Ihr System gelangen. Darüber hinaus können Sie Ihren Mac oder einzelne Dateien jederzeit nach Bedarf scannen.

Sie können Dateien, Ordner oder Volumes ganz einfach scannen, indem Sie sie per Drag & Drop auf das Anwendungsfenster oder das Dock-Symbol von Bitdefender Antivirus for Mac ziehen. Daraufhin wird der Scan-Assistent angezeigt, um Sie durch den Scan-Vorgang zu führen.

Sie können einen Scan wie folgt starten:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Schutz**.
2. Wechseln Sie zum Reiter **Virenschutz**.
3. Klicken Sie auf einen der drei Scan-Schaltflächen, um den gewünschten Scan zu starten.
   - **Quick Scan** - überprüft die sensibelsten Verzeichnisse Ihres Systems (beispielsweise die Verzeichnisse mit Dokumenten, Downloads, Mail-Downloads und temporären Dateien eines Benutzers) auf Bedrohungen.
   - **System-Scan** - durchsucht das gesamte System eingehend nach möglichen Bedrohungen. Alle eingebundenen Dateisysteme werden ebenfalls gescannt.

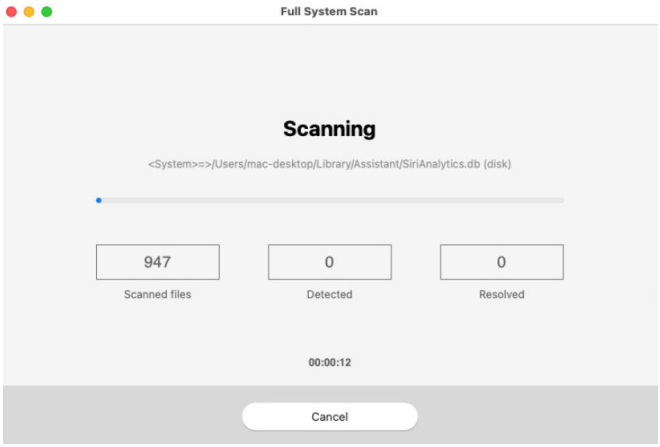
     > **Hinweis**
     > Je nach Größe Ihrer Festplatte kann ein vollständiger System-Scan einige Zeit in Anspruch nehmen (bis zu einer Stunde und mehr). Um die Systemleistung nicht zu beeinträchtigen, sollte diese Aufgabe nicht zeitgleich mit anderen ressourcenintensiven (z.B. Videobearbeitung) Aufgaben ausgeführt werden.
     >
     > Falls gewünscht, können Sie bestimmte Laufwerke vom Scan ausschließen, indem Sie sie in im Fenster Schutz zur Liste der **Ausnahmen** hinzufügen.

   - **Benutzerdefinierter Scan** - hiermit können einzelne Dateien, Verzeichnisse etc. auf Bedrohungen geprüft werden.

Sie können über das Dashboard auch einen System-Scan oder einen Quick Scan starten.

4.4.3. Scan-Assistent

Sobald Sie einen Scan starten, öffnet sich der Bitdefender Antivirus for Mac-Scan-Assistent.



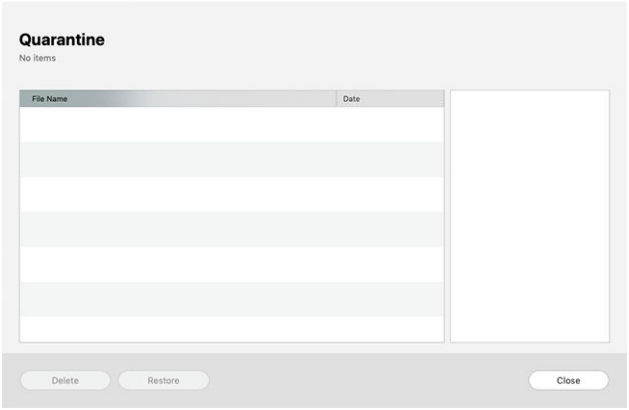
Während eines Scans werden Informationen zu gefundenen und behobenen Bedrohungen in Echtzeit angezeigt.

Warten Sie bis Bitdefender Antivirus for Mac den Prüfvorgang beendet hat.

> **Hinweis**
> Der Scan-Vorgang kann, abhängig von der Größe Ihrer Festplatte, eine Weile dauern.

4.4.4. Quarantäne

Mit Bitdefender Antivirus for Mac können infizierte oder verdächtige Dateien in einem sicheren Bereich, der Quarantäne, isoliert werden. Bedrohungen in Quarantäne können keinen Schaden anrichten, da sie dort nicht geöffnet oder ausgeführt werden können.



Der Bereich Quarantäne zeigt alle Dateien an, die sich zur Zeit im Quarantäne-Ordner befinden.

Um eine Datei aus der Quarantäne zu löschen, markieren Sie diese und klicken Sie dann auf **Löschen**. Wenn Sie eine Quarantäne-Datei am ursprünglichen Speicherort wiederherstellen möchten, klicken Sie zuerst auf die Datei und dann auf **Wiederherstellen**.

So können Sie eine Liste mit allen zur Quarantäne hinzugefügten Objekten anzeigen:

1. Klicken **Schutz** im Navigationsmenü der Bitdefender-Benutzeroberfläche.
2. Klicken Sie im Bereich **Quarantäne** auf **Öffnen**.

4.4.5. Bitdefender Shield (Echtzeitschutz)

Bitdefender bietet Ihnen Echtzeitschutz vor einer Vielzahl an Bedrohungen, indem es alle installierten Apps und ihre jeweiligen Updates sowie alle neuen und veränderten Dateien scannt.

So können Sie den Echtzeitschutz deaktivieren:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Einstellungen**.
2. Deaktivieren Sie **Bitdefender Shield** im Fenster **Schutz**.

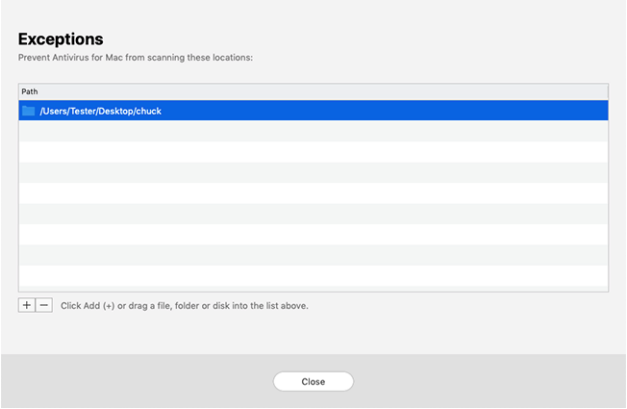
Warnung

Hierbei handelt es sich um ein grobes Sicherheitsrisiko. Wir empfehlen den Echtzeitschutz so kurz wie möglich zu deaktivieren. Während der Echtzeitschutz deaktiviert ist, sind Sie nicht vor Bedrohungen geschützt.

4.4.6. Scan-Ausnahmen

Wenn Sei möchten können Sie Bitdefender Antivirus for Mac so einstellen, dass spezielle Dateien, Ordner oder auch ein ganzer Datenträger, nicht gescannt werden. Zum Beispiel könnten Sie vom Scannen ausschließen:

- Dateien die fälschlicherweise als infiziert identifiziert wurden (bekannt als "false positives")
- Dateien die Scanfehler verursachen
- Backup-Laufwerke



In der Ausnahmeliste sind alle Pfade aufgeführt, die vom Scan ausgenommen wurden.

So können Sie die Ausnahmeliste aufrufen:

1. Klicken **Schutz** im Navigationsmenü der Bitdefender-Benutzeroberfläche.
2. Klicken Sie im Bereich **Ausnahmen** auf **Öffnen**.

Es gibt zwei Wege um eine Scan-Ausnahme einzurichten:

- Fügen Sie Dateien, Ordner oder Volumes per Drag & Drop zur Ausnahmeliste hinzu.
- Klicken Sie auf das Pluszeichen (+) unterhalb der Ausnahmeliste. Wählen Sie danach die Datei, den Ordner oder das Laufwerk, das vom Scan ausgeschlossen werden soll.

Um eine Scan-Ausnahme zu entfernen, wählen Sie den entsprechenden Eintrag aus der Liste aus und klicken Sie auf das Minuszeichen (-) unterhalb der Ausnahmeliste.

4.4.7. Internet-Schutz

Bitdefender Antivirus for Mac nutzt die Linkchecker-Erweiterungen, um Ihnen sicheres Surfen im Internet zu ermöglichen. Die Linkchecker-Erweiterungen lesen, verarbeiten und filtern den gesamten Datenverkehr und blockieren dabei schädlichen Inhalte.

Die Erweiterungen lassen sich in die folgenden Browser integrieren: Mozilla Firefox, Google Chrome and Safari.

Aktivieren der TrafficLight-Erweiterungen

So können Sie die TrafficLight-Erweiterungen aktivieren:

1. Klicken Sie in der **Internet-Schutz**-Kachel im Dashboard auf **Jetzt lösen**.
2. Das Fenster **Internet-Schutz** wird geöffnet.
   Der auf Ihrem System installierte Browser wird erkannt und angezeigt. Klicken Sie zur Installation der TrafficLight-Erweiterung in Ihrem Browser auf **Erweiterung herunterladen**.
3. Sie werden umgeleitet auf:
   https://www.bitdefender.com/solutions/trafficlight.html
4. Wählen Sie **Kostenloser Download**.
5. Folgen Sie den Anweisungen, um die TrafficLight-Erweiterung für Ihren Browser zu installieren.

Verwalten von Erweiterungseinstellungen

Ihnen steht eine große Auswahl an Funktionen zur Verfügung, die Sie vor allen möglichen Bedrohungen im Internet schützen. Sie können sie

aufrufen, indem Sie auf das TrafficLight-Symbol neben Ihren Browser-Einstellungen und danach auf **Einstellungen**-Schaltfläche klicken:

- **Bitdefender TrafficLight-Einstellungen**
  - Internet-Schutz - Verhindert, dass Sie Websites aufrufen, die zur Verbreitung von Malware sowie von Phishing- und Betrugsversuchen eingesetzt werden.
  - Suchberater - Warnt Sie schon in Ihren Suchergebnissen vor gefährlichen Websites.

- **Ausnahmen**
  Wenn Sie die Website, die Sie zu den Ausnahmen hinzufügen möchten, bereits aufgerufen haben, klicken Sie auf **Aktuelle Website zur Liste hinzufügen**.
  Wenn Sie eine weitere Website hinzufügen möchten, geben Sie deren Adresse in das entsprechende Feld ein und klicken Sie auf .
  Es wird keine Warnmeldung mehr angezeigt, auch wenn von den ausgenommenen Seiten eine Bedrohung ausgeht. Sie sollten dieser Liste nur Website hinzufügen, denen Sie uneingeschränkt vertrauen.

Seitenbewertung und Warnungen

Abhängig von der Linkchecker-Einstufung für die Webseite, die sie gerade besuchen, wird eines der folgenden Symbole in diesem Bereich eingeblendet:

Diese Seite ist sicher und kann aufgerufen werden. Sie können Ihre Arbeit fortsetzen.

Diese Webseite könnte gefährliche Inhalte haben. Lassen Sie Vorsicht walten, wenn Sie sie dennoch aufrufen möchten.

Sie sollten die Webseite sofort verlassen, da sie Malware oder andere Bedrohungen enthält.

In Safari sind die TrafficLight-Symbole schwarz hinterlegt.

4.4.8. Anti-Tracker

Viele der von Ihnen aufgerufenen Websites verwenden Tracker, um Informationen über Ihr Surf-Verhalten zu sammeln, entweder um sie mit anderen Unternehmen zu teilen oder um Werbeanzeigen einzublenden,

die für Sie relevanter sind. Website-Betreiber verwenden die hierdurch erzielten Einnahmen, um Ihnen kostenlose Inhalte anzubieten oder den eigenen Betrieb aufrechtzuerhalten. Das Sammeln dieser Informationen kann sich auch auf Ihre Surf-Geschwindigkeit auswirken und übermäßig Bandbreite in Anspruch nehmen.

Durch Aktivierung der Bitdefender Anti-Tracker-Erweiterung in Ihrem Browser verhindern Sie Tracking, sodass Ihre Daten während des Surfens im Netz privat bleiben. Darüber hinaus können Websites schneller geladen werden.

Die Bitdefender-Erweiterung ist mit den folgenden Web-Browsern kompatibel:

- Google Chrome
- Mozilla Firefox
- Safari

Die von uns erkannten Tracker sind in die folgenden Kategorien unterteilt:

- **Werbung** - Dient der Analyse von Website-Verkehr, von Nutzerverhalten oder von Datenverkehrsmustern von Website-Besuchern.
- **Kundeninteraktion** - Dient der Messung der Benutzerinteraktion mit verschiedenen Eingabemöglichkeiten wie Chat oder Support.
- **Wesentlich** - Dient der Überwachung kritischer Webseiten-Funktionen.
- **Site Analytics** - Dient der Sammlung von Daten über die Nutzung von Webseiten.
- **Social Media** - Dient der Überwachung von Social-Media-Zielgruppen sowie der Aktivitäten und Nutzerbindung über verschiedene Social-Media-Plattformen.

Aktivieren von Bitdefender Anti-Tracker

So können Sie die Bitdefender Anti-Tracker-Erweiterung in Ihrem Browser aktivieren:

1. Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Privatsphäre**.
2. Wechseln Sie zum Reiter **Anti-tracker**.

3. Klicken Sie neben dem Browser, für den Sie die Erweiterung aktivieren möchten, auf **Erweiterung aktivieren**.

Anti-Tracker-Benutzeroberfläche

Nach Aktivierung der Bitdefender Anti-Tracker-Erweiterung erscheint das Symbol neben der Suchleiste in Ihrem Webbrowser. Jedes Mal, wenn Sie eine Website besuchen, wird auf dem Symbol ein Zähler angezeigt, der Aufschluss über erkannte und blockierte Tracker gibt. Um weitere Details zu den blockierten Trackern anzuzeigen, klicken Sie auf das Symbol, um die Benutzeroberfläche zu öffnen. Neben der Anzahl der blockierten Tracker können Sie die Ladezeit der Seite und die Kategorien der erkannten Tracker einsehen. Klicken Sie auf die gewünschte Kategorie, um die Liste der Websites anzuzeigen, die Sie tracken.

Um Bitdefender davon abzuhalten, Tracker auf der aktuell von Ihnen besuchten Website zu blockieren, klicken Sie auf **Schutz für diese Website anhalten**. Diese Einstellung gilt nur, solange die Website geöffnet ist und wird beim Schließen der Website in den Ausgangszustand zurückgesetzt.

Um Trackern aus einer bestimmten Kategorie die Überwachung Ihrer Aktivität zu erlauben, klicken Sie auf die gewünschte Aktivität, und klicken Sie dann auf die entsprechende Schaltfläche. Klicken Sie erneut auf die gleiche Schaltfläche, falls Sie Ihre Meinung ändern.

Deaktivieren von Bitdefender Anti-Tracker

So können Sie die Bitdefender Anti-Tracker-Erweiterung in Ihrem Browser deaktivieren:

1. Öffnen Sie Ihren Internet-Browser.
2. Klicken Sie auf das -Symbol neben der Adressleiste in Ihrem Webbrowser.
3. Klicken Sie oben rechts auf das -Symbol.
4. Verwenden Sie zum Deaktivieren den entsprechenden Schalter.
   Das Bitdefender-Symbol wird grau.

Erlauben von Tracking auf einer Website

Wenn Sie beim Besuch einer bestimmten Website das Tracking erlauben möchten, können Sie die entsprechende Adresse wie folgt zu den Ausnahmen hinzufügen:

1. Öffnen Sie Ihren Webbrowser.
2. Klicken Sie auf das -Symbol neben der Suchleiste.
3. Drücke den Symbol in der oberen rechten Ecke.
4. Wenn Sie sich auf der Website befinden, die Sie zu Ausnahmen hinzufügen möchten, klicken Sie auf **Aktuelle Website zur Liste hinzufügen**.
   Wenn Sie eine weitere Website hinzufügen möchten, geben Sie deren Adresse in das entsprechende Feld ein und klicken Sie dann auf .

4.4.9. Safe Files

Bei Ransomware handelt es sich um Schadsoftware, die anfällige Systeme infiziert und den Zugriff darauf sperrt. Von den Benutzern wird dann für die Freigabe ihrer Daten ein Lösegeld erpresst. Diese Schadsoftware geht intelligent vor und zeigt Benutzern gefälschte Warnmeldungen an, um sie in Angst zu versetzen und sie dazu zu bringen, das geforderte Geld zu zahlen.

Durch den Einsatz neuester Technologien stellt Bitdefender die Integrität des Systems sicher. Kritische Systembereiche werden vor Ransomware-Angriffen geschützt, ohne dabei das System zu beeinträchtigen. Um zu verhindern, dass nicht vertrauenswürdige Anwendungen auf Ihre Dokumente, Fotos oder Videos zugreifen, bietet Ihnen Bitdefender Safe Files Ihnen die Möglichkeit, Ihre persönlichen Dateien in einem geschützten Umfeld abzulegen und selbst festzulegen, welche Apps autorisiert sind, Änderungen an diesen geschützten Dateien vorzunehmen.

So können Sie auch zu einem späteren Zeitpunkt weitere Dateien zur geschützten Umgebung hinzufügen:

1. Klicken **Schutz** im Navigationsmenü der Bitdefender-Benutzeroberfläche.
2. Wechseln Sie zum Reiter **Ransomware-Schutz**.

3. Klicken Sie im Bereich Sichere Dateien auf **Geschützte Dateien**.
4. Klicken Sie auf das Pluszeichen (+) unterhalb der Liste mit den geschützten Dateien. Wählen Sie danach die Datei, den Ordner oder das Laufwerk aus, das Sie vor dem Zugriff durch Ransomware schützen möchten.

Um Systembeeinträchtigungen zu vermeiden, sollten Sie nicht mehr als 30 Ordner hinzufügen oder mehrere Dateien in einem Ordner speichern.

Die Ordner Bilder, Dokumente, Desktop und Downloads werden standardmäßig vor Angriffen geschützt.

> **Hinweis**
> Benutzerdefinierte Ordner können nur für aktuelle Benutzer geschützt werden. Externe Laufwerke sowie System- und Anwendungsdateien können der Schutzumgebung nicht hinzugefügt werden.

Sie werden informiert, sobald eine unbekannte Anwendung mit ungewöhnlichen Verhalten versucht, die von Ihnen hinzugefügten Dateien zu verändern. Klicken Sie auf **Zulassen** oder **Blockieren**, um sie zur Liste der **verwalteten Anwendungen** hinzuzufügen.

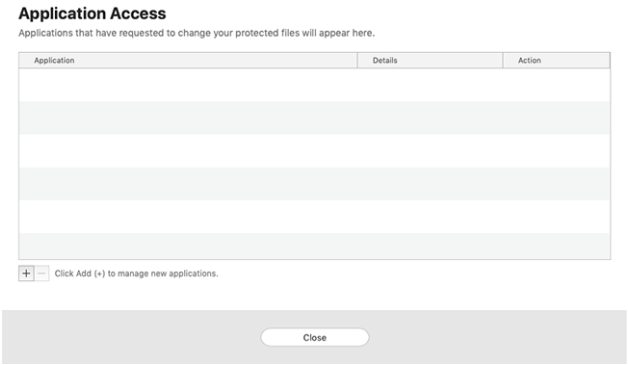
Anwendungszugriff

Anwendungen, die versuchen, geschützte Dateien zu verändern oder zu löschen, können als potenziell unsicher markiert und zur Liste der blockierten Anwendungen hinzugefügt werden. Falls eine solche Anwendung blockiert wurde und Sie sich sicher sind, dass ihr Verhalten normal ist, können Sie ihre Ausführung wie folgt zulassen:

1. Klicken **Schutz** im Navigationsmenü der Bitdefender-Benutzeroberfläche.
2. Wähle aus **Anti-Ransomware** Tab.
3. Klicken Sie im Bereich Sichere Dateien auf **Anwendungszugriff**.
4. Ändern Sie den Status neben der blockierten App auf Erlauben.

Ebenso können Sie den Status zugelassener Anwendungen auf blockiert setzen.

Nutzen Sie Drag&Drop oder klicken Sie auf das Pluszeichen (+), um weitere Apps zur Liste hinzuzufügen.



4.4.10. Time-Machine-Schutz

Der Bitdefender Time Machine Protection bietet zusätzliche Sicherheit für Ihr Backup-Laufwerk und alle darauf gespeicherten Dateien, indem es den Zugriff durch externe Quellen verhindert. Werden Dateien in Ihrem Time-Machine-Laufwerk von Ransomware verschlüsselt, können Sie sie auch ohne Lösegeldzahlung wiederherstellen.

Falls Sie Objekte aus einer Time-Machine-Sicherung wiederherstellen müssen, finden Sie die entsprechende Anleitung auf der Apple-Support-Seite.

Aktivierung und Deaktivierung des Time-Machine-Schutzes

So können Sie den Time-Machine-Schutz aktivieren oder deaktivieren:

1. Klicken Sie im Navigationsmenü der **Bitdefender-Benutzeroberfläche** auf **Schutz**.
2. Wähle aus **Anti-Ransomware** Tab.
3. Aktivieren oder deaktivieren Sie den Schalter **Time-Machine-Schutz**.

4.4.11. Alle beheben

Bitdefender Antivirus for Mac spürt automatisch mögliche Probleme, die die Sicherheit Ihres Systems beeinflussen können, auf und informiert Sie. So können Sicherheitsrisiken einfach und frühzeitig behoben werden.

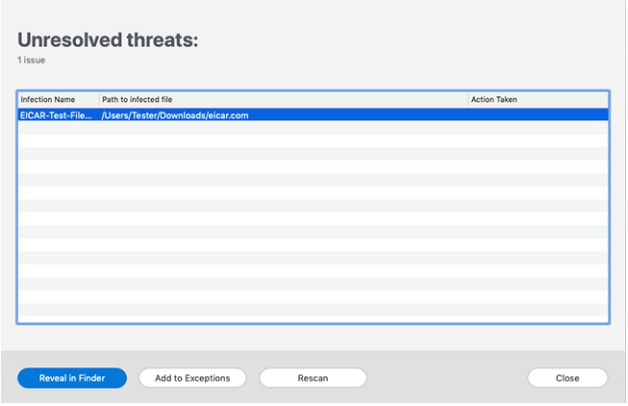
Beheben Sie die in Bitdefender Antivirus for Mac angezeigten Probleme, um schnell und einfach den optimalen Schutz für Ihr System und Ihre Daten sicherzustellen.

Zu den erkannten Problemen gehören:

- Das neueste Update der Bedrohungsinformationen wurde nicht von unserer Servern heruntergeladen.
- Auf Ihrem System wurden Bedrohungen gefunden, die das Produkt nicht automatisch beheben kann.
- Der Echtzeitschutz ist deaktiviert.

Um erkannte Probleme zu überprüfen und zu beheben:

1. Liegen keine Warnungen in Bitdefender vor, ist die Statusleiste grün. Wird ein Sicherheitsproblem gefunden, wechselt die Farbe der Statusleiste zu rot.
2. Überprüfen Sie die Beschreibung für weitere Informationen.
3. Wird ein Problem erkannt, können Sie mit einem Klick auf die entsprechende Schaltfläche Gegenmaßnahmen einleiten.



Die Liste der nicht behobenen Bedrohungen wird nach jedem System-Scan aktualisiert. Dies geschieht unabhängig davon, ob der Scan automatisch im Hintergrund durchgeführt oder von Ihnen angestoßen wurde.

Für nicht beseitigte Bedrohungen sind die folgenden Aktionen verfügbar:

- **Manuell löschen**. Führen Sie diese Aktion aus, um Infektionen manuell zu entfernen.
- **Zu den Ausnahmen hinzufügen**. Diese Aktion ist nicht für Bedrohungen verfügbar, die in Archiven gefunden werden.

4.4.12. Benachrichtigungen

Bitdefender führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer. Für jedes Ereignis, das die Sicherheit Ihres Systems oder Ihrer Daten betrifft, wird in den Bitdefender-Benachrichtigungen eine Nachricht erstellt, ähnlich einer neuen E-Mail in Ihrem Postfach.

Benachrichtigungen sind ein wichtiges Hilfsmittel für die Überwachung und Verwaltung Ihres Bitdefender-Schutzes. So können Sie z. B. überprüfen, ob ein Update erfolgreich durchgeführt wurde oder ob Bedrohungen oder Schwachstellen im System gefunden wurden. Zudem können Sie bei Bedarf weitere Aktionen ausführen oder die von Bitdefender ausgeführten Aktionen anpassen.

Klicken Sie im Navigationsmenü der Bitdefender-Benutzeroberfläche auf **Benachrichtigungen**, um auf das Benachrichtigungsprotokoll zuzugreifen. Bei jedem kritischen Ereignis wird auf dem 2-Symbol ein Zähler eingeblendet.

Je nach Art und Schwere werden Benachrichtigungen sortiert nach:

- **Kritisch** Diese Ereignisse weisen auf kritische Probleme hin. Sie sollten sich umgehend darum kümmern.
- **Warnung** Diese Ereignisse weisen auf nicht-kritische Probleme hin. Sie sollten sich darum kümmern, wenn Sie Zeit dafür haben.
- **Information** Diese Ereignisse weisen auf erfolgreich ausgeführte Vorgänge hin.

Mit einem Klick auf den jeweiligen Reiter erhalten Sie weitere Informationen zu den Ereignissen. Mit einem einfachen Klick auf den Ereignisnamen werden die folgenden Kurzinfos angezeigt: Kurzbeschreibung, die von Bitdefender durchgeführte Aktion sowie Datum und Zeitpunkt des Ereignisses. Unter Umständen werden Ihnen Optionen zur weiteren Vorgehensweise angeboten.

Zur übersichtlicheren Verwaltung der protokollierten Ereignisse enthält das Benachrichtigungsfenster Optionen, mit denen Sie alle Ereignisse in einem Abschnitt löschen oder als gelesen markieren können.

4.4.13. Updates

Jeden Tag werden neue Bedrohungen entdeckt und identifiziert. Deshalb ist es so wichtig, Bitdefender Antivirus for Mac über Updates ständig auf dem neuesten Stand zu halten.

Die Aktualisierung der Bedrohungsinformationen wird „on the fly“ durchgeführt. Das bedeutet, dass die zu aktualisierenden Dateien schrittweise ersetzt werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System zu keiner Zeit gefährdet.

- Wenn Bitdefender Antivirus for Mac up-to-date ist, spürt die Software die neuesten Threats auf und heilt infizierte Dateien.
- Wenn Bitdefender Antivirus für Mac nicht auf dem neuesten Stand ist, kann es die neuesten von Bitdefender Labs entdeckten Bedrohungen nicht erkennen und entfernen.

Benutzergesteuertes Update

Ein manuelles Update können Sie jederzeit durchführen.

Für regelmäßige Updates und Downloads ist eine aktive Internetverbindung nötig.

Führen Sie folgende Schritte für ein manuelles Update durch:

1. Klicken Sie auf die Schaltfläche **Aktionen** in der Menüleiste.
2. Wählen Sie **Update der Bedrohungsinformationen**.

Alternativ können Sie ein Update auch manuell anfordern, indem Sie CMD + U drücken.

Der Update-Fortschritt und die downgeloadeten Dateien werden eingeblendet.

Updates über einen Proxy Server

Bitdefender Antivirus for Mac kann nur über Proxy-Server aktualisiert werden, bei denen keine Authentifizierung erforderlich ist. Sie müssen dafür keine Programmeinstellungen konfigurieren.

Wenn Ihre Internetverbindung über einen Proxy-Server läuft, der eine Autorisierung verlangt, müssen Sie regelmäßig zu einer direkten Internetverbindung wechseln, um die neuesten Bedrohungsinformationen herunterladen zu können.

Upgrade auf eine neue Version durchführen

Von Zeit zu Zeit veröffentlichen wir Produkt-Updates, die neue Funktionen bringen oder bestimmte Aspekte der Software verbessern oder Probleme beheben. Bei diesen Updates kann es notwendig werden, das System neu zu starten, um die Installation neuer Dateien zu ermöglichen. Falls ein Update einen Neustart erforderlich macht, wird Bitdefender Antivirus for Mac standardmäßig bis zum Neustart des Systems die bereits vorhandenen Dateien nutzen. So beeinträchtigt der Aktualisierungsprozess den Benutzer nicht bei seiner Arbeit.

Ein Pop-up-Fenster fordert Sie auf das System neu zu starten, sobald das Update abgeschlossen wurde. Fall Sie diese Benachrichtigung verpassen, können Sie das System manuell neu starten oder in der Menüleiste auf **Für das Upgrade neu starten** klicken.

Suche nach Informationen über Bitdefender Antivirus for Mac

Informationen zur installierten Bitdefender Antivirus for Mac-Version finden Sie im Bereich **Info über**. Hier können Sie die Abonnementvereinbarung sowie die Datenschutzerklärung aufrufen und lesen sowie die Open-Source-Lizenzen anzeigen.

So rufen Sie das Fenster „Info über“ auf:

1. Öffnen Sie Bitdefender Antivirus for Mac.
2. Klicken Sie in der Menüleiste auf Bitdefender Antivirus for Mac und wählen Sie **Über Antivirus for Mac**.

4.5. Präferenzen konfigurieren

Dieses Kapitel enthält die folgenden Themen:

4.5.1. Zugriff auf Präferenzen

Um das Präferenzen-Fenster von Bitdefender Antivirus for Mac zu öffnen:

- Wählen Sie eine der folgenden Methoden:
  - Klicken **Einstellungen** im Navigationsmenü der Bitdefender-Benutzeroberfläche.
  - Klicken Sie in der Menüleiste auf Bitdefender Antivirus for Mac und wählen Sie **Präferenzen**.

4.5.2. Schutzeinstellungen

Über das Schutzeinstellungsfenster können Sie den gesamten Scan-Vorgang konfigurieren. Sie können die Aktionen, die bei infizierten oder verdächtigen Dateien vorgenommen werden sollen oder auch allgemeine Einstellungen konfigurieren.

- **Bitdefender Shield.** Bitdefender Shield bietet Echtzeitschutz vor einer Vielzahl von Bedrohungen, indem es alle installierten Anwendungen, ihre aktualisierten Versionen sowie neue und geänderte Dateien scannt. Wir raten davon ab, Bitdefender Shield zu deaktivieren. Wenn Sie es dennoch deaktivieren müssen, sollten Sie dies nicht länger als absolut notwendig tun. Wenn Bitdefender Shield deaktiviert ist, sind Sie nicht vor Bedrohungen geschützt.
- **Nur neue und veränderte Dateien scannen.** Aktivieren Sie dieses Kästchen, wenn Bitdefender Antivirus for Mac nur Dateien prüfen soll, die vorher noch nicht geprüft wurden oder seit dem letzten Scan verändert wurden.

  Sie können festlegen, dass diese Einstellung für benutzerdefinierte und Drag-&-Drop-Scans nicht angewandt wird, indem Sie das entsprechende Kästchen deaktivieren.
- **Backup-Inhalte nicht scannen.** Aktivieren Sie dieses Kästchen, um Backup-Dateien vom Scan auszuschließen. Wenn infizierte Dateien zu einem späteren Zeitpunkt wiederhergestellt werden, wird Bitdefender Antivirus for Mac sie automatisch erkennen und die entsprechenden Maßnahmen ergreifen.

4.5.3. Erweiterte Einstellungen

Sie können eine übergeordnete Aktion auswählen, die für alle Probleme und verdächtige Objekte, die während eines Scan-Vorgangs gefunden werden, durchgeführt werden soll.

Vorgehen bei infizierten Objekten

- **Versuchen, zu desinfizieren oder in die Quarantäne zu verschieben** - Wenn infizierte Dateien gefunden werden, versucht Bitdefender, sie zu desinfizieren (den Schadcode zu entfernen) oder sie in die Quarantäne zu verschieben.
- **Keine Aktion durchführen** - Es werden keine Aktionen für die gefundenen Dateien durchgeführt.

Vorgehen bei verdächtigen Objekten

- **Dateien in Quarantäne verschieben** - Wenn verdächtige Dateien gefunden werden, verschiebt Bitdefender sie in die Quarantäne.
- **Keine Aktion durchführen** - Für die erkannten Dateien wird keine Aktion ausgeführt.

4.5.4. Sonderangebote

Sind Sonderangebote verfügbar, wird das Bitdefender-Produkt Sie per Pop-up-Benachrichtigung darüber informieren. So können Sie von unseren Vorteilspreisen profitieren und Ihre Geräte länger schützen.

So können Sie Benachrichtigungen über Sonderangebote aktivieren oder deaktivieren:

1. Klicken **Einstellungen** im Navigationsmenü der Bitdefender-Benutzeroberfläche.
2. Wechseln Sie zum Reiter **Sonstige**.
3. Aktivieren oder deaktivieren Sie den Schalter **Meine Angebote**.

> **Hinweis**
> Die Option **Meine Angebote** ist standardmäßig aktiviert.

4.6. Häufig gestellte Fragen

Wie kann ich Bitdefender Antivirus for Mac testen, bevor ich mich für ein Abonnement entscheide?

Sie sind ein neuer Bitdefender-Kunde und möchten unser Produkt testen, bevor Sie es kaufen. Der Testzeitraum beträgt 30 Tage. Nach Ablauf dieser Frist können Sie das Produkt nur weiterverwenden, wenn Sie ein Bitdefender-Abonnement erwerben. So erhalten Sie die Bitdefender Antivirus for Mac-Testversion:

1. Erstellen Sie ein Bitdefender-Konto wie folgt:
   a. Gehe zu: https://central.bitdefender.com.
   b. Geben Sie die Daten in die entsprechenden Felder ein. Die hier eingetragenen Daten werden vertraulich behandelt.
   c. Bevor Sie fortfahren können, müssen Sie zunächst den Nutzungsbedingungen zustimmen. Rufen Sie die Nutzungsbedingungen auf und lesen Sie sie aufmerksam durch, da Sie hier die Bedingungen zur Nutzung von Bitdefender finden.
      Darüber hinaus können Sie auch die Datenschutzrichtlinie aufrufen und lesen.
   d. Klicken Sie auf **BENUTZERKONTO ERSTELLEN**.

2. Laden Sie Bitdefender Antivirus for Mac wie folgt herunter:
   a. Wähle aus **Meine Geräte** Panel, und klicken Sie dann auf **SCHUTZ INSTALLIEREN**.
   b. Wählen Sie eine der beiden verfügbaren Optionen:
      - **Schützen Sie dieses Gerät**
        i. Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
        ii. Speichern Sie die Installationsdatei.
      - **Schützen Sie andere Geräte**
        i. Wählen Sie diese Option und dann den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, klicken Sie auf die entsprechende Schaltfläche.
        ii. Klicken **DOWNLOADLINK SENDEN**.
        iii. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und klicken Sie auf **E-MAIL SENDEN**.

Beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Wenn der Link abläuft, müssen Sie einen neuen generieren, indem Sie die gleichen Schritte ausführen.

iv. Überprüfen Sie auf dem Gerät, auf dem Sie Ihr Bitdefender-Produkt installieren möchten, das E-Mail-Konto, das Sie eingegeben haben, und klicken Sie dann auf die entsprechende Download-Schaltfläche.

c. Führen Sie das heruntergeladene Bitdefender-Produkt aus.

Ich habe einen Aktivierungscode. Wie verlängere ich damit die Laufzeit meines Abonnements?

Wenn Sie einen Aktivierungscode von einem unserer Reseller erworben oder geschenkt bekommen haben, können Sie die Verfügbarkeit zu Ihrem Bitdefender-Abonnement hinzufügen.

Gehen Sie folgendermaßen vor, um ein Abonnement mit einem Aktivierungscode zu aktivieren:

1. Zugang Bitdefender Central.
2. Wähle aus **Meine Abonnements** Tafel.
3. Drücke den **AKTIVIERUNGSCODE** Schaltfläche und geben Sie dann den Code in das entsprechende Feld ein.
4. Klicken **AKTIVIEREN SIE** weitermachen.

Die Erweiterung wird jetzt in Ihrem Bitdefender-Konto sowie im rechten unteren Bereich der Oberfläche Ihres installierten Bitdefender Antivirus for Mac-Produkts angezeigt.

Das Scan-Protokoll zeigt noch nicht gelöste Probleme an. Wie kann ich diese beheben?

Mögliche noch nicht gelöste Probleme im Scan-Protokoll sind zum Beispiel:

- Archive mit eingeschränktem Zugriff (xar, rar usw.)
  Lösung: Lokalisieren Sie die Datei über die Option **Im Finder anzeigen** und löschen Sie sie von Hand. Vergessen Sie dabei nicht, den Papierkorb zu leeren.

- Postfächer mit eingeschränktem Zugriff (Thunderbird usw.)
  Lösung: Entfernen Sie den Eintrag mit der infizierten Datei mithilfe der Anwendung.
- Backup-Inhalte
  Lösung: Aktivieren Sie in den Schutz-Einstellungen die Option **Backup-Inhalte nicht scannen** oder schließen Sie die gefundenen Dateien mit **Zu den Ausnahmen hinzufügen** vom Scan aus.
  Werden infizierte Dateien zu einem späteren Zeitpunkt wiederhergestellt, erkennt Bitdefender Antivirus for Mac diese automatisch und leitet geeignete Maßnahmen ein.

> **Hinweis**
> Dateien mit beschränktem Zugriff sind Dateien, die Bitdefender Antivirus for Mac zwar öffnen, aber nicht bearbeiten kann.

Wo kann ich detaillierte Informationen zu den Produktaktivitäten einsehen?

Bitdefender führt ein Protokoll über alle wichtigen Aktionen, Statusänderungen und andere kritische Nachrichten über die eigenen Aktivitäten. Um auf diese Informationen zuzugreifen, klicken Sie im Navigationsmenü der Bitdefender-Oberfläche auf **Benachrichtigungen**.

Kann ich Bitdefender Antivirus for Mac über einen Proxy-Server aktualisieren?

Bitdefender Antivirus for Mac kann nur über Proxy-Server aktualisieren, die keine Authentifizierung erfordern. Sie müssen keine Programmeinstellungen konfigurieren.

Wenn Sie sich über einen Proxyserver mit dem Internet verbinden, der eine Authentifizierung erfordert, müssen Sie regelmäßig zu einer direkten Internetverbindung wechseln, um Aktualisierungen der Bedrohungsinformationen zu erhalten.

Wie kann ich Bitdefender Antivirus for Mac entfernen?

Gehen Sie folgendermaßen vor, um Bitdefender Antivirus for Mac zu entfernen:

1. Öffnen Sie **Finder** und wählen Sie den Programme-Ordner.
2. Öffnen Sie den Bitdefender-Ordner und doppelklicken Sie auf BitdefenderUninstaller.

3. Klicken **Deinstallieren** und warten Sie, bis der Vorgang abgeschlossen ist.
4. Klicken **Schließen** beenden.

> **Wichtig**
> Wenn ein Fehler auftritt, können Sie sich wie in beschrieben an den Bitdefender-Kundendienst wenden Hier wird Ihnen geholfen (Seite 305).

Wie entferne ich die Linkchecker-Erweiterungen aus meinem Browser?

- So können Sie die TrafficLight-Erweiterungen aus Mozilla Firefox entfernen:
  1. Gehen Sie zu **Tools** und wählen Sie **Add-ons**.
  2. Klicken Sie in der Spalte links auf **Erweiterungen**.
  3. Wählen Sie die Erweiterung aus und klicken Sie auf **Entfernen**.
  4. Starten Sie den Browser neu, um den Entfernungsvorgang abzuschließen.

- So können Sie die TrafficLight-Erweiterung aus Google Chrome entfernen:
  1. Klicken Sie oben rechts auf **Mehr** ⋮.
  2. Gehen Sie zu **Weitere Tools** und wählen Sie **Erweiterungen**.
  3. Klicken Sie auf das **Entfernen** -Symbol neben der Erweiterung, die Sie entfernen möchten.
  4. Klicken Sie auf **Entfernen**, um den Entfernungsvorgang zu bestätigen.

- So können Sie Bitdefender TrafficLight aus Safari entfernen:
  1. Rufen Sie die **Einstellungen** auf oder nutzen Sie die Tastenkombination **Befehl-Komma(,)**.
  2. Wählen Sie **Erweiterungen**.
     Eine Liste mit allen installierten Erweiterungen wird angezeigt.
  3. Wählen Sie die Bitdefender TrafficLight-Erweiterung aus und klicken Sie auf **Deinstallieren**.

4. Klicken Sie erneut auf **Deinstallieren**, um den Deinstallationsvorgang zu bestätigen.

Wann sollte ich Bitdefender VPN verwenden?

Bei Aufrufen, Herunterladen oder Hochladen von Inhalten im Internet sollten Sie stets Vorsicht walten lassen. Um sicherzustellen, dass Sie beim Surfen im Netz jederzeit geschützt sind, empfehlen wie den Einsatz von Bitdefender VPN, wenn Sie:

- Verbindungen zu öffentlichen WLAN-Netzwerken herstellen möchten
- auf Inhalte zugreifen möchten, die regionalen Zugangsbeschränkungen unterliegen, egal ob Sie zuhause oder im Ausland sind
- Ihre persönlichen Daten vor Zugriff schützen möchten (Benutzernamen, Passwörter, Kreditkartendaten etc.)
- Ihre IP-Adresse verbergen möchten

Wirkt sich Bitdefender VPN auf die Akkulaufzeit meines Gerätes aus?

Bitdefender VPN wurde entwickelt, um Ihre persönlichen Daten zu schützen, Ihre IP-Adresse bei Verbindungen mit ungesicherten WLAN-Netzwerken zu verbergen und Ihnen den Zugriff auf Inhalte mit länderspezifischen Zugangsbeschränkungen zu ermöglichen. Um Ihren Akku zu entlasten, empfehlen wir, das VPN nur bei Bedarf zu nutzen und die Verbindung danach wieder zu trennen.

Warum wird meine Internetverbindung langsamer, wenn ich eine Verbindung mit Bitdefender VPN herstelle?

Bitdefender VPN ist auf einen ressourcenschonenden Betrieb beim Surfen im Netz ausgelegt. Ihre Internetverbindung bzw. die Entfernung zum Server, mit dem Sie eine Verbindung hergestellt haben, können sich jedoch negativ auf die Verbindungsgeschwindigkeit auswirken. Wenn es nicht unbedingt notwendig ist, dass Sie sich von Ihrem Standort aus mit einem weit entfernten Server verbinden (z. B. von Deutschland aus nach China), sollten Sie in solchen Fällen Bitdefender VPN erlauben, automatisch eine Verbindung mit dem nächstgelegenen Server herzustellen bzw. einen Server zu finden, der näher an Ihrem Standort liegt.

5. MOBILE SICHERHEIT FÜR ANDROID

5.1. Was ist Bitdefender Mobile Security?

Über das Internet kann man schnell und bequem Rechnungen bezahlen, Urlaube buchen sowie Waren und Dienstleistungen erwerben. Die verstärkte Nutzung dieser Online-Dienste geht jedoch auch mit hohen Risiken einher. Ohne die entsprechenden Sicherheitsvorkehrungen können personenbezogene Daten schnell in die falschen Hände gelangen. Was ist also wichtiger, als der Schutz der Daten, die in unseren Online-Konten und Smartphones zu finden sind?

Mit **Bitdefender Mobile Security** können Sie:

- Ihr Android-Smartphone und -Tablet mit minimalen Auswirkungen auf die Akkulaufzeit optimal schützen
- sich vor Handybetrug mit gefährlichen Links schützen
- unser sicheres VPN für schnelles, anonymes und sorgenfreies Surfen im Netz nutzen
- Im Falle von Diebstahl oder Verlust können Sie Ihr Android-Gerät jederzeit per Fernzugriff orten, sperren oder sämtliche Daten löschen
- überprüfen, ob Ihr E-Mail-Konto von Datenpannen oder Datenlecks betroffen ist

5.2. Erste Schritte

5.2.1. Systemanforderungen

Bitdefender Mobile Security läuft auf allen Geräten ab Android 5.0. Für Bedrohungs-Scans über die Cloud wird eine aktive Internet-Verbindung benötigt.

5.2.2. So installieren Sie Bitdefender Mobile Security

- **Über Bitdefender Central**
  - Android
    1. Gehen Sie zu: https://central.bitdefender.com.

2. Melden Sie sich bei Ihrem Bitdefender-Konto an.
3. Rufen Sie den Bereich **Meine Geräte** auf.
4. Tippen Sie auf **SCHUTZ INSTALLIEREN** und dann auf **Dieses Gerät schützen**.
5. Wählen Sie den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, tippen Sie auf die entsprechende Schaltfläche.
6. Sie werden zur **Google Play**-App weitergeleitet. Tippen Sie in Google Play auf Installieren.

- Unter Windows, macOS und iOS
  1. Gehe zu: https://central.bitdefender.com.
  2. Melden Sie sich bei Ihrem Bitdefender-Konto an.
  3. Wähle aus **Meine Geräte** Tafel.
  4. Tippen Sie auf **SCHUTZ INSTALLIEREN** und dann auf **Andere Geräte schützen**.
  5. Wählen Sie den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, drücken Sie auf die entsprechende Schaltfläche.
  6. Tippen Sie auf **DOWNLOAD LINK SENDEN**.
  7. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und tippen Sie auf **E-MAIL VERSENDEN**. Bitte beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Nach Ablauf des Links müssen Sie einen neuen Link generieren. Führen Sie dazu die bereits beschriebenen Schritte erneut aus.
  8. Rufen Sie auf dem Gerät, auf dem Bitdefender installiert werden soll, das angegebene E-Mail-Konto auf und tippen Sie in der E-Mail auf die Download-Schaltfläche.

- **Über Google Play**
  Suchen Sie nach Bitdefender Mobile Security, um die App aufzurufen und zu installieren.
  Sie können auch den QR-Code einscannen:

Bevor Sie die Bestätigungsschritte abschließen können, müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Mobile Security nutzen dürfen.

Tippen Sie auf **Fortfahren**, um zum nächsten Fenster zu gelangen.

5.2.3. Melden Sie sich bei Ihrem Bitdefender-Konto an

Zur Verwendung von Bitdefender Mobile Security müssen Sie Ihr Gerät mit einem Bitdefender-, Facebook-, Google-, Apple- oder Microsoft-Konto verknüpfen, indem Sie sich über die App bei Ihrem Konto anmelden. Beim ersten Öffnen der App werden Sie zur Anmeldung bei einem Benutzerkonto aufgefordert.

Wenn Sie Bitdefender Mobile Security über Ihr Bitdefender-Konto installiert haben, wird die App versuchen, sich automatisch bei diesem Konto anzumelden.

So verknüpfen Sie Ihr Gerät mit einem Bitdefender-Konto:

1. Geben Sie die E-Mail-Adresse und das Passwort für Ihr Bitdefender-Konto in die entsprechenden Felder ein. Falls Sie noch kein Bitdefender-Konto haben und jetzt eines anlegen möchten, klicken Sie auf den entsprechenden Link.
2. Tippen Sie auf **ANMELDEN**.

Tippen Sie zur Anmeldung mit einem Facebook-, Google- oder Microsoft-Konto im Bereich Oder melded Sie sich an über auf den entsprechenden Dienst. Sie werden zur Anmeldeseite des ausgewählten Dienstes weitergeleitet. Befolgen Sie die Anweisungen zur Verknüpfung Ihres Benutzerkontos mit Bitdefender Mobile Security.

Notiz

Bitdefender hat keinen Zugriff auf Ihre vertraulichen Informationen, so zum Beispiel das Passwort, das Sie zur Anmeldung in Ihrem Konto verwenden, oder die persönlichen Informationen Ihrer Freunde und Kontakte.

5.2.4. Den Schutz konfigurieren

Nach der erfolgreichen Anmeldung in der App wird das Fenster Schutz konfigurieren angezeigt. Um Ihr Gerät zu schützen, sollten Sie die folgende Anleitung befolgen:

- **Abonnementstatus**. Um mit Bitdefender Mobile Security umfassend geschützt zu sein, müssen Sie Ihr Produkt zunächst mit einem Abonnement aktivieren. Dieses legt fest, wie lange Sie das Produkt nutzen können. Nach Ablauf des Abonnements wird die App nicht mehr funktionieren und Ihr Gerät nicht mehr schützen.

  Wenn Sie einen Aktivierungscode haben, tippen Sie auf **ICH HABE EINEN CODE** und danach auf **AKTIVIEREN**.

  Falls Sie sich mit einem neuen Bitdefender-Benutzerkonto angemeldet haben und über keinen Aktivierungscode verfügen, können Sie das Produkt 14 Tage kostenlos testen.

- **Internet-Schutz**. Falls Ihr Gerät zur Aktivierung des Internet-Schutzes die Eingabehilfe-Option benötigt, tippen Sie auf **AKTIVIEREN**. Sie werden zum Menü für die Eingabehilfe weitergeleitet. Tippen Sie auf Bitdefender Mobile Security und aktivieren Sie den entsprechenden Schalter.

- **Virenscanner**. Führen Sie einen einmaligen Scan durch, um sicherzustellen, dass auf Ihrem Gerät keine Bedrohungen vorliegen. Tippen Sie zum Start des Scan-Vorgangs auf **JETZT SCANNEN**.

  Mit Beginn des Scan-Vorgangs wird das Dashboard angezeigt. Hier können Sie den Sicherheitsstatus Ihres Geräts einsehen.

5.2.5. Dashboard

Tippen Sie in der App-Übersicht Ihres Geräts auf das Symbol für Bitdefender Mobile Security, um die App zu öffnen.

Im Dashboard finden Sie Informationen zum Sicherheitsstatus Ihres Geräts. Hier unterstützt Sie auch der Autopilot bei der Verbesserung

Ihrer Gerätesicherheit, indem er Ihnen Empfehlungen zu den einzelnen Funktionen anzeigt.

Die Statuskarte oben im Fenster informiert Sie mit eindeutigen Meldungen und auffälligen Farben über den Sicherheitsstatus Ihres Geräts. Liegen in Bitdefender Mobile Security keine Warnmeldungen vor, ist die Statuskarte grün. Wurde ein Sicherheitsproblem gefunden, wechselt die Farbe der Statuskarte nach rot.

Um einen wirksamen Betrieb und noch besseren Schutz bei Ihren verschiedenen Aktivitäten sicherzustellen, fungiert der **Bitdefender-Autopilot** als Ihr persönlicher Sicherheitsberater. Je nachdem, was Sie gerade machen, liefert der Bitdefender-Autopilot Ihnen kontextabhängige Empfehlungen, die sich an Ihrer Gerätenutzung und an Ihren Anforderungen orientieren. So lernen Sie alle Vorteile der Funktionen in Ihrer Bitdefender Mobile Security-App kennen und können umfassend davon profitieren.

Wenn ein Prozess ausgeführt wird oder eine Funktion Ihre Aufmerksamkeit erfordert, wird eine Kachel mit weiteren Informationen und möglichen Aktionen im Dashboard angezeigt.

Sie können auf die Funktionen von Bitdefender Mobile Security zugreifen und einfach über die untere Navigationsleiste navigieren:

Virenscanner

Hiermit können Sie Bedarf-Scans starten oder Speicher-Scans aktivieren. Weitere Informationen finden Sie im Kapitel Virenscanner (Seite 200).

Internet-Schutz

Lässt Sie sicher im Web surfen, indem er Sie vor potenziell schädlichen Seiten warnt. Weitere Informationen finden Sie im Kapitel Internet-Schutz (Seite 203).

VPN

Verschlüsselt die Internetkommunikation und hilft Ihnen so, Ihre Privatsphäre in jedem beliebigen Netzwerk zu schützen. Weitere Informationen finden Sie unter VPN (Seite 204).

Betrugswarnung

Schützt Sie, indem es Sie vor schädlichen Links warnt, die per SMS, Messaging-Anwendungen und Arten von Benachrichtigungen eingehen. Weitere Informationen finden Sie unter Betrugswarnung (Seite 208).

Diebstahlschutz

Hiermit können Sie die Diebstahlschutzfunktionen aktivieren und deaktivieren und die Einstellungen für den Diebstahlschutz konfigurieren. Weitere Informationen finden Sie im Kapitel Diebstahlschutz-Funktionen (Seite 211).

Kontoschutz

Prüft, ob die Datensicherheit Ihrer Online-Konten kompromittiert wurde. Weitere Informationen finden Sie im Kapitel Kontoschutz (Seite 215).

App-Sperre

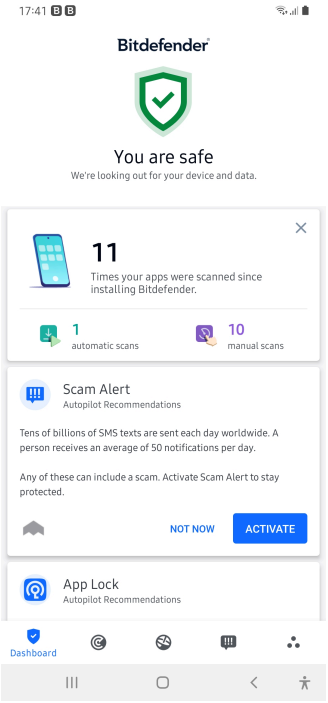
Hiermit können Sie Ihre installierten Anwendungen durch Festlegung einer PIN für den Zugriff schützen. Weitere Informationen finden Sie im Kapitel App-Sperre (Seite 217).

Berichte

Zeichnet alle wichtigen Aktionen, Statusänderungen und andere kritische Meldungen im Zusammenhang mit der Aktivität Ihres Geräts auf. Weitere Informationen finden Sie unter Berichte (Seite 221).

WearON

Kommuniziert mit Ihrer Smartwatch, damit Sie Ihr Telefon schneller wiederfinden können. Weitere Informationen finden Sie im Kapitel WearON (Seite 222).



5.3. Virenscanner

Bitdefender schützt Ihr Gerät und Ihre Daten mit Scans während der Installation und bei Bedarf vor schädlichen Anwendungen.

In der Benutzeroberfläche des Virenscanners finden Sie eine Liste aller Bedrohungstypen, nach denen Bitdefender sucht, einschließlich ihrer Definition. Tippen Sie auf die jeweilige Bedrohung, um die Definition anzuzeigen.

> **Notiz**
> Stellen Sie sicher, dass Ihr Mobilgerät mit dem Internet verbunden ist. Sollte keine Internet-Verbindung bestehen, wird der Scan-Vorgang nicht gestartet.

- **Scans bei Installation**

Bitdefender Mobile Security scannt automatisch all neu installierten Anwendungen mithilfe der Cloud-Technologie. Der gleiche Scan-Vorgang wird bei jedem Update einer installierten App wiederholt.

Wenn die Anwendung als schädlich eingestuft wird, wird eine Aufforderung angezeigt, die Anwendung zu deinstallieren. Tippen Sie auf **Deinstallieren**, um zum Deinstallationsbildschirm der Anwendung zu gelangen.

- **Bedarf-Scans**

  Wenn Sie einmal unsicher sein sollten, ob eine Anwendung auf Ihrem Gerät sicher ist, können Sie einen Bedarf-Scan starten.

  So können Sie einen Bedarf-Scan starten:

  1. Tippen Sie in der unteren Navigationsleiste auf **Virenscanner** in
  2. Tippen Sie auf **SCAN STARTEN**.

  > **Notiz**
  > Für den Virenscanner werden unter Android 6 zusätzliche Berechtigungen benötigt. Tippen Sie auf **SCAN STARTEN** und wählen Sie danach **Zulassen** für folgende Anfragen aus:
  >
  > - Zulassen, dass der **Virenschutz** Anrufe tätigt und verwaltet?
  > - Zulassen, dass der **Virenschutz** auf Fotos, Medien und Dateien auf Ihrem Gerät zugreift?

  Der Scan-Fortschritt wird angezeigt. Sie können den Vorgang jederzeit abbrechen.

Bitdefender Mobile Security scannt standardmäßig den internen Speicher Ihres Gerätes sowie vorhandene SD-Karten. So können gefährliche Anwendungen, die sich auf der Karte befinden könnten, erkannt werden, bevor Sie Schaden anrichten können.

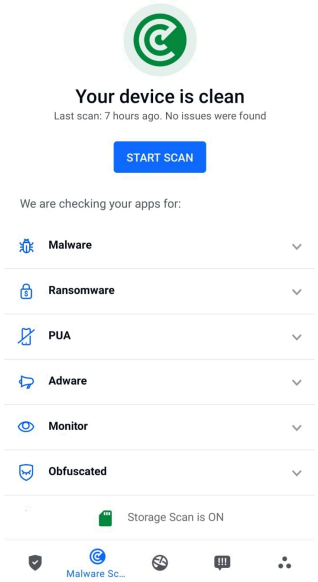
So können Sie die Einstellung Speicher prüfen deaktivieren:

1. Tippen Sie in der unteren Navigationsleiste auf **Mehr**.
2. Tippen Sie auf **Einstellungen**.
3. Deaktivieren Sie im Bereich Virenscanner den Schalter **Speicher prüfen**.

Wird eine schädliche Anwendung gefunden, werden entsprechende Informationen zu dieser Anwendung angezeigt. Tippen Sie auf **DEINSTALLIEREN**, um sie zu entfernen.

Die Virenscanner-Kachel zeigt den Status Ihres Geräts an. Ein grüne Kachel zeigt, dass Ihr Gerät geschützt ist. Ein rote Kachel bedeutet, dass ein Scan durchgeführt werden muss oder Ihre Aufmerksamkeit gefordert ist.

Wenn Sie über ein Gerät mit Android Version 7.1 oder höher verfügen, können Sie über einen Kurzbefehl auf den Virenscanner zugreifen und eine Virensuche schnell starten, ohne Bitdefender Mobile Security zu öffnen. Halten Sie einfach das Symbol Bitdefender auf Ihrem Startbildschirm oder in Ihrem App-Drawer, und wählen Sie dann das Symbol für .



5.3.1. Erkennung von App-Anomalien

Bitdefender App Anomaly Detection ist eine neuartige Technologie, die in den Bitdefender Malware Scanner integriert ist und durch kontinuierliche Überwachung und Erkennung böswilliger Verhaltensweisen eine zusätzliche Schutzebene bietet und den Benutzer benachrichtigt, wenn verdächtige Aktivitäten erkannt werden.

Die App-Anomalieerkennung von Bitdefender schützt Benutzer auch dann, wenn sie unwissentlich eine gefährliche App installiert haben, die eine Zeit lang inaktiv läuft, oder eine scheinbar vertrauenswürdige App, die ihre Funktionalität beeinträchtigt und böswillig wird.

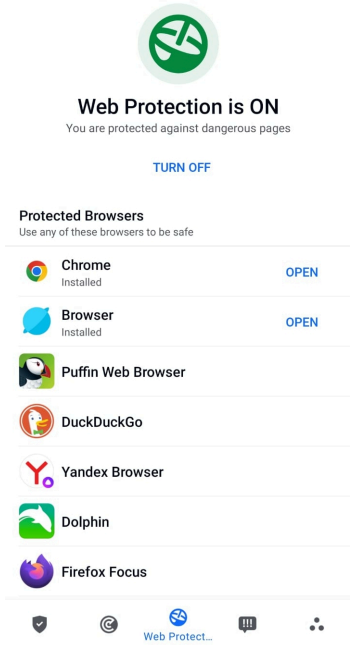
5.4. Internet-Schutz

Der Internet-Schutz nutzt die Bitdefender-Cloud-Dienste, um die von Ihnen im Standard-Android-Browser, in Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser und Dolphin aufgerufenen Webseiten zu überprüfen.

Notiz

Für den Surfschutz werden unter Android 6 zusätzliche Berechtigungen benötigt.

Erteilen Sie die Erlaubnis zur Registrierung als Accessibility-Dienst und tippen Sie nach Aufforderung auf **AKTIVIEREN**. Tippen Sie auf **Antivirus** und aktivieren Sie den Schalter. Bestätigen Sie anschließend, dass Sie dem Zugriff auf die Berechtigungen Ihre Geräts zustimmen.



Der Internet-Schutz von Bitdefender ist so konfiguriert, dass Sie bei jedem Aufruf einer Bank-Website zur Verwendung von Bitdefender VPN aufgefordert werden. Die Benachrichtigung wird in der Statusleiste angezeigt. Wir empfehlen Ihnen, Bitdefender VPN zu verwenden, während Sie in Ihr Bankkonto eingeloggt sind, damit Ihre Daten vor möglichen Sicherheitsverletzungen geschützt sind.

So können Sie die Benachrichtigung durch den Internet-Schutz deaktivieren:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Einstellungen**.
3. Deaktivieren Sie den entsprechenden Schalter im Bereich Internet-Schutz.

5.5. VPN

Mit Bitdefender VPN schützen Sie Ihre Daten bei Verbindungen mit ungesicherten WLAN-Netzwerken wie zum Beispiel in Flughäfen,

Einkaufszentren, Cafés oder Hotels. So vermeiden Sie bedauerliche Vorfälle wie den Diebstahl Ihrer persönlichen Daten oder Versuche, Ihre Geräte-IP-Adresse für Hacker offenzulegen.

Das VPN dient als Tunnel zwischen Ihrem Gerät und dem Netzwerk, mit dem Sie sich verbinden. Ihre Verbindung wird abgesichert, Ihren Daten werden professionell nach Bankenstandard verschlüsselt und Ihre IP-Adresse bleibt jederzeit unsichtbar. Ihr Datenverkehr wird über spezielle Server weitergeleitet, was es nahezu unmöglich macht, Ihr Gerät neben den unzähligen anderen Geräten zu identifizieren, die ebenfalls unsere Dienste in Anspruch nehmen. Darüber hinaus können Sie mit VPN im Internet auch auf solche Inhalte zugreifen, die üblicherweise regionalen Zugangsbeschränkungen unterliegen.

> **Notiz**
> In manchen Ländern wird Internetzensur betrieben. Aus diesem Grund ist die Nutzung von VPNs hier gesetzlich verboten. Um rechtliche Konsequenzen zu vermeiden, wird Ihnen bei der ersten Nutzung der Bitdefender VPN-App eine Warnmeldung angezeigt. Durch die weitere Nutzung der App bestätigen Sie, dass Sie sich aller einschlägigen Rechtsvorschriften in Ihrem Land sowie der möglichen Risiken, denen Sie sich aussetzen, bewusst sind.

Sie haben zwei Optionen zur Aktivierung oder Deaktivierung von Bitdefender VPN:

- Tippen Sie in der VPN-Kachel des Dashboards auf **VERBINDEN**.
  Der Status von Bitdefender VPN wird angezeigt.

- Tippen Sie in der unteren Navigationsleiste auf **VPN** und danach auf **VERBINDEN**.
  Tippen Sie auf **Verbinden**, um sich und Ihre Geräte bei Verbindungen mit ungesicherten WLAN-Netzwerken zu schützen.
  Tippen Sie auf **Trennen**, um die Verbindung wieder aufzuheben.

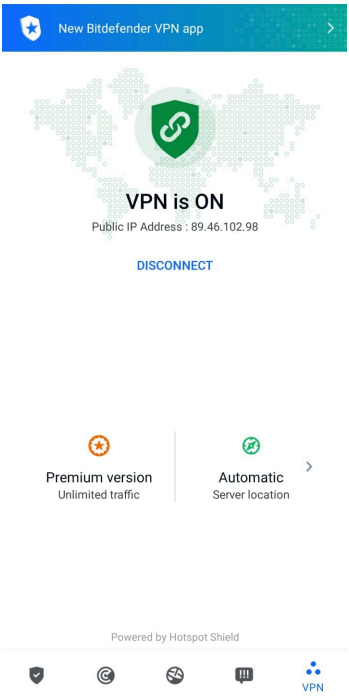
> **Notiz**
> Wenn Sie VPN das erste Mal einschalten, werden Sie gebeten, Bitdefender zu erlauben, eine VPN-Verbindung herzustellen, die den Netzwerkdatenverkehr überwacht. Tippen Sie auf **OK** um fortzufahren.

Auf Geräten ab Android 7.1 können Sie eine Verknüpfung zu Bitdefender VPN nutzen, ohne die Bitdefender Mobile Security-App öffnen zu müssen.

Halten Sie einfach das Symbol Bitdefender auf Ihrem Startbildschirm oder in Ihrem App-Drawer, und wählen Sie dann das Symbol .

Um Ihren Akku zu schonen, empfehlen wir Ihnen, die VPN-Funktion zu deaktivieren, wenn Sie sie nicht mehr benötigen.

Falls Sie über ein Premium-Abonnement verfügen und sich mit einem Server Ihrer Wahl verbinden möchten, tippen Sie in der VPN-Funktion auf Serverstandort und wählen Sie den gewünschten Standort aus. Weitere Details zu den VPN-Abonnements finden Sie unter



5.5.1. VPN-Einstellungen

Für eine erweiterte Konfiguration Ihres VPN:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Einstellungen**.

Im VPN-Bereich können Sie die folgenden Optionen konfigurieren:

- VPN-Schnellzugriff – eine Benachrichtigung wird in der Statusleiste Ihres Geräts angezeigt, über die Sie das VPN schnell aktivieren können.
- Warnung bei offenen WLAN-Netzwerken - Jedes Mal, wenn Sie sich mit einem offenen WLAN-Netzwerk verbinden, werden Sie in der Statusleiste Ihres Geräts zur Verwendung des VPN aufgefordert.

5.5.2. Abonnements

Mit Bitdefender VPN erhalten Sie ein kostenloses Datenvolumen von 200 MB pro Tag, um Ihre Verbindung bei Bedarf abzusichern. Sie werden automatisch mit dem besten Serverstandort verbunden.

Wenn Sie sich für ein Upgrade auf die Premium-Version entscheiden, entfällt das Datenlimit und Sie können durch die freie Wahl des Serverstandorts Inhaltsbeschränkungen überall auf der Welt umgehen.

Sie können jederzeit ein Upgrade auf Bitdefender Premium VPN vornehmen, indem Sie im VPN-Fenster auf **Premium aktivieren** tippen.

Das Bitdefender Premium VPN-Abonnement ist nicht an das Bitdefender Mobile Security-Abonnement gebunden, d. h. Sie können es während der gesamten Laufzeit nutzen, unabhängig vom Status Ihres Sicherheitsabonnements. Falls das Bitdefender Premium VPN-Abonnement ausläuft, aber das Abonnement für Bitdefender Mobile Security noch aktiv ist, werden Sie wieder auf die kostenlose Version umgestellt.

Bitdefender VPN ist plattformunabhängig und in den Windows-, macOS-, Android- und iOS-Produkten von Bitdefender verfügbar. Nach einem Premium-Upgrade können Sie Ihr Abonnement in allen Produkten nutzen, vorausgesetzt, dass Sie sich mit dem gleichen Bitdefender-Benutzerkonto anmelden.

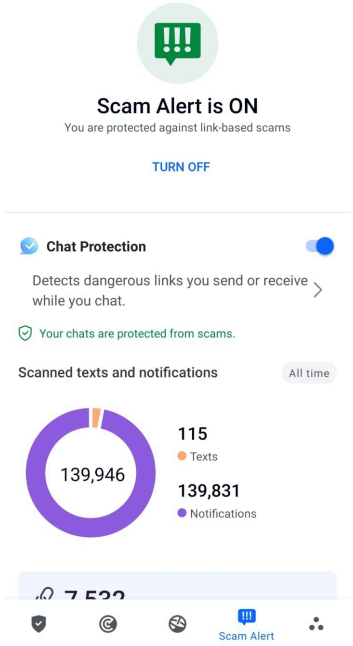
> **Notiz**
> Bitdefender VPN ist auch als eigenständige Anwendung auf allen unterstützten Betriebssystemen einsetzbar, d. h. unter Windows, macOS, Android und iOS.

5.6. Betrugswarnung

Die Betrugswarnung dient der Prävention von potenziell gefährlichen Situationen, bevor sie zum Problem werden können, so auch Malware-Bedrohungen. Die Betrugswarnung überwacht alle eingehenden SMS-Nachrichten und Android-Benachrichtigungen in Echtzeit.

Sie werden per Warnmeldung über den Eingang von Benachrichtigungen mit gefährlichen Links informiert. Bitdefender bietet Ihnen dann zwei Optionen an. Sie können die Information ignorieren oder die **DETAILS ANZEIGEN**. Dadurch erhalten Sie weitere Informationen über den Vorfall sowie wichtige Empfehlungen, wie z. B.:

- Öffnen Sie den gefundenen Link nicht und leiten Sie ihn nicht weiter.
- Löschen Sie im Falle von SMS wenn möglich die gesamte Nachricht.
- Blockieren Sie den Absender, wenn es sich dabei nicht um einen Kontakt handelt, den Sie kennen und dem Sie vertrauen.
- Löschen Sie die App, die gefährliche Links über Benachrichtigungen verschickt.



Notiz

Einschränkungen im Android-Betriebssystem verhindern, dass Bitdefender Textnachrichten löschen oder andere direkte Maßnahmen in Bezug auf SMS-Nachrichten und weitere Quellen gefährlicher Benachrichtigungen ergreifen kann. Wenn Sie die Warnmeldung der Betrugswarnung ignorieren und versuchen, gefährliche Link dennoch zu öffnen, wird der Internet-Schutz von Bitdefender diese automatisch erkennen und verhindern, dass Ihr Gerät infiziert wird.

5.6.1. Aktivieren der Betrugswarnung

Um die Betrugswarnung zu aktivieren, müssen Sie der Bitdefender Mobile Security-App Zugriff auf die SMS-Nachrichten und das Benachrichtigungssystem gewähren:

1. Öffnen Sie die auf Ihrem Android-Telefon oder -Tablet installierte Bitdefender Mobile Security-App.
2. Tippen Sie im Hauptfenster der Bitdefender-App in der unteren Navigationsleiste auf die Option **Betrugswarnung** und dann auf **AKTIVIEREN**.
3. Tippen Sie auf **ZULASSEN**.
4. Setzen Sie Bitdefender Security in der Liste der Apps mit Zugriff auf Benachrichtigungen auf die Position **EIN**.
5. Tippen Sie zur Bestätigung auf **ZULASSEN**.
6. Kehren Sie zum Bildschirm Betrugswarnung zurück und tippen Sie auf **ZULASSEN**, damit Bitdefender eingehende SMS-Nachrichten scannen kann.

5.6.2. Echtzeit-Chat-Schutz

Chat-Nachrichten sind die wohl bequemste Möglichkeit, um mit Freunden und Familie in Kontakt zu bleiben. Sie sind aber auch ein Einfallstor für gefährliche Links.

Wenn Sie die Chat-Schutzfunktion aktivieren, schützt die Betrugswarnung nicht nur Ihre Textnachrichten und Benachrichtigungen, sondern auch Ihre Chats vor linkbasierten Angriffen, indem es gefährliche Links erkennt, die Sie beim Chatten senden oder empfangen.

So aktivieren Sie den Chat-Schutz:

1. Öffnen Sie die auf Ihrem Android-Telefon oder -Tablet installierte Bitdefender Mobile Security-App.
2. Tippen Sie im Hauptfenster der Bitdefender-App in der unteren Navigationsleiste auf die Option **Betrugswarnung**.
3. Oben im Reiter Betrugswarnung finden Sie die Option Chat-Schutz. Setzen Sie den entsprechenden Schalter auf **EIN**.

> **Notiz**
> Derzeit ist der Chat-Schutz mit den folgenden Anwendungen kompatibel:
>
> - WhatsApp
> - Facebook Messenger
> - Telegram
> - Discord

5.7. Scam Copilot

Bei dieser Funktion handelt es sich um einen KI-gestützter Chatbot, der von Bitdefender trainiert wurde, um verschiedene Betrugsszenarien, Phishing-Angriffe, Desinformationskampagnen und Fake-Websites zu erkennen.

So aktivieren Sie Scam Copilot:

1. Öffnen Sie die Bitdefender Mobile Security-App. Im Dashboard finden Sie eine eigene Kachel für den Scam Copilot. Tippen Sie auf **Aktivieren**.
2. Erteilen Sie der Bitdefender Mobile Security-App die Berechtigung zur Nutzung der Bedienungshilfen, indem Sie auf die Schaltfläche **AKTIVIEREN** tippen.
3. Erteilen Sie die Berechtigung für Benachrichtigungen durch Tippen auf **Zulassen**.

Scam Copilot ist nun auf Ihrem Gerät konfiguriert.

Sie können jetzt auf den Reiter für den Scam Copilot zugreifen. Hier finden Sie:

- **Chatbot zur Betrugserkennungs:** Lassen Sie den Chatbot verdächtige Nachrichten überprüfen.

- **Präventionsassistent:** Hilft Ihnen, mehr über Betrugsmaschen zu erfahren und sich effektiver davor zu schützen.
- **Automatisches Erkennen von Betrugsversuchen:** Status und Kontrollzentrum.
- **SMS-Filter:** Lassen Sie gefährliche Nachrichten direkt in Ihrer Nachrichten-App filtern.

5.8. Diebstahlschutz-Funktionen

Bitdefender kann Ihnen dabei helfen, Ihr Gerät zu finden, und verhindert, dass Ihre privaten Daten in die falschen Hände gelangen.

Sie müssen nur den Diebstahlschutz über das Gerät aktivieren und können dann bei Bedarf jederzeit und mit jedem Browser auf **Bitdefender Central** zugreifen.

> **Notiz**
> In der Oberfläche des Diebstahlschutzes finden Sie auch einen Link zu unserer Bitdefender Central-App im Google Play Store. Über diesen Link können Sie die App herunterladen, falls Sie dies noch nicht getan haben.

Bitdefender Mobile Security bietet die folgenden Diebstahlschutz-Funktionen:

Fernortung

Hiermit können Sie den Standort Ihres Geräts in Google Maps anzeigen. Der Standort wird alle 5 Sekunden aktualisiert, eine Bewegung kann also nachverfolgt werden.

Die Genauigkeit der Ortung hängt davon ab, auf welche Weise Bitdefender den Standort bestimmt:

- Wenn GPS im Gerät aktiviert ist, kann sein Standort bis auf ein paar Meter genau bestimmt werden, solange das Gerät in Reichweite der GPS-Satelliten (d. h. nicht in einem Gebäude) ist.
- Wenn sich das Gerät in einem Gebäude befindet, kann sein Standort auf mehrere zehn Meter genau bestimmt werden, solange WLAN aktiviert ist und Drahtlosnetzwerke in Reichweite des Geräts sind.

- Andernfalls wird der Standort allein über Daten aus dem Mobilfunknetzwerk bestimmt, wodurch die Genauigkeit auf einen Umkreis von ein paar hundert Metern sinkt.

Fernsperrung

Frieren Sie den Bildschirm Ihres Geräts ein, und legen Sie eine PIN fest, mit der er wieder aktiviert werden kann.

Fernlöschung

Löschen Sie alle persönlichen Daten von Ihrem Gerät.

Signal an das Gerät senden (Aufschrei)

Sie können aus der Ferne eine Nachricht an das Gerät senden, die auf dem Bildschirm angezeigt wird, oder ein lautes Tonsignal über die Lautsprecher abspielen lassen.

Wenn Sie Ihr Gerät verlieren, können Sie den potenziellen Finder wissen lassen, wie er es Ihnen zukommen lassen kann, indem Sie auf dem Bildschirm des Geräts eine Nachricht anzeigen lassen.

Wenn Sie Ihr Gerät verlegt haben, liegt es mit einiger Wahrscheinlichkeit ganz in der Nähe (in der Wohnung oder im Büro). Sie finden es ganz leicht, indem Sie es eine lauten Ton abspielen lassen. Der Ton wird abgespielt, auch wenn das Gerät auf lautlos gestellt ist.

5.8.1. Aktivierung des Diebstahlschutzes

Zur Aktivierung der Diebstahlschutzfunktionen müssen Sie nur den Konfigurationsvorgang über die Diebstahlschutz-Kachel im Dashboard abschließen.

Alternativ können Sie den Diebstahlschutz folgendermaßen aktivieren:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Tippen Sie auf **Diebstahlschutz**.
3. Tippen Sie auf **AKTIVIEREN**.
4. Der folgende Prozess wird eingeleitet, um Sie bei der Aktivierung dieser Funktion zu unterstützen:

Notiz

Für den Diebstahlschutz werden unter Android 6 zusätzliche Berechtigungen benötigt.

Um sie zu aktivieren, gehen Sie folgendermaßen vor:

a. Tippen Sie auf **DIEBSTAHLSCHUTZ AKTIVIEREN** und danach auf **AKTIVIEREN**.

b. Erteilen Sie dem **Virenschutz** die Berechtigung, auf Ihren Gerätestandort zuzugreifen.

a. **Administratorrechte erteilen**
Diese Rechte sind für den Betrieb des Diebstahlschutz unbedingt erforderlich und müssen eingeräumt werden, um diesen Vorgang fortzusetzen.

b. **Anwendungs-PIN festlegen**
Um einen unbefugten Zugriff auf Ihr Gerät zu verhindern, muss ein PIN-Code festgelegt werden, der bei jedem Zugriffsversuch auf Ihr Gerät zunächst eingegeben werden muss. Bei Geräten, die die Fingerabdruckerkennung unterstützen, kann anstelle des festgelegten PIN-Codes auch die Bestätigung per Fingerabdruck verwendet werden.
Die gleiche PIN wird von der App-Sperre verwendet, um Ihre installierten Anwendungen zu schützen.

c. **Foto aufnehmen aktivieren**
Ist Foto aufnehmen aktiviert, wird Bitdefender bei jedem erfolglosen Zugriffsversuch ein Foto der betreffenden Person aufnehmen.
Im Detail heißt das: Wird dreimal hintereinander die falsche PIN, das falsche Passwort oder der falsche Fingerabdruck eingegeben, wird mit der Frontkamera ein Foto aufgenommen. Das Foto wird dann mit Zeitstempel und einem Hinweis auf den Aufnahmegrund gespeichert und kann in Bitdefender Mobile Security im Fenster für den Diebstahlschutz eingesehen werden.
Alternativ können Sie das aufgenommene Foto auch über Ihr Bitdefender-Benutzerkonto einsehen:

i. Gehe zu: https://central.bitdefender.com.

ii. Melden Sie sich bei Ihrem Konto an.

iii. Wähle aus **Meine Geräte** Tafel.

iv. Wählen Sie Ihr Android-Gerät aus und wechseln Sie dann zum Reiter **Diebstahlschutz**.

v. Tippen Sie neben **Aufnahmen einsehen** auf ⋮, um die zuletzt aufgenommenen Fotos anzuzeigen.
Es werden nur die zwei aktuellsten Fotos gespeichert.

Nach Aktivierung der Diebstahlschutzfunktion können Sie die Web-Steuerungsbefehle durch Antippen der entsprechenden Optionen einzeln aktivieren oder deaktivieren.

5.8.2. Zugriff auf Diebstahlschutz-Funktionen über Bitdefender Central

> **Notiz**
> Für die Diebstahlschutz-Funktionen muss die Option **Hintergrunddaten** in den Datennutzungseinstellungen Ihres Gerätes aktiviert sein.

So können Sie über Ihr Bitdefender-Konto auf die Diebstahlschutzfunktionen zugreifen:

1. Rufen Sie **Bitdefender Central** auf.
2. Wähle aus **Meine Geräte** Tafel.
3. Wählen Sie im Fenster **MEINE GERÄTE** die gewünschte Gerätekarte, indem Sie auf die entsprechende Schaltfläche **Details anzeigen** tippen.
4. Wechseln Sie zum Reiter **Diebstahlschutz**.
5. Tippen Sie auf die Schaltfläche, die der gewünschten Funktion entspricht:
   Orten - zeigt den Standort Ihres Geräts auf Google Maps.
   IP ANZEIGEN - Zeigt die letzte IP-Adresse für das ausgewählte Gerät an.
   Alarm - Sie können eine Nachricht eingeben, die auf dem Bildschirm Ihres Geräts angezeigt werden soll, und/oder das Gerät einen Alarmton abspielen lassen.
   Sperren - Ihr Gerät sperren und einen PIN-Code zum Entsperren festlegen.

Daten löschen - alle Daten von Ihrem Gerät löschen.

> **Wichtig**
> Nach einer Löschung funktionieren die Diebstahlschutz-Funktionen nicht mehr.

5.8.3. Diebstahlschutz-Einstellungen

So können Sie die Fernbefehle aktivieren oder deaktivieren:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Diebstahlschutz**.
3. Aktivieren oder deaktivieren Sie die gewünschten Optionen.

5.9. Kontoschutz

Der Bitdefender-Kontoschutz erkennt, ob die Datensicherheit der Benutzerkonten kompromittiert wurde, über die Sie Ihre Online-Zahlungen und -Einkäufe abwickeln und sich bei Ihren Apps oder Websites anmelden. Die unter Ihren Konten gespeicherten Daten umfassen Passwörter, Kreditkartendaten und Bankinformationen. Wurden diese nicht ausreichend abgesichert, kann es zu Identitätsdiebstahl und Verletzungen Ihrer Privatsphäre kommen.

Nach der Bestätigung wird der Privatsphärestatus des Benutzerkontos umgehend angezeigt.

Im Hintergrund werden automatisch weitere Prüfungen durchgeführt und Sie können darüber hinaus täglich manuelle Prüfungen durchführen.

Sie erhalten eine Benachrichtigung, sobald neue Datenschutzverletzungen bekannt werden, die eines Ihrer bestätigten E-Mail-Konten betreffen.

So können Sie Ihre persönlichen Daten schützen:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Tippen Sie auf **Kontoschutz**.
3. Tippen Sie auf **ERSTE SCHRITTE**.

4. Die E-Mail-Adresse, die zur Erstellung Ihres Bitdefender-Benutzerkontos verwendet wurde, erscheint und wird automatisch zur Liste der überwachten Konten hinzugefügt.
5. Um ein weiteres Konto hinzuzufügen, tippen Sie im Fenster Kontoschutz auf **BENUTZERKONTO HINZUFÜGEN**, und geben Sie die E-Mail-Adresse ein.
   Tippen Sie zum Fortfahren auf **HINZUFÜGEN**.
   Bitdefender muss für dieses Konto vor der Preisgabe privater Daten erst eine Kontovalidierung durchführen. Sie erhalten zu diesem Zweck unter der angegebenen E-Mail-Adresse einen Bestätigungscode.
   Rufen Sie Ihre E-Mails ab und geben Sie den erhaltenen Code in Ihrer App im Bereich **Kontoschutz** ein. Falls Sie Bestätigungs-E-Mail in Ihrem Posteingang nicht finden können, überprüfen Sie bitte Ihren Spam-Ordner.
   Der Privatsphärestatus des bestätigten Kontos wird angezeigt.

Wurden Datenschutzverletzungen bei einem Ihrer Benutzerkonten festgestellt, empfehlen wir Ihnen, so schnell wie möglich das entsprechende Passwort zu ändern. Mit diesen Tipps sorgen Sie für sichere Passwörter:

- Verwenden Sie mindestens acht Zeichen.
- Verwenden Sie Groß- und Kleinbuchstaben.
- Verwendenden Sie mindestens eine Zahl oder Sonderzeichen wie #, @, % oder !.

Nachdem Sie ein Konto gesichert haben, das von einer Datenschutzverletzung betroffen war, können Sie die Änderungen bestätigen, indem Sie die identifizierten Datenpannen als Gelöst markieren. Gehen Sie dazu wie folgt vor:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Konto Privatsphäre**.
3. Tippen Sie auf das Konto, das Sie gerade gesichert haben.
4. Tippen Sie auf die Datenpanne, wegen der Sie das Benutzerkonto abgesichert haben.
5. Tippen Sie auf **GELÖST**, um zu bestätigen, dass das Konto gesichert wurde.

Wenn alle gefundenen Datenschutzverletzungen als **Gelöst** markiert wurden, wird das Konto nicht mehr als von einer Datenpanne betroffen angezeigt, zumindest bis es zu einer weiteren Datenpanne kommt.

Gehen Sie folgendermaßen vor, um nicht mehr jedes Mal benachrichtigt zu werden, wenn automatische Scans durchgeführt werden:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Einstellungen**.
3. Deaktivieren Sie den entsprechenden Schalter im Bereich Kontoschutz.

5.10. App-Sperre

Installierte Anwendungen so z.B. für E-Mail, Fotos oder Nachrichten können persönliche Daten enthalten, die Sie vor fremden Zugriff durch selektive Zugangssperren schützen können.

Mit der App-Sperre können Sie unbefugten Zugriff auf Ihre Anwendungen verhindern, indem Sie einen PIN-Code für den Zugriff festlegen. Der PIN-Code muss 4-8 Ziffern enthalten und bei jedem Zugriff auf die zugriffsbeschränkten Anwendungen eingegeben werden.

Die biometrische Authentifizierung (z. B. Bestätigung per Fingerabdruck oder Gesichtserkennung) kann anstelle des festgelegten PIN-Codes verwendet werden.

5.10.1. App-Sperre wird aktiviert

Um den Zugriff auf ausgewählte Anwendungen einzuschränken, können Sie die App-Sperre über die Kachel im Dashboard konfigurieren, die nach Aktivierung des Diebstahlschutzes angezeigt wird.

Alternativ können Sie die App-Sperre folgendermaßen aktivieren:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Tippen Sie auf **App-Sperre**.
3. Klopfen **ANMACHEN**.
4. Erlauben Sie Bitdefender Security den Zugriff auf die Nutzungsdaten.
5. **Über anderen Apps einblenden** erlauben.

6. Öffnen Sie die App erneut, konfigurieren Sie den Zugriffscode und tippen Sie auf **PIN FESTLEGEN**.

> **Notiz**
> Dieser Schritt steht nur zur Auswahl, wenn Sie die PIN noch nicht beim Diebstahlschutz eingerichtet haben.

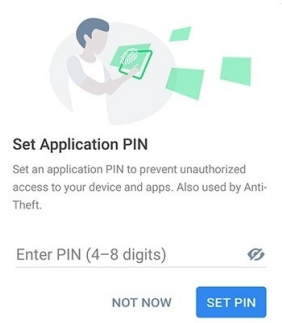
7. Aktivieren Sie die Option Foto aufnehmen, um Eindringlinge zu erwischen, die versuchen, auf Ihre privaten Daten zuzugreifen.

> **Notiz**
> Für die Funktion Foto aufnehmen werden unter Android 6 zusätzliche Berechtigungen benötigt. Erlauben Sie dem **Virenschutz** das Aufnehmen von Fotos und Videos, um sie zu aktivieren.

8. Wählen Sie die Apps aus, die Sie schützen möchten.

Wird fünfmal in Folge die falsche PIN eingegeben oder der falsche Fingerabdruck verwendet, tritt eine 30-sekündige Sperre ein. Auf diese Weise werden Versuche auf geschützte Apps zuzugreifen unterbunden.

> **Notiz**
> Die gleiche PIN wird vom Diebstahlschutz verwendet, um den Standort Ihres Geräts zu ermittelt.



5.10.2. Sperrmodus

Wenn Sie eine App zum ersten Mal zur App-Sperre hinzufügen, erscheint der Bildschirm App-Sperre-Modus, in dem Sie auswählen können, wann die App-Sperre-Funktion die auf Ihrem Gerät installierten Apps schützen soll.

Ihnen stehen die folgenden Optionen zur Auswahl:

- **Entsperren immer erforderlich** - Der PIN-Code oder Fingerabdruck müssen bei jedem Aufruf einer gesperrten App eingegeben werden.
- **Bis zur Bildschirmabschaltung entsperrt lassen** - Sie können bis zur nächsten Bildschirmabschaltung auf die Apps zugreifen.
- **Nach 30 Sekunden sperren** - Sie können innerhalb von 30 Sekunden bereits geschlossene Apps wieder aufrufen.

So können Sie die ausgewählte Einstellung wieder ändern:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Einstellungen**.
3. Tippen Sie im Bereich App-Sperre auf **Entsperren immer erforderlich**.
4. Wählen Sie gewünschte Option aus.

5.10.3. App-Sperre-Einstellungen

Für eine erweiterte Konfiguration der App-Sperre:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Einstellungen**.

Im Bereich der App-Sperre können Sie die folgenden Optionen konfigurieren:

- **Vorschlag zu sensiblen Apps** - Sie erhalten bei jeder Installation einer sensiblen App eine Sperrbenachrichtigung.
- **Entsperren immer erforderlich** - Wählen Sie eine der verfügbaren Optionen für das Sperren und Entsperren aus.
- **Intelligentes Entsperren** - Ihre Apps bleiben bei Verbindungen mit vertrauenswürdigen WLAN-Netzwerken entsperrt.
- **Zufallstastatur** - Verhindern Sie durch zufällige Anordnung der Ziffern das Ablesen Ihrer PIN.

5.10.4. Foto aufnehmen

Mit der Foto-aufnehmen-Funktion von Bitdefender erwischen Sie Ihre Freunde oder Verwandten auf frischer Tat. So können Sie ihnen klar

machen, dass Ihre persönlichen Dateien und installierten Anwendungen nicht für Ihre Augen bestimmt sind.

Es funktioniert ganz einfach: Wird dreimal hintereinander die falsche PIN oder der falsche Fingerabdruck eingegeben, wird mit der Frontkamera ein Foto aufgenommen. Das Foto wird dann mit Zeitstempel und einem Hinweis auf den Aufnahmegrund gespeichert und kann in Bitdefender Mobile Security über die App-Sperre-Funktion angezeigt werden.

> **Notiz**
> Diese Funktion steht nur auf Telefonen mit Frontkamera zur Verfügung.

So können Sie die Funktion Foto aufnehmen für die App-Sperre konfigurieren:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Einstellungen**.
3. Aktivieren Sie den entsprechenden Schalter im Bereich Foto aufnehmen.

Die Fotos, die nach Eingabe einer falschen PIN aufgenommen werden, werden im App-Sperre-Fenster angezeigt und können dort als Vollbild eingesehen werden.

Alternativ können Sie diese auch über Ihr Bitdefender-Konto anzeigen:

1. Gehe zu: https://central.bitdefender.com.
2. Melden Sie sich bei Ihrem Konto an.
3. Rufen Sie den Bereich **Meine Geräte** auf.
4. Wählen Sie Ihr Android-Gerät und dann die **Diebstahlschutz** Tab.
5. Klopfen neben **Überprüfen Sie Ihre Schnappschüsse** , um die zuletzt aufgenommenen Fotos anzuzeigen.

Nur die beiden neuesten Fotos werden gespeichert.

So können Sie das Hochladen der aufgenommenen Fotos auf Ihr Bitdefender-Benutzerkonto beenden:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Einstellungen**.

3. Deaktivieren Sie im Bereich Foto aufnehmen die Option **Fotos hochladen**.

5.10.5. Intelligentes Entsperren

Damit die App-Sperre Sie nicht bei jedem Aufrufen einer geschützten App nach Ihrer PIN oder Ihrem Fingerabdruck fragt, können Sie das intelligente Entsperren aktivieren.

Mit der Funktion für das intelligente Entsperren können Sie vertrauenswürdige WLAN-Netzwerke festlegen. Bei Verbindung mit einem dieser Netzwerke werden die Blockierungseinstellungen der App-Sperre für die geschützten Apps deaktiviert.

So können Sie die Funktion Intelligentes Entsperren konfigurieren:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **App-Sperre**.
3. Tippen Sie auf die Schaltfläche .
4. Tippen Sie auf den Schalter neben **Intelligentes Entsperren**, falls die Funktion noch nicht aktiviert ist.
   Bestätigen Sie mit Ihrem Fingerabdruck oder Ihrer PIN.
   Wenn Sie die Funktion zum ersten Mal aktivieren, müssen Sie die Standortberechtigung aktivieren. Tippen Sie auf die Schaltfläche **ZULASSEN** und dann erneut auf **ZULASSEN**.
5. Tippen Sie auf **HINZUFÜGEN**, um Ihre aktuelle WLAN-Verbindung als vertrauenswürdig festzulegen.

Falls Sie es sich anders überlegen, können Sie die Funktion jederzeit deaktivieren. Alle bisher als vertrauenswürdig eingestuften WLAN-Netzwerke gelten dann wieder als nicht vertrauenswürdig.

5.11. Berichte

Die Berichtsfunktion protokolliert alle Ereignisse im Zusammenhang mit den Scans auf Ihrem Gerät.

Für jedes sicherheitsrelevante Ereignis auf Ihrem Gerät wird den Berichten eine neue Nachricht hinzugefügt.

So können Sie auf den Bereich Berichte zugreifen:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Tippen Sie auf **Berichte**.

Im Fenster Berichte finden Sie die folgenden Reiter:

- **WÖCHENTLICHE BERICHTE** - Hier können Sie den Sicherheitsstatus und die durchgeführten Aktionen für die aktuelle und vorausgegangene Woche einsehen. Der Bericht für die aktuelle Woche wird jeweils Sonntags erstellt und werden benachrichtigt, sobald er verfügbar ist.
  In diesem Bereich wird jede Woche ein neuer Hinweis angezeigt. Schauen Sie also regelmäßig vorbei, um optimalen Nutzen aus der App zu ziehen.
  So können Sie die Benachrichtigung für jeden neuen Bericht deaktivieren:
  1. Klopfen **Mehr** in der unteren Navigationsleiste.
  2. Klopfen **Einstellungen**.
  3. Deaktivieren Sie den Schalter **Benachrichtigung bei neuen Berichten** im Bereich Berichte.
- **AKTIVITÄTSPROTOKOLL** - Hier können Sie ausführliche Informationen zu den Aktivitäten Ihrer Bitdefender Mobile Security-App seit Installation auf Ihrem Android-Gerät einsehen.
  So können Sie das verfügbare Aktivitätsprotokoll löschen:
  1. Klopfen **Mehr** in der unteren Navigationsleiste.
  2. Klopfen **Einstellungen**.
  3. Tippen Sie auf **Aktivitätsprotokoll löschen** und danach auf **LÖSCHEN**.

5.12. WearON

Mit Bitdefender WearON können Sie Ihr Smartphone schnell und einfach wiederfinden, egal ob Sie es bei der Arbeit im Besprechungsraum oder unter eine Kissen auf dem Sofa vergessen haben. Das Gerät lässt sich auch dann aufspüren, wenn es auf lautlos gestellt ist.

Lassen Sie diese Funktion aktiviert, damit Sie Ihr Smartphone jederzeit zur Hand haben.

Notiz
Diese Funktion benötigt Android 4.3 und Android Wear.

5.12.1. Aktivierung von WearON

Zur Verwendung von WearON müssen Sie Ihre Smartwatch mit der Bitdefender Mobile Security-Anwendungen verbinden und die Funktion über den folgenden Sprachbefehl aktivieren:

Start: <Wo ist mein Telefon>

Bitdefender WearON verfügt über zwei Befehle:

1. **Telefonalarm**
   Mit der Phone-Alert-Funktion können Sie Ihr Smartphone schnell wiederfinden, wenn Sie sich zu weit davon entfernt haben.
   Wenn Sie eine Smartwatch nutzen, erkennt diese automatisch die App auf Ihrem Telefon und vibriert, wenn die Entfernung zwischen Smartwatch und Gerät zu groß wird und die Bluetooth-Verbindung unterbrochen wird.
   Öffnen Sie zur Aktivierung dieser Funktion Bitdefender Mobile Security, tippen Sie im Menü auf **Allgemeine Einstellungen** und wählen Sie im Bereich WearON den entsprechenden Schalter aus.
2. **Scream**
   Es war noch nie so einfach, Ihr Telefon aufzuspüren. Sie haben vergessen, wo Ihr Telefon liegt? Tippen Sie einfach auf den Scream-Befehl auf Ihrer Uhr, um den Scream-Alarm auszulösen.

5.13. Info über

Gehen Sie folgendermaßen vor, um Informationen zur installierten Bitdefender Mobile Security-Version abzurufen, die Abonnementvereinbarung und Datenschutzerklärung aufzurufen und zu lesen und die Open-Source-Lizenzen anzuzeigen:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Einstellungen**.
3. Tippen Sie im Bereich Über auf die gewünschte Option.

5.14. Häufig gestellte Fragen

Wofür benötigt Bitdefender Mobile Security eine Internet-Verbindung?

Die Anwendung muss mit den Bitdefender-Servern kommunizieren, um den Sicherheitsstatus der Anwendungen, die gescannt werden, und der Webseiten, die Sie besuchen, zu bestimmen. Darüber hinaus erhält es so die Befehle, die bei Verwendung der Diebstahlschutzfunktionen über Ihr Bitdefender-Konto verschickt werden.

Wofür benötigt Bitdefender Mobile Security die einzelnen Berechtigungen?

- Internet-Zugang -> dient der Kommunikation mit der Cloud.
- Gerätstatus und Identität ermitteln -> hiermit wird ermittelt, ob Ihr Gerät mit dem Internet verbunden ist, und bestimmte Geräteinformationen ausgelesen, die nötig sind, um eine einzigartige ID für die Kommunikation mit der Bitdefender-Cloud zu erstellen.
- Browser-Lesezeichen anlegen und benutzen -> erlaubt dem Internet-Schutz schädliche Websites aus dem Browser-Verlauf zu löschen.
- Protokolle lesen -> anhand der Android-Protokolle kann Bitdefender Mobile Security Malware-Aktivität erkennen.
- Standort -> dient der Standortermittlung per Fernzugriff.
- Kamera -> wird für die Funktion Foto aufnehmen benötigt.
- Speicher -> wird benötigt, um dem Virenscanner die Prüfung der SD-Karte zu erlauben.

Wie unterbinde ich die Übermittlung von Informationen zu verdächtigen Apps an Bitdefender?

Bitdefender Mobile Security übermittelt standardmäßig Berichte über von Ihnen installierte verdächtige Apps an die Bitdefender-Server. Diese Informationen sind für die Verbesserung der Gefahrenerkennung unerlässlich und können uns helfen, unser Produkt noch besser zu machen. Falls Sie uns keine Informationen über verdächtige Anwendungen mehr schicken möchten. Gehen Sie wie folgt vor, falls Sie uns keine Informationen über verdächtige Apps mehr übermitteln möchten:

1. Klopfen **Mehr** in der unteren Navigationsleiste.

2. Klopfen **Einstellungen**.
3. Deaktivieren Sie im Bereich Virenscanner die Option **In-the--Cloud-Erkennung**.

Wo kann ich Einzelheiten zu den Aktivitäten der App einsehen?

Bitdefender Mobile Security führt ein Protokoll über alle wichtigen Aktionen, Statusänderungen und andere wichtige Nachrichten über eigene Aktivitäten. So können Sie die Aktivitäten der App einsehen:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Berichte**.
   Im Fenster WOCHENBERICHTE können Sie auf die Berichte zugreifen, die jede Woche erstellt werden, und im Fenster AKTIVITÄTSPROTOKOLL können Sie Informationen über die Aktivität Ihrer Bitdefender-App anzeigen.

Ich habe den PIN-Code vergessen, mit dem ich meine Anwendung geschützt habe. Was kann ich tun?

1. Zugang Bitdefender-Zentrale.
2. Wähle aus **Meine Geräte** Tafel.
3. Tippen Sie auf die gewünschte Gerätekachel und dann oben rechts auf ⋮.
4. Wählen **Einstellungen**.
5. Sie können den PIN-Code im Feld **Anwendungs-PIN** abrufen.

Wie kann ich den PIN-Code ändern, den ich für die App-Sperre und den Diebstahlschutz festgelegt habe?

So können Sie den PIN-Code ändern, den Sie für die App-Sperre und den Diebstahlschutz festgelegt haben:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **Einstellungen**.
3. Tippen Sie im Bereich Diebstahlschutz auf **Sicherheits-PIN**.
4. Geben Sie den aktuellen PIN-Code ein.
5. Geben Sie den neuen PIN-Code ein.

Wie kann ich die App-Sperre deaktivieren?

Es gibt keine eigene Option zur Deaktivierung der App-Sperre, Sie müssen dazu lediglich die Kästchen neben den ausgewählten Apps deaktivieren. Dazu wird die festgelegte PIN oder der Fingerabdruck abgefragt.

Wie kann ich ein weiteres WLAN-Netzwerk als vertrauenswürdig einstufen?

Sie müssen Ihr Gerät zunächst mit dem Drahtlosnetzwerk verbinden, das Sie als vertrauenswürdig festlegen möchten. Gehen Sie danach wie folgt vor:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Klopfen **App-Sperre**.
3. Tippen Sie oben rechts auf .
4. Tippen Sie neben dem Netzwerk, das Sie als vertrauenswürdig festlegen möchten, auf **HINZUFÜGEN**.

Wie deaktiviere ich die Anzeige von Fotos, die mit meinem Gerät aufgenommen wurden?

So können Sie die Anzeige von Fotos deaktivieren, die mit Ihren Geräten aufgenommen wurden:

1. Zugang Bitdefender-Zentrale.
2. Tippen Sie oben rechts auf dem Bildschirm auf .
3. Klicken Sie im Schiebemenü auf **Einstellungen**.
4. Deaktivieren Sie die Option **Mit Ihren Geräten aufgenommene Fotos anzeigen/nicht anzeigen**.

Wie kann ich sicher im Netz einkaufen und bezahlen?

Online-Einkäufe sind mit großen Risiken verbunden, wenn einige Details übersehen werden. Um zu verhindern, dass auch Sie zum Betrugsopfer werden, sollten Sie folgende Empfehlungen beachten:

- Halten Sie Ihre Sicherheitslösung immer auf dem neuesten Stand.
- Stellen Sie bei Online-Zahlungen sicher, dass Käuferschutz gewährleistet wird.
- Nutzen Sie in öffentlichen und ungesicherten WLAN-Netzwerken eine VPN-Verbindung zur Verbindung mit dem Internet.

- Prüfen Sie die Passwörter Ihrer Online-Benutzerkonten. Stellen Sie sicher, dass sie neben Groß- und Kleinbuchstaben auch Zahlen und Sonderzeichen (@, !, %, # usw.) enthalten.
- Übermitteln Sie Informationen ausschließlich über sichere Verbindungen. Achten Sie darauf, dass die Adresse der Website mit HTTPS:// und nicht mit HTTP:// beginnt.

Wann sollte ich Bitdefender VPN verwenden?

Bei Aufrufen, Herunterladen oder Hochladen von Inhalten im Internet sollten Sie stets Vorsicht walten lassen. Um sicherzustellen, dass Sie beim Surfen im Netz jederzeit geschützt sind, empfehlen wie den Einsatz von Bitdefender VPN, wenn Sie:

- Verbindungen zu öffentlichen WLAN-Netzwerken herstellen möchten
- auf Inhalte zugreifen möchten, die regionalen Zugangsbeschränkungen unterliegen, egal ob zuhause oder im Ausland
- Ihre persönlichen Daten vor Zugriff schützen möchten (Benutzernamen, Passwörter, Kreditkartendaten etc.)
- Ihre IP-Adresse verbergen möchten

Wirkt sich Bitdefender VPN auf die Akkulaufzeit meines Gerätes aus?

Bitdefender VPN wurde entwickelt, um Ihre persönlichen Daten zu schützen, Ihre IP-Adresse bei Verbindungen mit ungesicherten WLAN-Netzwerken zu verbergen und Ihnen den Zugriff auf Inhalte mit länderspezifischen Zugangsbeschränkungen zu ermöglichen. Um Ihren Akku zu entlasten, empfehlen wir, das VPN nur bei Bedarf zu nutzen und die Verbindung danach wieder zu trennen.

Warum wird meine Internetverbindung langsamer, wenn ich eine Verbindung mit Bitdefender VPN herstelle?

Bitdefender VPN ist auf einen ressourcenschonenden Betrieb beim Surfen im Netz ausgelegt. Ihre Internetverbindung bzw. die Entfernung zum Server, mit dem Sie eine Verbindung hergestellt haben, können sich jedoch negativ auf die Verbindungsgeschwindigkeit auswirken. Wenn es nicht unbedingt notwendig ist, dass Sie sich von Ihrem Standort aus mit einem weit entfernten Server verbinden (z. B. von Deutschland aus nach China), sollten Sie in solchen Fällen Bitdefender VPN erlauben, automatisch eine Verbindung mit dem nächstgelegenen

Server herzustellen bzw. einen Server zu finden, der näher an Ihrem Standort liegt.

Kann ich das mit meinem Gerät verknüpfte Bitdefender-Konto ändern?

Ja, Sie können jederzeit Ihrem Gerät ein anderes Bitdefender-Konto zuordnen. Gehen Sie dazu folgendermaßen vor:

1. Klopfen **Mehr** in der unteren Navigationsleiste.
2. Tippen Sie auf Ihre E-Mail-Adresse.
3. Tippen Sie auf **Melden Sie sich bei Ihrem Konto ab**. Wenn ein PIN-Code festgelegt wurde, werden Sie aufgefordert, ihn einzugeben.
4. Bestätigen Sie Ihre Auswahl.
5. Geben Sie die E-Mail-Adresse und das Passwort Ihres Benutzerkontos in die entsprechenden Felder ein und tippen Sie auf **ANMELDEN**.

Welche Auswirkungen hat Bitdefender Mobile Security auf die Leistung und die Batterielebensdauer meines Geräts?

Die Auswirkungen sind minimal. Die Anwendung läuft nur, wenn es absolut notwendig ist, d.h. wenn Sie sie installieren, wenn Sie die Anwendung aufrufen oder eine Sicherheitsprüfung durchführen. Bitdefender Mobile Security läuft nicht im Hintergrund, wenn Sie Ihre Freunde anrufen, Nachrichten schreiben oder Spiele spielen.

Was ist ein Geräteadministrator?

Geräteadministrator ist eine Android-Funktion, über die Bitdefender Mobile Security die Berechtigungen erhält, die es zur Ausführung bestimmter Aktionen per Fernzugriff benötigt. Ohne diese Berechtigungen könnte die Fernsperrung nicht funktionieren und die Fernlöschung könnte Ihre Daten nicht löschen. Sollten Sie die App entfernen wollen, müssen Sie vor der Deinstallation diese Berechtigungen wieder entziehen unter **Einstellungen > Sicherheit > Geräteadministratoren auswählen**.

Behebung des "Kein Google-Token"-Fehlers, der bei der Anmeldung bei Bitdefender Mobile Security auftritt.

Dieser Fehler tritt auf, wenn das Gerät mit keinem Google-Konto verknüpft ist oder wenn es zwar mit einem Konto verknüpft ist, es aber wegen eines vorübergehenden Problems keine Verbindung zu Google herstellen kann. Die folgenden Schritte können das Problem beheben:

- Rufen Sie Android-Einstellungen > Anwendungen > Anwendungen verwalten > Bitdefender Mobile Security auf und tippen Sie auf **Daten löschen**. Melden Sie sich dann erneut an.
- Ihr Gerät muss mit einem Google-Konto verknüpft sein.
  Sie können das überprüfen, indem Sie Einstellungen -> Konten & Synchronisierung aufrufen und dort nachsehen, ob unter **Konten verwalten** ein Google-Konto aufgeführt ist. Fügen Sie Ihr Konto hinzu, falls es nicht aufgeführt ist, starten Sie das Gerät neu und melden Sie sich erneut bei Bitdefender Mobile Security an.
- Starten Sie Ihr Gerät neu, und versuchen Sie es dann erneut.

In welchen Sprachen ist Bitdefender Mobile Security erhältlich?

Bitdefender Mobile Security ist derzeit in den folgenden Sprachen verfügbar:

- Brasilianisch
- Tschechisch
- Niederländisch
- Englisch
- Französisch
- Deutsch
- Griechisch
- Ungarisch
- Italienisch
- Japanisch
- Koreanisch
- Polnisch
- Portugiesisch
- Rumänisch
- Russisch
- Spanish
- Schwedisch

- Thai
- Türkisch
- Vietnamesisch

Weitere Sprachen werden in zukünftigen Versionen hinzukommen. Um die Sprache der Bitdefender Mobile Security-Oberfläche zu ändern, rufen Sie die Einstellungen **Sprache & Tastatur** Ihres Geräts auf und legen Sie die gewünschte Sprache fest.

6. MOBILE SICHERHEIT FÜR IOS

6.1. Was ist Bitdefender Mobile Security for iOS?

Über das Internet kann man schnell und bequem Rechnungen bezahlen, Urlaube buchen sowie Waren und Dienstleistungen erwerben. Die verstärkte Nutzung dieser Online-Dienste geht jedoch auch mit hohen Risiken einher. Ohne die entsprechenden Sicherheitsvorkehrungen können personenbezogene Daten schnell in die falschen Hände gelangen. Was ist also wichtiger, als der Schutz der Daten, die in unseren Online-Konten und Smartphones zu finden sind?

Mit Bitdefender Mobile Security for iOS können Sie:

- Profitieren Sie von maximalem Schutz bei minimalen Auswirkungen auf die Akkulaufzeit
- Schützen Sie Ihre Daten: Passwörter, Adressen, persönliche und finanzielle Informationen
- Überprüfen Sie Ihr Telefon jederzeit auf Sicherheitslücken und beheben Sie gefährliche Fehlkonfigurationen
- Vermeiden Sie die unbeabsichtigte Preisgabe von Daten und Missbrauch durch installierte Anwendungen
- Scannt Ihr Gerät, um die optimalen Sicherheits- und Privatsphäreeinstellungen für Sie zu ermitteln
- Erhalten Sie Einblicke in Ihre Online-Aktivitäten und einen Überblick über verhinderte Vorfälle
- Überprüfen Sie Ihre Benutzerkonten auf Datenpannen und Datenlecks
- Verschlüsseln Sie Ihren Internetdatenverkehr mit dem integrierten VPN

Bitdefender Mobile Security for iOS wird kostenlos zur Verfügung gestellt und muss mit einem Bitdefender-Konto aktiviert werden. Einige wichtige Funktionen von Bitdefender, so z. B. unser 'Internet-Schutz', erfordern jedoch ein kostenpflichtiges Abonnement, um für unsere Nutzer zugänglich zu sein.

6.2. Erste Schritte

6.2.1. Systemanforderungen

Bitdefender Mobile Security for iOS läuft auf jedem Gerät ab iOS 12 und benötigt eine aktive Internetverbindung, um aktiviert zu werden und um zu erkennen, ob Ihre Online-Konten von Datenlecks betroffen sind.

6.2.2. Installation von Bitdefender Mobile Security for iOS

- **Über Bitdefender Central**
  - Für iOS
    1. Rufen Sie{1}Bitdefender Central{2} auf.
    2. Rufen Sie den Bereich {1}Meine Geräte{2} auf.
    3. Tippen Sie auf **SCHUTZ INSTALLIEREN** und dann auf **Dieses Gerät schützen**.
    4. Wählen Sie den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, tippen Sie auf die entsprechende Schaltfläche.
    5. Sie werden zur **App Store**-App weitergeleitet. Tippen Sie im App Store auf Installieren.
  - Für Windows, macOS, Android
    1. Zugang Bitdefender-Zentrale.
    2. Wähle aus **Meine Geräte** Tafel.
    3. Tippen Sie auf **SCHUTZ INSTALLIEREN** und dann auf **Andere Geräte schützen**.
    4. Wählen Sie den Besitzer des Geräts aus. Wenn das Gerät jemand anderem gehört, drücken Sie auf die entsprechende Schaltfläche.
    5. Tippen Sie auf **DOWNLOAD LINK SENDEN**.
    6. Geben Sie eine E-Mail-Adresse in das entsprechende Feld ein und tippen Sie auf **E-MAIL VERSENDEN**. Bitte beachten Sie, dass der generierte Download-Link nur für die nächsten 24 Stunden gültig ist. Nach Ablauf des Links müssen Sie

einen neuen Link generieren. Führen Sie dazu die bereits beschriebenen Schritte erneut aus.

7. Rufen Sie auf dem Gerät, auf dem Bitdefender installiert werden soll, das angegebene E-Mail-Konto auf und tippen Sie in der E-Mail auf die Download-Schaltfläche.

- **Über App Store**
  Suchen Sie nach Bitdefender Mobile Security for iOS, um die App aufzurufen und zu installieren.

Beim ersten Öffnen der App wird ein Einführungsfenster mit Informationen zu den Produktfunktionen angezeigt. Tippen Sie auf Erste Schritte, um das nächste Fenster zu öffnen.

Bevor Sie die Bestätigungsschritte abschließen können, müssen Sie zunächst der Abonnementvereinbarung zustimmen. Bitte nehmen Sie sich einen Moment Zeit, um die Abonnementvereinbarung zu lesen, da Sie hier die Bedingungen finden, unter denen Sie Bitdefender Mobile Security for iOS nutzen dürfen.

Tippen Sie auf **Fortfahren**, um zum nächsten Fenster zu gelangen.

6.2.3. Melden Sie sich bei Ihrem Bitdefender-Konto an

Zur Verwendung von Bitdefender Mobile Security for iOS müssen Sie Ihr Gerät mit einem Bitdefender-, Facebook-, Google-, Apple-, Microsoft-Konto verknüpfen, indem Sie sich über die App bei Ihrem Konto anmelden. Beim ersten Öffnen der App werden Sie zur Anmeldung bei einem Benutzerkonto aufgefordert.

So verknüpfen Sie Ihr Gerät mit einem Bitdefender-Konto:

1. Geben Sie die E-Mail-Adresse für Ihr Bitdefender-Benutzerkonto in das entsprechende Feld ein, und tippen Sie dann auf **WEITER**. Wenn Sie noch kein Bitdefender-Benutzerkonto haben und eines erstellen möchten, tippen Sie auf den entsprechenden Link und folgen Sie dann den Anweisungen auf dem Bildschirm, bis das Benutzerkonto aktiviert ist.
   Tippen Sie zur Anmeldung mit einem Facebook-, Google-, Apple- oder Microsoft-Konto im Bereich **Oder melded Sie sich an über** auf den entsprechenden Dienst. Sie werden zur Anmeldeseite des ausgewählten Dienstes weitergeleitet. Befolgen Sie die Anweisungen

zur Verknüpfung Ihres Benutzerkontos mit Bitdefender Mobile Security for iOS.

> **Notiz**
> Bitdefender hat keinen Zugriff auf Ihre vertraulichen Informationen, so zum Beispiel das Passwort, das Sie zur Anmeldung in Ihrem Konto verwenden, oder die persönlichen Informationen Ihrer Freunde und Kontakte.

2. Geben Sie Ihr Passwort ein und tippen danach Sie auf **ANMELDEN**.

Von hier aus gelangen Sie auch zur Bitdefender-Datenschutzerklärung.

6.2.4. Dashboard

Tippen Sie im App-Depot Ihres Geräts auf das Symbol für Bitdefender Mobile Security for iOS, um die Andwendungsoberfläche anzuzeigen.

Beim ersten Aufrufen der App werden Sie aufgefordert, Ihre Zustimmung zur Übermittlung von Bitdefender-Benachrichtigungen zu erteilen. Tippen Sie auf **Zulassen**, um von Bitdefender über alle relevanten Neuigkeiten zu Ihrer App auf dem Laufenden gehalten zu werden. Sie können die Bitdefender-Benachrichtigungen jederzeit unter Einstellungen > Benachrichtigungen > Mobile Security verwalten.

Tippen Sie auf das entsprechende Symbol am unteren Rand des Bildschirms, um den gewünschten Bereich aufzurufen.

Internet-Schutz

Stellen Sie eine sichere Internetnutzung sicher und verhindern Sie, dass weniger sichere Apps auf nicht vertrauenswürdige Domains zugreifen. Weitere Informationen finden Sie unter Internet-Schutz (Seite 239).

VPN

Schützen Sie Ihre Privatsphäre unabhängig davon, welches Netzwerk Sie gerade nutzen, indem Sie Ihre Kommunikation stets verschlüsseln. Weitere Informationen finden Sie unter VPN (Seite 241).

Kontoschutz

Erfahren Sie, ob Ihre E-Mail-Konten von Datenschutzverletzungen betroffen sind. Weitere Informationen finden Sie unter Kontoschutz (Seite 244).

Tippen Sie auf das ···-Symbol Ihres Gerätes, während Sie sich im Hauptmenü der Anwendung befinden, um weitere Optionen anzuzeigen. Die folgenden Optionen werden angezeigt:

- **Käufe wiederherstellen** - Hier können Sie frühere Abonnements, die Sie über Ihr iTunes-Konto erworben haben, wiederherstellen.
- **Einstellungen** - von hier aus haben Sie Zugriff auf:
  - **VPN-Einstellungen**
    - **Vereinbarung** - hier können Sie die Nutzungsbedingungen einsehen, unter denen Sie den Bitdefender VPN-Dienst nutzen dürfen. Wenn Sie auf **Ich bin nicht mehr einverstanden** tippen, können Sie Bitdefender VPN zumindest solange nicht nutzen, bis Sie wieder auf **Ich bin einverstanden** tippen.
    - **Warnung bei offenen WLAN-Netzwerken** - hier können Sie die Produktbenachrichtigung aktivieren oder deaktivieren, die bei jeder Verbindung mit einem ungesicherten WLAN-Netzwerk erscheint.
      Der Zweck dieser Benachrichtigung ist es, Ihnen dabei zu helfen, Ihre Daten durch die Verwendung von Bitdefender VPN vor unbefugten Zugriff zu schützen.
  - **Web-Schutz-Einstellungen**
    - **Vereinbarung** - hier können Sie die Nutzungsbedingungen einsehen, unter denen Sie den Bitdefender-Internet-Schutz-Dienst nutzen dürfen. Wenn Sie auf **Ich bin nicht mehr einverstanden** tippen, können Sie Bitdefender VPN zumindest solange nicht nutzen, bis Sie wieder auf **Ich bin einverstanden** tippen.
    - **Internet-Schutz-Benachrichtigung aktivieren** - Benachrichtigt Sie, dass der Internet-Schutz nach Beendigung einer VPN-Sitzung aktiviert werden kann.
  - **Produktberichte**
- **Feedback** - Hiermit starten Sie Ihre Standard-E-Mail-Anwendung, über die Sie uns Ihre Meinung zur App zukommen lassen können.
- **App-Info** - Hiermit rufen Sie Informationen zur installierten Version sowie die Abonnementvereinbarung, Datenschutzrichtlinie

und Informationen zur Einhaltung der Bedingungen von Open-Source-Lizenzen ein.

6.3. Scan

Mit Bitdefender Mobile Security for iOS können Sie Ihr Gerät auf Sicherheitslücken und potenzielle Bedrohungen scannen. Ein solcher Scan sucht nach:

- **Betriebssystemversion1}:** Sucht nach den neuesten Updates für Ihre iOS-Version.
- **Passcode/Biometrie:** Prüft, wie gut der Zugriff auf Ihr Gerät gesichert ist.
- **Internet-Schutz:** Überprüft den Status des Internet-Schutzmoduls.
- **Kontoschutz:** Sucht nach überwachten Benutzerkonten, die im Kontoschutzmodul aufgeführt sind.
- **WLAN prüfen:** Überprüft, wie sicher das Netzwerk ist, mit dem Sie gerade verbunden sind.

Der Schutzstatus wird nach einem manuellen Scan ermittelt.

Nach dem ersten Scan werden Sie von Bitdefenders Autopilot-Empfehlungen begrüßt. Der Autopilot ist Ihr persönlicher Sicherheitsberater, der Ihnen kontextbezogene Empfehlungen auf Grundlage Ihrer Gerätenutzung und Anforderungen gibt. Auf diese Weise können Sie wirklich alle Vorteile Ihrer App nutzen.

> **Notiz**
> Beim ersten Aufrufen der App werden Sie aufgefordert, einen Scan durchzuführen.

6.4. Betrugsalarm

Die in Bitdefender Mobile Security für iOS verfügbare Scam Alert-Funktion schützt Apple-Benutzer proaktiv vor Phishing-Betrügereien. Scam Alert für iOS umfasst zwei Schutzebenen, die Betrugsversuche überwachen, die über SMS/MMS-Nachrichten und Kalendereinladungen übermittelt werden:

- **Textnachrichtenfilter (SMS, MMS)**
  Diese Funktion identifiziert und filtert unerwünschte SMS- und MMS-Nachrichten.

Eine bösartige SMS/MMS (Short Message Service/Multimedia Messaging Service) bezieht sich auf eine Art von Nachricht, die mit schädlicher Absicht an mobile Geräte gesendet wird. Diese Nachrichten sollen Schwachstellen ausnutzen, Empfänger täuschen oder dem Gerät, den persönlichen Daten oder der Sicherheit des Ziels Schaden zufügen.

- **Kalender-Einladungs-Link-Scanner**
  Diese Funktion erkennt Spam-Kalender und -Ereignisse, die gefährliche Links enthalten. Der Kalendervirus ist eine Art Spam, der die Kalender-App Ihres iPhones befällt und lästig und potenziell gefährlich sein kann:
  - Sie erhalten unerwünschte Kalendereinladungen oder Ereignisbenachrichtigungen, wenn Sie versehentlich eine gefälschte Kalendereinladung annehmen, die von Hackern oder Spammern an Ihre E-Mail-Adresse gesendet wurde.
  - Wenn Sie auf den Link in der Einladung klicken, abonnieren Sie unwissentlich den Kalender des Absenders, wodurch dieser Ihnen weitere Spam-Ereignisse senden kann.
  - Die Spam-Ereignisse können Links oder Anhänge enthalten, die Sie beim Öffnen zu Phishing-Seiten oder anderen Cyber-Bedrohungen führen könnten.

6.4.1. So richten Sie den Betrugsalarm ein

Um die Betrugswarnung zu aktivieren, müssen Sie der Bitdefender Mobile Security-App Zugriff auf Kalenderbenachrichtigungen und SMS-Nachrichten gewähren:

So aktivieren Sie die SMS-Filterung:

Damit Bitdefender mit dem Filtern von Nachrichten beginnen kann, müssen Sie die Option „Unbekannte Absender filtern“ in den Einstellungen der Nachrichten-App manuell aktivieren:

1. Öffne das **Einstellungen** App auf Ihrem iPhone oder iPad.
2. Scrollen Sie nach unten und wählen Sie aus **Mitteilungen** In der Liste.
3. Tippen Sie auf die **Unbekannt und Spam** Abschnitt.
4. Umschalten **Filtern Sie unbekannte Absender** in die Ein-Position.

5. Wählen **Mobile Sicherheit** im Abschnitt SMS-Filterung und wählen Sie dann **Aktivieren**.

Bitdefender kann jetzt Junk-Nachrichten auf Ihrem iPhone/iPad filtern.

> **Notiz**
> Aufgrund von iOS-Einschränkungen kann die Bitdefender-SMS-Filterung nur für SMS- und MMS-Nachrichten verwendet werden, die von Personen stammen, die Sie nicht in Ihren Kontakten gespeichert haben. Das bedeutet, dass Nachrichten von Personen, die sich bereits in Ihrer Kontaktliste befinden, und iMessage-Nachrichten von niemandem gefiltert werden.

So aktivieren Sie den Kalender-Scan:

1. Öffne das **Bitdefender Mobile Security** App auf Ihrem iPhone oder iPad installiert.
2. Gehe zum **Betrugsalarm** Option in der unteren Navigationsleiste und drücken Sie **Jetzt einrichten**.
3. Klopfen **Weitermachen** und tippen Sie dann auf **Aktivieren**.
4. Wählen **OK** um Bitdefender Zugriff auf Ihren Kalender zu gewähren. Ein Kalenderscan beginnt sofort.

6.5. Scam Copilot

Bei dieser Funktion handelt es sich um einen KI-gestützter Chatbot, der von Bitdefender trainiert wurde, um verschiedene Betrugsszenarien, Phishing-Angriffe, Desinformationskampagnen und Fake-Websites zu erkennen.

So aktivieren Sie Scam Copilot:

1. Öffnen Sie die Bitdefender Mobile Security-App. Im Dashboard finden Sie eine eigene Kachel für den Scam Copilot. Tippen Sie auf **Aktivieren**.
2. Sie müssen die SMS-Filter wie unten beschrieben aktivieren:
   a. Öffnen Sie die **Einstellungen** auf Ihrem Gerät.
   b. Wählen Sie **Nachrichten** aus der Liste.
   c. Wählen Sie **Unbekannt und Spam**.
   d. Aktivieren Sie den Schalter bei **Unbekannte Absender filtern**.

e. Wählen Sie **Mobile Security** im SMS-Filter.

3. Tippen Sie danach auf**Fortfahren**.
4. Kalender-Scan aktivieren. Ein Pop-up erscheint kurz nachdem Sie die Schaltfläche **Aktivieren** gedrückt haben. Tippen Sie auf **Vollständigen Zugriff erlauben**.

Scam Copilot ist nun auf Ihrem Gerät konfiguriert.

Sie können jetzt auf den Reiter für den Scam Copilot zugreifen. Hier finden Sie:

- **Chatbot zur Betrugserkennungs:** Lassen Sie den Chatbot verdächtige Nachrichten überprüfen.
- **Präventionsassistent:** Hilft Ihnen, mehr über Betrugsmaschen zu erfahren und sich effektiver davor zu schützen.
- **Automatisches Erkennen von Betrugsversuchen:** Status und Kontrollzentrum.
- **SMS-Filter:** Lassen Sie gefährliche Nachrichten direkt in Ihrer Nachrichten-App filtern.

6.6. Internet-Schutz

Der Bitdefender-Internet-Schutz lässt Sie sicher im Netz surfen, indem es Sie vor potenziell schädlichen Webseiten warnt und Sie darauf hinweist, wenn weniger sichere installierte Apps versuchen, auf nicht vertrauenswürdige Domains zuzugreifen.

Wenn eine URL auf eine bekannte Phishing-Seite oder betrügerische Website oder auf schädliche Inhalte wie Spyware oder Viren verweist, wird die Webseite blockiert und eine Warnung angezeigt.

> **Wichtig**
> Wenn Sie sich in einer Region befinden, in dem die Nutzung eines VPN-Dienstes gesetzlich eingeschränkt ist, ist der Internet-Schutz nicht verfügbar.

So können Sie den Internet-Schutz aktivieren:

1. Tippen Sie auf das Symbol {1}{2}{3}{4}{5}{6} unten auf dem Bildschirm.
2. Tippen Sie auf **Ich bin einverstanden**.

3. Aktivieren Sie den Schalter bei Internet-Schutz.

> **Notiz**
> Beim ersten Aktivieren des Internet-Schutzes werden Sie unter Umständen aufgefordert, Bitdefender die Erlaubnis zur Einrichtung der VPN-Konfiguration zur Überwachung Ihres Netzwerkdatenverkehrs zu erteilen. Tippen Sie zum Fortfahren auf **Zulassen**. Wenn Sie zum Schutz Ihres Smartphones eine Authentifizierungsmethode (Fingerabdruck oder PIN) festgelegt haben, wird diese jetzt abgefragt. Um den Aufruf nicht vertrauenswürdiger Domains erkennen zu können, nutzt der Internet-Schutz die VPN-Dienste.

> **Wichtig**
> Der Internet-Schutz und das VPN können nicht gleichzeitig genutzt werden. Sobald eines von beiden aktiviert wird, wird das andere (wenn es zu diesem Zeitpunkt aktiv ist) deaktiviert.

6.6.1. Bitdefender-Benachrichtigung

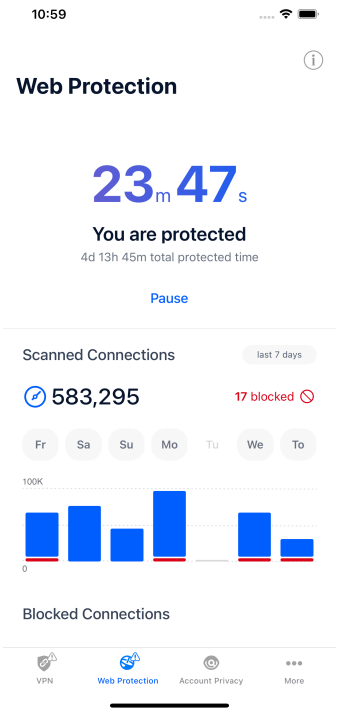
Wenn Sie versuchen, eine als unsicher eingestufte Website zu besuchen, wird die Website blockiert. Um Sie auf das Ereignis aufmerksam zu machen, werden Sie von Bitdefender in der Benachrichtigungszentrale und in Ihrem Browser benachrichtigt. Die Warnseite enthält Informationen wie die URL der Website und die erkannte Bedrohung, Sie müssen dann selbst entscheiden, wie Sie weiter vorgehen möchten.

Außerdem werden Sie in der Benachrichtigungszentrale benachrichtigt, wenn eine weniger sichere App versucht, auf nicht vertrauenswürdige Domains zuzugreifen. Tippen Sie auf die angezeigte Benachrichtigung, um ein Fenster aufzurufen, in dem Sie entscheiden können, wie Sie weiter vorgehen möchten.

Die folgenden Optionen stehen für beide Fälle zur Auswahl:

- Die Website durch Tippen auf **ICH GEHE LIEBER AUF NUMMER SICHER** verlassen.
- Die Website durch Tippen auf die angezeigte Benachrichtigung und danach auf **Ich möchte die Seite aufrufen** trotz Warnung aufrufen.

Bestätigen Sie Ihre Auswahl.



6.7. VPN

Mit Bitdefender VPN schützen Sie Ihre Daten bei Verbindungen mit ungesicherten WLAN-Netzwerken wie zum Beispiel in Flughäfen, Einkaufszentren, Cafés oder Hotels. So vermeiden Sie bedauerliche Vorfälle wie den Diebstahl Ihrer persönlichen Daten oder Versuche, Ihre Geräte-IP-Adresse für Hacker offenzulegen.

Das VPN dient als Tunnel zwischen Ihrem Gerät und dem Netzwerk, mit dem Sie sich verbinden. Ihre Verbindung wird abgesichert, Ihren Daten werden professionell nach Militärstandard verschlüsselt und Ihre IP-Adresse bleibt jederzeit unsichtbar. Ihr Datenverkehr wird über einen speziellen Server weitergeleitet, was es Ihrem Provider unmöglich macht, Ihr Gerät unter den unzähligen anderen Geräten zu identifizieren, die ebenfalls unsere Dienste in Anspruch nehmen. Darüber hinaus können Sie mit Bitdefender Password Manager im Internet auch auf solche

Inhalte zugreifen, die üblicherweise regionalen Zugangsbeschränkungen unterliegen.

> **Notiz**
> In manchen Ländern wird Internetzensur betrieben. Aus diesem Grund ist die Nutzung von VPNs hier gesetzlich verboten. Um rechtliche Konsequenzen zu vermeiden, wird Ihnen bei der ersten Nutzung der Bitdefender VPN-App eine Warnmeldung angezeigt. Durch die weitere Nutzung der App bestätigen Sie, dass Sie sich aller einschlägigen Rechtsvorschriften in Ihrem Land sowie der möglichen Risiken, denen Sie sich aussetzen, bewusst sind.

So können Sie Bitdefender VPN aktivieren:

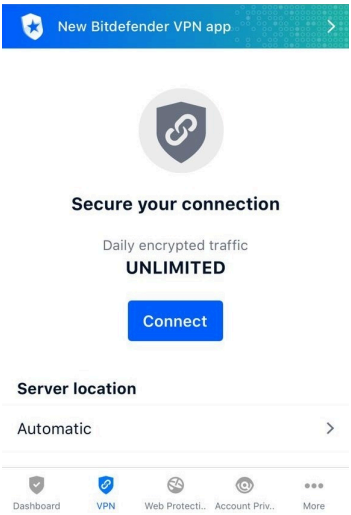
1. Tippen Sie auf die Symbol unten auf dem Bildschirm.
2. Tippen Sie auf **Verbinden**, um sich und Ihre Geräte bei Verbindungen mit ungesicherten WLAN-Netzwerken zu schützen.
   Tippen Sie auf **Trennen**, um die Verbindung wieder aufzuheben.

> **Notiz**
> Beim ersten Aktivieren des VPNs werden Sie aufgefordert, Bitdefender die Erlaubnis zur Einrichtung der VPN-Konfiguration zur Überwachung Ihres Netzwerkdatenverkehrs zu erteilen. Tippen Sie zum Fortfahren auf **Zulassen**. Wenn Sie zum Schutz Ihres Smartphones eine Authentifizierungsmethode (Fingerabdruck oder PIN) festgelegt haben, wird diese jetzt abgefragt.

Das VPN-Symbol wird bei aktivem VPN in der Statusleiste angezeigt.

Um Ihren Akku zu schonen, empfehlen wir Ihnen, VPN zu deaktivieren, wenn Sie es nicht mehr benötigen.

Falls Sie über ein Premium-Abonnement verfügen und sich mit einem Server Ihrer Wahl verbinden möchten, tippen Sie in der VPN-Benutzeroberfläche auf Automatisch und wählen Sie den gewünschten Standort aus. Weitere Details zu den VPN-Abonnements finden Sie unter Abonnements (Seite 243).



6.7.1. Abonnements

Mit Bitdefender VPN erhalten Sie ein kostenloses Datenvolumen von 200 MB pro Tag, um Ihre Verbindung bei Bedarf abzusichern. Sie werden automatisch mit dem besten Serverstandort verbunden.

Wenn Sie sich für ein Upgrade auf die Premium-Version entscheiden, entfällt das Datenlimit und Sie können durch die freie Wahl des Serverstandorts Inhaltsbeschränkungen überall auf der Welt umgehen.

Sie können jederzeit ein Upgrade auf Bitdefender Premium VPN vornehmen, indem Sie im VPN-Fenster auf **Premium VPN aktivieren** tippen. Sie können sich zwischen einem jährlichen und einem monatlichen Abonnement entscheiden.

Ein Bitdefender Premium-VPN-Abonnement läuft unabhängig von dem kostenlosen Bitdefender Mobile Security for iOS-Abonnement, d. h. Sie können es über den gesamten Verfügbarkeitszeitraum hinweg nutzen. Bei Ablauf des Bitdefender Premium-VPN-Abonnement kehren Sie automatisch zum kostenlosen Angebot zurück.

Bitdefender VPN ist plattformunabhängig und in den Windows-, macOS-, Android- und iOS-Produkten von Bitdefender verfügbar. Nach einem Premium-Upgrade können Sie Ihr Abonnement in allen Produkten nutzen, vorausgesetzt, dass Sie sich mit dem gleichen Bitdefender-Benutzerkonto anmelden.

Notiz

Bitdefender VPN ist auch als eigenständige Anwendung auf allen unterstützten Betriebssystemen einsetzbar, d. h. unter Windows, macOS, Android und iOS.

6.8. Kontoschutz

Der Bitdefender-Kontoschutz erkennt, ob die Datensicherheit der Benutzerkonten kompromittiert wurde, über die Sie Ihre Online-Zahlungen und -Einkäufe abwickeln und sich bei Ihren Apps oder Websites anmelden. Die unter Ihren Konten gespeicherten Daten umfassen Passwörter, Kreditkartendaten und Bankinformationen. Wurden diese nicht ausreichend abgesichert, kann es zu Identitätsdiebstahl und Verletzungen Ihrer Privatsphäre kommen.

Nach der Bestätigung wird der Privatsphärestatus des Benutzerkontos umgehend angezeigt.

Tippen Sie auf **Auf Datenlecks prüfen**, um zu prüfen, ob Ihre Benutzerkonten von Datenschutzverletzungen betroffen sind.

So können Sie Ihre persönlichen Daten schützen:

1. Tippen Sie auf die Symbol unten auf dem Bildschirm.
2. Tippen Sie auf **Konto hinzufügen**.
3. Geben Sie Ihre E-Mail-Adresse in das entsprechende Feld ein und tippen Sie danach auf **Weiter**.
   Bitdefender muss für dieses Konto vor der Preisgabe privater Daten erst eine Kontovalidierung durchführen. Sie erhalten zu diesem Zweck unter der angegebenen E-Mail-Adresse einen Bestätigungscode.
4. Rufen Sie Ihre E-Mails ab und geben Sie den erhaltenen Code in Ihrer App im Bereich **Kontoschutz** ein. Falls Sie Bestätigungs-E-Mail in Ihrem Posteingang nicht finden können, überprüfen Sie bitte Ihren Spam-Ordner.
   Der Privatsphärestatus des bestätigten Kontos wird angezeigt.

Wurden Datenschutzverletzungen bei einem Ihrer Benutzerkonten festgestellt, empfehlen wir Ihnen, so schnell wie möglich das entsprechende Passwort zu ändern. Mit diesen Tipps sorgen Sie für sichere Passwörter:

- Verwenden Sie mindestens acht Zeichen.
- Verwenden Sie Groß- und Kleinbuchstaben.
- Verwendenden Sie mindestens eine Zahl oder Sonderzeichen wie #, @, % oder !.

Nachdem Sie ein Konto gesichert haben, das von einer Datenpanne betroffen war, können Sie die Änderungen bestätigen, indem Sie die identifizierten Datenpannen als **Gelöst** markieren. Gehen Sie dazu wie folgt vor:

1. Tippen Sie neben der von Ihnen gelösten Datenpannen auf ···.
2. Tippen Sie auf **Als gelöst markieren**.

Wenn alle gefundenen Datenpannen als Gelöst markiert wurden, wird das Konto nicht mehr als von einer Datenpanne betroffen angezeigt, zumindest bis es zu einer weiteren Datenpanne kommt.

6.9. Häufig gestellte Fragen

Wie schützt mich Bitdefender Mobile Security for iOS vor Viren und Cyberbedrohungen?

Bitdefender Mobile Security for iOS bietet absoluten Schutz vor allen Cyberbedrohungen und wurde eigens entwickelt, um Ihre sensiblen Daten vor neugierigen Augen zu schützen.

Sie erhalten eine Vielzahl an leistungsfähigen Sicherheits- und Datenschutzfunktionen für Ihr iPhone oder iPad - und dazu Bonusfunktionen, einschließlich VPN und Internet-Schutz.

Bitdefender Mobile Security for iOS reagiert umgehend auf Viren und Malware, ohne die Leistung Ihres Systems zu beeinträchtigen.

Für welche Geräte und Betriebssysteme ist Bitdefender Mobile Security for iOS geeignet?

Bitdefender Mobile Security for iOS schützt Ihre unter iOS laufenden Smartphones und Tablets vor allen Cyberbedrohungen.

Warum benötige ich Bitdefender Mobile Security for iOS auf Computern mit Apple OS?

Auf Ihrem iPhone oder iPad sind sehr persönliche Daten gespeichert. Da müssen sich jederzeit darauf verlassen können, dass diese Daten geschützt sind. Mit Bitdefender Mobile Security for iOS sind Sie absolut

sicher vor Cyberbedrohungen und brauchen sich keine Gedanken um den Schutz Ihrer privaten Daten zu machen, wenn Sie online sind, ohne dass Ihre täglichen Aktivitäten im Internet dadurch behindert werden.

Erhalte ich mit meinen Bitdefender Mobile Security for iOS-Abonnement auch ein VPN?

Bitdefender Mobile Security for iOS beinhaltet eine Basisversion von Bitdefender VPN inkl. kostenlosem großzügigem Datenvolumen (200 MB pro Tag, 6 GB pro Monat).

7. VPN

7.1. Was ist Bitdefender Password Manager

Das VPN dient als Tunnel zwischen Ihrem Gerät und dem Netzwerk, mit dem Sie eine Verbindung herstellen, um Ihre Verbindung zu sichern, die Daten mit militärischer Verschlüsselung zu verschlüsseln und Ihre IP-Adresse zu verbergen, egal wo Sie sich befinden. Ihr Datenverkehr wird über einen separaten Server umgeleitet; Dies macht es unmöglich, Ihr Gerät von Ihrem ISP anhand der unzähligen anderen Geräte, die unsere Dienste nutzen, zu identifizieren. Darüber hinaus können Sie, während Sie über Bitdefender VPN mit dem Internet verbunden sind, auf Inhalte zugreifen, die normalerweise in bestimmten Bereichen eingeschränkt sind.

Hinweis
In einigen Ländern wird das Internet zensiert, weshalb der Einsatz von VPN dort gesetzlich nicht erlaubt ist. Um rechtliche Folgen vorzubeugen, kann es sein, dass eine Warnmeldung angezeigt wird, wenn Sie zum ersten Mal versuchen, die Funktion von Bitdefender Password Manager zu verwenden. Wenn Sie die Funktion dann verwenden, bestätigen Sie damit, dass Sie die relevanten Bestimmungen Ihres Landes kennen und sich der entsprechenden Risiken bewusst sind.

7.1.1. Verschlüsselungsprotokolle

Die Standard-Cipher-Suiten, die im Hydra-Client und -Server aktiviert sind, sind unten angegeben. Alle anderen Cipher-Suiten sind deaktiviert.

Hydra-Client-Cipher-Suites:

- ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

Hinweis

Das serverseitige Set ist deutlich restriktiver; sowohl der Hydra-Client als auch der -Server lehnen alle Modi außer GCM mit AES ab. Der Hydra-Server erfordert serverseitige Priorität stärkerer Ciper-Suiten und lehnt TLS-Handshakes ab, wenn eine schwächere Suite von einem Client angefordert wird. Diese Liste ist während der Laufzeit auf der Server-Seite konfigurierbar.

7.2. Installation

7.2.1. Vor der Installation

Bevor Sie Bitdefender Password Manager installieren, sollten Sie für eine reibungslose Installation sicherstellen, dass folgende Schritte durchgeführt wurden:

- Stellen Sie sicher, dass das Zielgerät für die Bitdefender-Installation die Systemvoraussetzungen erfüllt. Wenn das Gerät die Systemvoraussetzungen nicht erfüllt, kann Bitdefender nicht installiert werden. Falls es doch installiert wird, kann es zu Leistungseinbußen und Stabilitätsproblemen kommen.

  Eine vollständige Liste der Systemanforderungen finden Sie unter Systemanforderungen (Seite 248).
- Melden Sie sich mit einem Administrator-Konto am Gerät an.
- Ihr Gerät sollte während der Installation mit dem Internet verbunden sein, auch wenn Sie von CD oder DVD installieren. Falls neuere Versionen der Anwendungsdateien aus dem Installationspaket verfügbar sind, kann Bitdefender diese dann herunterladen und installieren.

7.2.2. Systemanforderungen

- **Für Windows-Benutzer**
  - **Betriebssystem:** Windows 7 mit Service Pack 1, Windows 8, Windows 8.1, Windows 10 und Windows 11
  - **Speicher (RAM):** 1 GB
  - **Verfügbarer freier Festplattenspeicher:** 500 MB freier Speicher
  - **.NET Framework:** Mindestversion 4.5.2

Wichtig
Die Systemleistung kann auf Geräten mit CPUs der alten Generation beeinträchtigt werden.

- **Für macOS-Benutzer**
  - **Betriebssystem:** macOS Sierra (10.12) und höher
  - **Verfügbarer freier Festplattenspeicher:** 100 MB freier Speicher
- **Für Android-Benutzer**
  - **Betriebssystem:** Android 5.0 oder höher
  - **Speicher:** 100 MB
  - Eine aktive Internet-Verbindung
- **Für iOS-Benutzer**
  - **Betriebssystem:** iOS 12 und höher
  - **Speicher auf iPhone:** 50 MB
  - **Speicher auf iPad:** 100 MB
  - Eine aktive Internetverbindung

7.2.3. Bitdefender Password Manager wird installiert

Folgen Sie den Installationsanweisungen für Ihr Betriebssystem:

- **Für Windows-Benutzer**
  1. Um Bitdefender Password Manager auf einem Windows-PC zu installieren, laden Sie einfach das Installationspaket von https://www.bitdefender.com/solutions/vpn/download herunter. Alternativ können Sie den Download auch über die E-Mail starten, die Sie nach dem Kauf erhalten haben.
  2. Doppelklicken Sie auf das heruntergeladene Installationsprogramm, um es auszuführen.
  3. Wenn das Dialogfenster der Benutzerkontensteuerung angezeigt wird, klicken Sie auf Ja.
  4. Warten Sie, bis der Download abgeschlossen ist.

5. Wählen Sie über das Klappmenü im Installer die Sprache, in der die Software installiert werden soll.
6. Markieren Sie das Kästchen neben „Hiermit bestätige ich, dass ich die Nutzungsbedingungen und die Datenschutzerklärung gelesen habe und sie akzeptiere“ und klicken Sie dann auf **INSTALLATION STARTEN**.
7. Warten Sie, bis der Installationsvorgang abgeschlossen ist.
8. Jetzt können Sie sich mit Ihrem Bitdefender Central-Konto **ANMELDEN**. Wenn Sie noch kein Central-Konto haben, können Sie über die Schaltfläche **KONTO ERSTELLEN** ein neues Konto erstellen.
9. Wählen Sie **Ich habe einen Aktivierungscode**, wenn Sie bereits einen Premium VPN-Abonnement erworben haben.
   Alternativ können Sie auf **TESTPHASE BEGINNEN** klicken und damit die Software 7 Tage lang kostenlos testen, bevor Sie eine Kaufentscheidung treffen.
10. Geben Sie den Code ein, den Sie per E-Mail erhalten haben, und klicken Sie dann auf **PREMIUM AKTIVIEREN**.
11. Nach kurzer Wartezeit ist Bitdefender Password Manager installiert und Sie können es auf Ihrem Computer nutzen.

❍ **Für macOS-Benutzer**

1. Um Bitdefender Password Manager auf macOS zu installieren, laden Sie einfach das Installationspaket von https://www.bitdefender.com/solutions/vpn/download herunter. Alternativ können Sie den Download auch über die E-Mail starten, die Sie nach dem Kauf erhalten haben.
2. Der Installer wird auf Ihrem Mac gespeichert. Doppelklicken Sie auf die -Paket-Datei im Downloads-Ordner.
3. Folgen Sie den angezeigten Anweisungen. Klicken Sie dann auf **Fortfahren**.
4. Sie werden Schritt für Schritt durch die Installation von Bitdefender Password Manager auf Ihrem Mac geleitet. Klicken Sie zweimal auf **Fortfahren**.

5. Klicken Sie, wenn Sie die Lizenzvereinbarung gelesen haben und sie akzeptieren, auf **Zustimmen**.
6. Klicken Sie auf **Installieren**.
7. Geben Sie den Benutzernamen und das Kennwort eines Administrators ein und klicken Sie danach auf **Software installieren**.
8. Sie erhalten eine Meldung, dass eine von Bitdefender signierte Systemerweiterung blockiert wurde. Dabei handelt es sich nicht um einen Fehler, sondern nur um eine Sicherheitsmaßnahme. Klicken Sie auf **Sicherheitseinstellungen öffnen**.
9. Klicken Sie auf das Schlosssymbol, um die Sperre aufzuheben. Geben Sie Namen und Passwort eines Administrators ein und klicken Sie dann auf **Freischalten**.
10. Klicken Sie auf **Zulassen**, um die Systemerweiterung für Bitdefender Bitdefender zu laden. Schließen Sie dann das Fenster Sicherheit und Datenschutz und das Bitdefender-Installationsprogramm.
11. Klicken Sie auf das Schildsymbol in der Menüleiste und **melden Sich sich** an Ihrem Bitdefender-Central-Konto an. Wenn Sie noch keines haben, erstellen Sie bitte eines.
12. Wählen Sie **Ich habe einen Aktivierungscode**, wenn Sie bereits einen Premium-VPN-Abonnement erworben haben. Ansonsten können Sie wählen **TESTVERSION STARTEN** um das Produkt 7 Tage lang kostenlos zu testen, bevor Sie sich zur Zahlung verpflichten.
13. Geben Sie den per E-Mail erhaltenen Code ein und klicken Sie dann auf **Aktiviere Code** Taste.
14. Nach kurzer Wartezeit ist Bitdefender Password Manager installiert und Sie können es auf Ihrem Mac nutzen.

❍ **Für Android-Benutzer**

1. Auf Android-Geräten installieren Sie Bitdefender Password Manager, indem Sie zunächst den **Google Play Store** auf Ihrem Smartphone oder Tablet öffnen.

2. Suchen Sie nach Bitdefender Password Manager und wählen Sie die entsprechende App aus.
3. Tippen Sie auf die Schaltfläche **Installieren** und warten Sie, bis der Download abgeschlossen ist.
4. Tippen Sie auf **Öffnen**, um die App zu starten.
5. Markieren Sie das Kästchen neben „Ich akzeptiere die Nutzungsbedingungen und Datenschutzerklärung“ und tippen Sie auf **Fortfahren**.
6. Jetzt können Sie sich mit Ihrem Bitdefender Central-Konto **Anmelden**. Wenn Sie noch kein Central-Konto haben, können Sie über die Schaltfläche **Konto erstellen** ein neues Konto erstellen.
7. Wählen Sie {1}Ich habe einen Aktivierungscode{2}, wenn Sie bereits einen Premium-VPN-Abonnement erworben haben.
   Alternativ können Sie auf „7-tägige Testphase starten“ klicken und damit die Software 7 Tage lang kostenlos testen, bevor Sie eine Kaufentscheidung treffen.
8. Geben Sie den Code ein, den Sie per E-Mail erhalten haben, und tippen Sie dann auf **Code aktivieren**.

❍ **Für iOS-Benutzer**

1. Öffnen Sie zur Installation von Bitdefender Password Manager unter iOS zunächst den **App Store** auf Ihrem iPhone oder iPad.
2. Suchen nach Bitdefender Password Manager und wählen Sie diese App aus.
3. Tippen Sie auf das Symbol **Herunterladen** und warten Sie, bis der Download abgeschlossen ist.
4. Klopfen **Offen** um die App auszuführen.
5. Markieren Sie das Kästchen neben **Ich akzeptiere die Nutzungsbedingungen und die Datenschutzerklärung** und tippen Sie auf **Fortfahren**.
6. Jetzt können Sie sich mit Ihrem Bitdefender Central-Konto **Anmelden**. Wenn Sie noch kein Konto haben, können Sie über die Schaltfläche **Konto erstellen** ein neues Konto erstellen.

7. Tippen Sie auf **Zulassen**, wenn Sie Benachrichtigungen von Bitdefender Password Manager erhalten möchten.
8. Wählen **Ich habe einen Aktivierungscode** wenn Sie ein Premium-VPN-Abonnement erworben haben.
   Andernfalls können Sie 7 Tage Testversion starten auswählen, um das Produkt 7 Tage lang kostenlos zu testen, bevor Sie sich zur Zahlung verpflichten.
9. Geben Sie den per E-Mail erhaltenen Code ein und tippen Sie dann auf **Aktiviere Code**.

7.3. Bitdefender VPN richtig nutzen

7.3.1. Bitdefender VPN öffnen

- **Unter Windows**
  Es gibt verschiedene Möglichkeiten, das **Bitdefender VPN-Hauptfenster** zu öffnen:
  - **Über die Taskleiste**
    Rechtsklicken Sie auf das rote Schildsymbol in der Taskleiste und wählen Sie dann im Menü **Anzeigen**.
  - **Über die Bitdefender-Benutzeroberfläche**
    Wenn bereits ein Bitdefender-Sicherheitsprodukt wie z. B. Bitdefender Total Security oder Bitdefender Antivirus Plus auf Ihrem Windows-Computer installiert ist, können Sie Bitdefender VPN auch von dort aus öffnen:
    1. Klicken Sie links in der Bitdefender-Benutzeroberfläche auf **Privatsphäre**.
    2. Klicken Sie im VPN-Bereich auf **VPN öffnen**.
  - **Über Ihren Desktop**
    Doppelklicken Sie auf die Bitdefender VPN-Verknüpfung auf Ihrem Desktop.
- **Unter macOS**
  Sie können die Bitdefender VPN-App öffnen, indem Sie auf das Symbol in der Menüleiste oben rechts auf dem Bildschirm klicken.

Wenn Sie das Bitdefender-Schild in der Menüleiste nicht finden können, verwenden Sie das Mac-Launchpad oder den Finder, um es wieder anzuzeigen:

- **Über das Launchpad**
  1. Drücken Sie **F4** auf Ihrer Tastatur, um das Launchpad auf Ihrem Mac aufzurufen.
  2. Suchen Sie unter den installierten Apps nach der Bitdefender VPN-App oder geben Sie **Bitdefender VPN** im Launchpad ein, um die Ergebnisse zu filtern.
  3. Wenn Sie die Bitdefender VPN-App gefunden haben, können Sie auf das entsprechende Symbol klicken, um sie an die Menüleiste anzuheften.

- **Über den Finder**
  1. Klicken Sie unten links im Dock auf den **Finder** (das blaue Quadrat mit dem lächelnden Gesicht).
  2. Klicken Sie danach auf **Los** in der Menüleiste oben links auf dem Bildschirm.
  3. Wählen Sie im Menü die Option **Programme**, um den Ordner Programme auf Ihrem Mac aufzurufen.
  4. Öffnen Sie im Ordner Programme den Ordner **Bitdefender** und doppelklicken Sie dann auf die **Bitdefender VPN**-App.

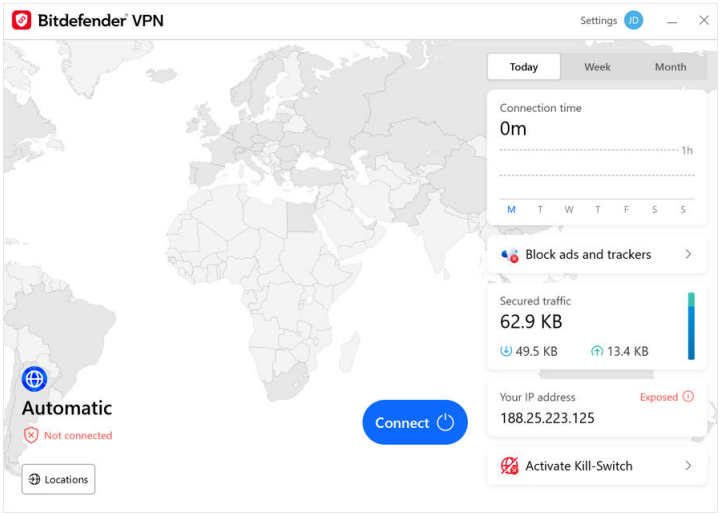
Hinweis

Um Bitdefender VPN auf Ihren Android- oder iOS-Mobilgeräten aufzurufen, müssen Sie Bitdefender VPN-App nach der Installation lediglich öffnen.

7.3.2. Verbindung mit Bitdefender Password Manager herstellen

In der VPN-Benutzeroberfläche wird der Status der App angezeigt, verbunden oder getrennt. Der Serverstandort wird für Anwender mit der kostenlosen Version von Bitdefender automatisch auf den geeignetsten Server festgelegt. Premium-Anwender können den Serverstandort selbst wählen, indem sie ihn aus der Liste Virtueller Standort auswählen.

Zum Herstellen bzw. Trennen der Verbindung müssen Sie in der VPN-Oberfläche lediglich auf die Einschalttaste klicken.



- **Unter Windows:** Das Symbol in der Taskleiste zeigt ein grünes Häkchen an, wenn das VPN verbunden ist. Ein schwarzes Häkchen zeigt an, dass keine VPN-Verbindung besteht. Wenn eine Verbindung zu einem manuell ausgewählten Standort besteht, wird die IP-Adresse im Hauptfenster angezeigt.
- **Unter macOS:** Das Symbol in der Menüleiste ist schwarz, wenn das VPN verbunden ist, und weiß, wenn die VPN-Verbindung getrennt ist. Klicken Sie auf die kreisförmige Schaltfläche in der Mitte der Benutzeroberfläche und warten Sie, bis die Verbindung hergestellt wird.
- **Unter Android & iOS:** So stellen Sie unter Android, iOS und iPadOS eine Bitdefender VPN-Verbindung her:
  - **In der Bitdefender VPN-App:** Zum Herstellen bzw. Trennen der Verbindung müssen Sie in der VPN-Oberfläche lediglich auf die Einschalttaste tippen. Der Status von Bitdefender VPN wird angezeigt.
  - **In der Bitdefender Mobile Security-App:**

1. Rufen Sie das VPN-Symbol in der unteren Navigationsleiste von Bitdefender Mobile Security auf.
2. Tippen Sie auf **VERBINDEN**, um sich bei Verbindungen mit ungesicherten WLAN-Netzwerken zu schützen. Tippen Sie auf **TRENNEN**, wenn Sie die VPN-Verbindung deaktivieren möchten.

7.3.3. Verbindung mit einem anderen Server herstellen

Mit einem Premium-Abonnement können Sie mit Bitdefender Password Manager jederzeit eine Verbindung zu einem unserer Server in aller Welt herstellen. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie die Bitdefender Password Manager-App.
2. Tippen Sie im unteren Bereich der Programmoberfläche auf die Schaltfläche **Virtueller Standort**.
3. Wählen Sie ein beliebiges Land aus.
4. Klicken Sie unten auf die Schaltfläche **Verbindung nach [Land] aufbauen**.

- Das Taskleistensymbol zeigt ein grünes Häkchen an, wenn das VPN verbunden ist.
- Die IP-Adresse des virtuellen Servers wird auf dem Startbildschirm angezeigt, während eine Verbindung mit Bitdefender VPN besteht.
- Eine Zusammenfassung Ihrer Verbindungszeit, die Menge des gesicherten Datenverkehrs und die letzten 5 Standorte, mit denen Sie eine Verbindung hergestellt haben, werden ebenfalls auf dem Haupt-Dashboard angezeigt.

7.4. Einstellungen & Funktionen von Bitdefender Password Manager

7.4.1. Einstellungen aufrufen

Die Bitdefender Password Manager-Einstellungen finden Sie auf folgendem Wege:

- **Unter Windows**

1. Öffnen Sie Bitdefender Password Manager, indem Sie auf das Symbol in der Taskleiste doppelklicken oder indem Sie mit der rechten Maustaste darauf klicken und „Anzeigen“ wählen.
2. Klicken Sie links auf die Schaltfläche **Einstellungen** (ein Zahnradsymbol).

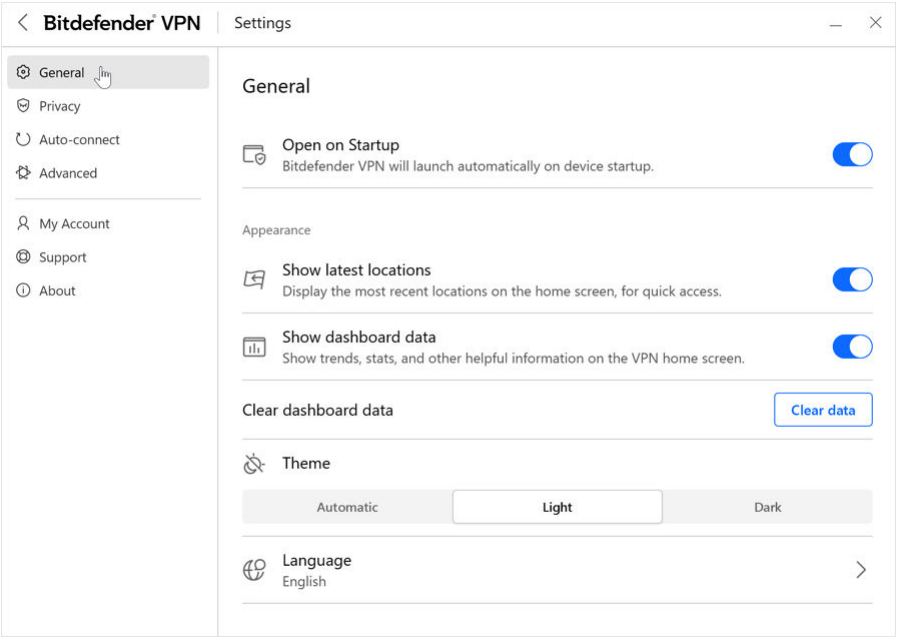
- **Unter macOS**
  1. Öffnen Sie Bitdefender Password Manager auf Ihrem macOS-Gerät, indem Sie in der Menüleiste auf das entsprechende Symbol klicken.
  2. Klicken Sie rechts oben in der Bitdefender Password Manager-Oberfläche auf das Zahnradsymbol und wählen Sie „Einstellungen“.
- **Unter Android**
  1. Öffnen Sie die Bitdefender Password Manager-App auf Ihrem Gerät.
  2. Klicken Sie rechts oben in der Bitdefender Password Manager-Oberfläche auf das Zahnradsymbol.
- **Unter iOS**
  1. Öffne das Bitdefender Password Manager App auf Ihrem Gerät.
  2. Klicken Sie auf die Zahnradschaltfläche in der oberen rechten Ecke des Bitdefender Password Manager Schnittstelle.

7.4.2. Allgemein

Hier können Sie Folgendes ändern:

- **Beim Start öffnen**– Bitdefender VPN wird beim Gerätestart automatisch gestartet.
- **Neueste Standorte anzeigen**– Zeigen Sie die neuesten Standorte auf dem Startbildschirm an, um schnell darauf zugreifen zu können.
- **Dashboard-Daten anzeigen** – Zeigen Sie Trends, Statistiken und andere hilfreiche Informationen auf dem VPN-Startbildschirm an.
- **Löschen Sie Dashboard-Daten**– Alle Ihre Dashboard-Daten werden gelöscht und alle Zähler zurückgesetzt.

- **Thema**– Hell/Dunkel-Thema
- **Sprache**– Ändern Sie die Sprache von Bitdefender VPN.
- **Benachrichtigungen**– Verwalten Sie Ihre Benachrichtigungseinstellungen.
- **Helfen Sie mit, Bitdefender VPN zu verbessern**– Senden Sie anonyme Produktberichte, um uns zu helfen, Ihr Erlebnis zu verbessern.
- **Alle Einstellungen zurücksetzen**– Setzen Sie das VPN auf seine ursprünglichen Einstellungen zurück, ohne es neu zu installieren.



7.4.3. Funktionen

Privatsphäre

Internet Kill-Switch

Die Not-Aus-Funktion ist eine weitere Neuerung in Bitdefender Password Manager. Wenn diese Funktion aktiviert ist, wird sämtlicher Internet-

Datenverkehr gestoppt, falls die VPN-Verbindung aus irgend einem Grund abreißen sollte. Sobald der Zugang zum Internet wieder steht, wird die VPN-Verbindung wieder hergestellt.

So aktivieren Sie die Not-Aus-Funktion:

- **Unter Windows**
  1. Öffnen Sie die Bitdefender Password Manager-App auf Ihrem Gerät, indem Sie auf das entsprechende Symbol in der Taskleiste doppelklicken oder mit der rechten Maustaste darauf klicken und **Anzeigen** auswählen.
  2. Klick auf das **Einstellungen** Schaltfläche (dargestellt durch ein Zahnrad) auf der linken Seite der Benutzeroberfläche.
  3. Wählen Sie **Erweitert**.
  4. Aktivieren Sie die Option **Internet-Not-Aus**.

- **Auf Android**
  1. Öffne das Bitdefender Password Manager App auf Ihrem Gerät.
  2. Klicken Sie auf die Zahnradschaltfläche in der oberen rechten Ecke des Bitdefender Password Manager Schnittstelle.
  3. Aktivieren Sie unter **Einstellungen** die Option **Internet-Not-Aus**.

- **Auf iOS**
  1. Öffne das Bitdefender Password Manager App auf Ihrem Gerät.
  2. Klicken Sie auf die Zahnradschaltfläche in der oberen rechten Ecke des Bitdefender Password Manager Schnittstelle.
  3. Unter **Einstellungen**, aktivieren Sie die **Notausschalter** Möglichkeit.

     Hinweis
     Diese Funktion ist auch für macOS-Geräte ab Betriebssystemversion 10.15.4 verfügbar.

Werbeblocker und Anti-Tracker

Diese Funktionen sollen Ihnen helfen, Ihre Privatsphäre zu wahren und das Internet in vollen Zügen zu genießen, ohne von aufdringlicher

Werbung und neugierigen Unternehmen belästigt zu werden. Sie helfen Ihnen dabei, Werbung zu blockieren und Online-Tracking zu unterbinden.

Werbeblocker

Der **Werbeblocker** blockiert Werbeanzeigen, Pop-ups, laute Videowerbung und Werbebanner. So können Websites schneller geladen, übersichtlicher angezeigt und sicherer genutzt werden.

So aktivieren Sie den Werbeblocker:

1. Suchen Sie in den **Einstellungen** die Funktion **Werbeblocker und Anti-Tracker**.
2. Setzen Sie den Schalter auf die Position **EIN**.

Anti-Tracker

Mit dem **Anti-Tracker** blockieren Sie Tracker, die von Werbetreibenden eingesetzt werden, um Ihre Online-Aktivitäten nachzuverfolgen und Profile von Ihnen zu erstellen. Einige Websites funktionieren möglicherweise nicht, wenn Tracker blockiert werden, aber durch Hinzufügen der URL zu Ihrer Whitelist können Sie hier Abhilfe schaffen.

So aktivieren Sie den Anti-Tracker:

1. Suchen Sie die **Werbeblocker und Antitracker** Funktion ein **Einstellungen**.
2. Schalten Sie den Schalter auf die um **AN** Position.

Whitelist

Einige Websites werden möglicherweise nicht ordnungsgemäß geladen, wenn Sie ihren Tracker-Code und ihre Werbung blockieren. Wenn Sie die URLs dieser Domänen zur Whitelist hinzufügen, kann dieses Problem zwar behoben werden, aber bedenken Sie, dass Ihnen beim Aufrufen dieser Websites Werbung angezeigt wird und Tracker-Code aktiv ist.

Gehen Sie wie folgt vor, um Websites hinzufügen, für die Sie die Anzeige von Werbung und die Verwendung von Trackern erlauben möchten:

1. Suchen Sie die **Werbeblocker und Antitracker** Funktion ein **Einstellungen**.

2. Klicken Sie auf den **Verwalten**-Link. Wechseln Sie dann zum Abschnitt Whitelist in diesem Fenster und klicken Sie auf den entsprechenden **Verwalten**-Link.
3. Klicken Sie auf **Website hinzufügen** und geben Sie die gewünschte URL ein.

Autom. verbinden

Egal ob unterwegs, bei der Arbeit in einem Café oder beim Warten am Flughafen: Oftmals ist es am bequemsten, sich mit einem öffentlichen WLAN zu verbinden, um Zahlungen anzuweisen, E-Mails abzurufen oder einen schnellen Blick in soziale Netzwerke zu werfen. Aber hier können auch Datenjäger lauern, die nur darauf warten, dass Ihre persönlichen Daten durch das Netzwerk wandern.

Zum Schutz vor den Gefahren ungesicherter oder unverschlüsselter öffentlicher WLAN-Hotspots verfügt Bitdefender Password Manager über die Funktion zur automatischen Verbindungsherstellung. Damit wird Bitdefender Password Manager, je nach Ihren vorgenommenen Einstellungen und Ihrem Betriebssytem, in bestimmten Situationen automatisch aktiviert.

- Unter **Windows** kann die Funktion zur automatischen Verbindungsherstellung für die folgenden Szenarien aktiviert werden:
  - **Start:** Mit VPN beim Start von Windows verbinden.
  - **Ungesichertes WLAN:** Das VPN bei allen Verbindungen mit öffentlichen oder ungesicherten WLAN-Netzwerken verwenden.
  - **Peer-to-Peer-Apps:** VPN-Verbindung herstellen, wenn eine Peer-to-Peer-Filesharing-App gestartet wird.
  - **Apps und Domänen:** Das VPN grundsätzlich für bestimmte Apps und Websites verwenden.

    Hinweis

    1. Klicken Sie auf den **Verwalten**-Link.
    2. Suchen Sie nach der App, für die Sie das VPN verwenden möchten, markieren Sie den Namen der App und klicken Sie dann auf **Hinzufügen**.

  - **Website-Kategorien:** VPN-Verbindung beim Besuch bestimmter Website-Kategorien herstellen. Bitdefender VPN kann

automatische Verbindungen für die folgenden Website-Kategorien herstellen:

- Finanzen
- Online-Zahlungen
- Gesundheitswesen
- Filesharing
- Online-Partnersuche
- Nicht jugendfreie Inhalte

> **Hinweis**
> Sie können für jede Kategorie einen anderen Server auswählen, mit dem sich das VPN verbinden soll.

- Unter **macOS** kann die Funktion zur automatischen Verbindungsherstellung für die folgenden Szenarien aktiviert werden:
  - **Start:** Mit VPN beim Start von macOS verbinden.
  - **Ungesichertes WLAN:** Verwenden Sie das VPN, wenn Sie sich mit öffentlichen oder ungesicherten WLAN-Netzwerken verbinden.
  - **Peer-to-Peer-Apps:** Stellen Sie eine Verbindung zum VPN her, wenn Sie eine Peer-to-Peer-Dateifreigabe-App starten.
  - **Anwendungen:** Für bestimmte Apps immer eine VPN-Verbindung herstellen.
- Unter **Android** und **iOS**> kann die Funktion zur automatischen Verbindungsherstellung von Bitdefender Password Manager nur für Verbindungen mit ungesicherten oder öffentlichen WLAN-Netzwerken aktiviert werden.

Fortschrittlich

Split Tunneling

Das Split Tunneling in Ihrem VPN ist eine Funktion, mit der Sie einen Teil des Datenverkehrs Ihrer Geräte und Anwendungen durch ein verschlüsseltes VPN leiten können, während andere Anwendungen oder Geräte direkt auf das Internet zugreifen. Dies ist zum Beispiel

nützlich, wenn Sie Dienste nutzen möchten, die für eine ordnungsgemäße Funktion Ihren Standort benötigen, gleichzeitig aber potenziell sensible Kommunikationsverbindungen und Daten absichern möchten.

Wenn Sie die Funktion **Split Tunneling** aktivieren, umgehen ausgewählte Apps und Websites das VPN und greifen direkt auf das Internet zu.

Gehen Sie wie folgt vor, um die Anwendungen und Websites zur Umgehung des VPNs festzulegen:

1. Klicken Sie nach Aktivierung der Funktion auf den **Verwalten**-Link.
2. Klicken Sie auf **Hinzufügen**.
3. Suchen Sie nach der jeweiligen Anwendung bzw. geben Sie die URL der gewünschten Website ein und klicken Sie auf **Hinzufügen**.

> **Hinweis**
> Wenn Sie eine Website hinzufügen, gilt die Umgehung für die gesamte Domäne einschließlich aller Unterdomänen.

> **Wichtig**
> Auf **macOS**-Geräten ist das Split Tunneling nur für Websites verfügbar.

App Traffic Optimizer

Mit dem App Traffic Optimizer in Bitdefender Password Manager können Sie den Datenverkehr für die wichtigsten Apps auf Ihrem Gerät priorisieren, ohne dass Sie mit Ihrer Verbindung Risiken für Ihre Privatsphäre eingehen. VPNs leiten den Internetverkehr durch einen sicheren Tunnel um und schützen ihn mit zuverlässigen Verschlüsselungsalgorithmen.

Die Kombination dieser Verfahren kann jedoch auch Nachteile haben, vor allem mit Blick auf die Verbindungsgeschwindigkeit. Dabei kann die Verbindung durch verschiedene Faktoren ausgebremst werden. Die häufigsten sind die Entfernung zum genutzten Server, Netzwerküberlastungen und eine hohe Bandbreitennutzung. Haben auch Sie eine VPN-Verbindung schon unterbrochen, weil Sie einfach zu langsam war? Damit ist mit Bitdefender Password Manager jetzt Schluss.

Wie funktioniert der App Traffic Optimizer?

Bestimmte Anwendungen und Dienste, so z. B. Streaming-Plattformen, Torrent-Clients und Spiele, benötigen mehr Bandbreite.

Eine Dauernutzung könnte sich also negativ auf Ihre Verbindungsgeschwindigkeit auswirken. Mit der Nutzung eines VPN-Tunnels geht naturgemäß schon eine gewisse Verlangsamung Ihrer Verbindung einher; eine zusätzliche Belastung Ihrer Verbindung könnte Ihr Online-Erlebnis daher spürbar beeinträchtigen.

Der App Traffic Optimizer in Bitdefender Password Manager ist eine Funktion, die durch die Priorisierung von Apps Abhilfe bei langsamen VPN-Verbindungen schafft. Sie legen fest, welcher App die meiste Bandbreite erhalten soll, und die neue Funktion weist die Ressourcen entsprechend zu. Wenn Sie beispielsweise in einem Online-Meeting sind und feststellen, dass die Qualität Ihrer Verbindung nicht ausreicht, können Sie mit App Traffic Optimizer den Datenverkehr Ihrer Videokonferenz-Software priorisieren.

Normalerweise müssten VPN-Nutzer in diesem Fall alle störenden Prozesse auf ihrem Gerät schließen oder sogar ihre VPN-Verbindung deaktivieren. Mit den App Traffic Optimizer müssen Sie nicht nie wieder zwischen Privatsphäre und Verbindungsgeschwindigkeit entscheiden.

App Traffic Optimizer richtig nutzen

Aktuell ist die Funktion nur auf Windows-Geräten verfügbar und ermöglicht es Ihnen, den Datenverkehr für bis zu drei Anwendungen zu priorisieren.

Und so können Sie die Funktion ganz einfach aktivieren und konfigurieren:

1. Starten Sie die Bitdefender VPN-Anwendung auf Ihrem Windows-Computer.
2. Klicken Sie auf die Schaltfläche in der Seitenleiste, um die VPN-Einstellungen aufzurufen.
3. Rufen Sie den Reiter **Allgemein** auf und aktivieren Sie die Funktion **App Traffic Optimizer**. Die Farbe des Schalters wechselt von grau zu blau.

So legen Sie die Anwendungen fest, die von dieser Funktion priorisiert werden:

1. Drücke den**Verwalten**Verknüpfung.
2. Suchen Sie nach der App, für die Sie den Datenverkehr optimieren möchten, markieren Sie den Namen der App und klicken Sie dann

auf **Hinzufügen**. Die Anwendung wird danach im Abschnitt **Priorisiert** angezeigt.

> **Hinweis**
> Wenn Sie die Anwendung, die Sie priorisieren möchten, erst kürzlich geöffnet haben, können Sie alternativ auch auf die Schaltfläche "+" im Fenster App Traffic Optimizer klicken.

3. Trennen Sie die Verbindung zu Bitdefender VPN und stellen Sie sie wieder her, nachdem Sie Anwendungen hinzugefügt oder aus der Liste entfernt haben.

Um eine App aus dem App Traffic Optimizer zu entfernen, klicken Sie einfach auf das Symbol neben dem Namen der App.

> **Notiz**
> Der App Traffic Optimizer ist unter macOS nicht verfügbar.

Protokoll

Hier können Sie den Protokolltyp auswählen, den Sie für die Datenübertragung verwenden möchten. Folgende Optionen stehen zur Verfügung:

- **Automatisch** - Bitdefender VPN wählt das optimale Protokoll für Ihr spezifisches Gerät und Netzwerk aus.
- **Hydra-Katapult** - Schnell und sicher, ideal für Streaming und Gaming.
- **OpenVPN UDP** - Optimiert für hohe Geschwindigkeiten. Allerdings ist dieses Protokoll hinsichtlich des Datenverlusts nicht so zuverlässig wie andere Protokolle in der Liste.
- **OpenVPN TCP** - Auf Zuverlässigkeit ausgelegt. Stellt sicher, dass Ihre Daten vollständig übermittelt werden, ist jedoch nicht so schnell wie OpenVPN UDP.
- **Wireguard** - Neueres Protokoll, das starke Sicherheit und ein hohes Leistungsniveau bietet.

Doppelsprung

Mit dieser Funktion können Sie die Server verwalten, über die Ihr Internetverkehr gesendet und doppelt verschlüsselt werden soll. Ihre

Daten werden über zwei VPN-Server statt über einen geleitet, wodurch es schwieriger wird, Ihre Internetaktivitäten zu verfolgen.

Notiz
Sie können insgesamt nur 5 Double-Hop-Standorte hinzufügen. Sie können die benutzerdefinierten Double-Hops jedoch jederzeit in Ihrer Liste löschen und andere erstellen.

Wichtig
Die Verwendung von Servern auf verschiedenen Kontinenten im selben Double-Hop kann Ihre Verbindungsgeschwindigkeit verlangsamen.

7.5. Bitdefender Password Manager deinstallieren

Bei der Entfernung von Bitdefender Password Manager gehen Sie ganz ähnlich vor wie bei der Entfernung anderer Programme:

- **Bitdefender Password Managervon Windows-Geräten deinstallieren**
  - Unter **Windows 7**:
    1. Klicken Sie auf **Start**, rufen Sie die **Systemsteuerung** auf und doppelklicken Sie auf **Programme und Funktionen**.
    2. Suchen Sie nach **Bitdefender Password Manager** und wählen Sie **Deinstallieren**.
       Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.
  - Unter **Windows 8** und **Windows 8.1**:
    1. Finden Sie auf der Windows-Startseite die **Systemsteuerung** (z.B. durch die Eingabe von "Systemsteuerung" auf der Startseite) und klicken Sie auf das entsprechende Symbol.
    2. Klicken Sie auf **Programm deinstallieren** oder **Programme und Features**.
    3. Finden **Bitdefender Password Manager** und auswählen **Deinstallieren**.
       Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.
  - Unter **Windows 10** und **Windows 11**:
    1. Klicken Sie auf **Start** und danach auf **Einstellungen**.

2. Klicken Sie in den Einstellungen auf das **System**-Symbol und wählen Sie **Installierte Anwendungen**.
3. Finden **Bitdefender Password Manager** und auswählen **Deinstallieren**.
4. Klicken Sie erneut auf **Deinstallieren**, um Ihre Auswahl zu bestätigen.
   Warten Sie, bis der Deinstallationsvorgang abgeschlossen ist.

- **Von macOS-Geräten deinstallieren**
  1. Klicken Sie in der Menüleiste auf **Los** und wählen Sie **Anwendungen**.
  2. Doppelklicken Sie auf den **Bitdefender**-Ordner.
  3. Führen Sie **BitdefenderUninstaller** aus.
  4. Markieren Sie im neuen Fenster das Kästchen neben **Bitdefender Password Manager** und klicken Sie dann auf **Deinstallieren**.
  5. Geben Sie den Namen und das Passwort eines gültigen Administratorkontos ein und klicken Sie auf **OK**.
  6. Zum Abschluss erhalten Sie eine Meldung, dass Bitdefender Password Manager erfolgreich deinstalliert wurde. Klicken Sie auf **Schließen**.

- **Von Android-Geräten deinstallieren**
  1. Öffnen Sie den **Play Store**.
  2. Suchen Sie nach **Bitdefender Password Manager**.
  3. Wählen Sie auf der Bitdefender Password Manager-Seite im App Store die Option **Deinstallieren**.
  4. Bestätigen Sie durch Antippen von **OK**.

- **Von iOS-Geräten deinstallieren**
  1. Halten Sie die Bitdefender Password Manager-App mit Ihrem Finger gedrückt.
  2. Wählen Sie **App löschen**.
  3. Tippen Sie auf **Löschen**.

7.6. Häufig gestellte Fragen

Wann sollte ich Bitdefender VPN verwenden?

Bei Aufrufen, Herunterladen oder Hochladen von Inhalten im Internet sollten Sie stets Vorsicht walten lassen. Um beim Surfen im Netz jederzeit geschützt zu sein, empfehlen wir die Nutzung des VPNs, wenn Sie:

- Verbindungen zu öffentlichen WLAN-Netzwerken herstellen möchten
- auf Inhalte zugreifen möchten, die regionalen Zugangsbeschränkungen unterliegen, egal ob Sie zuhause oder im Ausland sind
- Ihre persönlichen Daten vor Zugriff schützen möchten (Benutzernamen, Passwörter, E-Mail-Adressen, Kreditkartendaten etc.)
- Ihre IP-Adresse verbergen möchten

Kann ich mit Bitdefender VPN eine Stadt auswählen?

Ja. Aktuell können Sie mit Bitdefender VPN für Windows, macOS, Android und iOS Städte auswählen. Diese Städte stehen Ihnen derzeit zur Auswahl:

- **USA:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, New York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Kanada:** Montreal, Toronto, Vancouver
- **UK:** London, Manchester

Kann Bitdefender VPN als eigenständige App installiert werden?

Die VPN-App wird automatisch zusammen mit Ihrer Bitdefender-Sicherheitslösung installiert, kann aber auch als eigenständige App über die Produktseite, den Google Play Store und den App Store installiert werden.

Gibt Bitdefender meine IP-Adresse und übertragenen persönlichen Daten an Dritte weiter?

Nein, mit Bitdefender VPN wird Ihre Privatsphäre zu 100 % gewahrt. So kann niemand (Werbeanbieter, Internetdienstleister, Versicherungen usw.) auf Ihre Online-Protokolle zugreifen.

Welcher Verschlüsselungsalgorithmus kommt zum Einsatz?

Bitdefender VPN verwendet auf allen Plattformen das Hydra-Protokoll, eine 256-Bit-AES-Verschlüsselung bzw. die höchste sowohl vom Client als auch vom Server unterstützte Verschlüsselung mit Perfect Forward Secrecy. Das bedeutet, dass die Verschlüsselungsschlüssel für jede neue VPN-Sitzung erzeugt und nach Beendigung der Sitzung aus dem Speicher gelöscht werden.

Kann ich auf Inhalte mit regionalen Zugangsbeschränkungen zugreifen?

Mit Premium VPN erhalten Sie Zugriff auf ein ausgedehntes Netzwerk mit virtuellen Standorten in aller Welt.

Wird es die Akkulaufzeit meines Geräts beeinträchtigen?

Bitdefender VPN wurde entwickelt, um Ihre persönlichen Daten zu schützen, Ihre IP-Adresse bei Verbindungen mit ungesicherten WLAN-Netzwerken zu verbergen und Ihnen den Zugriff auf Inhalte mit länderspezifischen Zugangsbeschränkungen zu ermöglichen. Um Ihren Akku zu entlasten, empfehlen wir, das VPN nur bei Bedarf zu nutzen und die Verbindung danach wieder zu trennen.

Warum verlangsamt das VPN meine Internetverbindung?

Bitdefender VPN ist auf einen ressourcenschonenden Betrieb beim Surfen im Netz ausgelegt. Abhängig von der Entfernung zwischen Ihrem tatsächlichen Standort und dem Standort des Servers, mit dem Sie eine Verbindung aufbauen, sind geringfügige Geschwindigkeitseinbußen jedoch zu erwarten. Sie fallen in der Regel aber so gering aus, dass sie bei normaler Online-Nutzung unbemerkt bleiben. Wenn es nicht unbedingt notwendig ist, dass Sie sich von Ihrem Standort aus mit einem weit entfernten Server verbinden (z. B. von Deutschland aus nach Pakistan), sollten Sie in solchen Fällen dem VPN erlauben, automatisch eine Verbindung mit dem nächstgelegenen Server herzustellen bzw. einen Server zu finden, der näher an Ihrem Standort liegt.

8. PASSWORTMANAGER

8.1. Was ist Bitdefender Password Manager

Bitdefender Password Manager ist ein plattformübergreifender Dienst, mit dem Benutzer ihre Online-Passwörter speichern und verwalten können. Auf Grundlage der besten und sichersten bekannten Verschlüsselungsalgorithmen gewährleistet er ein Höchstmaß an Sicherheit. Er ist sowohl als mobile App als auch als Browsererweiterung verfügbar und dient Benutzern als geräteübergreifende Lösung für die Verwaltung von Identität, Passwörtern, Online-Banking und allen anderen Arten sensibler Daten.

Bitdefender Password Manager kann Ihre Passwörter für alle Websites und Online-Dienste mithilfe eines einzigen Master-Passworts automatisch speichern, automatisch ausfüllen, generieren und verwalten. So wird die Verwaltung Ihrer digitalen Identität zum Kinderspiel.

8.1.1. So wird die Sicherheit gewährleistet

Die Bitdefender Password Manager-Software stützt sich auf modernste Verschlüsselungsalgorithmen, die bestmögliche Datensicherheit gewährleisten, so z. B. AES-256-CCM, SH512 und BCRYPT sowie HTTPS- und WSS-Protokolle für die Datenübertragung. Alle beteiligten Daten werden jederzeit lokal ver- und entschlüsselt. So hat ausschließlich der Kontoinhaber Zugang zu den unter dem Benutzerkonto gespeicherten Informationen sowie zum Master-Passwort, das für den Zugang und die anschließende Nutzung der betreffenden Daten verwendet wird.

8.2. Erste Schritte

8.2.1. Systemanforderungen

Sie können die neueste Version von Bitdefender Password Manager nur auf Geräten mit den folgenden Betriebssystemen nutzen:

- **Für PC-Benutzer:**
  - Windows 7 mit Service Pack 1
  - Windows 8

- Windows 8.1
- Windows 10
- Windows 11

- **Für macOS-Benutzer:**
  - macOS 10.14 (Mojave) und neuere macOS-Betriebssysteme

> **Notiz**
> Bitte beachten Sie, dass die Systemleistung auf Geräten mit Prozessoren älterer Generationen beeinträchtigt sein kann.

- **Für iOS-Benutzer:**
  - iOS 11.0 oder neuere iOS-Betriebssysteme

- **Für Android-Benutzer:**
  - Android 5.1 und neuere Android-Betriebssysteme

> **Notiz**
> - Die Funktion zum Entsperren per Fingerabdruck wird ab **Android 6.0** unterstützt.
> - Die Funktion für das automatische Einfügen wird ab **Android 8.0** unterstützt und ist mit iPhone, iPad und iPod touch kompatibel.

Software-Anforderungen

Um Bitdefender Password Manager und alle Funktionen nutzen zu können, müssen Ihre Windows- oder macOS-Geräte die folgenden Softwareanforderungen erfüllen:

- **Microsoft Edge** (basierend auf Chromium 80 und höher)
- **Mozilla Firefox** (ab Version 65)
- **Google Chrome** (ab Version 72)
- **Safari** (ab Version 12)

> **Notiz**
> Die Softwareanforderungen gelten nicht für Android und iOS.

Warnung

Werden diese Systemanforderungen nicht erfüllt, ist die Bitdefender Password Manager-Installation nicht möglich oder es kommt zu Fehlfunktionen des Produkts.

8.2.2. Installation

In diesem Kapitel erfahren Sie, wie Sie den {1}{2} in den Webbrowsern unter Windows und macOS sowie auf Ihren Android- oder iOS-Geräten installieren.

Wichtig

Stellen Sie vor der Installation sicher, dass Sie über ein gültiges Password Manager-Abonnement in Ihrem **Bitdefender Central**-Konto verfügen, damit diese Browsererweiterung die Gültigkeit über Ihr Konto bestätigen kann.

Sie finden Ihre aktiven Abonnements in Bitdefender Central unter **Meine Abonnements**.

Installation auf Windows- und macOS-Geräten

Anders als die meisten Desktop-Anwendungen und Softwarelösungen, die auf diesen Geräten installiert und eingerichtet werden müssen, wird der Bitdefender Password Manager als Browsererweiterung - auch Add-on genannt - bereitgestellt, die im Handumdrehen zu Ihrem bevorzugten Browser hinzugefügt und aktiviert werden kann.

Das Produkt unterstützt derzeit die folgenden Browser: **Google Chrome**, **Mozilla Firefox**, **Microsoft Edge** und **Safari**.

1. Rufen Sie https://central.bitdefender.com/ auf und melden Sie sich bei Ihrem Benutzerkonto an.
   Wenn Sie noch kein Konto haben, klicken Sie auf **Benutzerkonto erstellen** und geben Sie dann Ihren vollständigen Namen, eine E-Mail-Adresse und ein Passwort ein.
2. Klicken Sie im Menü links auf **Meine Geräte**.
3. Klicken Sie unter **Meine Geräte** auf **+ Gerät hinzufügen**.
4. Dadurch wird ein neues Fenster geöffnet. Klicken Sie hier auf **Password Manager**.
5. Klicken Sie auf **Dieses Gerät**.

Wenn Sie die Installation auf einem anderen Gerät vornehmen möchten, klicken Sie auf Weitere Geräte. Sie können dann einen Download-Link per E-Mail an das jeweilige Gerät senden oder die URL für die Installation selbst kopieren.

6. Wählen Sie anschließend den Browser aus, für den Sie die Password Manager-Erweiterung installieren möchten.
7. Über die entsprechende Schaltfläche gelangen Sie direkt zum Erweiterungsangebot des Browsers. Folgen Sie dort einfach den Anweisungen auf dem Bildschirm, wie im Folgenden gezeigt:

   Microsoft Edge

   - Klicken Sie auf **Abrufen**.
   - Klicken Sie jetzt auf **Erweiterung hinzufügen**.

   Google Chrome

   - Klicken Sie auf **Chrome hinzufügen**.
   - Klicken Sie im Bestätigungsfeld auf **Erweiterung hinzufügen**.

   Mozilla Firefox

   - Klicken Sie auf **Zu Firefox hinzufügen**.
   - Klicken Sie oben rechts im Fenster auf **Installieren**.

   Safari

   - Klicken Sie auf **Laden** und danach auf **Installieren**.
   - Öffnen Sie Safari und klicken Sie im Menü oben auf **Einstellungen**.
   - Klicken Sie in den Einstellungen auf den Reiter **Erweiterungen**.
   - Markieren Sie das Kontrollkästchen neben dem Password Manager, um ihn zu aktivieren.

Legen Sie nach Abschluss dieser Schritte ein sicheres Master-Passwort fest und klicken Sie auf **Master-Passwort speichern**, nachdem Sie die **Nutzungsbedingungen** gelesen und akzeptiert haben.

Wichtig

Bitte beachten Sie, dass Sie dieses Master-Passwort benötigen, um auf die im Bitdefender Password Manager gespeicherten Passwörter, Kreditkarteninformationen und Notizen zuzugreifen. Das Master-Passwort dient als Schlüssel, der eine Nutzung des Produkts erst möglich macht.

Warnung

Nach Erstellung des Master-Passworts erhalten Sie einen **24-stelligen Wiederherstellungsschlüssel**. **Bewahren Sie Ihren Wiederherstellungsschlüssel an einem sicheren Ort auf und verlieren Sie ihn nicht**. Dieser Schlüssel ist die einzige Möglichkeit, auf Ihre im Password Manager gespeicherten Passwörter zuzugreifen, sollten Sie das zuvor für Ihr Konto eingerichtete **Master-Passwort vergessen**.

❍ Klicken Sie danach auf **Schließen**.

Installation auf Android-Geräten

Der Bitdefender Password Manager lässt sich auf Android-Telefonen und -Tablets am einfachsten installieren, indem Sie die App direkt von Google Play herunterladen.

GET IT ON Google Play

Sie können die Bitdefender Password Manager-App aber auch über Ihr **Bitdefender Central**-Konto installieren:

1. Melden Sie sich dazu auf Ihrem Android-Mobilgerät bei Ihrem Bitdefender Central-Konto an, indem Sie https://login.bitdefender.com/central/login aufrufen.
2. Wählen **Meine Geräte** in der linken Seitenleiste des Bildschirms.
3. Im **Meine Geräte** Abschnitt, fahren Sie fort, indem Sie auf klicken **+ Gerät hinzufügen**.
4. Diese Aktion wird dazu führen, dass ein neues Fenster erscheint. Wählen **Passwortmanager** im Selektionsbild.
5. Wählen **Dieses Gerät**.
   Wenn Sie die Installation auf einem anderen Gerät vornehmen möchten, klicken Sie auf **Weitere Geräte**. Sie können dann einen

Download-Link per E-Mail an das jeweilige Gerät senden oder die URL für die Installation selbst kopieren.

6. Sie werden zu **Google Play** weitergeleitet. Tippen Sie auf **Installieren**, um dem Bitdefender Password Manager auf Ihr Android herunterzuladen.

7. Öffnen Sie nach Abschluss des Downloads die Password Manager-App.

8. Wenn Sie nicht automatisch bei Ihrem Konto angemeldet werden, melden Sie sich mit Ihrem Benutzernamen und Passwort an.
   Nachdem Sie diese Schritte befolgt haben, legen Sie ein starkes Master-Passwort fest und drücken Sie dann die **Master-Passwort speichern** Schaltfläche, nachdem Sie gelesen haben und damit einverstanden sind **Geschäftsbedingungen**.

   Wichtig
   Beachten Sie, dass Sie dieses Master-Passwort benötigen, um alle im Bitdefender Password Manager gespeicherten Passwörter, Kreditkarteninformationen und Notizen freizuschalten. Dies ist im Wesentlichen der Schlüssel, der es dem Besitzer ermöglicht, dieses Produkt zu verwenden.

   Warnung
   Beim Erstellen des Master-Passworts erhalten Sie eine **24-stelliger Wiederherstellungsschlüssel**. Notieren Sie sich Ihren Wiederherstellungsschlüssel an einem sicheren Ort und verlieren Sie ihn nicht. Dieser Schlüssel ist die einzige Möglichkeit, auf Ihre in Password Manager gespeicherten Passwörter zuzugreifen, falls dies doch passieren sollte **vergessen Sie das Master-Passwort** zuvor für Ihr Konto eingerichtet.

   ❍ Sie können drücken **Schließen** wenn fertig.

9. Legen Sie eine **4-stellige PIN** fest. Wenn Sie jetzt zu einer anderen App wechseln und dann zum Password Manager zurückkehren, müssen Sie so das zuvor eingerichtete Master-Passwort nicht erneut eingeben. Falls verfügbar, können Sie auch die Gesichtserkennung oder die Authentifizierung per Fingerabdruck aktivieren.

10. Tippen Sie auf **Automatisches Ausfüllen aktivieren**, um die Android-Einstellungen für das automatische Ausfüllen zu konfigurieren.

> **Notiz**
> Wenn Sie diesen Schritt überspringen, können Sie die Android-Funktion zum automatischen Ausfüllen auch zu einem späteren Zeitpunkt aktivieren und anpassen, indem Sie die Anweisungen unter Intelligentes automatisches Ausfüllen (Seite 286) befolgen.

11. Es wird eine Liste mit Anwendungen angezeigt, die Passwörter automatisch ausfüllen können.
    Wählen Sie **Password Manager** und bestätigen Sie dann, dass Sie dieser App vertrauen.
    Tippen Sie auf **OK**.

12. Geben Sie die PIN ein, die Sie in **Schritt 9** eingerichtet haben, um diese Aktion zu bestätigen.

Die Installation auf Ihrem Android-Gerät ist damit abgeschlossen.

Installation auf iOS-Geräten

Der Bitdefender Password Manager lässt sich auf iOS- und iPadOS-Geräten am einfachsten installieren, indem Sie die App direkt aus dem App Store herunterladen.

Download on the App Store

Die Installation der Bitdefender Password Manager-App kann auch über Ihren erfolgen Bitdefender-Zentrale Konto:

1. Melden Sie sich dazu auf Ihrem iPhone oder iPad bei Ihrem Bitdefender Central-Konto an, indem Sie https://login.bitdefender.com/central/login aufrufen.
2. Wählen **Meine Geräte** in der linken Seitenleiste des Bildschirms.
3. Im **Meine Geräte** Abschnitt, fahren Sie fort, indem Sie auf klicken **+ Gerät hinzufügen**.
4. Diese Aktion wird dazu führen, dass ein neues Fenster erscheint. Wählen **Passwortmanager** im Selektionsbild.
5. Wählen **Dieses Gerät**.
   Wenn Sie auf einem anderen Gerät installieren möchten, wählen Sie **Andere Geräte**. Sie können dann einen Download-Link per E-Mail an

das jeweilige Gerät senden oder die URL für die Installation direkt kopieren.

6. Sie werden zum **App Store** weitergeleitet. Tippen Sie auf das Wolkensymbol mit einem nach unten zeigenden Pfeil, um den Bitdefender Password Manager für iOS herunterzuladen.

7. Öffnen Sie nach Abschluss der Installation die Bitdefender App und markieren Sie das kleine Kästchen auf dem Bildschirm. Wählen Sie **Fortfahren**, nachdem Sie die **Nutzungsbedingungen** gelesen und akzeptiert haben.

8. Wenn Sie nicht automatisch bei Ihrem Konto angemeldet werden, melden Sie sich mit Ihrem Benutzernamen und Passwort an.
   Nachdem Sie diese Schritte befolgt haben, legen Sie ein starkes Master-Passwort fest und drücken Sie dann die **Master-Passwort speichern** Schaltfläche, nachdem Sie gelesen haben und damit einverstanden sind **Geschäftsbedingungen**.

   Wichtig
   Beachten Sie, dass Sie dieses Master-Passwort benötigen, um alle im Bitdefender Password Manager gespeicherten Passwörter, Kreditkarteninformationen und Notizen freizuschalten. Dies ist im Wesentlichen der Schlüssel, der es dem Besitzer ermöglicht, dieses Produkt zu verwenden.

   Warnung
   Beim Erstellen des Master-Passworts erhalten Sie eine **24-stelliger Wiederherstellungsschlüssel**. Notieren Sie sich Ihren Wiederherstellungsschlüssel an einem sicheren Ort und verlieren Sie ihn nicht. Dieser Schlüssel ist die einzige Möglichkeit, auf Ihre in Password Manager gespeicherten Passwörter zuzugreifen, falls dies doch passieren sollte **vergessen Sie das Master-Passwort** zuvor für Ihr Konto eingerichtet.

   ❍ Sie können drücken **Schließen** wenn fertig.

9. Ein ... kreieren **4-stellige PIN**, wenn Sie also zu einer anderen App wechseln und dann zu Password Manager zurückkehren, müssen Sie das zuvor eingerichtete Master-Passwort nicht erneut eingeben. Falls verfügbar, können Sie auch die Gesichtserkennung oder die Authentifizierung per Fingerabdruck aktivieren.

Die Installation auf Ihrem iOS/iPadOS-Gerät ist damit abgeschlossen.

8.2.3. Geteilter Plan

Der Bitdefender Password Manager Shared Plan ermöglicht es mehreren Benutzern, auf dasselbe Abonnement zuzugreifen und es zu nutzen. Es bietet einen zentralen Ansatz für den Software-Zugang, die Verwaltung und den Support und stellt eine kostengünstige Lösung für die gemeinsame Nutzung des Passwort-Manager-Dienstes durch mehrere Benutzer dar.

- Die Person, die für den gemeinsamen Abonnement-Plan verantwortlich ist, bekannt als der Plan-Manager, kann den Dienst unter den Mitgliedern teilen.
- Jedes Mitglied erhält ein eigenes Bitdefender Central-Konto, das mit seiner E-Mail-Adresse verknüpft ist, und Zugang zum Password Manager-Dienst.

Gemeinsame Nutzung von Bitdefender Password Manager mit mehreren Benutzern

Mitglieder einladen

Um einen oder mehrere Benutzer zum gemeinsamen Abonnement hinzuzufügen, muss der Planmanager die folgenden Schritte ausführen:

1. Melden Sie sich bei Ihrem Bitdefender Central-Konto unter https://central.bitdefender.com/ an.
2. Gehen Sie zum Menü **Meine Abonnements** auf der linken Seite der Seite.
3. Wählen Sie **Mitglied einladen** im **Bitdefender Password Manager Shared Plan** Panel.
4. Geben Sie die E-Mail-Adresse jeder Person ein, mit der Sie Ihr Abonnement teilen möchten, und klicken Sie dann auf **Senden**. Es können maximal 3 Mitglieder auf einmal hinzugefügt werden.
5. Die Einrichtungsanweisungen werden sofort per E-Mail an die neuen Mitglieder gesendet. Klicken Sie auf **Schließen**, um das Bestätigungsfenster zu verlassen.

Notiz

Mitglieder haben 24 Stunden Zeit, Ihre Einladung anzunehmen, sobald sie per E-Mail an sie gesendet wurde.

- Eingeladene Mitglieder werden mit dem Status „Eingeladen“ angezeigt.
- Sie werden sie als „aktive“ Mitglieder sehen, nachdem sie die Einladung angenommen haben. Sie werden außerdem per E-Mail über jede angenommene Einladung benachrichtigt.

Entfernen von Mitgliedern

Der Zugriff auf den Bitdefender Password Manager Shared Plan geht für entfernte Mitglieder verloren. Wenn der Planmanager beschließt, ein Abonnementmitglied zu entfernen, erhält das Mitglied eine E-Mail-Benachrichtigung. Für die folgenden 30 Tage wird das Ex-Mitglied auf einen 30-Tage-Bitdefender-Passwortmanager umgestellt **Probeversion** mit vollem Funktionsumfang. Der Dienst wird dann deaktiviert.

Der Planmanager kann Benutzer auf folgende Weise aus dem gemeinsamen Plan entfernen:

1. Melden Sie sich bei Ihrem Bitdefender Central-Konto unter https://central.bitdefender.com/ an.
2. Gehen Sie zum Menü **Meine Abonnements** auf der linken Seite der Seite.
3. Klicken Sie im Bereich **Bitdefender Password Manager Shared Plan** auf **Verwalten** und wählen Sie dann im Menü **Mitglieder bearbeiten**.
4. Klicken Sie auf die Schaltfläche **Entfernen**, um ein Mitglied aus dem gemeinsamen Plan zu entfernen.
5. Wählen Sie **Ja, Mitglied entfernen** und klicken Sie dann auf die Schaltfläche **Bearbeitung beenden**, damit die Änderungen wirksam werden.

Notiz

Wenn ein Mitglied aus dem gemeinsamen Plan gelöscht wird, ändert sich sein Status in **Zur Entfernung** anstehend, bis es vollständig entfernt ist.

Eine Einladung annehmen

Sie erhalten eine E-Mail, wenn Sie jemand einlädt, ein Abonnementmitglied für den Bitdefender Password Manager Shared Plan zu werden. Sie haben 24 Stunden Zeit, eine Einladung anzunehmen, sobald sie an Sie gesendet wurde.

Um die Einladung anzunehmen und Zugriff auf die Passwort-Manager-Funktionen zu erhalten, muss der Benutzer die folgenden Schritte ausführen:

1. Öffnen Sie die E-Mail mit dem Titel **[Starten Sie die Nutzung Ihres Bitdefender-Abonnements als Mitglied]** und klicken Sie auf die Schaltfläche **IN CENTRAL AKTIVIEREN**.
2. Die Bitdefender Central-Seite wird dann in Ihrem Browser geöffnet.
   - Wenn Sie bereits ein Bitdefender-Benutzerkonto haben, das mit der E-Mail verknüpft ist, an die die Einladung gesendet wurde, **melden Sie sich an**, um Ihr gemeinsames Abonnement zu beanspruchen.
   - Wenn Sie noch kein Bitdefender-Benutzerkonto haben, klicken Sie auf **Erstellen** und melden Sie sich mit der gleichen E-Mail an, mit der Sie die Einladung erhalten haben, um Ihr gemeinsames Abonnement zu beanspruchen.
     - Geben Sie Ihren vollständigen Namen ein
     - Geben sie ihre E-Mailadresse ein
     - Geben Sie Ihr Passwort ein
     - Klicken Sie auf die Schaltfläche Konto erstellen und Sie werden angemeldet.
3. Nachdem Sie sich angemeldet haben, klicken Sie auf dem Willkommensbildschirm, der Sie darüber informiert, dass Ihr Bitdefender Password Manager-Abonnement jetzt aktiv ist, auf **Starten**.
4. Befolgen Sie die Schritte auf dem Bildschirm, die auch in beschrieben sind Installation (Seite 272).

Notiz

Die E-Mail-Adresse des Planmanagers wird in Ihrem Bitdefender Central-Konto oben im Passwort-Manager-Menü und auf der Abonnementkarte unter „Meine Abonnements“ angezeigt.

Wenn Sie Hilfe beim gemeinsamen Plan benötigen, nehmen Sie bitte Kontakt mit ihnen auf.

8.3. Import und Export Ihrer Passwörter

Mit dem Bitdefender Password Manager ist die Kommunikation und der Austausch von Daten mit externen Quellen, Plattformen und Software-Tools problemlos möglich. So ist gewährleistet, dass die häufige Anforderung hinsichtlich des Imports bzw. Exports von Passwörtern in bzw. aus dem Bitdefender Password Manager mühelos erfüllt wird.

8.3.1. Produktkompatibilität

Der Bitdefender Password Manager ermöglicht eine nahtlose Datenübertragung aus den folgenden Anwendungen:

- **1Password**
- **Bitwarden**
- **Bitdefender Password Manager**
- **ByePass**
- **Chrome browser**
- **Claro**
- **Dashlane**
- **Edge browser**
- **ESET Password Manager v2**
- **ESET Password Manager v3**
- **StickyPassword**
- **Watchguard**
- **Firefox browser**
- **Gestor de contraseñas – Claro**

- **Gestor de contraseñas – SIT**
- **Gestor de contraseñas – Telnor**
- **KeePass 2.x**
- **LastPass**
- **Panda Dome Passwords**
- **PassWatch**
- **Saferpass**
- **SFR Cybersécurité**
- **SIT**
- **F-Secure**
- **Telnor**

> **Notiz**
> Wenn der Name des Browsers oder des Passwortmanagers, aus dem Sie Daten übertragen möchten, nicht in der Liste aufgeführt ist, erfahren Sie in unserer Online-Anleitung, wie Sie eine CSV-Datei mit Daten aus nicht unterstützten Passwortmanagern erstellen und bearbeiten können, um sie dann in den **Bitdefender Password Manager** zu importieren: https://www.bitdefender.de/consumer/support/answer/12244/

Dieser Datentransfer zwischen dem Bitdefender Password Manager und anderen Lösungen kann über die folgenden Datenformate erfolgen:

CSV, **JSON**, **XML**, **TXT**, **1pif** und **FSK**.

8.3.2. Import in den Password Manager

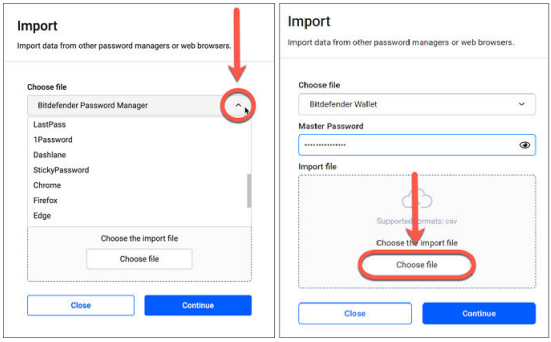
Der Bitdefender Password Manager ermöglicht Ihnen den einfachen Import von Passwörtern aus anderen Passwortmanagern und Browsern. Wenn Sie von einem anderen Passwortverwaltungsdienst zu Bitdefender Password Manager wechseln möchten, haben Sie dort vermutlich eine beträchtliche Menge an Anmeldedaten wie Benutzernamen, Passwörter und andere Login-Informationen für Ihre Konten gespeichert.

Mit dem Umstieg auf den Bitdefender Password Manager möchten Sie diese gespeicherten Daten bestimmt auch mitnehmen.

Gehen Sie zum Import Ihrer gespeicherten Daten aus anderen Anwendungen und Webbrowsern in den Bitdefender Password Manager

wie folgt vor, **unabhängig vom Betriebssystem**, auf dem Sie dieses Produkt installiert haben:

1. Klicken Sie auf das Password Manager-Symbol in Ihrem Webbrowser (unter Windows und macOS) oder starten Sie die Password Manager-App (unter Android und iOS). Geben Sie nach Aufforderung Ihr **Master-Passwort** ein.
2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Einstellungen**.
3. Scrollen Sie nach unten zum Abschnitt **Daten** und klicken Sie auf die Option **Daten importieren**.
4. Wählen Sie im Dropdown-Menü den Namen der Passwortmanager-Anwendung oder des Browsers, aus dem Sie Ihre Konten importieren möchten. Geben Sie Ihr **Master-Passwort** in das entsprechende Feld ein und klicken Sie dann auf **Datei wählen**.



5. Durchsuchen Sie Ihre Ordner, um den Speicherort zu finden, an dem Sie die Datei mit Ihren Benutzernamen und Passwörtern gespeichert haben, die Sie aus Ihrem anderen Passwortmanager oder Webbrowser exportiert haben, und klicken Sie dann auf **Fortfahren**.

Nach dem Import sind Ihre Passwörter dann auf allen Geräten verfügbar, auf denen die Bitdefender Password Manager-App bzw. die Browsererweiterung installiert ist.

8.3.3. Export aus dem Password Manager

Mit dem Bitdefender Password Manager können Sie Ihre gespeicherten Passwörter (einschließlich Anmeldedaten, sichere Notizen usw.) ganz einfach in eine CSV-Datei (Comma-separated values) oder verschlüsselte Datei exportieren. So möchten wir Ihnen den Umstieg so einfach wie möglich machen, sollten Sie vom vom Bitdefender Password Manager zu einem anderen Passwortmanager-Dienst wechseln möchten.

> **Wichtig**
> Eine CSV-Datei ist **nicht** verschlüsselt und enthält Benutzernamen und Passwörter im Klartextformat. Das bedeutet, dass Ihre privaten Informationen von jedem gelesen werden können, der Zugriff auf Ihr Gerät hat. Wir empfehlen Ihnen daher, die folgenden Schritte nur auf einem vertrauenswürdigen Gerät durchzuführen.

So exportieren Sie Ihre Daten aus dem Bitdefender Password Manager:

1. Klicken Sie in Ihrem Webbrowser (unter Windows oder macOS) auf das Password Manager-Symbol oder starten Sie die Password Manager-Anwendung (unter Android oder iOS). Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.
2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Einstellungen**.
3. Scrollen Sie nach unten zum Abschnitt **Daten** und klicken Sie auf die Option **Daten exportieren**.
4. Ihnen sollten nun die folgenden beiden Optionen angezeigt werden:
   - **CSV**
   - **Passwortgeschützte Dateien**

   Wählen Sie die gewünschte Option, geben Sie Ihr Master-Passwort ein und klicken Sie auf **Daten exportieren**.

   > **Notiz**
   > Wenn Sie die Option "Passwortgeschützte Datei" wählen, werden Sie aufgefordert, die Daten mit der Liste Ihrer Konten mit einem Passwort zu verschlüsseln, so dass nur Sie bei Bedarf darauf zugreifen können.

5. Ihr Webbrowser/Ihre App speichert eine Datei mit dem Namen Bitdefender Password Manager_exported_data_aktuelles-datum auf

Ihrem System im Standard-Download-Ordner. Sie enthält alle Ihre im Bitdefender Password Manager gespeicherten Daten.

Nach dem Export Ihrer Daten können Sie diese in einen Passwortmanager Ihrer Wahl hochladen.

8.4. Funktionen und Merkmale

In diesem Kapitel lernen Sie alle Merkmale und Funktionen des Bitdefender Password Managers kennen und erfahren wofür und wie man Sie optimal einsetzt.

8.4.1. Richtiger Umgang mit Passwörtern

Passwortgenerator

Die wichtigste Regel für mehr Sicherheit im Internet ist die konsequente Nutzung von zufällig gewählten Passphrasen für jeden Dienst, für den ein Benutzerkonto erstellt werden muss. Dabei darf jede Passphrase immer nur einmal vergeben werden. Die Wiederverwendung von Passwörtern über mehrere Dienste hinweg ist die Hauptursache für Identitätsdiebstahl und andere Schäden im Zusammenhang mit der betrügerischen Übernahme von Konten.

Diese Funktion hilft Benutzern bei der Erstellung sicherer, komplexer und einzigartiger Passwörter für jedes neue Online-Benutzerkonto. Sie müssen nie sich nie wieder selbst sichere Passwörter ausdenken und merken oder darauf achten, das gleiche Passwort nicht mehrfach zu vergeben.

Sie finden den **Passwortgenerator** im entsprechenden Reiter oben in der Password Manager-Benutzeroberfläche.

Der Generator gibt je nach Einstellung Passwörter **mit 4 bis 32 Zeichen** aus.

Sie können auch festlegen, welche Arten von Zeichen im zufällig generierten Passwort enthalten sein sollen oder nicht, indem Sie die entsprechenden Kästchen aktivieren oder deaktivieren. **(Kleinbuchstaben, Großbuchstaben, Zahlen, Sonderzeichen)**

Klicken Sie auf die Schaltfläche rechts neben dem angezeigten Passwort, um das vorgeschlagene Passwort zu ändern.

Wenn Sie das angezeigte Passwort verwenden möchten, klicken Sie auf **Passwort verwenden**. Die Zeichenfolge wird in der Zwischenablage gespeichert.

> **Notiz**
> Ihre zuvor erstellten Passwörter werden vorübergehend im Passwortverlauf gespeichert, auf den Sie über die Schaltfläche **Passwortverlauf** zugreifen können.

Passworterfassung

Mit dieser Funktion im Password Manager werden Sie aufgefordert, alle neuen Passwörter sofort nach der Erstellung zu speichern. Der Password Manager fordert Benutzer auf, ihre neu erstellten Passwörter zu speichern, damit sie sofort der von Bitdefender bereitgestellten ultrasicheren Umgebung hinzugefügt werden können.

Intelligentes automatisches Ausfüllen

Der Bitdefender Password Manager kann so eingerichtet werden, dass er Ihre Anmeldedaten und vor allem Ihre Passwörter automatisch ausfüllt. Von uns entwickelte Algorithmen erkennen bereits besuchte Websites und füllen Ihre Anmeldedaten für Sie aus, so dass Sie bei jeder Anmeldung bei Ihren Diensten Zeit sparen.

1. Klicken Sie unter Windows oder macOS auf das **Password Manager**-Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Password Manager**-App.
   Geben Sie nach Aufforderung Ihr **Master-Passwort** ein.
2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Einstellungen**.
3. Klicken Sie auf **Geräteeinstellungen**.
4. Hier finden Sie eine Schaltfläche, die entweder **Automatisches Ausfüllen deaktivieren** oder **Automatisches Ausfüllen aktivieren** anzeigt. Diese Einstellung steuert den Betriebszustand der Funktion für das intelligente automatische Ausfüllen.

Sicherheitsbericht

Der Sicherheitsbericht ist ein Tool, das Berichte auf Grundlage verschiedener Funktionen erstellt, die Ihrer digitalen Sicherheit dienen.

So werden Sie nach Bewertung der Sicherheit vorhandener Passwörter zum Beispiel informiert, ob ein Passwort Ihre sofortige Aufmerksamkeit erfordert. Auch doppelte Passwörter werden erkannt. Sie werden dann aufgefordert, diese Passwörter entsprechend zu ändern, um die mit der Mehrfachnutzung verbundenen Risiken zu vermeiden.

Der Bericht liefert Ihnen hauptsächlich Informationen zu Ihren Passwortgewohnheiten, d. h. zu mehrfach genutzten Passwörtern, schwachen oder anderweitig kompromittierten Passwärtern und E-Mail-Adressen.

Dazu wird die Liste der verschlüsselten Hashes von Troys Website lokal auf Ihrem Gerät verglichen, um zu prüfen, ob sie die entsprechenden Hashes Ihrer Passwörter enthält. Wenn eine Übereinstimmung gefunden wird, werden Sie benachrichtigt, damit Sie Ihre Passwörter und andere Anmeldedaten ändern können.

Sie können den **Sicherheitsbericht** aufrufen, indem Sie den Password Manager öffnen und in der Menüleiste oben auf die entsprechende Schaltfläche klicken.

Plattformübergreifende Synchronisierung

Wenn Sie Ihre Passwörter einmal im Bitdefender Password Manager gespeichert haben, können Sie diese auch auf all Ihren Windows-, Mac-, Android- oder iOS-Geräten in Chrome, Safari, Firefox und Edge oder in den mobilen Apps speichern und jederzeit sicher darauf zugreifen.

> **Notiz**
> Bitdefender verfügt zudem über einen **Offlinemodus**. So können Sie jederzeit und von überall auf Ihre Passwörter zugreifen, auch wenn Sie einmal keinen Zugang zum Internet haben.

Löschen von Einträgen

Um gespeicherte Passwörter zu löschen, klicken Sie zuerst auf das Bearbeitungssymbol neben dem Eintrag, den Sie entfernen möchten. Die Einträge finden Sie im Reiter **Konten**. Scrollen Sie nach unten und klicken Sie auf **Löschen**. Sie werden gefragt, ob Sie das Konto wirklich entfernen möchten. Klicken Sie zur Bestätigung auf **Entfernen**.

8.4.2. Richtiger Umgang mit Konten

Authentifizierung

Die Authentifizierung im Bitdefender Password Manager erfolgt über die **PIN**, die bei der Installation des Produkts festgelegt wurde. (Bitte beachten Sie, dass die Funktion **Automatisch sperren** den Password Manager sperrt oder Sie nach einer gewissen Zeit der Inaktivität im Browser oder dem Schließen der mobilen App abmeldet).

Alternativ ist die Authentifizierung, falls verfügbar, auch durch biometrische Verfahren möglich, so z. B. durch **Fingerabdruck** oder **Gesichtserkennung**.

So **aktivieren oder deaktivieren** Sie die biometrische Authentifizierung:

1. Klicken Sie unter Windows oder macOS auf die **Password Manager** Symbol in Ihrem Webbrowser.

   Starten Sie unter Android oder iOS die **Password Manager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.

2. Öffnen Sie das Password Manager-Menü , um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Einstellungen** Menüpunkt.
3. Klicke auf **Geräteeinstellungen**.
4. Hier finden Sie eine Schaltfläche, die entweder **Biometrie deaktivieren** oder **Biometrie aktivieren** anzeigt. Diese Einstellung steuert den Betriebszustand der Funktion für biometrische Authentifizierung.

Zurücksetzen des Master-Passworts

Wichtig
Die Funktion **Master-Passwort ändern** ist auf Mobilgeräten nicht verfügbar. Sie können Ihr Master-Passwort ausschließlich über die Browser-Erweiterung Bitdefender Password Manager auf einem Windows-PC oder einem macOS-Gerät ändern oder wiederherstellen.

Gehen Sie wie folgt vor, um Ihr**Master-Passwort** als Vorsichtsmaßnahme zu ändern und ein neues Master-Passwort im Bitdefender Password Manager festzulegen:.

1. Klicken Sie nach Installation der Browsererweiterung auf das **Password Manager**-Symbol in der Symbolleiste Ihres Browsers.
2. Geben Sie Ihr aktuelles Master-Passwort ein, um den Tresor zu entsperren.

   > **Wichtig**
   > Falls Sie Ihr aktuelles Master-Passwort vergessen haben, klicken Sie auf diesem Bildschirm stattdessen auf die Option **Ich habe mein Passwort vergessen**. Geben Sie den **24-stelligen Wiederherstellungsschlüssel** ein, den Sie bei der Ersteinrichtung Ihres Bitdefender Password Managers erhalten haben. Geben Sie danach ein neues Master-Passwort ein. **Falls Sie** sowohl Ihr **Master-Passwort** als auch den **Wiederherstellungsschlüssel** vergessen oder verlegt haben, wenden Sie sich **als letzte Option an einen Bitdefender-Mitarbeiter, um Hilfe beim Zurücksetzen Ihres Kontos zu erhalten**. Beim Zurücksetzen Ihres Kontos werden **alle in Bitdefender Password Manager gespeicherten Daten und Passwörter gelöscht**.

3. Öffnen Sie das Password Manager-Menü , um die Seitenleiste auf der linken Seite zu erweitern, und klicken Sie auf **Einstellungen** Menüpunkt.
4. Klicken Sie im Abschnitt **Konto** auf **Mein Konto**.
5. Ein Fenster mit Informationen zu Ihrem Password Manager-Abonnement wird angezeigt.
   Klicken Sie auf **Master-Passwort ändern**.
6. Sie werden zu einem neuen Fenster weitergeleitet, in dem Sie ein neues Master-Passwort festlegen können. Geben Sie zunächst Ihr aktuelles Master-Kennwort und danach das neue Master-Passwort ein. Das neue Master-Kennwort muss mindestens 8 Zeichen lang sein und mindestens einen Kleinbuchstaben, einen Großbuchstaben und eine Zahl enthalten.
7. Klicken Sie im Anschluss auf **Ändern**.
8. Warten Sie einen Moment, bis Bitdefender das alte Master-Passwort zurückgesetzt hat.

Schließen Sie Ihren Webbrowser nicht!

9. Im nächsten Schritt erhalten Sie einen neuen **24-stelligen Wiederherstellungsschlüssel**. Bewahren Sie Ihren Wiederherstellungsschlüssel an einem sicheren Ort auf und **verlieren Sie ihn nicht**. Dieser Schlüssel ist die einzige Möglichkeit, auf Ihre im Password Manager gespeicherten Passwörter zuzugreifen, sollten Sie Ihr Master-Passwort vergessen.
   Klicken Sie im Anschluss auf **Schließen**.

10 Sie werden von Bitdefender Password Manager abgemeldet.
· Geben Sie zum Entsperren des Tresors das neue Master-Passwort ein, das Sie gerade festgelegt haben.

8.4.3. Weitere Funktionen

Verwaltung von Identitäten

Mit dieser Funktion können Benutzer mehrere Identitäten speichern und mit dem Password Manager ihre Daten in Webformularen automatisch ausfüllen. So wird Online-Shopping schnell, einfach und sicher.

Wie alles andere im Password Manager sind auch die sensiblen Daten, die zu diesen gespeicherten Identitäten gehören, verschlüsselt und nur auf dem Gerät des Benutzers abrufbar.

So können Sie im Password Manager eine Identität hinzufügen:

1. Klicken Sie unter Windows oder macOS auf die **Password Manager** Symbol in Ihrem Webbrowser.
   Starten Sie unter Android oder iOS die **Password Manager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.

2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Einstellungen**.

3. Klicken Sie unten auf **Identität hinzufügen**.

4. Geben Sie die Daten ein, die gespeichert werden sollen, und klicken Sie auf **Speichern**.

Verwalten von Kreditkarten

Mit dieser Funktion können Sie Ihre Kreditkartendaten speichern und automatisch eingeben, um einfacher, schneller und sicherer einzukaufen.

So können Sie im Password Manager eine Kreditkarte hinzufügen:

1. Klicken Sie unter Windows oder macOS auf die **Password Manager** Symbol in Ihrem Webbrowser.

   Starten Sie unter Android oder iOS die **Password Manager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.

2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Kreditkarten**.

3. Drücken Sie auf die **Identität hinzufügen** Knopf unten.

4. Vervollständigen Sie die Details, die Sie speichern möchten, und drücken Sie dann **Speichern**.

Meine Absicherung

Mit der Funktion Meine Absicherung können Sie sich jederzeit per Fernzugriff abmelden und Ihren Browserverlauf auf Ihrem Computer, Tablet oder Mobilgerät löschen. Wir empfehlen diese Funktion besonders dann, wenn Sie Ihr Gerät nicht alleine nutzen.

So finden und aktivieren Sie diese Funktion:

1. Klicken Sie unter Windows oder macOS auf die **Password Manager** Symbol in Ihrem Webbrowser.

   Starten Sie unter Android oder iOS die **Password Manager** Anwendung.
   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.

2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Meine Absicherung**.

3. Klicken Sie auf **Alle Sitzungen absichern**.

Wenn Sie nur ein einzelnes Gerät absichern möchten, suchen Sie es in der Liste der Geräte, auf denen der Password Manager installiert oder im Browser aktiviert ist.

Notizen

Die Funktion Sichere Notizen ist Ihr geheimes Notizbuch, in dem Sie vertrauliche Informationen speichern, ordnen und zur besseren Übersicht farblich kennzeichnen können. So sind die Informationen nicht nur gut organisiert, sondern auch sicher und vor fremden Zugriff geschützt.

So finden und aktivieren Sie diese Funktion:

1. Klicken Sie unter Windows oder macOS auf die **Password Manager** Symbol in Ihrem Webbrowser.

   Starten Sie unter Android oder iOS die **Password Manager** Anwendung.

   Wenn Sie dazu aufgefordert werden, geben Sie Ihre ein Master Passwort.

2. Öffnen Sie das Passwort Manager-Menü, um die Menüleiste links einzublenden und klicken Sie auf den Menüpunkt **Notizen**.

3. Klicken Sie auf **Notiz hinzufügen**.

   Geben Sie die Informationen ein, die Sie sicher aufbewahren möchten, und klicken Sie auf **Speichern**.

8.5. Häufig gestellte Fragen

Es gibt Fragen zum Bitdefender Password Manager, die uns immer wieder begegnen. Die passenden Antworten haben wir an dieser Stelle für Sie zusammengestellt. Hier erfahren Sie alles Wissenswerte über Ihr Bitdefender-Konto, den Import von Passwörtern, unsere Datensicherheitsprotokolle und andere wichtige Themen, die unsere Kunden beschäftigen.

Allgemeine Fragen zum Bitdefender Password Manager

Wie werde ich das Password Manager-Pop-up in meiner Bitdefender-Sicherheitslösung los?

Die Password Manager-Benachrichtigung, die in Bitdefender Total Security, Internet Security und Antivirus Plus angezeigt wird, können Sie

durch Klicken auf die Schaltfläche "x" schließen. Das Fenster "Verwalten Sie Ihre Passwörter mit dem Bitdefender Password Manager" erscheint zufällig ein paar Mal, wird danach aber nicht wieder angezeigt. Sie können diese Werbemitteilung abstellen, indem Sie die **Benachrichtigungen zu Empfehlungen** in den Bitdefender-Einstellungen auf "Aus" stellen.

Was passiert, wenn mein Bitdefender Password Manager-Abonnement abläuft?

Wenn Ihr Password Manager-Abonnement abläuft und nicht mehr aktiv ist, haben Sie maximal 90 Tage Zeit, um Ihre Passwörter zu exportieren. Ihre Passwörter werden für weitere 30 Tage als Sicherungskopie gespeichert. Während dieser 90 Tage können Sie Ihre Daten nur exportieren. Sie können den Password Manager nicht weiter verwenden. Die Funktion zum automatischen Ausfüllen von Passwörtern funktioniert dann nicht mehr, ebenso wie die Möglichkeit, neue Passwörter zu generieren.

Nach Ablauf der 90-tägigen Frist haben Sie weitere 30 Tage Zeit, um den Bitdefender-Support zu kontaktieren und die Wiederherstellung Ihrer Passwörter in der Live-Datenbank zu veranlassen. Sie können dann Ihre Passwörter aus dem Bitdefender Password Manager exportieren.

Ihre Daten werden in der Live-Datenbank nur bis zum Ende des Tages aufbewahrt, an dem Sie Ihre Anfrage auf Wiederherstellung gestellt haben. Um Mitternacht wird die Datenbank gelöscht - falls Sie die 30-tägige Nachfrist noch nicht überschritten haben, können die Passwörter aus der Sicherungskopie erneut wiederhergestellt werden. Die gesicherten Rohdaten in der Datenbank können dem Benutzer auf Anfrage zur Verfügung gestellt werden, die Datenbank ist jedoch verschlüsselt und die Informationen sind nicht zugänglich.

Was ist ein Master-Passwort, und warum muss ich es mir merken?

Das Master-Passwort ist der Schlüssel, der die Tür zu allen in Ihrem Bitdefender Password Manager-Konto gespeicherten Passwörtern öffnet. Das Master-Passwort muss mindestens 8 Zeichen lang sein. Erstellen Sie also ein starkes Master-Passwort, merken Sie es sich gut und geben Sie es niemals an Dritte weiter. Um ein starkes Master-Passwort zu erstellen, empfehlen wir Ihnen, eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (z. B. #, $ oder @) zu verwenden.

Wie verhindere ich, dass Bitdefender mich bei jedem Öffnen des Browsers nach meinem Master-Passwort fragt?

Wenn Sie Ihr Gerät sperren, ohne den Browser zu schließen, wird der Password Manager nicht gesperrt und Sie können nach Ihrer Rückkehr sofort auf Ihre Daten zugreifen. Als Sicherheitsmaßnahme müssen Sie sich jedoch bei jedem erneuten Öffnen des Browsers mit Ihrem Bitdefender Central-Konto anmelden und dann Ihr Master-Passwort eingeben.

- Um die Aufforderung zur Anmeldung bei Central zu deaktivieren, rufen Sie die Einstellungen auf und aktivieren Sie die Option "Anmeldereiter beim Start deaktivieren".
- Um die Aufforderung zur Eingabe des Master-Passworts zu deaktivieren, markieren Sie die Option "Meine Anmeldedaten speichern" im Fenster "Ihren Tresor entsperren".

Warum wird mein Master-Passwort nicht gespeichert und was passiert, wenn ich es vergesse?

Wir speichern Ihr Master-Passwort nicht auf unseren Servern, damit nur Sie auf Ihr Konto zugreifen können. Das gewährleistet maximale Sicherheit. Wenn der Bitdefender Password Manager Ihr Master-Passwort nicht erkennt, vergewissern Sie sich, dass Sie es richtig eingegeben haben und die Feststelltaste auf der Tastatur nicht aktiviert ist.

Falls Sie das Master-Passwort vergessen, können Sie jederzeit Ihren Wiederherstellungsschlüssel nutzen, um den Password Manager zu entsperren. Bei der ersten Anmeldung erhalten Sie vom Bitdefender Password Manager einen **Wiederherstellungsschlüssel**, mit dem Sie den Zugang zu Ihrem Konto wiederherstellen können, ohne Ihre Daten zu verlieren.

Falls Sie sowohl das Master-Passwort als auch den Wiederherstellungsschlüssel vergessen oder verlegt haben, können Sie sich als letzte Option an einen Bitdefender-Mitarbeiter wenden, um Ihr Konto zurücksetzen zu lassen.

> **Wichtig**
> Beim Zurücksetzen Ihres Kontos werden alle im Bitdefender Password Manager gespeicherten Daten und Passwörter gelöscht.

Können sich mehrere Benutzer ein Bitdefender Password Manager-Abonnement teilen?

Aktuell ist es nicht möglich, dass mehrere Benutzer ein Password Manager-Abonnement nutzen. Aber wir arbeiten daran, diese Möglichkeit in naher Zukunft bereitzustellen.

Was ist der Offlinemodus und wie funktioniert er?

Der Offlinemodus wird automatisch aktiviert, wenn Ihre Internetverbindung während der Nutzung des Bitdefender Password Managers unterbrochen wird. Wenn Sie bereits angemeldet sind und Ihr Master-Passwort eingegeben haben, können Sie im Offline-Modus auch dann auf Ihre Passwörter zugreifen, wenn keine Internetverbindung verfügbar ist.

Wie kann ich den Bitdefender Password Manager deinstallieren?

Gehen Sie zur Deinstallation des Bitdefender Password Managers wie folgt vor:

- Unter Windows und macOS:
  Entfernen Sie die Password Manager-Erweiterung aus Ihrem Webbrowser. Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol und wählen Sie "Entfernen".
- Android:
  Tippen Sie auf die Password Manager-App und halten Sie sie gedrückt. Ziehen Sie sie dann an den oberen Rand des Bildschirms zum Menüpunkt "Deinstallieren".
- Unter iOS und iPadOS:
  Tippen Sie auf die Password Manager-App und halten Sie sie gedrückt, bis alle Apps auf Ihrem Bildschirm zu wackeln beginnen. Tippen Sie jetzt auf das X oben links neben dem Bitdefender-Symbol.

Datenschutz- und Sicherheitsfragen rund um den Bitdefender Password Manager

Können Bitdefender-Mitarbeiter meine Passwörter einsehen?

Auf keinen Fall. Der Schutz Ihrer Daten hat für uns oberste Priorität. Das ist auch der wichtigste Grund, warum wir Ihr Master-Passwort nicht auf unseren Datenservern speichern: Damit niemand außer Ihnen Zugang zu Ihrem Konto hat, nicht einmal die Mitarbeiter unseres Unternehmens. Jedes Passwort und jedes Konto sind mit dem stärksten Datensicherheitsalgorithmus hochgradig verschlüsselt. Der uns

angezeigte Code erscheint lediglich als eine zufällig zusammengewürfelte Folge von Zahlen und Buchstaben.

Was würde bei einem Hack der Password Manager-Server passieren?

Jedes Passwort wird lokal auf Ihrem Gerät verschlüsselt, bevor es überhaupt in die Nähe unserer Server gelangt. Sollten Hacker also in unser System eindringen, würden sie nur Seiten mit zufälligen Folgen aus Buchstaben und Zahlen sehen, ohne Ihren Schlüssel, um sie zu entschlüsseln. Das bedeutet, dass Sie und Ihre Kontodaten bei uns jederzeit sicher sind.

9. SCHUTZ DER DIGITALEN IDENTITÄT

9.1. Was ist Bitdefender Password Manager

Schutz der Privatsphäre und Sicherheit im Internet stehen heutzutage im Mittelpunkt des Interesses von Internetnutzern. Und dafür gibt es viele gute Gründe. Weil es immer wieder zu größeren Datenpannen kommt, ist es unerlässlich, den Schutz und die Sicherheit Ihrer persönlich identifizierbaren Informationen (PII) zu gewährleisten.

Doch was gilt als persönlich identifizierbare Information? Ursprünglich galten vor allem sensible Daten wie der vollständige Name, die Sozialversicherungsnummer, der Führerschein, die Postanschrift oder Kreditkarteninformationen als PII. Mittlerweile fallen darunter auch weniger sensible Daten wie Postleitzahlen, IP-Adressen oder Anmeldekennung. Im Laufe der Zeit könnte Ihr digitaler Fußabdruck, d. h. die Daten, die Sie beim Surfen im Internet hinterlassen, einige dieser Informationen umfassen.

Bitdefender Password Manager ist Ihr ganz privater Weg zu mehr Freiheit im Internet, über den Sie sich die Kontrolle über Ihr digitales Leben zurückholen. Dazu benötigen Sie lediglich Ihren Namen, Ihre meistgenutzte E-Mail-Adresse und Ihre Telefonnummer. Auf Grundlage dieser Angaben suchen wir sowohl im öffentlich zugänglichen Internet als auch im Darknet nach persönlichen Informationen, die öffentlich zugänglich sind.

Im Funktionsumfang von Bitdefender Password Manager ist Folgendes enthalten:

- **Überwachung und Erkennung:** Der Dienst überwacht mehr als 100 personenbezogene Daten wie Kreditkartennummern oder Postanschrift und zeigt Ihnen alle Daten in Ihrem Online-Fußabdruck übersichtlich an.

  > **Notiz**
  > Bitdefender speichert und verarbeitet keine personenbezogenen Daten. Es werden nur Hinweise auf mögliche Datenpannen gespeichert, ohne dass dafür sensible Daten einbezogen werden.

- **Echtzeitwarnungen:** Sie erhalten Benachrichtigungen über Datenpannen und im Darknet gefundene Daten, persönliche

Informationen im öffentlich zugänglichen Internet sowie potenzielle Identitätsbetrüger in den sozialen Medien.

- **Lösungen:** Unser Dienst schlägt konkrete Maßnahmen vor, die zur Lösung von Problemen erforderlich sind, und erinnert Sie daran, wenn ein Problem nicht vollständig gelöst wurde. Sie können sich zudem anleiten lassen, wie Sie personalisierte Werbung unterbinden, Ihre Daten exportieren oder Tracking deaktivieren können.

9.2. Erste Schritte

9.2.1. Digital Identity Protection aktivieren

Aktivieren Sie Ihr Bitdefender Digital Identity Protection-Abonnement, nachdem Ihre Bestellung aufgegeben und bezahlt wurde.

1. Öffnen Sie die Bestätigungs-E-Mail, die Sie kurz nach Abschluss Ihrer Bestellung erhalten haben, und klicken Sie auf **ERSTE SCHRITTE**.
2. Sie werden auf https://central.bitdefender.com weitergeleitet.
   Melden Sie sich bei Ihrem Bitdefender Central-Konto an. Wenn Sie noch kein Konto haben, erstellen Sie bitte eins.
3. Nach der Anmeldung wird das Abonnement automatisch mit Ihrem Central-Konto verknüpft und der Einrichtungsvorgang eingeleitet.

Alternativ:

- Rufen Sie in Central links im Fenster den Bereich **Meine Abonnements** auf und klicken Sie auf **+ Mit Code aktivieren**.
- Geben Sie den 10-stelligen Schlüssel ein, den Sie mit Ihrer Bestätigungs-E-Mail erhalten haben, und klicken Sie auf Sie **AKTIVIEREN**.
- Wählen Sie nach Aufforderung aus, wie Sie den Code verwenden möchten, und klicken Sie dann auf **AKTIVIEREN**.

9.2.2. Digital Identity Protection konfigurieren

1. Rufen Sie https://central.bitdefender.com auf und melden Sie sich bei Ihrem Benutzerkonto an.
   Wenn Sie noch kein Konto haben, klicken Sie auf **Benutzerkonto erstellen** und geben Sie dann Ihren vollständigen Namen, eine E-Mail-Adresse und ein Passwort ein.

2. Rufen Sie den Bereich Digital Identity Protection auf.
   Die Willkommensseite wird angezeigt.
3. Klicken Sie auf **STARTEN**.
4. Sie werden nun darüber informiert, welche Informationen Sie angeben müssen. Ihre Daten werden grundsätzlich nur verschlüsselt und sicher verwahrt.
   Klicken Sie auf **WEITER**.
5. Geben Sie Ihren Vornamen, Ihren zweiten Vornamen (falls vorhanden) und Ihren Nachnamen in die entsprechenden Felder ein, und klicken Sie dann auf **WEITER**.
6. Geben Sie Ihre E-Mail-Adresse ein und klicken Sie auf **WEITER**.
   Stellen Sie sicher, dass es sich dabei um eine gültige E-Mail-Adresse handelt, auf die Sie zugreifen können.
7. An die von Ihnen angegebene Adresse wird ein Sicherheitscode gesendet.
   Öffnen Sie die E-Mail, kopieren Sie den Code und fügen Sie ihn in das entsprechende Feld ein.
   Klicken Sie danach auf **PRÜFEN**.
8. Wählen Sie Ihr Land und geben Sie Ihre Telefonnummer ein und klicken Sie danach auf **WEITER**.
9. Sie sollten kurz darauf einen Sicherheitscode erhalten.
   Geben Sie den Code ein und klicken Sie dann auf **PRÜFEN**.
10. Klicken Sie nach Abschluss der anfänglichen Prüfung auf **ABSCHLIEßEN**.

> **Notiz**
> Sie werden benachrichtigt, wenn bei dieser anfänglichen Überprüfung Datenpannen, persönlich identifizierbare Informationen oder mögliche Versuche von Identitätsbetrug gefunden werden.

Die Einrichtung von Bitdefender Password Manager ist damit abgeschlossen.

9.2.3. Ihren Digitalen Fußabdruck, Datenpannen und möglichen Identitätsbetrug überprüfen

Nachdem Sie die Einrichtung abgeschlossen haben, führt Bitdefender Password Manager einen Online-Check durch, um möglichem

Identitätsbetrug, Datenpannen und persönlich identifizierbaren Informationen im öffentlich zugänglichem Internet auf die Spur zu kommen. Wir empfehlen, alle Informationen in den Reitern **DIGITALER FUßABDRUCK**, **DATENPANNEN** und **ÜBERPRÜFUNG AUF IDENTITÄTSBETRUG** genau zu prüfen.

- Überprüfen Ihres digitalen Fußabdrucks (Seite 301)
- Überprüfen von Datenpannen (Seite 302)
- Überprüfen von möglichem Identitätsbetrug (Seite 303)

9.2.4. Verbessern Sie die Prüfung

Wir nutzen die von Ihnen bereitgestellten Daten, um das öffentlich zugängliche Internet sowie das Dark Web auf mögliche Aktivitäten zu überwachen, die sich negativ auf Ihre Privatsphäre oder Ihren guten Ruf auswirken könnten.

Wenn Sie eine weitere E-Mail-Adresse oder eine weitere Telefonnummer hinzufügen möchten, klicken Sie auf ⊕, dann auf **E-MAIL-ADRESSE HINZUFÜGEN** oder **TELEFONNUMMER HINZUFÜGEN** und folgen Sie den Anweisungen.

9.3. Dashboard

Im Dashboard werden alle Informationen aus den Bereichen **DIGITALER FUßABDRUCK**, **DATENPANNEN** und **ÜBERPRÜFUNG AUF IDENTITÄTSBETRUG** zusammengefasst.

Sie finden dort die folgenden Informationen:

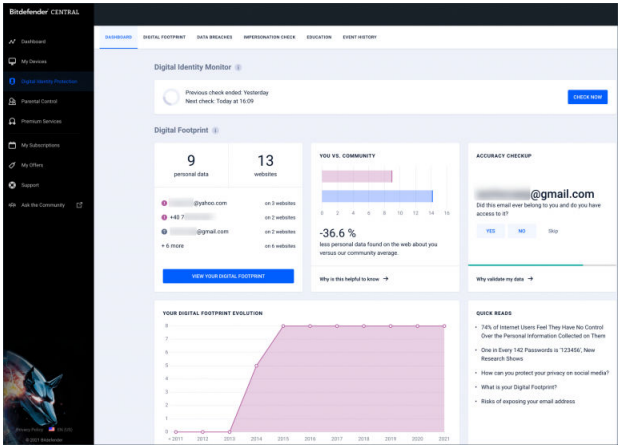
- Ihre offengelegten Daten und Ihre Quellen im Netz
- Die durchschnittliche Anzahl der offengelegten Daten unter allen Nutzern
- Die Entwicklung Ihres digitalen Fußabdrucks
- Datenschutzrelevante Inhalte
- Datenpannen
- Die durchschnittliche Anzahl der Datenpannen unter allen Nutzern

9.3.1. Identitätsüberwachung

Bitdefenders System sucht ausschließlich anhand zutreffender Informationen nach neuen personenbezogenen Daten, die im offenen

Internet oder im Darknet veröffentlicht wurden und überprüft alle wichtigen sozialen Netzwerke nach Anzeichen von Identitätsbetrug.

Klicken Sie auf **JETZT PRÜFEN**, um einen Online-Scan durchzuführen.



9.4. Digitaler Fußabdruck

Hier werden Ihre persönlich identifizierbaren Informationen und ihre Quellen angezeigt. Es liegt an Ihnen zu beurteilen, ob die Offenlegung der Informationen im Internet eine Bedrohung darstellt.

Unsere KI-gestützte Überwachung ist zur Erkennung neuer Bedrohungen in hohem Maße auf zutreffende Daten angewiesen. Lassen Sie uns daher bitte wissen, ob die Informationen zutreffen oder nicht.

Sobald Sie bestätigen, dass Daten zu Ihnen gehören, fügen wir sie unserem Überwachungssystem hinzu und verbessern so die Chancen, in Zukunft weitere Informationen zu finden.

9.4.1. Überprüfen Ihres digitalen Fußabdrucks

So überprüfen Sie Ihren digitalen Fußabdruck:

1. Rufen Sie den Reiter **DIGITALER FUßABDRUCK** auf.
2. Informationen, die noch nicht bestätigt wurden, erscheinen mit dem Option **Bestätigen** auf der rechten Seite. Klicken Sie auf **Bestätigen** und danach auf Ja oder Nein.

Notiz

Jede bestätigte Information wird unserem Überwachungsalgorithmus hinzugefügt, wodurch die Ergebnisgenauigkeit unserer Dienste verbessert wird. Informationen, die verworfen werden, werden nicht mehr angezeigt, bleiben aber weiterhin im Internet verfügbar.

9.5. Datenschutzverletzungen

Wenn es Hackern gelingt, die Sicherheitsvorkehrungen eines Unternehmens zu umgehen und an Ihre persönlichen Daten zu gelangen, um sie im Darknet zu verkaufen, spricht man von Datenpannen. In den meisten Fällen haben es Cyberkriminelle auf Anmeldedaten, persönlich identifizierbare Informationen (PII), medizinische Daten und Bankdaten abgesehen.

Jedes Unternehmen oder jeder Dienst kann Opfer von Datenpannen werden, doch mit Größe des Kundenstamms steigt auch die Attraktivität eines Ziels. Datenlecks betreffen in der Regel Namen, E-Mail-Adressen, Benutzernamen, Passwörter, Postanschriften, Telefonnummern, Sozialversicherungsnummern (SSN) und Kreditkartendaten (Nummer, Ablaufdatum, CVV).

9.5.1. Überprüfen von Datenpannen

So können Sie Ihren Datenpannen einsehen:

1. Rufen Sie den Reiter **DATENPANNEN** auf.
2. Unter einigen Einträgen finden Sie eine Liste mit Aktionen, die zur Absicherung Ihres Benutzerkontos erforderlich sind. Klicken Sie nach Abschluss einer Aktion auf das nebenstehende Kästchen, um die Durchführung zu bestätigen.

   Wenn Sie sich nicht sicher sind, wie eine Aufgabe durchzuführen ist, können Sie jederzeit auf den Link in der Aufgabenbeschreibung klicken. Sie werden dann auf eine Seite weitergeleitet, auf der Sie alle erforderlichen Schritte finden.

   Nicht alle Datenpannen können auf so behoben werden. Bei einigen, wie z. B. **Sammlung Nr. 1**, werden keine Schritte angezeigt. Stattdessen werden Sie zu Artikeln im Internet weitergeleitet, in denen Sie weitere Hilfe finden können.

Notiz

Bitdefender speichert oder verarbeitet keine personenbezogenen Daten. Es werden nur Verweise auf potenzielle Datenschutzverletzungen aufbewahrt, ohne sensible Daten einzubeziehen.

9.6. Überprüfung auf Identitätsbetrug

Kriminelle, die im Fachjargon als "Pretexter" bezeichnet werden, sind sehr geschickt darin, sich als jemand anders auszugeben. Sie schlüpfen dabei in die Rolle einer vertrauenswürdigen Person, um ihre Opfer zu täuschen und sich Zugang zu sensiblen Informationen zu verschaffen. Die Praxis des "Pretexting" ist definiert als das Vortäuschen der Identität einer anderen Person, um den Empfänger dazu zu bringen, sensible Daten wie Passwörter, Kreditkartennummern oder andere vertrauliche Informationen preiszugeben.

Bitdefender Password Manager überwacht 25 Social-Media-Plattformen und informiert Sie umgehend über Profile, bei denen der Verdacht auf Identitätsbetrug besteht.

9.6.1. Überprüfen von möglichem Identitätsbetrug

Im Reiter **ÜBERPRÜFUNG AUF IDENTITÄTSBETRUG** werden alle potenziellen Versuche angezeigt. Für jeden Fund stehen drei Möglichkeiten zur Auswahl:

- Es handelt sich um versuchten Identitätsbetrug
- Es handelt sich um Ihr eigenes Profil
- Es handelt sich um ein fremdes Profil

Je nach Auswahl empfiehlt Bitdefender Password Manager konkrete Schritte, um das Problem zu lösen. Sie können jeden Schritt nach Abschluss als **Erledigt** markieren.

9.7. News

Der Reiter "News" dient als Wissensdatenbank, in der Benutzer weiterführende Informationen zum Schutz ihrer digitalen Identität finden können.

Die Artikel hier können in die folgenden Kategorien eingeteilt werden:

- Schwachstellen
- Sicherheitsrisiken
- Identitätsprüfung

Klicken Sie zum Lesen des vollständigen Artikels auf den entsprechenden **Lesen Sie mehr**-Link.

9.8. Ereignisverlauf

Der Bereich Ereignisverlauf dient der anhaltenden Kommunikation mit unseren Benutzern. Hier finden Sie eine chronologisch geordnete Liste von Ereignissen im Zusammenhang mit dem Schutz Ihrer digitalen Identität.

Neben neu entdeckten Bedrohungen (falls vorhanden) finden Sie auf dieser Seite auch nützliche Tipps zum richtigen Verhalten im Internet, um sich besser gegen mögliche Verletzungen Ihrer Privatsphäre zu wappnen.

Im Ereignisverlauf finden Sie die folgenden Informationen:

- Durchgeführte Aktionen
- Updates des Dienstes
- Datenschutzverletzungen

10. HILFE UND SUPPORT

10.1. Hier wird Ihnen geholfen

Bitdefender bietet seinen Kunden konkurrenzlos schnellen und kompetenten Support. Sollten sich Probleme ergeben oder Sie eine Frage zu Ihrem Bitdefender-Produkt haben, so stehen Ihnen verschiedene Online-Quellen zur Verfügung, wo Sie Lösungen und Antworten finden.

10.2. Online-Ressourcen

Bei Problemen und Fragen in Zusammenhang mit Bitdefender stehen verschiedene Online-Ressourcen zur Verfügung.

- Bitdefender-Support-Center:
  https://www.bitdefender.de/consumer/support/
- Die Bitdefender Expert Community:
  https://community.bitdefender.com/de
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Weitere Informationen über Computersicherheit, Bitdefender-Produkte und unsere Firma finden Sie über Ihre Lieblingssuchmaschine.

10.2.1. Bitdefender-Support-Center

Das Bitdefender-Support-Center ist eine Online-Sammlung von Informationen zu Ihren Bitdefender-Produkten. Hier sind in einem leicht zugänglichen Format Berichte zu den Ergebnissen des fortlaufenden technischen Supports sowie der Bugfix-Aktivitäten der Bitdefender-Support- und Entwicklungsteams gespeichert. Hinzu kommen Artikel zur Bedrohungsvorbeugung, detaillierte Erklärungen zur Verwaltung von Bitdefender-Lösungen und vieles mehr.

Die Bitdefender Support Center ist zudem öffentlich zugänglich und komplett durchsuchbar. Durch diese Art der Informationsbereitstellung bieten wir unseren Kunden eine weitere Möglichkeit, technische Grundlagen und Fachwissen über unsere Produkte zu erlangen. Alle berechtigen Informationsanfragen oder Fehlermeldungen von Bitdefender-Kunden finden sich über kurz oder lang im Bitdefender

Support Center wieder und dienen als Bugfix-Anleitungen, Umgehungslösungen oder Informationsartikel, die die Hilfedateien des Produkts ergänzen sollen.

Das Bitdefender Support Center ist jederzeit unter der folgenden Adresse erreichbar: https://www.bitdefender.de/support/consumer.html.

10.2.2. Die Bitdefender Experten Community

Die Experten-Community ist eine Plattform, auf der sich Bitdefender-Experten, -Anwender und -Fans einbringen, Ideen austauschen, sich gegenseitig unterstützen und ihr Wissen und ihre Lösungen mit anderen teilen. Hier werden zudem viele Ideen geboren und unsere Entwickler finden wichtiges Feedback. Unsere Community-Mitglieder sind erfahrene Bitdefender-Anwender, die Freude daran haben, anderen zu helfen. Dank ihres unschätzbaren Beitrags und ihres freiwilligen Engagements konnten wir eine Wissensdatenbank schaffen, in der Anwender nützliche Antworten und Anleitungen finden können, aber auch das Zwischenmenschliche seinen Platz hat.

Hier können Sie in einen echten Austausch mit Menschen treten, die Bitdefender selbst auf ihren Geräten nutzen. Die Community verbindet Sie mit unseren Mitgliedern und verschafft Ihrer Stimme Gehör. Hier werden Sie sich gerne einbringen, weil Sie wissen, dass Ihre Meinung und Ihr Beitrag respektiert und geschätzt werden. Als Anbieter Ihrer Wahl sind wir stets bestrebt, Ihnen beispiellos schnellen und kompetenten Support zu bieten und möchten Sie an unserer Seite wissen. Darum haben wir diese Community geschaffen.

Hier geht's zur Website unserer Expert Community:

https://community.bitdefender.com/de

10.2.3. Bitdefender Cyberpedia

In der Bitdefender Cyberpedia finden Sie alles Wissenswerte zu den neuesten Cyberbedrohungen. Hier teilen Bitdefender-Experten Tipps und Tricks, wie Sie sich vor Hackern, Datenschutzverletzungen, Identitätsdiebstahl und Social-Media-Identitätsbetrug schützen können.

Die Bitdefender Cyberpedia finden Sie hier:

https://www.bitdefender.com/cyberpedia/.

10.3. Kontaktinformation

Effiziente und kundenorientierte Kommunikation ist der Schlüssel zu einem erfolgreichen Geschäftsmodell. Bereits seit 2001 setzt BITDEFENDER alles daran, die bereits hochgesteckten Erwartungen unserer Kunden und Partner immer wieder zu übertreffen und diese Tradition wollen wir auch in Zukunft fortführen. Für jedwede Fragen stehen wir Ihnen deshalb gerne zur Verfügung. Kontaktieren Sie uns dazu einfach über unser **Bitdefender Support Center**.

https://www.bitdefender.de/consumer/support/

10.3.1. Lokale Vertriebspartner

Die Bitdefender Händler stehen für Fragen und Informationen in ihren jeweiligen Regionen jederzeit zur Verfügung, sowohl für vertriebliche als auch für allgemeine Anfragen.

So finden Sie einen Bitdefender Distributor in Ihrem Land:

1. Rufen Sie https://www.bitdefender.com/partners/partner-locator.html</link> auf.
2. Geben Sie über die entsprechenden Optionen Ihren Wohnort und Ihr Land an.

GLOSSAR

Aktivierungs-Code

Dabei handelt es sich um einen eindeutigen Schlüssel, der käuflich erworben und zur Aktivierung eines Produkts oder eines Dienstes verwendet werden kann. Mit einem Aktivierungscode kann ein gültiges Abonnement für einen bestimmten Zeitraum und eine bestimmte Anzahl an Geräten aktiviert werden. Zudem kann mit einem solchen Code eine Abonnement verlängert werden, solange es sich auf das gleiche Produkt oder den gleichen Dienst bezieht.

ActiveX

ActiveX ist ein Programmuster, dass von anderen Programmen und Betriebssystemkomponenten unter Windows aufgerufen werden kann. Die ActiveX Technologie wird von Microsofts Internet Explorer benutzt, damit interaktive Webseiten eher wie Programme und nicht wie statische Seiten angezeigt werden. Mit ActiveX können die Benutzer z.B. Fragen stellen oder beantworten, Buttons verwenden, oder verschiedenartige Interaktionen mit der Webseite herstellen. ActiveX-Steuerelemente werden oft in Visual Basic geschrieben. Erwähnenswert ist, dass bei AktiveX die Sicherheitskontrollen fehlen, deshalb raten Computersicherheitsexperten davon ab, AktiveX über das Internet zu nutzen.

Advanced Persistent Threat

Advanced Persistent Threat (APT) nutzen Sicherheitslücken im System, um wichtige Daten zu stehlen und an ihre Quellen zu übermitteln. Organisationen, Unternehmen und Regierungsbehörden sind eine große Zielgruppe, die von dieser Bedrohung ins Visier genommen wird. Advanced Persistent Threats sollen so lange wie möglich unentdeckt bleiben. Während dieser Zeit sollen sie das System überwachen und wichtige Daten sammeln, ohne dabei die Zielcomputer zu beschädigen. Die Bedrohung wird durch PDF-Dateien oder Office-Dokumente in das Netzwerk eingebracht, die keinen Verdacht erregen, so dass jeder Benutzer diese Dateien ausführen kann.

Adware

Adware wird häufig mit einer anderen Anwendung kombiniert, die kostenlos ist, solange der Nutzer die Adware akzeptiert. Adware-

Anwendungen werden in der Regel installiert, nachdem der Nutzer einer Lizenzvereinbarung zugestimmt hat. In der Lizenzvereinbarung wird auch der Zweck der Anwendung genannt, und somit liegt keine Rechtswidrigkeit vor. Allerdings können Popup-Anzeigen mit der Zeit sehr lästig werden und in manchen Fällen die Systemperformance beeinträchtigen. Zudem kann aufgrund der Daten, die manche dieser Programme sammeln, die Privatsphäre von Nutzern verletzt werden, die sich über die Bedingungen in der Lizenzvereinbarung nicht völlig im Klaren waren.

Archiv

Ein Datenträger, ein Magnetband oder ein Ordner mit Dateien, die von einem Backup erzeugt wurden.

Eine Datei, die eine oder mehrere Dateien in einem komprimierten Format enthält.

Hintertür

Eine Sicherheitslücke eines Systems, die der Entwickler oder Administrator absichtlich hinterlässt. Der Grund dafür muss nicht immer bösartig sein. Manche Betriebssysteme haben schon standardmäßig privilegierte Konten eingerichtet, damit diese von den Kundendienst-Technikern oder Programmierern der Hersteller benutzt werden können.

Boot-Sektor

Der erste Sektor einer Festplatte oder Diskette. Hier liegen Daten, die das Betriebssystem zum Booten (Starten) braucht.

Bootvirus

Eine Bedrohung, der den Bootsektor einer Festplatte oder eines Diskettenlaufwerks infiziert. Beim Versuch von einer Diskette, die mit einem Bootvirus infiziert ist, zu booten wird diese Bedrohung im Arbeitsspeicher aktiviert. Bei jedem Neustart wird die Bedrohung so im Arbeitsspeicher aktiviert und überträgt sich auf eingelegte Wechselmedien.

Botnetz

Das Wort "Botnetz" setzt sich aus Bestandteilen der Wörter "Roboter" und "Netzwerk" zusammen. Bei Botnetzen handelt es sich um Netzwerke aus mit Bedrohungen infizierten Geräten, die mit dem Internet verbunden und für den Versand von Spam, den Diebstahl von Daten, die Fernsteuerung

von anfälligen Geräten oder die Verbreitung von Spyware, Ransomware und anderen Bedrohungsarten verwendet werden. Ziel ist es, möglichst viele mit dem Internet verbundene Geräte zu infizieren, so z. B. PCs, Server, Mobilgeräte oder IoT-Geräte in den Netzwerken großer Unternehmen oder Branchen.

Browser

Kurzform für Web-Browser, ein Programm, mit dem Internetseiten aufgerufen und angezeigt werden können. Bekannte Browser sind Microsoft Internet Explorer, Mozilla Firefox und Google Chrome. Dies sind graphische Browser, was bedeutet, dass sie sowohl Grafiken als auch Texte anzeigen können. Weiterhin können die meisten Browser Multimedia-Daten wie Klang- und Videodateien anzeigen, wobei sie für diverse Formate Plug-Ins (zusätzliche Softwarekomponenten) benutzen.

Brute-Force-Angriff

Ein Angriff mit dem Ziel, sich Zugang zu einem passwortgeschützten System zu verschaffen, bei dem in schneller Abfolge häufige Passwortkombinationen durchprobiert werden.

Befehlszeile

Die Befehlszeile ist eine zeichenorientierte Benutzerschnittstelle. Die Kommunikation zwischen Benutzer und Computer findet ausschließlich durch die Eingabe von bestimmten Befehlen statt, die sich aus einzelnen Buchstabenfolgen zusammensetzen. Als Eingabegerät wird eine Tastatur benutzt. Die Verwendung einer Maus ist nicht möglich. Auf der Befehlszeile werden die einzelnen Anweisungen in einer bestimmten Befehlssprache eingegeben, die vom Computer und seiner Software ausgewertet und mit den entsprechenden Ergebnissen auf dem Ausgabegerät (meistens ein Monitor) wieder an den Benutzer übergeben werden.

Cookies

In der Internetbranche werden mit Cookies kleine Dateien bezeichnet, die Daten über einzelne Computer enthalten und die von den Werbetreibenden analysiert und verwendet werden, um die Interessen und Vorlieben der Benutzer herauszufinden. Die Cookie-Technologie wird stetig weiterentwickelt mit dem Ziel Benutzern nur noch solche Werbung anzuzeigen, die ihren Interessen entspricht. Für viele ist dies ein zweischneidiges Schwert. Einerseits ist es praktisch, nur Anzeigen zu sehen, an denen man interessiert ist. Anderseits bedeutet es, dass

Online-Aktivitäten der Benutzer gewissermaßen auf Schritt und "Klick" verfolgt werden. Es ist also verständlich, dass in diesem Zusammenhang Datenschutz ein umstrittenes Thema ist und viele sich unwohl fühlen, quasi als SKU-Nummer (die Strichcodes auf den Packungen, die im Geschäft an der Theke gescannt werden) betrachtet zu werden. Auch wenn diese Sicht etwas extrem erscheint, ist sie doch manchmal korrekt.

Cybermobbing

Wenn Altersgenossen oder Fremde absichtlich Kinder misshandeln, um sie körperlich zu verletzen. Um emotionale Schäden anzurichten, schicken die Täter verletzende Nachrichten oder unvorteilhafte Fotos, so dass sich ihre Opfer von anderen isolieren oder entmutigt werden.

Wörterbuchangriff

Ein Angriff mit dem Ziel, sich Zugang zu einem passwortgeschützten System zu verschaffen, bei dem alle möglichen Wörter aus einem Wörterbuch als potenzielle Passwörter eingegeben werden. Dieselbe Methode wird auch verwendet um Schlüssel für verschlüsselte Nachrichten oder Dokumente zu erraten. Wörterbuchangriffe funktionieren, weil viele Benutzer kurze, leicht zu erratende Wörter als Passwörter benutzen.

Laufwerk

Ein Gerät, das rotierende Speichermedien lesen und beschreiben kann. Ein Festplatten-Laufwerk liest und beschreibt Festplatten. Ein Disketten-Laufwerk liest und beschreibt Disketten. Laufwerke können sowohl interner (im Rechner eingebaut) als auch externer (in einem Gehäuse, das an den Rechner angeschlossen wird) Art sein.

Download

Kopiert Daten (gewöhnlich eine ganze Datei) von einer Hauptquelle auf ein Peripheriegerät. Der Begriff bezeichnet oft den Kopiervorgang von einem Online Service auf den eigenen Rechner. Download oder Herunterladen kann auch das Kopieren einer Datei von einem Netzwerkserver auf einen Netzwerkrechner bedeuten.

E-Mail

Elektronische Post. Ein Dienst, der Nachrichten an andere Rechner über ein lokales oder ein globales Netzwerk übermittelt.

Ereignisanzeige

Ereignisse oder Erscheinungen, die in einem Programm vorkommen. Ereignisse können Benutzeraktionen, wie zum Beispiel Mausklicks oder Tastatureingaben, oder Systemereignisse, wie zum Beispiel ungenügender Speicher, sein.

Exploits

Eine Möglichkeit, Fehler oder Schwachstellen in Computersoftware und -hardware für seine Zwecke auszunutzen. So können Hacker die Kontrolle über Computer oder Netzwerke übernehmen.

Falsch Positiv

Erscheint, wenn ein Virenscanner eine Datei als infiziert erkennt, obwohl dies nicht der Fall ist.

Dateierweiterungen

Der Teil hinter dem Punkt im Dateinamen. Die Erweiterung oder Extension beschreibt die Art der Daten, die in einer Datei gespeichert sind. Viele Betriebssysteme benutzen Dateierweiterungen, z.B. Unix, VMS und MS-DOS. Sie sind gewöhnlich ein bis drei Buchstaben lange (alte Betriebssysteme können oft nicht mehr als drei Buchstaben unterstützen). Beispiele sind "exe" ausführbare Dateien, "ps" für PostScript oder "txt" für Text-Dateien.

Heuristisch

Eine Methode, um neue Bedrohungen zu identifizieren. Diese Scan-Methode benötigt keine konkreten Bedrohungsinformationen. Der Vorteil eines heuristischen Scans ist, dass man nicht von einer neuen Variante einer alten Bedrohung getäuscht werden kann. Manchmal kann jedoch auch ein verdächtiger Code in einem normalen Programm gemeldet werden, ein sogenannter Fehlalarm oder "falsch-positive Meldung" wird angezeigt.

Honigtopf

Ein Computersystem, das als Köder dient, um Hacker anzulocken und danach ihr Verhalten zu beobachten. Daraus lassen sich Schlüsse ziehen, mit welchen Methoden Sie Daten sammeln. Besonders Unternehmen und Konzerne setzen auf den Einsatz dieser "Honigtöpfe", um ihren Sicherheitslage zu verbessern.

IP

Internet Protocol - Das TCP/IP Protokoll ist verantwortlich für die korrekte IP Adressierung und die korrekte Zustellung der Datenpakete.

Java-Applet

Ein Java Programm, das nur auf Webseiten läuft. Um ein Applet auf einer Webseite zu benutzen, gibt man den Namen und die Größe (Länge und Breite in Pixel) an, die das Applet einnehmen kann. Wenn die Webseite abgerufen wird, lädt der Browser das Applet vom Server herunter und führt es auf der Benutzermaschine (dem Client) aus. Applets sind keine Anwendungen, da sie von strengen Sicherheitsprotokollen gesteuert werden.

Obwohl Applets z. B. auf dem Client laufen, können diese keine Daten auf der Maschine des Clients lesen oder schreiben. Zusätzlich sind die Applets dahingehend beschränkt, dass sie nur Daten aus der Domain lesen und schreiben können, zu der sie gehören.

Keylogger

Ein Keylogger ist eine Anwendung, die alle Ihre Tastenanschläge aufzeichnet. Keylogger sind an sich nicht schädlich. Sie können auch legitim eingesetzt werden, um beispielsweise die Aktivitäten von Angestellten oder Kindern zu überwachen. Sie werden jedoch zunehmend von Cyber-Kriminellen mit bösartiger Absicht eingesetzt (um beispielsweise private Daten wie Benutzernamen oder Passwörter zu sammeln).

Makrovirus

Eine Bedrohungsart, die in einem Dokument als eingebettetes Makro verschlüsselt wird. Viele Anwendungen, wie Microsoft Word und Excel, unterstützen leistungsstarke Makrosprachen. Diese Anwendungen ermöglichen das Einbetten eines Makros in ein Dokument, welches dann bei jedem Öffnen des Dokuments ausgeführt wird.Ein Makro ist eine Aufzeichnung des Ablaufs von Routineaufgaben innerhalb des makrofähigen Programms, das dann immer wieder verwendet werden kann.

E-Mail-Client

Ein E-Mail-Client ist eine Anwendung, die das Senden und Empfangen von E-Mails ermöglicht.

Speicher

Interne Speicherbereiche im Rechner. Der Begriff Arbeitsspeicher bezeichnet Datenträger in Form von sehr schnellen Chips. Dies steht im Gegensatz zu Speicherplatz, der sich auf Magnetbändern

oder Datenträgern befindet. Jeder Rechner hat eine gewisse Menge Arbeitsspeicher. Dieser wird auch Hauptspeicher oder RAM bezeichnet.

Nicht-heuristisch

Diese Scan-Methode benötigt konkrete Bedrohungsinformationen. Der Vorteil eines nicht-heuristischen Scans ist, dass er nicht von einer Scheinbedrohung getäuscht werden kann und so Fehlalarme verhindert.

Online-Missbrauchstäter

Wenn Personen versuchen, Minderjährige oder Jugendliche anzusprechen, um sie in illegale sexuelle Aktivitäten zu verwickeln. Soziale Netzwerke sind der ideale Ort, um verletzlichen Kindern nachzustellen und sie zu sexuellen Aktivitäten zu verführen, sei es online oder persönlich.

Gepackte Programme

Eine Datei in einem komprimierten Format. Viele Betriebssysteme und Anwendungen enthalten Befehle, mit denen Dateien komprimiert werden können, so dass diese weniger Speicherplatz benötigen. Zum Beispiel: Angenommen, Sie haben einen Text, der 10 aufeinander folgende Leerzeichen enthält. Normalerweise belegen diese Leerzeichen dann 10 Bytes an Speicherplatz.

Ein Programm, das Dateien komprimiert, würde die Leerzeichen durch ein Sonderzeichen „Leerzeichenreihe“ ersetzen, gefolgt von der Zahl der Leerzeichen, die ersetzt wurden. In diesem Fall sind nur noch zwei Bytes notwendig statt zehn. Das wäre ein Beispiel für eine Komprimierungstechnik, es gibt aber noch viele andere.

Pfad

Zeigt die Stelle an, an der sich eine Datei in einem Rechner befindet. Diese Pfadangaben enthalten gewöhnlich den hierarchischen Aufbau des Dateiverzeichnisses: Laufwerke, Ordner, Unterverzeichnisse, die Datei und ihre Erweiterung.

Der Weg zwischen zwei Punkten, wie zum Beispiel der Kommunikationskanal zwischen zwei Rechnern.

Phishing

Das Senden einer E-Mail an einen Benutzer, in der der Sender sich als Vertreter eines legitimen Unternehmens ausgibt und versucht, den Empfänger so zu manipulieren, dass er persönliche Informationen

preisgibt, die dann zum Diebstahl der Identität verwendet werden können. Die E-Mail leitet den Benutzer dann auf eine Webseite, auf der er aufgefordert wird, vertrauliche Daten wie Kreditkartennummern, TANs oder PINs preiszugeben. Es wird oft vorgegeben, dass dies aus Gründen der Aktualisierung geschehen soll. Diese Webseiten sind jedoch gefälscht und wurden eigens für den Diebstahl dieser Daten eingerichtet.

Photon

Photon ist eine innovative und unaufdringliche Bitdefender-Technologie, die eigens entwickelt wurde, um die Auswirkungen der Sicherheitslösung auf die Systemleistung zu minimieren. Durch die Hintergrundüberwachung aller PC-Aktivitäten werden Nutzungsprofile erstellt, mit denen Start- und Scan-Prozesse optimiert werden können.

Polymorphes Virus

Eine Bedrohung, die ihre Form mit jeder Datei, die sie infiziert, ändert. Da diese Bedrohungen kein beständiges binäres Muster haben, sind sie sehr schwer zu erkennen.

Schnittstelle

Stelle eines Rechners, an die ein Gerät angeschlossen werden kann. Rechner haben verschiedenartige Schnittstellen. Im Inneren gibt es Schnittstellen zum Anschluss von Festplatten, Grafikkarten und Tastaturen. Extern haben Rechner Schnittstellen zum Anschluss von Modems, Druckern und anderen Peripheriegeräten.

In TCP/IP und UDP Netzwerken, ein Endpunkt zu logischen Verbindungen. Die Schnittstellennummer gibt die Art der Schnittstelle an. Zum Beispiel, Schnittstelle 80 wird für HTTP Traffic verwendet.

Ransomware

Bei Ransomware handelt es sich um schädliche Programme, die anfällige Systeme für den Benutzer sperren und für deren Freigabe Lösegeld erpressen. CryptoLocker, CryptoWall und TeslaWall sind nur einige Beispiele für Ransomware, die es auf Benutzercomputer abgesehen haben.

Die Infektion kann sich durch das Aufrufen eine Spam-Nachricht, das Herunterladen eines E-Mail-Anhangs oder die Installation von Anwendungen ausbreiten, ohne dass der Benutzer es überhaupt bemerkt. Ransomware-Hacker nehmen herkömmliche Benutzer und Unternehmen ins Visier.

Berichtsdatei

Eine Datei, die stattgefundene Aktivitäten aufzeichnet. Zum Beispiel speichert BitDefender eine Prokolldatei mit den geprüften Pfaden, Ordnern, der Anzahl der gescannten Archive und Dateien sowie der Anzahl der gefundenen infizierten oder verdächtigen Dateien.

Rootkit

Bei einem Rootkit handelt es sich um eine Sammlung von Software-Tools, mit denen auf ein System mit Administratorrechten zugegriffen werden kann. Der Begriff wurde ursprünglich nur für UNIX-Systeme verwendet und beschrieb rekompilierte Tools, mit denen sich Angreifer Administratorrechte verschaffen und so ihre Anwesenheit vor den tatsächlichen Administratoren verbergen konnten.

Die Hauptaufgabe eines Rootkits besteht darin, Prozesse, Dateien und Protokolle zu verstecken. Sie können auch Daten von Terminals, Netzwerkverbindungen oder Peripheriegeräten abfangen, falls Sie eine entsprechende Software eingebaut haben.

Rootkits sind nicht grundsätzlich schädlich. Einige Systeme und Anwendungen verstecken z. B. wichtige Dateien mithilfe von Rootkits. Sie werden jedoch oft dazu missbraucht, Bedrohungen zu verbergen oder unbemerkt einen Eindringling einzuschleusen. In Kombination mit anderen Bedrohungen stellen Rootkits eine große Gefahr für Ihr System dar. Denn sie können den Datenverkehr abhören, Sicherheitslücken in Ihrem System schaffen, Dateien und Zugangsdaten verändern, und das alles, ohne entdeckt zu werden.

Skript

Ein anderer Begriff für Makro- oder Batchdatei. Ein Skript ist eine Befehlsliste, die ohne Benutzereingriff ausgeführt werden kann.

Spam

Junk-E-Mail oder Junk-Postings in Newsgroups. Im Allgemeinen versteht man darunter jede Art von unerwünschter E-Mail.

Spyware

Software, die unentdeckt vom Nutzer private und geheime Anwenderdaten über seine Internetverbindung abgreift. Dies geschieht in der Regel zu Werbezwecken. Typischerweise sind Spyware-Anwendungen als verborgene Komponenten in Freeware- oder Shareware-Programmen

enthalten, die aus dem Internet heruntergeladen werden können. Die große Mehrzahl von Shareware- und Freeware-Anwendungen ist natürlich frei von Spyware. Ist die Spyware einmal installiert, überwacht sie die Nutzeraktivitäten und überträgt diese Daten im Hintergrund an einen Dritten. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter und Kreditkartennummern sammeln.

Einer Bedrohung durch ein trojanisches Pferd ähnelt Spyware darin, dass die Anwender das Produkt unwissentlich gemeinsam mit etwas anderem installieren. Opfer von Spyware wird man oft dann, wenn man sich bestimmte Peer-to-Peer-Dateiaustauschprogramme herunterlädt.

Ganz abgesehen von den Fragen der Ethik und des Datenschutzes belegt Spyware auch unnötig Systemressourcen und Bandbreite, indem über die Internetverbindung des Nutzers Informationen an den Spyware-Heimatserver gesendet werden. Da Spyware Speicher und Systemressourcen verbraucht, können die im Hintergrund laufenden Anwendungen zu Systemabstürzen oder allgemeiner Systeminstabilität führen.

Startup Objekt (Autostart-Objekt)

Jede Datei, die sich in diesem Ordner befindet, wird geöffnet, wenn der Rechner gestartet wird. Das können z. B. ein Startbildschirm, eine Sounddatei, die beim Systemstart abgespielt wird, ein Erinnerungskalender oder auch Apps sein. Gewöhnlich wird eine Alias-Datei (Verknüpfung) statt der eigentlichen Datei in diesen Ordner gelegt.

Abonnement

Ein Kaufvertrag, der Benutzern das Recht einräumt, ein bestimmtes Produkt oder eine Dienstleistung auf einer bestimmten Anzahl von Geräten und für einen bestimmten Zeitraum in Anspruch zu nehmen. Ein abgelaufenes Abonnement kann unter Verwendung der vom Nutzer beim Ersterwerb angegebenen Informationen automatisch verlängert werden.

Infobereich

Die Symbolleiste wurde mit Windows 95 eingeführt und befindet sich auf der Windows Task-Leiste (gewöhnlich unten rechts, dort wo sich auch die Uhrzeit befindet). Sie enthält kleine Symbole zur Information und zum leichteren Zugriff auf Systemfunktionen wie Drucker, Modems, Lautstärke und anderes. Um auf die Details und Optionen dieser Funktionen zuzugreifen, ist ein Doppelklick oder ein Klick mit der rechten Maustaste erforderlich.

TCP/IP

Transmission Control Protocol/Internet Protocol – im Internet weit verbreiteter Netzwerkprotokollsatz, der die Kommunikation zwischen verbundenen Computernetzwerken mit verschiedenen Hardware-Architekturen und Betriebssystemen ermöglicht. TCP/IP bietet eine Möglichkeit, all diese unterschiedlichen Komponenten zu Kommunikationszwecken miteinander zu verbinden.

Bedrohung

Ein Programm oder ein Stück Code, das auf einen Rechner kopiert wird und sich allein ausführt, ohne dass es der Besitzer des Rechners will oder merkt. Die meisten Bedrohungen können sich auch selbst vervielfältigen. Alle Computerbedrohungen wurden von Menschen programmiert. Eine einfache Bedrohung, die sich immer wieder vervielfältigen kann, ist sehr einfach zu programmieren. Sogar eine solch einfache Bedrohung kann gefährlich sein, da sie im Handumdrehen sämtlichen Arbeitsspeicher belegen und so das System lahmlegen kann. Noch gefährlicher sind Bedrohungen, die sich über Netzwerke hinweg selbst weiterversenden und Sicherheitssysteme umgehen.

Update der Bedrohungsinformationen

Das binäre Muster einer Bedrohung, wird von der Sicherheitslösung zur Erkennung und Beseitigung einer Bedrohung genutzt.

Trojaner

Ein bösartiges Programm, das sich als eine legitime Anwendung ausgibt. Anders als Schad-Software und Würmer vervielfältigen sich Trojaner nicht selbst, können aber dennoch großen Schaden anrichten. Einer der heimtückischsten Trojaner ist ein Programm, das behauptet Ihren Rechner von Bedrohungen zu befreien, stattdessen aber den Rechner infiziert.

Der Begriff entstammt einer Geschichte in Homers "Ilias", in der die Griechen ihren Feinden, den Trojanern, angeblich als Sühnegabe ein riesiges hölzernes Pferd schenkten. Aber nachdem die Trojaner das Pferd in die Stadt gebracht hatten, schlichen sich die im Bauch des hölzernen Pferdes versteckten Soldaten bei Nacht heraus, öffneten die Tore der Stadt und ermöglichten somit ihren Landsleuten, in die Stadt einzudringen und auf diese Weise Troja zu besetzen.

Update (Aktualisierung)

Eine neue Software- oder Hardwareversion, die eine ältere Version desselben Produkts ersetzt. Die Update-Installationsroutine eines Programms prüft oft, ob eine ältere Versionen auf dem Rechner installiert ist, da sonst kein Update installiert werden kann.

Bitdefender verfügt über eine eigene Update-Funktion, über die Sie manuell nach Updates suchen oder das Produkt automatisch aktualisieren lassen können.

Virtual Private Network (VPN)

Mit dieser Technologie ist es möglich, eine zeitlich begrenzte und verschlüsselte direkte Verbindung mit einem bestimmten Netzwerk auch über ein weniger gut gesichertes Netzwerk aufzubauen. Auf diese Weise können Daten sicher und verschlüsselt versandt und empfangen werden und sind für neugierige Augen nur schwer einsehbar. Bei einem Sicherheitsnachweis handelt es sich um eine Authentifizierung, die ausschließlich über einen Benutzernamen und ein Passwort erfolgen kann.

Wurm

Ein Programm, das sich selbst kopiert und über ein Netzwerk verbreitet. Es kann sich nicht an andere Programme anhängen.