HANDLEIDING

Bitdefender CONSUMER SOLUTIONS

Ultimate Security

Bitdefender Ultimate Security

Handleiding

Publication date 20/01/2025

Juridische mededeling

Bitdefender

Inhoudsopgave

OVER DEZE GIDS

Doel en beoogde doelgroep

Uw Bitdefender Total Security-abonnement kan tot 10 verschillende pc's, Macs, iOS- en Android-smartphones en -tablets beschermen. Het beheer van de beveiligde apparaten kan worden gedaan via een Bitdefender-account, dat gekoppeld moet zijn aan een actief abonnement.

Deze gids biedt hulp bij de installatie en het gebruik van de producten die bij uw abonnement zijn inbegrepen: Bitdefender Total Security (voor Windows), Bitdefender Antivirus for Mac (voor macOS), Bitdefender Mobile Security (voor Android) en Bitdefender Mobile Security voor iOS.

U kunt ontdekken hoe u Bitdefender op verschillende apparaten configureert om ze te beschermen tegen allerlei bedreigingen.

Hoe deze handleiding te gebruiken

Deze gids is georganiseerd rond de vier producten die deel uitmaken van Bitdefender Total Security:

- Totale beveiliging voor pc (pagina 4)
  Leer hoe u het product gebruikt op uw Windows-pc's en -laptops.
- Antivirus voor Mac (pagina 162)
  Leer hoe u het product op uw Macs gebruikt.
- Mobiele beveiliging voor Android (pagina 207)
  Leer hoe u het product kunt gebruiken op uw Android-smartphones en -tablets.
- Mobiele beveiliging voor iOS (pagina 241)
  Leer hoe u het product kunt gebruiken op uw iOS-gebaseerde smartphones en tablets.
- VPN (pagina 257)
  [en] Learn how to hide your online identity using Bitdefender VPN on any of your devices.
- Wachtwoordbeheerder
  [en] Keep track and safely store of all of your passwords and credentials with Password Manager.

- Digitale identiteitsbescherming (pagina 298)
  [en] Learn how you can protect and monitor your digital identity.
- Hulp vragen (pagina 307)
  Ontdek waar u hulp kunt zoeken als er iets onverwachts opduikt.

Conventies die in deze gids worden gebruikt

Typografische conventies

In deze gids worden verschillende tekststijlen gebruikt, zodat de tekst leesbaarder is. De weergave en betekenis worden in de onderstaande tabel voorgesteld.

Weergave	Beschrijving
voorbeeld-syntaxis	Voorbeelden van syntaxis worden weergegeven in een niet-proportioneel lettertype.
https://www.bitdefender.com	De URL-koppeling wijst naar een externe locatie op http- of ftp-servers.
documentation@bitdefender.com	E-mailadressen worden in de tekst ingevoegd voor contactgegevens.
Over deze gids (pagina 1)	Dit is een interne koppeling naar een locatie in het document.
bestandsnaam	Namen van bestanden en mappen worden weergegeven in een niet-proportioneel lettertype.
optie	Alle productopties worden **vet** weergegeven.
trefwoord	Sleutelwoorden en belangrijke zinsdelen worden **vet** weergegeven.

Waarschuwingen

De waarschuwingen zijn grafisch gemarkeerde opmerkingen in de tekst die extra informatie over de huidige paragraaf onder de aandacht brengen.

Opmerking

De opmerking is slechts een kort commentaar. Hoewel u opmerkingen kunt weglaten, kunnen ze toch waardevolle informatie bieden zoals over een specifieke functie of een koppeling naar een verwant onderwerp.

Belangrijk

Dit vereist uw aandacht en het wordt niet aanbevolen dit te negeren. Doorgaans betreft het niet-kritieke, maar belangrijke informatie.

Waarschuwing

Dit is kritische informatie die u aandachtig moet lezen. Er zullen geen ernstige problemen optreden als u de aanwijzingen volgt. U moet de informatie lezen en begrijpen omdat hier iets wordt beschreven dat hoge risico's inhoudt.

Verzoek om commentaar

We willen u uitnodigen ons te helpen dit boek te verbeteren. Wij hebben alle informatie zo goed mogelijk getest en gecontroleerd. Laat ons weten of u enige tekortkomingen hebt ontdekt in dit boek of als u ideeën hebt om dit te verbeteren, zodat wij u de best mogelijke documentatie kunnen bieden.

U kunt contact met ons opnemen door een e-mail te sturen naar documentation@bitdefender.com. Wij verzoeken u al uw e-mails met betrekking tot de documentatie in het Engels te schrijven, zodat we uw opmerkingen op een efficiënte manier kunnen verwerken.

1. TOTALE BEVEILIGING VOOR PC

1.1. Installatie

1.1.1. Voorbereiden voor installatie

Voordat u Bitdefender Ultimate Security installeert, moet u deze voorbereidingen voltooien om ervoor te zorgen dat de installatie vlot verloopt:

- Controleer of de apparaat waarop u Bitdefenderwilt installeren, voldoet aan de minimale systeemvereisten. Als de apparaat niet aan alle systeemvereisten voldoet, wordt het Bitdefender niet geïnstalleerd, of als het toch geïnstalleerd wordt, zal het niet goed werken en zal het systeem vertragen en instabiel worden. Raadpleeg Systeemvereisten (pagina 4) voor een complete lijst van systeemvereisten.
- Meld u aan bij de apparaat met een beheerdersaccount.
- Verwijder alle gelijksoortige software van de apparaat. Indien iets wordt opgemerkt tijdens het Bitdefender-installatieproces, zult u een bericht krijgen om het te verwijderen. Als u twee beveiligingsprogramma's tegelijk uitvoert, kan dit hun werking beïnvloeden en ernstige problemen met het systeem veroorzaken. Windows Defender zal uitgeschakeld zijn tijdens de installatie.
- Schakel alle firewall-programma's die mogelijk op uw apparaat worden uitgevoerd uit of verwijder ze. Als u twee firewallprogramma's tegelijk uitvoert, kan dit hun werking beïnvloeden en ernstige problemen met het systeem veroorzaken. Windows Firewall zal uitgeschakeld zijn tijdens de installatie.
- Het wordt aanbevolen uw apparaat verbonden te laten met Internet tijdens de installatie, zelfs wanneer u vanaf een cd/dvd installeert. Indien er nieuwere versies van de toepassingsbestanden in het installatiepakket beschikbaar zijn, kan Bitdefender deze downloaden en installeren.

1.1.2. Systeemvereisten

U kan Bitdefender Ultimate Security uitsluitend installeren op apparaaten met de volgende besturingssystemen:

- Windows 7 met Service Pack 1
- Windows 8.1
- Windows 10
- 2,5 GB beschikbare vrije ruimte op de harde schijf (ten minste 800 MB op de systeemschijf)
- 2 GB geheugen (RAM)

Belangrijk
Systeemprestaties kunnen worden beïnvloed voor apparaten die CPU's van een oudere generatie hebben.

Opmerking
Om na te gaan welk Windows-besturingssysteem op uw apparaat wordt uitgevoerd en voor hardwaregegevens:

- Klik in **Windows 7**, met de rechtermuisknop op **Mijn Computer** op het bureaublad, en selecteer dan **Eigenschappen** uit het menu.
- Zoek in **Windows 8**, vanuit het Windows-startscherm **Computer** (u kunt bijvoorbeeld starten met het typen van "computer", rechtstreeks in het startscherm), en rechterklik op het pictogram ervan. In **Windows 8.1**, zoek **Deze pc**.
  Selecteer **Eigenschappen** in het onderste menu. Zoek in **Systeem** naar informatie over uw systeemtype.
- Typ in **Windows 10 Systeem** in het zoekvak op de taakbalk en klik op het pictogram ervan. Kijk in het **Systeem** gebied om informatie te vinden over uw systeemtype.

1.1.3. Softwarevereisten

Om Bitdefender te kunnen gebruiken, evenals alle functies ervan, moet uw apparaat voldoen aan de volgende softwarevereisten:

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

1.1.4. Uw Bitdefender-product installeren

U kunt Bitdefender installeren vanaf de installatiedisk of via de web installer die u naar uw apparaat kunt downloaden vanaf de **Bitdefender Central**.

Indien uw aankoop van toepassing is op meer dan één apparaat, herhaalt u het installatieproces en activeert u uw product op elke apparaat met dezelfde account. De account die u moet gebruiken, is deze die uw actieve abonnement van Bitdefender bevat.

Installeer vanaf Bitdefender Central

Via de Bitdefender Central kunt u de installatiekit die met het aangekochte abonnement overeenkomt, downloaden. Zodra het installatieproces voltooid is, is Bitdefender Ultimate Security geactiveerd.

Om Bitdefender Ultimate Security te downloaden van Bitdefender Central:

1. Ga naar **Bitdefender Central**.
2. Selecteer het paneel **Mijn Apparaten** en klik dan op **BESCHERMING INSTALLEREN**.
3. Kies een van de twee beschikbare opties:

   - **Dit apparaat beschermen**

     a. Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.

     b. Sla het installatiebestand op.

   - **Bescherm andere apparaten**

     a. Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.

     b. Klik op **DOWNLOADKOPPELING VERZENDEN**.

     c. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL VERZENDEN**.
     De gegenereerde downloadlink is slechts 24 uur geldig. Indien de link vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.

d. Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailadres dat u ingevoerd hebt en klik op de overeenkomstige downloadknop.

4. Wacht tot het downloaden voltooid is en voer het installatieprogramma uit.

Bevestigen van de installatie

Bitdefender controleert eerst uw systeem om de installatie te valideren.

Als uw systeem niet voldoet aan de minimale systeemvereisten voor het installeren van Bitdefender, wordt u op de hoogte gebracht van de gebieden die moeten worden verbeterd voordat u kunt doorgaan.

Als een niet-compatibele beveiligingsoplossing of een oudere versie van Bitdefender wordt gedetecteerd, wordt u gevraagd dit van uw systeem te verwijderen. Volg de richtlijnen om de software uit uw systeem te verwijderen, zodat problemen op een later tijdstip worden vermeden. U zult mogelijk uw apparaat opnieuw moeten opstarten om het verwijderen van de gedetecteerde beveiligingsoplossingen te voltooien.

Het installatiepakket voor Bitdefender Total Security wordt voortdurend bijgewerkt.

> **Opmerking**
> Het downloaden van de installatiebestanden kan lang duren, vooral bij tragere internetverbindingen.

Zodra de installatie gevalideerd is, verschijnt de installatiewizard. Volg de stappen om Bitdefender Ultimate Security te installeren.

Step 1 - Bitdefender installatie

Voordat u verdergaat met de installatie, moet u akkoord gaan met de Abonnementsovereenkomst. Lees de Abonnementsovereenkomst grondig door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Ultimate Security.

Sluit het venster als u niet akkoord gaat met deze voorwaarden. De installatieprocedure wordt afgebroken en u verlaat de installatie.

In deze stap kunnen twee bijkomende taken uitgevoerd worden:

- Zorg ervoor dat de optie **Productrapporten verzenden** geactiveerd blijft. Door deze optie toe te staan, worden rapporten met informatie

over uw gebruik van het product naar de Bitdefender-servers verzonden. Deze informatie is van essentieel belang om het product te verbeteren en kan ons helpen in de toekomst een betere ervaring te verschaffen. Merk op dat deze rapporten geen vertrouwelijke informatie bevatten, zoals uw naam of IP-adres, en dat ze niet voor commerciële doeleinden zullen gebruikt worden.

❍ Selecteer de taal waarin u het product wenst te installeren.

Klik op **INSTALLEREN** om het installatieproces van uw Bitdefender-product te starten.

Stap 2 - Installatieproces

Wacht tot de installatie is voltooid. Er wordt gedetailleerde informatie over de voortgang weergegeven.

Stap 3 - Installatie voltooid

Uw Bitdefender-product werd met succes geïnstalleerd.

Er wordt een overzicht van de installatie weergegeven. Als tijdens de installatie een actieve bedreiging wordt gedetecteerd en verwijderd, kan het opnieuw opstarten van het systeem nodig zijn.

Stap 4 - Apparaatanalyse

U wordt vervolgens gevraagd of u een analyse wilt uitvoeren van uw apparaat, om te verzekeren dat het veilig is. Tijdens deze stap zal Bitdefender kritieke systeemgebieden scannen. Klik op **Apparaatanalyse starten** om het te starten.

U kunt de scaninterface verbergen door te klikken op **Scan uitvoeren op de achtergrond**. Daarna kiest u of u op de hoogte wilt worden gebracht wanneer de scan is voltooid, of niet.

Wanneer de scan voltooid is, klikt u op **Bitdefender-interface openen**.

Opmerking
Indien u de scan niet wilt laten uitvoeren, klikt u gewoon op **Overslaan**.

Stap 5 - Aan de slag

In het venster **Aan de slag** kunt u de details van uw abonnement bekijken.

Klik op **VOLTOOIEN** om naar de Bitdefender Ultimate Security-interface te gaan.

Installeren vanaf de installatiedisk

Om Bitdefender te installeren vanaf de installatieschijf, plaatst u de schijf in het optische station.

Binnen enkele seconden moet een installatiescherm verschijnen. Volg de instructies om de installatie te starten.

Indien het installatiescherm niet verschijnt, gebruik Windows Explorer om naar de rootdirectory van de schijf te gaan en dubbelklik op het bestand autorun.exe.

Indien uw internetsnelheid traag is of uw systeem niet met het internet verbonden is, klikt u op de knop **Installeren vanaf cd/dvd**. In dat geval zal het Bitdefender-product dat op de disk beschikbaar is, geïnstalleerd worden, terwijl een nieuwere versie zal gedownload worden vanaf de Bitdefender-servers via de productupdate.

Bevestigen van de installatie

Bitdefender controleert eerst uw systeem om de installatie te valideren.

Als uw systeem niet voldoet aan de minimale systeemvereisten voor het installeren van Bitdefender, wordt u op de hoogte gebracht van de gebieden die moeten worden verbeterd voordat u kunt doorgaan.

Als een niet-compatibele beveiligingsoplossing of een oudere versie van Bitdefender wordt gedetecteerd, wordt u gevraagd dit van uw systeem te verwijderen. Volg de richtlijnen om de software uit uw systeem te verwijderen, zodat problemen op een later tijdstip worden vermeden. U zult mogelijk uw apparaat opnieuw moeten opstarten om het verwijderen van de gedetecteerde beveiligingsoplossingen te voltooien.

Het installatiepakket voor Bitdefender Total Security wordt voortdurend bijgewerkt.

> **Opmerking**
> Het downloaden van de installatiebestanden kan lang duren, vooral bij tragere internetverbindingen.

Zodra de installatie gevalideerd is, verschijnt de installatiewizard. Volg de stappen om Bitdefender Ultimate Security te installeren.

Stap 1 - Bitdefender Installatie

Voordat u doorgaat met de installatie, moet u akkoord gaan met de abonnementsovereenkomst. Neem even de tijd om de abonnementsovereenkomst te lezen, aangezien deze de algemene voorwaarden bevat waaronder u mag gebruiken Bitdefender Ultimate Security.

Als u niet akkoord gaat met deze voorwaarden, sluit u het venster. Het installatieproces wordt afgebroken en u verlaat de installatie.

Bij deze stap kunnen twee extra taken worden uitgevoerd:

- Houd de **Stuur productrapporten** optie ingeschakeld. Door deze optie toe te staan, worden rapporten met informatie over hoe u het product gebruikt naar de Bitdefender-servers verzonden. Deze informatie is essentieel voor het verbeteren van het product en kan ons helpen om in de toekomst een betere ervaring te bieden. Merk op dat deze rapporten geen vertrouwelijke gegevens bevatten, zoals uw naam of IP-adres, en dat ze niet voor commerciële doeleinden zullen worden gebruikt.
- Selecteer de taal waarin u het product wilt installeren.

Klik **INSTALLEREN** om het installatieproces van uw Bitdefender-product te starten.

Stap 2 - Installatie bezig

Wacht tot de installatie is voltooid. Gedetailleerde informatie over de voortgang wordt weergegeven.

Stap 3 - Installatie voltooid

Er wordt een samenvatting van de installatie weergegeven. Als er tijdens de installatie een actieve dreiging is gedetecteerd en verwijderd, kan het nodig zijn het systeem opnieuw op te starten.

Stap 4 - Apparaatanalyse

U wordt nu gevraagd of u een analyse van uw apparaat wilt uitvoeren om er zeker van te zijn dat het veilig is. Tijdens deze stap scant Bitdefender kritieke systeemgebieden. Klik **Start apparaatanalyse** om het te initiëren.

U kunt de scaninterface verbergen door op te klikken **Scan op de achtergrond uitvoeren**. Kies daarna of u op de hoogte wilt worden gehouden wanneer de scan is voltooid of niet.

Wanneer de scan voltooid is, klikt u op **Verdergaan met account maken**.

> **Opmerking**
> Als u de scan niet wilt uitvoeren, kunt u ook gewoon op klikken **Overslaan**.

Stap 5 - Bitdefender-account

Als u de initiële setup hebt voltooid, verschijnt het Bitdefender Account-scherm. U hebt een Bitdefender-account nodig om het product te activeren en de online functies te kunnen gebruiken. Zie Bitdefender Central voor meer informatie.

Ga verder volgens uw situatie.

❍ **Ik wil een Bitdefender-account maken**

1. Typ de vereiste informatie in de overeenkomende velden. De gegevens die u hier opgeeft, worden vertrouwelijk behandeld. Het wachtwoord moet minstens 8 tekens lang zijn, minstens één nummer of symbool en kleine letters en hoofdletters bevatten.
2. Voordat u verdergaat, moet u de Gebruiksvoorwaarden aanvaarden. De Gebruiksvoorwaarden bevatten de voorwaarden waaronder u Bitdefender mag gebruiken; lees ze dus grondig door. U kunt eveneens het Privacybeleid lezen.
3. Clik op **ACCOUNT MAKEN**.

> **Opmerking**
> Eens de account is aangemaakt, kunt u het gebruikte e-mailadres en wachtwoord gebruiken om in te loggen op uw account op https://central.bitdefender.com, of op de Bitdefender Central-app, indien de app geïnstalleerd is op een van uw Android- of iOS-apparaten. Ga naar Google Play, zoek Bitdefender Central op en tik op de installatie-optie om de Bitdefender Central-app voor Android te installeren. Ga naar de App Store, zoek Bitdefender Central op en tik op de installatie-optie om de Bitdefender Central-app voor iOS te installeren.

- **Ik heb al een Bitdefender-account**

  1. Klik op **Aanmelden**.
  2. Voer het e-mailadres in het daarvoor bestemde veld en klik daarna op **VOLGENDE**.
  3. Voer uw wachtwoord in en klik op **AANMELDEN**.
     Bent u het wachtwoord voor uw account kwijt of wilt u het gewoon opnieuw instellen:
     a. Klik op **Wachtwoord vergeten?**.
     b. Voer uw e-mailadres in en klik op **VOLGENDE**.
     c. Controleer uw e-mailaccount, voer de beveiligingscode in die u ontvangen hebt en klik op **VOLGENDE**.
        Of u kunt in de e-mail die we naar u gestuurd hebben, klikken op **Wachtwoord wijzigen**.
     d. Typ het nieuwe wachtwoord dat u wilt instellen, en typ het nogmaals. Klik op **OPSLAAN**.

     > **Opmerking**
     > Als u al een MyBitdefender-account hebt, kunt u deze gebruiken om u aan te melden bij uw Bitdefender-account. Als u uw wachtwoord bent vergeten, moet u eerst naar https://my.bitdefender.com gaan om het opnieuw in te stellen. Gebruik vervolgens de bijgewerkte inloggegevens om u aan te melden bij uw Bitdefender-account.

- **Ik wil mij aanmelden met mijn Microsoft-, Facebook- of Google-account**

  Om u aan te melden met uw Microsoft-, Facebook- of Google-account:

  1. Selecteer de service die u wilt gebruiken. U wordt omgeleid naar de aanmeldingspagina van die service.
  2. Volg de instructies die door de geselecteerde service worden gegeven om uw account te koppelen aan Bitdefender.

     > **Opmerking**
     > Bitdefender krijgt geen toegang tot vertrouwelijke informatie, zoals het wachtwoord van de account die u gebruikt om aan te melden of de persoonlijke informatie van uw vrienden en contactpersonen.

Stap 6 - Uw product activeren

> **Opmerking**
> Deze stap verschijnt indien u gekozen hebt om een nieuwe Bitdefender-account aan te maken in de vorige stap, of indien u zich hebt aangemeld met een account waarop een verlopen abonnement van toepassing is.

Er is een werkende internetverbinding vereist om de activering van uw product te voltooien.

Ga verder volgens uw situatie:

- Ik heb een activeringscode
  Activeer het product in dit geval door de volgende stappen te volgen:

  1. Voer de activatiecode in het veld Ik heb een activatiecode in en klik daarna op **DOORGAAN**.

     > **Opmerking**
     > U vindt uw activatiecode:
     >
     > - op het cd/dvd-label.
     > - op de productregistratiekaart.
     > - in de online aankoop e-mail.

  2. **Ik wil Bitdefender evalueren**
     In dat geval kunt u het product gedurende 30 dagen gebruiken. Om de proefperiode te beginnen, selecteert u **Ik heb geen abonnement, ik wil het product gratis uitproberen**, en klik dan op **DOORGAAN**.

Stap 7 - Aan de slag

In het venster **Aan de slag** kunt u de details van uw abonnement bekijken.

Klik **FINISH** om toegang te krijgen tot de Bitdefender Ultimate Security koppel.

1.2. Uw beveiliging beheren

1.2.1. Antivirusbeveiliging

Bitdefender beveiligt uw apparaat tegen alle types bedreigingen (malware, Trojanen, spyware, rootkits enz.). De BitDefender-bescherming is ingedeeld in twee categorieën:

- **Scannen bij toegang** - verhindert dat nieuwe bedreigingen uw systeem binnenkomen. Bitdefender zal bijvoorbeeld een Worddocument scannen op bekende gevaren wanneer u het opent, en een e-mailbericht wanneer u het ontvangt.

  Met Scannen bij toegang bent u zeker van bescherming in real time tegen bedreigingen, een essentieel onderdeel van elk computerbeveiligingsprogramma.

  > **Belangrijk**
  > Houd **Scannen bij toegang** ingeschakeld om te verhinderen dat bedreigingen uw apparaat infecteren.

- **Scannen op aanvraag** - hiermee kunt u de bedreiging die al op uw systeem aanwezig is, detecteren en verwijderen. Dit is de klassieke scan die door de gebruiker wordt geactiveerd. U selecteert het station, de map of het bestand dat BitDefender moet scannen, en BitDefender doet dat - op aanvraag.

Bitdefender scant automatisch alle verwisselbare media die op de apparaat zijn aangesloten om zeker te zijn dat ze veilig kunnen worden geopend. Zie Automatisch scannen van verwisselbare media (pagina 29) voor meer informatie.

Geavanceerde gebruikers kunnen scanuitzonderingen configureren als ze niet willen dat specifieke bestanden of bestandstypes worden gescand. Zie Scanuitsluitingen configureren (pagina 31) voor meer informatie.

Wanneer een bedreiging wordt gedetecteerd, zal Bitdefender automatisch proberen de kwaadwillige code uit het geïnfecteerde bestand te verwijderen en het originele bestand te reconstrueren. Deze bewerking wordt 'desinfecteren' genoemd. Bestanden die niet kunnen worden gedesinfecteerd, worden naar quarantaine verplaatst om de infectie in te dammen. Zie Bestanden in quarantaine beheren (pagina 33) voor meer informatie.

Als uw apparaat werd geïnfecteerd door bedreigingen, moet u Bedreigingen van uw systeem verwijderen (pagina 154) raadplegen. Om u te helpen bij het opruimen van de bedreigingen die niet kan worden verwijderd van het Windows-besturingssysteem op uw apparaat, biedt Bitdefender u de Reddingsomgeving (pagina 155). Dit is een vertrouwde omgeving, vooral ontworpen voor het verwijderen van bedreigingen, waarmee u uw apparaat onafhankelijk van Windows kunt opstarten. Wanneer het apparaat in de Noodomgeving wordt gebruikt, zijn Windows-dreigingen niet actief, waardoor het makkelijker is om ze te verwijderen.

Scannen bij toegang (real time-beveiliging)

Bitdefender biedt realtime bescherming tegen een breed gamma bedreigingen door alle bestanden en e-mailberichten waar toegang toe wordt gezocht, te scannen.

De real time-beveiliging in- of uitschakelen

De bescherming tegen bedreigingen in reële tijd in- of uitschakelen:

1. Klik in het navigatiemenu in de **Bitdefender-interface** op **Bescherming**.
2. Klik in het deelvenster **ANTIVIRUS** op **Openen**.
3. Schakel in het venster **Geavanceerd Bitdefender Shield** in of uit.
4. Indien u bescherming in reële tijd wenst uit te schakelen, verschijnt een waarschuwingsscherm. U moet uw keuze bevestigen door in het menu te selecteren hoelang u de real time-beveiliging wilt uitschakelen. U kunt de real time-beveiliging uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot een systeem opnieuw wordt opgestart. De realtime beveiliging wordt automatisch ingeschakeld als de geselecteerde tijd verloopt.

Waarschuwing

Dit is een kritiek beveiligingsprobleem. Wij raden u aan de real time-beveiliging zo kort mogelijk uit te schakelen. Als de real time-beveiliging is uitgeschakeld, wordt u niet beveiligd tegen bedreigingen.

De geavanceerde instellingen voor de realtime beveiliging configureren

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door Bitdefender worden aangeboden. U kunt de

instellingen voor de real time-beveiliging in detail configureren door een aangepast beschermingsniveau te maken.

Om degeavanceerde instellingen voor de realtime beveiliging te configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. In het venster **Geavanceerd** kunt u de scaninstellingen configureren.

Informatie over de scanopties

Deze informatie kan nuttig zijn:

- **Scan alleen toepassingen.** U kunt Bitdefender instellen om alleen geopende apps te scannen.
- **Scan potentieel ongewenste toepassingen.** Selecteer deze optie om te scannen op ongewenste toepassingen. Een potentieel ongewenste toepassing (PUA) of potentieel ongewenst programma (PUP) is software die meestal gebundeld wordt met freeware software en pop-ups weergeeft of een werkbalk installeert in de standaard browser. Sommige veranderen de startpagina of de zoekmachine, andere laten verschillende processen op de achtergrond lopen die de pc vertragen of tonen talrijke advertenties. Deze programma's kunnen worden geïnstalleerd zonder uw toestemming (ook wel adware genoemd) of worden standaard opgenomen in de express installatiekit (advertentie-gesteund).
- **Scripts scannen.** Met de functie Scripts scannen kan Bitdefender powershellscripts en office-documenten scannen die scriptgebaseerde malware zou kunnen bevatten.
- **Gedeelde netwerken scannen.** Om een extern netwerk vanaf uw apparaat veilig te gebruiken, raden we aan dat u de optie Gedeelde netwerken scannen ingeschakeld laat.
- **Procesgeheugen scannen.** Scant op kwaadaardige activiteiten in het geheugen van lopende processen.
- **Opdrachtregel scannen.** Scant de opdrachtregel van nieuw opgestarte toepassingen om bestandsloze aanvallen te voorkomen.
- **Archieven scannen.** Het scannen binnen archieven is een traag proces dat veel middelen vergt, en dat daarom niet wordt aanbevolen voor

real time-beveiliging. Archieven met geïnfecteerde bestanden vormen geen onmiddellijke dreiging voor de veiligheid van uw systeem. De dreiging kan uw systeem pas aantasten als het geïnfecteerde bestand wordt uitgepakt uit het archief en wordt uitgevoerd zonder dat de real time-beveiliging is ingeschakeld.

Beslist u om deze optie te gebruiken, schakel deze dan in en versleep de schuifregelaar langs de schaal om archieven die groter zijn dan een bepaalde waarde in MB (Megabytes) uit te sluiten.

- **Opstartsectoren scannen.** U kunt Bitdefender instellen om de opstartsectoren van uw harde schijf te scannen. Deze sector van de harde schijf bevat de noodzakelijke computercode om het opstartproces te starten. Wanneer een dreiging de opstartsector infecteert, kan de schijf ontoegankelijk worden en kunt u uw systeem niet opstarten en geen toegang krijgen tot uw gegevens.
- **Alleen nieuwe en gewijzigde bestanden scannen.** Door alleen nieuwe en gewijzigde bestanden te scannen, kunt u de algemene reactiviteit van uw systeem aanzienlijk verbeteren met een minimale inlevering op het vlak van beveiliging.
- **Keyloggers scannen.** Selecteer deze optie om uw systeem te scannen op keylogger apps. Keyloggers slaan op wat u op uw toetsenbord intypt en zenden via internet verslagen naar een kwaadwillend persoon (hacker). De hacker kan gevoelige informatie uit de gestolen gegevens halen, zoals bankrekeningnummers en wachtwoorden, en deze voor zijn eigen doeleinden gebruiken.
- **Vroege opstartscan.** Selecteer de optie **Vroege opstartscan** om uw systeem te scannen bij het opstarten, zodra alle kritieke diensten geladen zijn. De bedoeling van deze functie is om de detectie van bedreigingen bij de opstart van het systeem te verbeteren en de opstarttijd van uw systeem te verkorten.

Acties die worden ondernomen op gedetecteerde bedreigingen

U kunt de acties die door de realtime bescherming worden genomen configureren aan de hand van de volgende stappen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.

3. In het venster **Geavanceerd** scrolt u naar beneden tot u de optie **Dreigingsacties** ziet.
4. Configureer de scaninstellingen zoals dat nodig is.

De volgende acties kunnen worden ondernomen door de realtime beveiliging in Bitdefender:

Neem gepaste actie

Bitdefender zal de aanbevolen acties ondernemen op basis van het type van het gedetecteerde bestand:

- **Geïnfecteerde bestanden.** Bestanden die als besmet zijn gedetecteerd, komen overeen met een stukje bedreigingsinformatie gevonden in de informatiedatabase voor bedreigingen van Bitdefender. Bitdefender zal automatisch proberen de kwaadaardige code van een geïnfecteerd bestand te verwijderen en het originele bestand te reconstrueren. Deze bewerking wordt 'desinfecteren' genoemd.
  Bestanden die niet kunnen worden gedesinfecteerd, worden naar quarantaine verplaatst om de infectie in te dammen. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Zie Bestanden in quarantaine beheren (pagina 33) voor meer informatie.

  > **Belangrijk**
  > Voor specifieke types bedreigingen is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig boosaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand verwijderd van de schijf.

- **Verdachte bestanden.** Soms worden bestanden door de heuristische analyse aangemerkt als 'verdacht'. Verdachte bestanden kunnen niet worden gedesinfecteerd, omdat hiervoor geen standaard desinfectieroutine bestaat. Ze worden verplaatst naar quarantaine om een mogelijke infectie te voorkomen.
- **Archieven die geïnfecteerde bestanden bevatten.**
  - Archieven die alleen geïnfecteerde bestanden bevatten, worden automatisch verwijderd.
  - Als een archief zowel geïnfecteerde als schone bestanden bevat, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen op voorwaarde dat het programma het archief met de

schone bestanden opnieuw kan opbouwen. Als het niet mogelijk is het archief te reconstrueren, wordt u op de hoogte gebracht dat er geen actie kan worden ondernomen om zo te vermijden dat schone bestanden verloren gaan.

Naar quarantaine verplaatsen

Verplaatst gedetecteerde bestanden naar de quarantaine. In quarantaine geplaatst bestanden kunnen niet worden uitgevoerd of geopend; daardoor is er geen infectiegevaar meer. Zie Bestanden in quarantaine beheren (pagina 33) voor meer informatie.

Toegang weigeren

Wanneer een geïnfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd.

De standaardinstellingen herstellen

De standaardinstellingen voor de realtime-beveiliging garanderen een goede beveiliging tegen bedreigingen, met een minimale impact op de systeemprestaties.

De standaard real time-beveiligingsinstellingen herstellen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Scrol naar beneden in het venster **Geavanceerd** tot u de optie **Geavanceerde instellingen terugstellen** ziet. Selecteer deze optie om de antivirusinstellingen terug te stellen naar fabrieksinstellingen.

Scannen op aanvraag

Bitdefender heeft als hoofddoel uw apparaat vrij te houden van bedreigingen. Dit wordt gedaan door nieuwe bedreigingen uit uw apparaat weg te houden en door uw e-mailberichten en alle nieuwe bestanden, die u downloadt of kopieert naar uw systeem, te scannen.

Het risico bestaat dat een bedreiging zich reeds in uw systeem heeft genesteld voordat u Bitdefender installeert. Het is dan ook een bijzonder goed idee uw apparaat meteen te scannen op aanwezige bedreigingen nadat u Bitdefender hebt geïnstalleerd. En het is absoluut een goed idee om uw apparaat regelmatig te scannen op bedreigingen.

Scannen op aanvraag is gebaseerd op scantaken. Scantaken bepalen de scanopties en de objecten die moeten worden gescand. U kunt de apparaat scannen wanneer u dat wilt door de standaardtaken of uw eigen scantaken (door gebruiker gedefinieerde taken) uit te voeren. Als u specifieke locaties wilt scannen op uw apparaat of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren.

Een bestand of map scannen op bedreigingen

U moet bestanden en mappen scannen wanneer u vermoedt dat ze geïnfecteerd zijn. Klik met de rechtermuisknop op het bestand of de map die u wilt scannen, kies **Bitdefender** en selecteer **Scannen met Bitdefender**. De **Antivirusscanwizard** wordt weergegeven en begeleidt u doorheen het scanproces. Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.

Een snelle scan uitvoeren

Quick Scan gebruikt in-the-cloud scanning om bedreigingen die op uw systeem worden uitgevoerd, te detecteren. Het uitvoeren van een Snelle scan duurt doorgaans minder dan een minuut en gebruikt slechts een fractie van het systeemgeheugen dat gewone antivirusscans gebruiken.

Een snelle scan starten:

1. Klik in het navigatiemenu in de Bitdefender-interface op Bescherming.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het venster **Scans** op de **Scan uitvoeren** knop naast **Snelle scan**.
4. Volg de **Antivirusscanwizard** om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden. Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

Een systeemscan uitvoeren

De systeemscan scant de volledige apparaaten op alle types bedreigingen die de beveiliging in gevaar brengen, zoals malware, spyware, adware, rootkits en andere.

Opmerking

Omdat **Systeemscan** een grondige scan van het complete systeem uitvoert, kan de scan even duren. Het is daarom aanbevolen deze taak uit te voeren wanneer u de apparaaten niet gebruikt.

Voordat u een systeemscan uitvoert, wordt het volgende aanbevolen:

- Zorg ervoor dat Bitdefender up to date is met de informatiedatabase voor bedreigingen. Het scannen van uw apparaat met een oude informatiedatabase voor bedreigingen kan verhinderen dat Bitdefender nieuwe bedreigingen die sinds de laatste update zijn gevonden, detecteert. Zie Bitdefender up-to-date houden voor meer informatie.
- Alle open programma's afsluiten

Als u specifieke locaties wilt scannen op uw apparaat of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren. Zie Een aangepaste scan configureren (pagina 21) voor meer informatie.

Een systeemscan lanceren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het venster **Scans** op de **Scan uitvoeren** knop naast **Systeemscan**.
4. De eerste keer dat u de Systeemscan uitvoert, krijgt u een inleiding. Klik op **OK, BEGREPEN** om verder te gaan.
5. Volg de Antivirus Scan-wizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op gedetecteerde bestanden. Als er onopgeloste bedreigingen blijven, wordt u gevraagd de acties te kiezen die u daarop wilt ondernemen.

Een aangepaste scan configureren

In het venster **Scans beheren** kunt u Bitdefender zo instellen dat het scans uitvoert wanneer u denkt dat uw apparaat op mogelijke bedreigingen moet worden gecontroleerd. U kunt ervoor kiezen om een **Systeemscan** of **Snelle scan** in te plannen, of u kunt een aangepaste scan aanmaken.

Om een nieuwe aangepaste scan in detail te configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het venster **Scans** op **+Scan aanmaken**.
4. Voer in het veld **Taaknaam** een naam in voor de scan, selecteer vervolgens de locaties die u wilt laten scannen, en klik op **Volgende**.
5. Configureer deze algemene opties:
   - **Scan alleen toepassingen.** U kunt Bitdefender zo instellen dat alleen geopende apps worden gescand.
   - **Prioriteit scantaak.** U kunt kiezen welke impact een scanprocedure mag hebben op de prestaties van uw systeem.
     - Auto - De prioriteit van de scanprocedure hangt af van de systeemactiviteit. Om te verzekeren dat de scanprocedure geen invloed heeft op de systeemactiviteit, beslist Bitdefender of de scanprocedure met een hoge of lage prioriteit moet worden uitgevoerd.
     - Hoog - De prioriteit van de scanprocedure is hoog. Door deze optie te selecteren, laat u andere programma's trager werken, en verkort u de tijd die nodig is om de scanprocedure te voltooien.
     - Laag - De prioriteit van de scanprocedure is laag. Door deze optie te selecteren, laat u andere programma's sneller werken, en verlengt u de tijd die nodig is om de scanprocedure te voltooien.
   - **Acties na het scannen.** Kies welke actie Bitdefender moet ondernemen als er geen bedreigingen zijn gevonden:
     - Venster met samenvatting weergeven
     - Apparaat uitschakelen
     - Scanvenster sluiten
6. Als u de scanopties in detail wilt configureren, klikt u op **Geavanceerde opties weergeven**. U vindt informatie over de vermelde scans aan het einde van dit gedeelte.
   Klik op **Volgende**.

7. U kunt **Scantaak inplannen** indien gewenst inschakelen, en dan kiezen wanneer de aangepaste scan die u hebt gemaakt, moet beginnen.
   - ❍ Bij opstarten systeem
   - ❍ Dagelijks
   - ❍ Maandelijks
   - ❍ Wekelijks

   Kiest u Dagelijks, Maandelijks of Wekelijks, versleept u de schuifregelaar op de schaal om te kiezen wanneer de ingeplande scan moet starten.
8. Klik op **OPSLAAN** om de instellingen op te slaan en sluit het configuratievenster.
   Afhankelijk van de locaties die moeten worden gescand, kan het scannen even duren. Indien er tijdens de scanprocedure bedreigingen worden gevonden, wordt u gevraagd de acties te kiezen die in verband met de gedetecteerde bestanden moeten worden ondernomen.

Informatie over de scanopties

Misschien vindt u deze informatie nuttig:

- ❍ Als u bepaalde termen niet kent, kunt u ze opzoeken in de **woordenlijst**. U kunt ook nuttige informatie vinden door op het Internet te zoeken.
- ❍ **Scan mogelijk ongewenste applicaties.** Selecteer deze optie om te scannen op ongewenste toepassingen. Een mogelijk ongewenste applicatie (PUA) of mogelijk ongewenst programma (PUP) is software die meestal wordt meegeleverd met freeware software en die pop-ups weergeeft of een werkbalk installeert in de standaardbrowser. Sommigen van hen zullen de startpagina of de zoekmachine wijzigen, anderen zullen verschillende processen op de achtergrond uitvoeren die de pc vertragen of zullen talloze advertenties weergeven. Deze programma's kunnen zonder uw toestemming worden geïnstalleerd (ook wel adware genoemd) of worden standaard opgenomen in de kit voor snelle installatie (ondersteund door advertenties).
- ❍ **Archieven scannen.** Archieven die geïnfecteerde bestanden bevatten, zijn geen onmiddellijke dreiging voor de beveiliging van uw systeem. De dreiging kan uw systeem alleen beïnvloeden als het geïnfecteerde

bestand wordt uitgepakt uit het archief en uitgevoerd zonder dat de real time-beveiliging is ingeschakeld. Het is echter aanbevolen deze optie te gebruiken om eventuele potentiële dreigingen te detecteren en te verwijderen, zelfs als het niet om een onmiddellijke dreiging gaat. Versleep de schuifregelaar langs de schaal om archieven die groter zijn dan een bepaalde waarde in MB (Megabytes) uit te sluiten.

> **Opmerking**
> Als gearchiveerde bestanden worden gescand, duurt het scannen langer en worden er meer systeembronnen gebruikt.

- **Scan alleen nieuwe en gewijzigde bestanden.** Door alleen nieuwe en gewijzigde bestanden te scannen, kunt u de algehele reactietijd van het systeem aanzienlijk verbeteren met een minimum aan beveiliging.
- **Scan opstartsectoren.** U kunt Bitdefender instellen om de opstartsectoren van uw harde schijf te scannen. Deze sector van de harde schijf bevat de benodigde computercode om het opstartproces te starten. Wanneer een dreiging de opstartsector infecteert, kan de schijf ontoegankelijk worden en kunt u mogelijk uw systeem niet meer opstarten en geen toegang krijgen tot uw gegevens.
- **Geheugen scannen.** Selecteer deze optie om programma's te scannen die worden uitgevoerd in uw systeemgeheugen.
- **Register scannen.** Selecteer deze optie voor het scannen van registersleutels. Het Windows-register is een database die de configuratie-instellingen en opties opslaat voor de componenten van het Windows-besturingssysteem, evenals voor geïnstalleerde apps.
- **Cookies scannen.** Selecteer deze opties om de cookies te scannen die via browsers op uw computers zijn opgeslagen.
- **Keyloggers scannen.** Selecteer deze optie om uw systeem te scannen op keylogger-apps. Keyloggers registreren wat u op uw toetsenbord typt en sturen rapporten via internet naar een kwaadwillende persoon (hacker). De hacker kan uit de gestolen gegevens gevoelige informatie halen, zoals bankrekeningnummers en wachtwoorden, en daarmee persoonlijke voordelen behalen.

Antivirusscanwizard

Telkens wanneer u een scan op aanvraag start (bijvoorbeeld klik met de rechtermuisknop op een map, kies Bitdefender en selecteer **Scannen met**

Bitdefender), verschijnt de Antivirusscanwizard van Bitdefender. Volg de wizard om het scannen te voltooien.

> **Opmerking**
> Als de scanwizard niet verschijnt, kan de scan worden geconfigureerd om stil te worden uitgevoerd op de achtergrond. Zoek het pictogram voor de scanvoortgang in het **systeemvak**. U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

Stap 1 - Scan uitvoeren

BitDefender start het scannen van de geselecteerde objecten. U ziet real time-informatie over de scanstatus en statistieken (inclusief de verstreken tijd, een schatting van de resterende tijd en het aantal gedetecteerde bedreigingen).

Wacht tot BitDefender het scannen beëindigt. Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen.

De scan stoppen of pauzeren. U kunt het scannen op elk ogenblik stoppen door op **STOP** te klikken. U gaat dan rechtstreeks naar de laatste stap van de wizard. Klik op **PAUZE** om het scanproces tijdelijk te stoppen. Om het scannen te hervatten, klikt u op **HERVATTEN**.

Wachtwoordbeveiligde archieven. Wanneer een met een wachtwoord beschermd archief wordt gedetecteerd, kunt u afhankelijk van de scaninstellingen worden gevraagd het wachtwoord op te geven. Met een wachtwoord beveiligde archieven kunnen niet worden gescand, tenzij u het wachtwoord opgeeft. De volgende opties zijn beschikbaar:

- **Wachtwoord.** Als u wilt dat Bitdefender het archief scant, moet u deze optie selecteren en het wachtwoord invoeren. Als u het wachtwoord niet kent, kies dan een van de andere opties.
- **Geen wachtwoord vragen en dit object overslaan bij het scannen.** Selecteer deze optie om het scannen van dit archief over te slaan.
- **Alle wachtwoordbeveiligde items overslaan zonder ze te scannen.** Selecteer deze optie als u niet wilt worden lastig gevallen met betrekking tot wachtwoordbeveiligde archieven. Bitdefender zal ze niet kunnen scannen, maar er wordt wel een gegeven bewaard in het scanlogboek.

Kies de gewenste optie en klik op **OK** om door te gaan met scannen.

Stap 2 – Acties kiezen

Aan het einde van de scan wordt u gevraagd te kiezen welke acties moeten worden ondernemen op de gedetecteerde bestanden, als die er zijn.

> **Opmerking**
> Wanneer u een snelle scan of een systeemscan uitvoert, neemt Bitdefender automatisch de aanbevolen acties op bestanden die zijn gedetecteerd tijdens de scan. Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

De geïnfecteerde objecten worden weergegeven in groepen, die zijn gebaseerd op de bedreigingen waarmee ze zijn geïnfecteerd. Klik op de link van de bedreiging voor meer informatie over de geïnfecteerde objecten.

U kan een algemene actie selecteren die moet worden genomen voor alle groepen problemen of u kan afzonderlijke acties voor elke groep problemen selecteren. Een of meerdere van de volgende opties kunnen in het menu verschijnen.

Neem gepaste acties

Bitdefender zal de aanbevolen acties ondernemen, afhankelijk van het type gedetecteerd bestand:

- **Geïnfecteerde bestanden.** Bestanden die als geïnfecteerd zijn gedetecteerd, komen overeen met een stuk dreigingsinformatie dat is gevonden in de Bitdefender Threat Information Database. Bitdefender zal automatisch proberen de kwaadaardige code uit het geïnfecteerde bestand te verwijderen en het originele bestand te reconstrueren. Deze operatie wordt desinfectie genoemd.

  Bestanden die niet kunnen worden gedesinfecteerd, worden in quarantaine geplaatst om de infectie in te dammen. In quarantaine geplaatste bestanden kunnen niet worden uitgevoerd of geopend; daarom verdwijnt het risico om besmet te raken. Voor meer informatie, zie Bestanden in quarantaine beheren (pagina 33).

Belangrijk

Voor bepaalde soorten bedreigingen is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig kwaadaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand van de schijf verwijderd.

- **Verdachte documenten.** Bestanden worden door de heuristische analyse als verdacht gedetecteerd. Verdachte bestanden kunnen niet worden gedesinfecteerd, omdat er geen desinfectieroutine beschikbaar is. Ze worden in quarantaine geplaatst om een mogelijke infectie te voorkomen.
- **Archieven met geïnfecteerde bestanden.**
  - Archieven die alleen geïnfecteerde bestanden bevatten, worden automatisch verwijderd.
  - Als een archief zowel geïnfecteerde als schone bestanden bevat, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen op voorwaarde dat het het archief met de schone bestanden kan reconstrueren. Als archiefreconstructie niet mogelijk is, wordt u geïnformeerd dat er geen actie kan worden ondernomen om te voorkomen dat schone bestanden verloren gaan.

Verwijderen

Verwijdert gedetecteerde bestanden van de schijf.

Als er geïnfecteerde bestanden samen met schone bestanden in een archief zijn opgeslagen, zal Bitdefender proberen de geïnfecteerde bestanden te verwijderen en het archief opnieuw op te bouwen met de schone bestanden. Als het niet mogelijk is het archief te reconstrueren, wordt u op de hoogte gebracht dat er geen actie kan worden ondernomen om zo te vermijden dat schone bestanden verloren gaan.

Geen actie ondernemen

Er wordt geen actie ondernomen voor de geïnfecteerde bestanden. Als de scan is voltooid, kan u het scanlogbestand openen om informatie over deze bestanden te zien.

Klik op **Doorgaan** om de aangegeven acties toe te passen.

Stap 3 – Overzicht

Wanneer BitDefender het oplossen van de problemen heeft voltooid, verschijnen de scanresultaten in een nieuw venster. Als u uitgebreide informatie over het scanproces wenst, klikt u op **LOGBOEK WEERGEVEN** om het scanlogboek weer te geven.

> **Belangrijk**
> In de meeste gevallen desinfecteert BitDefender met succes de geïnfecteerde bestanden die het detecteert of isoleert het de infectie. Er zijn echter problemen die niet automatisch kunnen worden opgelost. Start indien nodig uw systeem opnieuw, zodat het installatieprogramma de installatie kan voltooien. Meer informatie en instructies over het handmatig verwijderen van een bedreiging vindt u onder Bedreigingen van uw systeem verwijderen (pagina 154).

Scanlogboeken controleren

Telkens wanneer er een scan wordt uitgevoerd, wordt er een scanverslag aangemaakt en Bitdefender slaat de gedetecteerde problemen op in het Antivirusvenster. Het scanlog bevat gedetailleerde informatie over het gevolgde scanproces, zoals de scanopties, het scandoel, de gevonden bedreigingen en de hierop uitgevoerde acties.

Zodra het scannen is voltooid, kunt u het scanlogboek direct vanaf de scanwizard openen door op **LOGBOEK WEERGEVEN** te klikken.

Een scanlog of een gedetecteerde infectie later bekijken:

1. Klik **Meldingen** in het navigatiemenu op de Bitdefender-interface.
2. In het tabblad **Alle** selecteert u de kennisgeving betreffende de recentste scan.
   Hier vindt u alle gebeurtenissen van scans op bedreigingen, inclusief bedreigingen die zijn gedetecteerd door Scannen bij toegang, door gebruiker gestarte scans en statuswijzigingen voor automatische scans.
3. In de kennisgevingenlijst kunt u controleren welke scans onlangs werden uitgevoerd. Klik op een kennisgeving om details erover weer te geven.
4. Klik op **Logboek weergeven** om het scanlogboek te openen.

Automatisch scannen van verwisselbare media

Bitdefender detecteert automatisch wanneer u een verwisselbaar opslagapparaat aansluit op uw apparaat en scant dit op de achtergrond wanneer de Autoscan-optie geactiveerd is. Dit is aanbevolen om infecties van uw apparaat door bedreigingen te voorkomen.

Gedetecteerde apparaten vallen in een van deze categorieën:

- Cd's/dvd's
- USB-sticks zoals flashpennen en externe harde schijven
- toegewezen (externe) netwerkstations

U kunt het automatisch scannen afzonderlijk configureren voor elke categorie opslagapparaten. Automatisch scannen van toegewezen netwerkstations is standaard uitgeschakeld.

Hoe werkt het?

Wanneer Bitdefender een verwisselbaar opslagapparaat detecteert, begint het het apparaat te scannen op bedreigingen (op voorwaarde dat de automatische scan voor dat type apparaat is ingeschakeld). U wordt via een pop-upvenster gemeld dat een nieuw apparaat is gedetecteerd en dat het wordt gescand.

Een Bitdefender-scanpictogram verschijnt in het **systeemvak**. U kunt op dit pictogram klikken om het scanvenster te openen en de scanvoortgang te bekijken.

Nadat de scan is voltooid, wordt het venster met de scanresultaten weergegeven om u te laten weten of u de bestanden op de verwisselbare media veilig kunt openen.

In de meeste gevallen verwijdert Bitdefender automatisch de gedetecteerde bedreigingen of isoleert het programma geïnfecteerde bestanden in quarantaine. Als er na de scan niet opgeloste bedreigingen zijn, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

Opmerking
Houd ermee rekening dat er geen actie kan worden ondernomen op geïnfecteerde of verdachte bestanden die op cd's/dvd's zijn gevonden. Zo kan er ook geen actie worden ondernemen op geïnfecteerde of verdachte bestanden die zijn gedetecteerd op toegewezen netwerkstations als u niet over de geschikte privileges beschikt.

Deze informatie kan nuttig zijn voor u:

- Wees voorzichtig wanneer u een cd/dvd gebruikt die besmet is met een bedreiging. De bedreiging kan niet van de schijf worden verwijderd (het medium is alleen-lezen). Zorg dat de real time-beveiliging is ingeschakeld om te verhinderen dat bedreigingen zich over uw systeem verspreiden. De beste werkwijze is het kopiëren van alle waardevolle gegevens van de schijf naar uw systeem en ze daarna verwijderen van de schijf.
- In sommige gevallen zal Bitdefender niet in staat zijn bedreigingen te verwijderen uit specifieke bestanden vanwege wettelijke of technische beperkingen. Een voorbeeld hiervan zijn bestanden die gearchiveerd zijn met een eigen technologie (dit is te wijten aan het feit dat het archief niet correct opnieuw kan worden gemaakt).
  Om te weten hoe u met bedreigingen moet omgaan, ga naar Bedreigingen van uw systeem verwijderen (pagina 154).

Scan verwisselbare media beheren

Automatische scans van verwisselbare media beheren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Selecteer het venster **Instellingen**.

De scanopties zijn vooraf geconfigureerd voor de beste detectieresultaten. Als er geïnfecteerde bestanden wordt gedetecteerd, probeert Bitdefender ze te desinfecteren (de kwaadaardige code verwijderen) of ze naar quarantaine te verplaatsen. Als beide acties mislukken, kunt u met de Antivirusscanwizard andere acties opgeven die moeten worden ondernemen op geïnfecteerde bestanden. De scanopties zijn standaard en u kunt ze niet wijzigen.

Voor de beste beveiliging is het aanbevolen om de geselecteerde optie van **Autoscan** in te schakelen voor alle types verwisselbare opslagapparaten.

Gastbestand scannen

Het gastbestand zit standaard in de installatie van uw besturingssysteem en wordt gebruik om hostnamen aan IP-adressen te koppelen, telkens wanneer u een nieuwe webpagina bezoekt, een verbinding maakt met een FTP of andere internetservers. Het is een gewoon tekstbestand en kwaadaardige programma's zouden het kunnen wijzigen. Geavanceerde gebruikers weten hoe ze het moeten gebruiken om vervelende advertenties, banners, cookies van derden of overvallers te blokkeren.

Om scan-gastbestanden te configureren:

1. Klik **Instellingen** in het navigatiemenu op de Bitdefender-interface.
2. Selecteer de **Geavanceerd** tabblad.
3. Schakel **Gastbestand scannen** in of uit.

Scanuitsluitingen configureren

Met Bitdefender kunt u specifieke bestanden, mappen of bestandsextensies uitsluiten van het scannen. Deze functie is bedoeld om te vermijden dat u in uw werk wordt gestoord en kan ook helpen de systeemprestaties te verbeteren. Uitsluitingen zijn voorzien voor gebruikers die over een gevorderde computerkennis beschikken. Als u deze kennis niet hebt, kunt u de aanbevelingen van een Bitdefender-vertegenwoordiger volgen.

U kunt de uitsluitingen configureren die u wilt toepassen op Scannen bij toegang of Scannen op aanvraag afzonderlijk, of op beide scantypes tegelijk. De objecten die zijn uitgesloten van scannen bij toegang, worden niet gescand, ongeacht of ze door u of door een toepassing worden geopend.

Opmerking

Uitzonderingen komen NIET in aanmerking voor contextueel scannen. Contextueel scannen is een type van scannen op aanvraag. Klik met de rechtermuisknop op het bestand of de map die u wilt scannen en selecteer **Scannen met BitDefender**.

Bestanden en mappen uitsluiten van het scannen

Om specifieke bestanden en mappen van het scannen uit te sluiten:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het venster **Instellingen** op **Uitzonderingen beheren**.
4. Klik op **+Een uitzondering toevoegen**.
5. Voer in het overeenkomende veld het pad in van de map die u wilt uitsluiten van het scannen.
   U kunt ook naar de map navigeren door te klikken op de knop Bladeren aan de rechterkant van de interface. Selecteer de map en klik op **OK**.
6. Schakel de schakelaar naast de beschermingsvoorziening die de map niet moet scannen, in. Er zijn drie opties:
   - Antivirus
   - Preventie van online dreigingen
   - Advanced Threat Defense
7. Klik op **Opslaan** om de wijzigingen op te slaan en het venster te sluiten.

Bestandsextensies uitsluiten van scannen

Wanneer u een bestandsextensie uitsluit van de scan, zal Bitdefender bestanden met die extensie niet meer scannen, ongeacht hun locatie op uw apparaat. De uitsluiting is ook van toepassing op bestanden op verwisselbare media, zoals cd's, dvd's, USB-opslagapparaten of netwerkstations.

> **Belangrijk**
> Ga voorzichtig te werk wanneer u extensies uitsluit van het scannen, want dergelijke uitsluitingen kunnen uw apparaat kwetsbaar maken voor bedreigingen.

Om bestandsextensies uit te sluiten van het scannen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. In de **Instellingen** venster, klik **Uitzonderingen beheren**.

4. Klik **+Voeg een uitzondering toe**.
5. Voer de extensies in die u van het scannen wilt uitsluiten met een puntje ervoor, en scheid ze van elkaar met puntkomma's (;).
   txt;avi;jpg
6. Schakel de schakelaar naast de beschermingsvoorziening die de extensie niet moet scannen, in.
7. Klik op **Opslaan**.

Scanuitsluitingen beheren

Als de geconfigureerde scanuitsluitingen niet langer nodig zijn, is het aanbevolen dat u ze verwijdert of dat u scanuitsluitingen uitschakelt.

Om scanuitsluitingen te beheren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het venster **Instellingen** op **Uitzonderingen beheren**. Er wordt een lijst met al uw uitzonderingen weergegeven.
4. Klik op een van de beschikbare knoppen om scanuitzonderingen te verwijderen of te bewerken. Ga als volgt te werk:
   - Om iets uit de lijst te verwijderen, klik op de knop ernaast.
   - Om een gegeven in de tabel te bewerken, klikt u ernaast op de knop **Bewerken**. Er verschijnt een nieuw venster. Hierin kunt u de extensie of het pad dat moet worden uitgezonderd, wijzigen, alsook de beveiligingsvoorziening die de extensie of het pad moet uitsluiten. Breng de nodige wijzigingen aan en klik daarna op **WIJZIGEN**.

Bestanden in quarantaine beheren

Bitdefender isoleert de door bedreigingen geïnfecteerde bestanden die het niet kan desinfecteren en de verdachte bestanden in een beveiligd gebied dat de quarantaine wordt genoemd. Wanneer een bedreiging in quarantaine is, kan het geen schade berokkenen, aangezien het niet kan worden uitgevoerd of gelezen.

Daarnaast scant Bitdefender de bestanden in quarantaine telkens de informatiedatabase voor bedreigingen geüpdatet wordt. Opgeruimde

bestanden worden automatisch terug naar hun originele locatie verplaatst.

De bestanden in quarantaine controleren en beheren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Ga naar het venster **Instellingen**.
   Hier ziet u de naam van de bestanden in quarantaine, alsook hun oorspronkelijke locatie en de naam van de gedetecteerde bedreigingen.
4. Bestanden in quarantaine worden automatisch beheerd door Bitdefender op basis van de standaard quarantaine-instellingen.
   Hoewel dit niet wordt aanbevolen, kunt u de quarantaine-instellingen aanpassen volgens uw voorkeur door te klikken op **Instellingen weergeven**.
   Klik op de schakelaars om deze optie in of uit te schakelen.
   Quarantaine opnieuw scannen na update van informatie over bedreigingen
   Houd deze optie ingeschakeld om bestanden in quarantaine automatisch te scannen na elke update van de informatiedatabase voor bedreigingen. Opgeruimde bestanden worden automatisch terug naar hun originele locatie verplaatst.
   Inhoud ouder dan 30 dagen verwijderen
   Bestanden in quarantaine die ouder zijn dan 30 dagen worden automatisch verwijderd.
   Maak uitzonderingen aan voor herstelde bestanden
   De bestanden die u vanuit quarantaine herstelt, worden zonder reparatie teruggezet naar hun oorspronkelijke locatie, en worden voor volgende scans automatisch uitgesloten.
5. Om een bestand in quarantaine te verwijderen, selecteert u het en klikt u op de knop **Verwijderen**. Als u een bestand uit de quarantaine wilt terugzetten naar de oorspronkelijke locatie, selecteert u het bestand en klikt u op **Terugzetten**.

1.2.2. Geavanceerde bescherming tegen bedreigingen

Bitdefender Geavanceerde dreigingscontrole is een innovatieve proactieve detectietechnologie die geavanceerde heuristische methoden gebruikt

voor het in real time detecteren van ransomware en andere nieuwe potentiële dreigingen.

Geavanceerde dreigingscontrole bewaakt voortdurend de toepassingen die op de apparaat worden uitgevoerd en zoekt naar acties die op bedreigingen lijken. Elk van deze acties krijgt een score en voor elk proces wordt een algemene score berekend.

Als veiligheidsmaatregel wordt u op de hoogte gesteld telkens er bedreigingen of mogelijk kwaadwillige processen worden gedetecteerd en geblokkeerd.

Advanced Threat Defense in- of uitschakelen

Advanced Threat Defense in- of uitschakelen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **ADVANCED THREAT DEFENSE** op **Openen**.
3. Ga naar het venster **Instellingen** en klik op de schakelaar naast **Bitdefender Advanced Threat Defense**.

> **Opmerking**
> Om uw systeem beschermd te houden tegen ransomware en andere bedreigingen, bevelen we u aan Advanced Threat Defense zo weinig mogelijk uit te schakelen.

Gedetecteerde kwaadwillige aanvallen controleren

Wanneer bedreigingen of mogelijk kwaadwillige processen worden gedetecteerd, blokkeert Bitdefender deze om uw apparaat te beschermen tegen ransomware of andere malware. U kunt de lijst met gedetecteerde kwaadwillige aanvallen op elk gewenst moment controleren aan de hand van de onderstaande stappen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **GEAVANCEERDE BEDREIGINGSVERDEDIGING** paneel, klik **Open**.
3. Ga naar het venster **Threat Defense**.
   De aanvallen die de voorbije 90 dagen werden gedetecteerd, worden getoond. Om meer informatie te lezen over de opgespoorde ransomware, de paden van het schadelijke proces en of het

onschadelijk maken met succes werd uitgevoerd, kunt u er gewoon op klikken.

Processen toevoegen aan uitzonderingen

U kunt uitzonderingsregels configureren voor vertrouwde toepassingen zodat Advanced Threat Defense ze niet blokkeert als ze acties uitvoeren die op bedreigingen lijken.

Om processen toe te voegen aan de uitsluitingenlijst van Advanced Threat Defense:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **GEAVANCEERDE BEDREIGINGSVERDEDIGING** paneel, klik **Open**.
3. In de **Instellingen** venster, klik **Uitzonderingen beheren**.
4. Klik **+Voeg een uitzondering toe**.
5. Voer het pad in van de map die u wilt uitsluiten van scannen in het overeenkomstige veld.
   U kunt ook naar het uitvoerbare bestand navigeren door te klikken op de knop Bladeren aan de rechterkant van de interface. Selecteer het bestand en klik op **OK**.
6. Schakel de schakelaar naast **Advanced Threat Defense** in.
7. Klik **Redden**.

Detectie van exploits

Een manier voor hackers om in te breken in systemen, is misbruik maken van specifieke bugs of kwetsbaarheden in computersoftware (toepassingen of plug-ins) en hardware. Om te garanderen dat uw apparaat vrij blijft van dergelijke aanvallen, die zich meestal heel snel verspreiden, maakt Bitdefender gebruik van de meest recente anti-exploittechnologieën.

Detectie van exploit in- en uitschakelen

Om detectie van exploits in en uit te schakelen:

❍ Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.

- In de **GEAVANCEERDE BEDREIGINGSVERDEDIGING** paneel, klik **Open**.
- Ga naar het venster **Instellingen** en klik op de schakelaar naast **Detectie exploits** om de voorziening in of uit te schakelen.

> **Opmerking**
> De optie Detectie van exploits is standaard ingeschakeld.

1.2.3. Preventie van online bedreigingen

Bitdefender Online Threat Prevention garandeert een veilige surfervaring door u te waarschuwen over mogelijke kwaadaardige websites.

Bitdefender biedt realtime bescherming tegen online bedreigingen voor:

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

Om de instellingen van Online Threat Prevention te configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **ONLINE THREAT PREVENTION** op **Instellingen**.

In de secties **Webbescherming** klikt u op de aan-uitschakelaars voor:

- Web attack prevention blokkeert bedreigingen die via het internet binnenkomen, met inbegrip van drive-by downloads.
- Search advisor is een component die de resultaten van uw zoekopdrachten en de koppelingen die op websites van sociale netwerken zijn geplaatst, beoordeelt door naast elk resultaat een pictogram te plaatsen.

  U mag deze webpagina niet bezoeken.

Deze webpagina kan gevaarlijke inhoud bevatten. Ga voorzichtig te werk als u beslist om deze pagina te bezoeken.

Dit is een veilige pagina om te bezoeken.

Search Advisor beoordeelt de zoekresultaten van de volgende zoekmachines op Internet:

- Google
- Yahoo!
- Bing
- Baidu

Search Advisor beoordeelt de koppelingen die zijn geplaatst op de volgende online sociale netwerkservices:

- Facebook
- Twitter

- Versleutelde webscan.
  Meer verfijnde aanvallen kunnen gebruik maken van beveiligd webverkeer om hun slachtoffers te misleiden. We raden u dan ook aan om de optie Versleutelde Webscan ingeschakeld te laten.
- Bescherming tegen fraude.
- Bescherming tegen phishing.

Scrol naar beneden tot u bij de sectie **Network Threat Prevention** komt. Hier vindt u de optie **Network Threat Prevention**. Houd deze optie ingeschakeld om uw apparaat te beschermen tegen aanvallen van complexe malware (zoals ransomware) op basis van kwetsbaarheden.

U kunt een lijst opmaken van websites, domeinen en IP-adressen die niet zullen worden gescand door de antibedreiging-, antiphishing- en antifraude-engines van Bitdefender. De lijst dient enkel de websites, domeinen en IP-adressen te bevatten die u volledig vertrouwt.

Om websites, domeinen en IP-adressen via de functie Online Threat Prevention van Bitdefender te configureren en te beheren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ONLINE BEDREIGINGSPREVENTIE** paneel, klik **Instellingen**.
3. Klik op **Uitzonderingen beheren**.

4. Klik **+Voeg een uitzondering toe**.
5. Voer in het overeenkomende veld de naam van de website of van het domein of het IP-adres in dat u wilt toevoegen aan de uitzonderingen.
6. Klik op de schakelaar naast **Online Threat Prevention**.
7. Om een item uit de lijst te verwijderen, klikt u op de knop ernaast. Klik **Redden** om de wijzigingen op te slaan en het venster te sluiten.

Bitdefender waarschuwt in de browser

Telkens wanneer u een website bezoekt die als onveilig is geclassificeerd, wordt de website geblokkeerd en wordt een waarschuwingspagina weergegeven in uw browser.

De pagina bevat informatie, zoals de URL van de website en de gedetecteerde bedreiging.

U moet beslissen wat u vervolgens wilt doen. De volgende opties zijn beschikbaar:

- Verlaat de website door te klikken op **BRENG ME TERUG NAAR EEN VEILIGE LOCATIE**.
- Ga ondanks de waarschuwing door met uw bezoek aan de website, door te klikken op **Ik begrijp de risico's; breng me toch naar de webpagina**.
- Als u zeker bent dat de gedetecteerde website veilig is, klikt u op **INDIENEN** om deze toe te voegen aan de uitzonderingen. We raden aan dat u enkel websites toevoegt die u volledig vertrouwt.

1.2.4. E-mailbescherming

Uw e-mail is een belangrijk onderdeel van uw digitale leven, en gezien de vele toepassingen in het echte leven, is het een favoriete aanvalsvector geworden voor kwaadwillenden en een van de belangrijkste cyberveiligheidsproblemen van de dagelijkse gebruiker.

E-mailbescherming is een beveiligingsfunctie waarmee u potentieel gevaarlijke inhoud in e-mails die u in uw inbox ontvangt, kunt scannen en identificeren. Deze functie is een pakket van verschillende technologieën die onder dezelfde beveiligingsmodule zijn samengebracht, zoals antiphishing-, antimalware-, antispam-, antifraude- en anti-scamsoftware.

Door een directe verbinding tot stand te brengen tussen Bitdefender en uw e-mailserviceprovider, staat u toe dat de antivirus uw e-mails rechtstreeks scant en elimineert u de beperkingen die ontstaan door het gebruik van verschillende apparaten of e-mailclients.

> **Opmerking**
> U kunt maximaal 5 verschillende e-mailaccounts beveiligen.

Uw account configureren

Deze functie is naadloos geïntegreerd in de gebruikersinterface. E-mailbescherming gebruiken:

1. Onder **Bescherming**, Klik **Open** in de **E-mailbescherming** kaart.
2. Kies uw e-mailprovider voor het e-mailaccount dat u wilt beschermen.

   > **Opmerking**
   > E-mailbescherming is momenteel beschikbaar voor Google-accounts, Outlook-accounts en binnenkort ook beschikbaar voor Yahoo Mail.

3. Klik op de **Aanmelden** knop.
   De bewerking wordt vervolgens voortgezet in uw browser.
4. Voer uw e-mailadres in en klik op de **Volgende** knop
5. Om verder te gaan, voert u uw wachtwoord in en klikt u op de **Volgende** knop.
6. Controleer de gevraagde toestemmingen op het scherm en laat Bitdefender uw e-mailaccount beschermen.

Uw e-mailaccount is nu beveiligd en al uw nieuwe inkomende e-mails worden gescand op bedreigingen.

> **Opmerking**
> Elke gescande e-mail wordt gemarkeerd met een label om het veiligheidsniveau aan te geven.

Dashboard

Het dashboard toont uw beveiligde e-mails, waaronder:

- configuratiedatum (de datum waarop het account is ingesteld voor E-mailbescherming)
- status (actief of inactief)
- aantal gefilterde e-mails in de afgelopen 30 dagen.
  Hier ziet u een grafiek met het aantal ontvangen veilige e-mails en gevaarlijke e-mails.

Om meerdere e-mailaccounts toe te voegen Klik op de **Voeg nog een account toe** en doorloop voor elk ervan het bovenstaande configuratieproces.

Om het scannen te onderbreken of een account te verwijderen vanuit deze functie klikt u op de drie stippen naast het betreffende account en klikt u op **Beheer account**.

1.2.5. Antispam

Spam is een term die wordt gebruikt voor het beschrijven van ongewenste e-mail. Spam is een groeiend probleem voor zowel individuele gebruikers als bedrijven. Het is niet mooi, u wilt niet dat uw kinderen het zien, u kunt erdoor ontslagen worden (omdat u teveel tijd verspilt of omdat u porno ontvangt op zakelijke e-mailadres) en u kunt niet verhinderen dat men u deze berichten blijft zenden. De op één na beste oplossing ligt dus voor de hand: de ontvangst van dergelijke berichten blokkeren. Jammer genoeg komen spamberichten voor in allerlei vormen en formaten en op zeer grote schaal.

BitDefender Antispam gebruikt opmerkelijke technologische innovaties en industriestandaard antispamfilters om spam op te sporen voordat deze het Postvak IN van de gebruiker bereikt. Zie Antispam-begrippen (pagina 42) voor meer informatie.

De Antispambeveiliging van Bitdefender is alleen beschikbaar voor e-mailclients die zijn geconfigureerd om e-mailberichten te ontvangen via het POP3-protocol. POP3 is een van de meest gebruikte protocollen voor het downloaden van e-mailberichten van een mailserver.

> **Opmerking**
> Bitdefender biedt geen antispambeveiliging voor e-mailaccounts die u aanspreekt via een e-mailservice op Internet.

De door Bitdefender gedetecteerde spamberichten worden gemarkeerd met het voorvoegsel [spam] in de onderwerpregel. Bitdefender verplaatst spamberichten automatisch naar een specifieke map:

- In Microsoft Outlook worden spamberichten verplaatst naar een map **Spam** die zich in de map **Verwijderde items** bevindt. Er wordt een **Spam**-map aangemaakt wanneer een e-mailbericht als spam wordt aangemerkt.
- In Mozilla Thunderbird worden spamberichten verplaatst naar een map **Spam** die zich in de map **Prullenbak** bevindt. Er wordt een **Spam**-map aangemaakt wanneer een e-mailbericht als spam wordt aangemerkt.

Als u andere e-mailclients gebruikt, moet u een regel maken om de e-mailberichten die door Bitdefender zijn gemarkeerd als [{1}spam{2}] te verplaatsen naar een aangepaste quarantainemap. Als de mappen Verwijderde items of Prullenbak worden verwijderd, wordt de map Spam ook verwijderd. Er wordt echter een nieuwe map Spam gemaakt zodra een e-mail als spam wordt bestempeld.

Antispam-begrippen

De antispamfunctie heeft de volgende functies en instellingen:

Antispam-filters

De Antispam-engine van Bitdefender omvat cloud-beveiliging en andere, verschillende filters die ervoor zorgen dat uw postvak spamvrij blijft, zoals **Vriendenlijst**, **Spammerslijst** en **Charsetfilter**.

Vriendenlijst / Spammerslijst

De meeste mensen communiceren regelmatig met een groep mensen of ontvangen zelfs berichten van bedrijven of organisaties op hetzelfde domein. Wanneer u gebruik maakt van **vrienden- of spammerslijsten**, kunt u gemakkelijk een indeling maken van de mensen van wie u e-mails wilt ontvangen, ongeacht de inhoud (vrienden), of van de mensen van wie u nooit meer wilt horen (spammers).

Opmerking

Wij raden u aan de namen en e-mailadressen van uw vrienden toe te voegen aan de **Vriendenlijst**. BitDefender blokkeert geen berichten van de namen in de lijst. Door het toevoegen van vrienden bent u zeker dat rechtmatige berichten worden doorgelaten.

Tekensetfilter

Heel wat spamberichten zijn geschreven in Cyrillische en/of Aziatische tekensets. Het tekensetfilter detecteert dit type berichten en labelt ze als SPAM.

Antispamgebruik

De BitDefender Antispam-engine gebruikt alle antispamfilters samen om vast te stellen of een bepaald e-mailbericht in uw **Postvak IN** moet belanden of niet.

Elke e-mail die van het internet komt, wordt eerst gecontroleerd met de **Vriendenlijst**/**Spammerslijst** filter. Als het adres van de afzender in de **Vriendenlijst** wordt gevonden, wordt de e-mail rechtstreeks naar uw **Postvak IN** verplaatst.

In het andere geval zal de filter **Spammerslijst** de e-mail overnemen om het adres van de afzender te controleren in zijn lijst. Als er een treffer wordt gevonden, wordt de e-mail gelabeld als SPAM en naar de map **Spam** verplaatst.

Anders zal de **Tekensetfilter** controleren of de e-mail in Cyrillische of Aziatische tekens is geschreven. Als dat het geval is, wordt de e-mail gelabeld als SPAM en verplaatst naar de map **Spam**.

Opmerking

Als de e-mail het label SEXUALLY EXPLICIT vermeldt in de onderwerpregel, zal Bitdefender dit bericht als SPAM beschouwen.

Ondersteunde e-mailclients en protocollen

Antispam bescherming is aanwezig voor alle POP3/SMTP e-mailclients. De BitDefender Antispam werkbalk is echter alleen geïntegreerd in:

- Microsoft Outlook 2007 / 2010 / 2013 / 2016 / 2019
- Mozilla Thunderbird 14 en hogere versies

De antispambeveiliging in- of uitschakelen

Antispambeveiliging is standaard ingeschakeld.

De Antispam-functie in of uit te schakelen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Schakel de schakelaar in het venster **ANTISPAM** in of uit.

De antispam-werkbalk in het venster van uw e-mailclient gebruiken

In het bovenste gebied van het venster van de e-mailclient ziet u de werkbalk Antispam. De werkbalk Antispam helpt u de antispambeveiliging direct vanaf uw e-mailclient te beheren. U kunt BitDefender gemakkelijk corrigeren als het programma een rechtmatig bericht als SPAM heeft gemarkeerd.

> **Belangrijk**
> BitDefender wordt geïntegreerd in de vaakst gebruikte e-mailclients via een gemakkelijk te gebruiken antispamwerkbalk. Raadpleeg Ondersteunde e-mailclients en protocollen (pagina 43) voor een complete lijst van ondersteunde e-mailclients.

Elke knop van de BitDefender-werkbalk wordt hieronder uitgelegd.

Instellingen - opent een venster waarin u de antispamfilters en de werkbalkinstellingen kunt configureren.

Is Spam - geeft aan dat de geselecteerde e-mail spam is. De e-mail wordt onmiddellijk verplaatst naar de map **Spam**. Als de antispamclouddiensten geactiveerd zijn, wordt het bericht naar Bitdefender Cloud gestuurd voor verdere analyse.

Geen Spam - geeft aan dat de geselecteerde e-mail geen spam is en Bitdefender deze niet had moeten labelen. De e-mail wordt verplaatst van de map **Spam** naar de directory **Postvak IN**. Als de antispamclouddiensten geactiveerd zijn, wordt het bericht naar Bitdefender Cloud gestuurd voor verdere analyse.

> **Belangrijk**
> De knop **Geen spam** wordt actief wanneer u een bericht selecteert dat door Bitdefender als SPAM is gemarkeerd (normaal bevinden deze berichten zich in de map **Spam**).

Spammer toevoegen - voegt de afzender van de geselecteerde e-mail toe aan de lijst met spammers. Mogelijk moet u op **OK** klikken om te bevestigen. De e-mailberichten die worden ontvangen van adressen in de Spammerslijst worden automatisch gemarkeerd als [spam].

Vriend toevoegen - voegt de afzender van de geselecteerde e-mail toe aan de vriendenlijst. Mogelijk moet u op **OK** klikken om te bevestigen. U zult altijd e-mailberichten van dit adres ontvangen, ongeacht de inhoud ervan.

Spammers - opent de lijst **Spammers** die alle e-mailadressen bevat waarvan u geen berichten wilt ontvangen, ongeacht hun inhoud. Zie Spammerslijst configureren (pagina 48) voor meer informatie.

Vrienden - opent de **Vriendenlijst** die alle e-mailadressen bevat waarvan u altijd e-mailberichten wilt ontvangen, ongeacht hun inhoud. Zie De Vriendenlijst configureren (pagina 46) voor meer informatie.

Detectiefouten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u de antispamfilter gemakkelijk corrigeren (door aan te geven welke e-mailberichten niet als [spam] aangemerkt moeten worden). Hierdoor helpt u de efficiëntie van de antispamfilter te verbeteren. Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map met ongewenste e-mails waar uw spamberichten zijn geplaatst.
3. Selecteer het rechtmatige bericht dat door Bitdefender verkeerdelijk is gemarkeerd als [spam]].
4. Klik op de knop **Vriend toevoegen** op de antispamwerkbalk van Bitdefender om de afzender van de geselecteerde e-mail toe aan de vriendenlijst. Mogelijk moet u op **OK** klikken om te bevestigen. U zult altijd e-mailberichten van dit adres ontvangen, ongeacht de inhoud ervan.
5. Klik op de knop **Geen spam** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Het e-mailbericht wordt verplaatst naar de map Postvak IN.

Niet-gedetecteerde spamberichten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u gemakkelijk aanduiden welke e-mailberichten niet als spam moeten worden gedetecteerd. Hierdoor helpt u de efficiëntie van de antispamfilter te verbeteren. Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map Postvak IN.
3. Selecteer de niet-gedetecteerde spamberichten.
4. Klik op de knop **Is spam** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Ze worden onmiddellijk als [spam] gemarkeerd en naar de map met ongewenste e-mail verplaatst.

Werkbalkinstellingen configureren

Om de instellingen van de antispamwerkbalk voor uw e-mailclient te configureren, klikt u op de knop **Instellingen** op de werkbalk en vervolgens op het tabblad **Instellingen werkbalk**.

U hebt hier de volgende opties:

- **Markeer e-mailberichten met spam als 'gelezen'** - markeert spamberichten automatisch als gelezen, zodat u er niet door wordt gestoord als ze aankomen.
- U kunt kiezen of u al dan niet bevestigingsvensters wilt weergeven wanneer u op de knoppen **Spammer toevoegen** en **Vriend toevoegen** klikt op de antispamwerkbalk.
  Bevestigingsvensters kunnen verhinderen dat u e-mailafzenders per ongeluk toevoegt aan een Vrienden-/Spammerslijst.

De Vriendenlijst configureren

De **Vriendenlijst** is een lijst van alle e-mailadressen waarvan u altijd berichten wilt ontvangen, ongeacht hun inhoud. Berichten van uw vrienden worden niet als spam gelabeld, zelfs niet wanneer de inhoud op spam lijkt.

Opmerking
Elke e-mail die afkomstig is van een adres in de **Vriendenlijst**, wordt automatisch en zonder verdere verwerking in uw Postvak IN geleverd.

De Vriendenlijst configureren en beheren:

- Als u Microsoft Outlook of Thunderbird gebruikt, klik dan op de knop Vrienden op de **Bitdefender antispamwerkbalk**.
- U kunt ook:
  1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
  2. Klik in het deelvenster **ANTISPAM** op **Instellingen**.
  3. Ga naar het venster **Vrienden beheren**.

Om een e-mailadres toe te voegen, selecteert u de optie **E-mailadres**, voert u het adres in en klikt u vervolgens op **TOEVOEGEN**. Syntax: name@domain.com.

Om alle e-mailadressen van een specifiek domein toe te voegen, selecteert u de optie **Domeinnaam**, voert u de domeinnaam in en klikt u op **TOEVOEGEN**. Syntax:

- @domain.com en domain.com - alle ontvangen e-mailberichten van domain.com komen in uw **Postvak IN** terecht, ongeacht hun inhoud;
- domein - alle ontvangen e-mailberichten van domein (ongeacht de domeinachtervoegsels) worden als SPAM gelabeld;
- com - alle ontvangen e-mailberichten met het domeinachtervoegsel com worden als SPAM gelabeld;

Het is aanbevolen het toevoegen van volledige domeinen toe te vermijden, maar in sommige situaties kan dit nuttig zijn. U kunt bijvoorbeeld het e-maildomein toevoegen van het bedrijf waarvoor u werkt of de domeinen van uw vertrouwde partners toevoegen.

Om een item uit de lijst te verwijderen, klik je op de overeenkomstige knop ernaast. Om alle items uit de lijst te verwijderen, klikt u op **Lijst wissen**.

U kunt de vriendenlijst opslaan naar een bestand zodat u het kunt gebruiken op een andere apparaat of na het opnieuw installeren van het product. Om de vriendenlijst op te slaan, klikt u op de knop Opslaan en slaat u het op naar de gewenste locatie. Het bestand zal de extensie .bwl hebben.

Om een eerder opgeslagen Vriendenlijst te laden, klikt u op **LADEN** en opent u het overeenkomende .bwl-bestand. Om de inhoud van de bestaande lijst te resetten wanneer u een eerder opgeslagen lijst laadt, vinkt u het vakje naast **Huidige lijst overschrijven** aan.

Spammerslijst configureren

De **Spammerslijst** is een lijst van alle e-mailadressen waarvan u geen berichten wilt ontvangen, ongeacht hun inhoud. Alle e-mailberichten die worden ontvangen van een adres van de **Spammerslijst**, worden automatisch en zonder verdere verwerking als SPAM gelabeld.

De Spammerslijst configureren en beheren:

- Als u Microsoft Outlook of Thunderbird gebruikt, klik dan op de knop **Spammers** op de **Bitdefender antispamwerkbalk** geïntegreerd in uw mailclient.
- Alternatief:
  1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
  2. In de **ANTI SPAM** paneel, klik **Instellingen**.
  3. Ga naar het venster **Spammers beheren**.

Om een e-mailadres toe te voegen, selecteert u de **E-mailadres** voert u het adres in en klikt u op **TOEVOEGEN**. Syntaxis: naam@domein.com.

Om alle e-mailadressen van een specifiek domein toe te voegen, selecteert u de **Domeinnaam** optie, voer de domeinnaam in en klik op **TOEVOEGEN**. Syntaxis:

- @domain.comand domain.com - alle ontvangen e-mailberichten van domain.com komen in uw **Postvak IN** terecht, ongeacht hun inhoud;
- domein - alle ontvangen e-mailberichten van het domein (ongeacht de domeinachtervoegsels) worden gemarkeerd als SPAM;
- com - alle ontvangen e-mailberichten met het domeinachtervoegsel com worden als SPAM gelabeld.

Het is aanbevolen het toevoegen van volledige domeinen toe te vermijden, maar in sommige situaties kan dit nuttig zijn.

Waarschuwing

Voeg geen domeinen van legitieme webgebaseerde e-maildiensten (zoals Yahoo, Gmail, Hotmail of andere) toe aan de lijst met spammers. Anders zullen de e-mailberichten die worden ontvangen van een geregistreerde gebruiker van een dergelijke dienst als spam worden gedetecteerd. Als u bijvoorbeeld **yahoo.com** toevoegt aan de lijst Spammers, zullen alle e-mailberichten afkomstig van **yahoo.com** adressen worden gemarkeerd als [spam].

Om een item uit de lijst te verwijderen, klikt u op het overeenkomstige knop ernaast. Klik op om alle vermeldingen uit de lijst te verwijderen **Duidelijke lijst**.

U kunt de vriendenlijst opslaan naar een bestand zodat u het kunt gebruiken op een andere apparaat of na het opnieuw installeren van het product. Om de spammerslijst op te slaan, klikt u op de knop **Opslaan** en slaat u het op naar de gewenste locatie. Het bestand zal de extensie .bwl hebben.

Om een eerder opgeslagen Spammerslijst te laden, klikt u op **LADEN** en opent u het overeenkomende .bwl-bestand. Om de inhoud van de huidige lijst opnieuw in te stellen wanneer u een eerder opgeslagen lijst laadt, selecteert u Huidige lijst overschrijven.

De lokale antispamfilters configureren

Zoals beschreven in Antispam-begrippen (pagina 42), gebruikt Bitdefender een combinatie van verschillende antispamfilters voor het identificeren van spam. De antispamfilters zijn vooraf geconfigureerde voor een efficiënte bescherming.

Belangrijk

Afhankelijk van het feit of rechtmatige e-mails ontvangt in Aziatische of Cyrillische tekens, kunt u de instelling die dergelijke e-mails blokkeert, in- of uitschakelen. De overeenkomende instelling is uitgeschakeld in de gelokaliseerde versies van het programma die dergelijke tekensets gebruiken (bijvoorbeeld in de Russische of Chinese versie).

De lokale antispamfilters configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTI SPAM** paneel, klik **Instellingen**.

3. Ga naar het venster **Instellingen** en klik op de overeenkomstige aan-uitschakelaars.

Als u Microsoft Outlook of Thunderbird gebruikt, kunt u de lokale antispamfilters rechtstreeks vanuit uw e-mailclient configureren. Klik op de knop ⚙ **Instellingen** op de Bitdefender-antispamwerkbalk (normaal gesproken in het bovenste deel van het venster van de mailclient), en vervolgens op het tabblad **Antispamfilters**.

De cloudinstellingen configureren

"In-the cloud"-detectie maakt gebruik van de Bitdefender Cloud-services om u efficiënte antispambeveiliging te bieden die altijd up-to-date is.

De cloudbeveiliging werkt zolang Bitdefender Antispam is ingeschakeld.

Voorbeelden van rechtmatige e-mails of spam-e-mails kunnen worden verzonden naar Bitdefender Cloud wanneer u detectiefouten of niet-gedetecteerde spam-e-mails aanduidt. Hiermee kan de antispam-detectie van Bitdefender worden verbeterd.

Configureer het verzenden van e-mailvoorbeelden naar Bitdefender Cloud door de gewenste opties te selecteren door deze stappen te volgen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTI SPAM** paneel, klik **Instellingen**.
3. Ga naar de **Instellingen** venster en klik op de overeenkomstige schakelaars voor in- of uitschakelen.

Als u Microsoft Outlook of Thunderbird gebruikt, kunt u de lokale clouddetectie rechtstreeks vanuit uw e-mailclient configureren. Klik op de knop ⚙ **Instellingen** op de Bitdefender-antispamwerkbalk (normaal gesproken in het bovenste deel van het venster van de mailclient), en vervolgens op het tabblad **Cloudinstellingen**.

1.2.6. Firewall

De Firewall beschermt uw apparaat tegen inkomende en uitgaande onrechtmatige verbindingspogingen, zowel op lokale netwerken als op internet. Dit kan worden vergeleken met een wachter bij uw poort – de toepassing traceert verbindingspogingen en beslist welke moeten worden toegestaan en welke moeten worden geblokkeerd.

De Bitdefender-firewall gebruikt een reeks regels om gegevens te filteren die naar en van uw systeem zijn overgedragen.

In normale omstandigheden maakt Bitdefender automatisch een regel wanneer een toepassing toegang probeert te krijgen via internet. U kunt regels voor toepassingen ook handmatig toevoegen of bewerken.

Als veiligheidsmaatregel wordt u op de hoogte gebracht telkens wanneer voor een mogelijke kwaadaardige toepassing de toegang tot het internet geblokkeerd wordt.

Bitdefender wijst automatisch een netwerktype toe aan elke netwerkverbinding die het detecteert. Afhankelijk van het netwerktype is de firewall-beveiliging ingesteld op het geschikte niveau voor elke aansluiting.

Meer informatie over de firewall-instellingen voor elk netwerktype en de manier waarop u de netwerkinstellingen kunt bewerken, vindt u onder Verbindingsinstellingen beheren (pagina 54).

De firewall-beveiliging in- of uitschakelen

Firewallbescherming in- of uitschakelen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Schakel in het venster **FIREWALL** de schakelaar in of uit.

Waarschuwing

Omdat het uw apparaat blootstelt voor onbevoegde verbindingen, mag het uitschakelen van de firewall slechts een tijdelijke maatregel zijn. Schakel de firewall zo snel mogelijk opnieuw in.

Toepassingsregels toevoegen

De firewallregels beheren die de toegang bepalen van de toepassingen tot netwerkbronnen en het internet.

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **FIREWALL** op **Instellingen**.
3. Ga naar het venster **Toegang toepassingen**.

U kunt de laatste programma's (processen) zien die door Bitdefender Firewall en het internetnetwerk waarmee u verbonden bent, zijn gepasseerd. Om de regels te zien die voor een specifieke app

zijn gemaakt, klikt u er gewoon op en vervolgens op de koppeling **Toepassingsregels bekijken**. Het venster **Regels** wordt geopend.

Voor elke regel wordt de volgende informatie weergegeven:

- **NETWERK** - het proces en de netwerkadaptertypes (thuis / kantoor, openbaar of alle) waar de regel op van toepassing is. Regels zijn automatisch gecreëerd voor het filteren van netwerk- of internettoegang via elke adapter. Standaard zijn de regels van toepassing op elk netwerk. U kan handmatig regels creëren of bewerken voor het filteren van de netwerk- of internettoegang van een applicatie via een specifieke adapter (bijvoorbeeld een draadloze netwerkadapter)
- **PROTOCOL** - het IP-protocol waarvoor de regel geldt. Standaard zijn de regels van toepassing op willekeurig welk protocol.
- **VERKEER** - de regel is in beide richtingen van toepassing. Inkomend en uitgaand.
- **POORTEN** - het poortprotocol waarvoor de regel geldt. Standaard zijn de regels op alle poorten van toepassing.
- **IP** - het internetprotocol (IP) waarvoor de regel geldt. Standaard zijn de regels van toepassing op elk IP-adres.
- **TOEGANG** - of de toepassing al dan niet netwerk- of internettoegang krijgt onder de opgegeven omstandigheden.

Om de regels voor de geselecteerde app te bewerken of te verwijderen, klikt u op het pictogram ⋯.

- **Regel bewerken** - opent een venster waarin u de huidige regel kunt bewerken.
- **Regel verwijderen** - u kunt ervoor kiezen de huidige reeks regels voor de geselecteerde app te verwijderen.

Toepassingsregels toevoegen

Om een toepassingsregel toe te voegen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **FIREWALL** paneel, klik **Instellingen**.
3. Klik in het venster **Regels** op **Regel toevoegen**.

Hier kunt u de volgende wijzigingen toepassen:

- **Pas deze regel toe op alle toepassingen.** Schakel deze schakelaar in om de gemaakte regel op alle apps toe te passen.
- **Programmapad.** Klik op **BROWSEN** en selecteer de app waarop de regel van toepassing is.
- **Machtiging.** Selecteer een van de beschikbare machtigingen:

Machtiging	Beschrijving
Toestaan	De opgegeven toepassing zal netwerk-/internettoegang krijgen onder de opgegeven omstandigheden.
Weigeren	De opgegeven toepassing zal geen netwerk-/internettoegang krijgen onder de opgegeven omstandigheden.

- **Netwerktype**. Selecteer het type netwerk waarop de regel van toepassing is. U kunt het type wijzigen door het keuzemenu **Netwerktype** te openen en een van de beschikbare types uit de lijst te selecteren.

Netwerktype	Beschrijving
Eender welk netwerk	Alle verkeer tussen uw apparaat en andere apparaaten, ongeacht het netwerktype toestaan.
Thuis/Kantoor	Sta al het verkeer toe tussen uw apparaat en andere apparaten in het lokale netwerk.
Openbaar	Alle verkeer blokkeren is uitgeschakeld.

- **Protocol.** Selecteer uit het menu het IP-protocol waarop de regel van toepassing is.
  - Als u een regel voor alle protocollen wilt laten gelden, schakelt u het selectievakje **Alle** in.
  - Als u wilt dat de regel van toepassing is op TCP, selecteert u **TCP**.
  - Als u wilt dat de regel van toepassing is op UDP, selecteert u **UDP**.
  - Als u wilt dat de regel van toepassing is op ICMP, selecteert u **ICMP**.
  - Als u wilt dat de regel van toepassing is op IGMP, selecteert u **IGMP**.
  - Als u wilt dat de regel van toepassing is op GRE, selecteert u **GRE**.

- Indien u wilt dat de regel van toepassing is op een specifiek protocol, typt u het nummer dat aan het protocol dat u wilt filteren in het lege bewerkveld.

> **Opmerking**
> IP-protocolnummers worden toegewezen door de Internet Assigned Numbers Authority (IANA). De volledige lijst van toegewezen IP-protocolnummers is te vinden op http://www.iana.org/assignments/protocol-numbers.

- **Richting.** Selecteer in het menu de verkeersrichting waarvoor de regel geldt.

Richting	Beschrijving
Uitgaand	De regel zal alleen voor uitgaand verkeer worden toegepast.
Inkomend	De regel zal alleen voor inkomend verkeer worden toegepast.
Beide	De regel zal in beide richtingen worden toegepast.

Klik in het onderste gedeelte van het venster op de knop **Geavanceerde instellingen** om de volgende instellingen aan te passen:

- **Aangepast Lokaal Adres.** Specificeer het lokale IP-adres en de poort waarop de regel van toepassing is.
- **Aangepast Extern Adres.** Specificeer het externe IP-adres en de poort waarop de regel van toepassing is.

Om de huidige reeks regels te verwijderen en de standaardregels terug te stellen, klikt u up **Regels resetten** in het venster **Regels**.

Verbindingsinstellingen beheren

Ongeacht of u een verbinding maakt met het internet via Wi-Fi of een Ethernet-adapter, kunt u bepalen welke instellingen van toepassing moeten zijn om veilig te navigeren. De opties waar u uit kunt kiezen, zijn:

- **Dynamisch** – het netwerktype zal automatisch ingesteld worden op basis van het profiel van het verbonden netwerk, Thuis/kantoor of Openbaar. Wanneer dit gebeurt, zullen enkel Firewall-regels voor het specifieke netwerktype of deze die gedefinieerd zijn om op alle netwerktypes te gelden, van toepassing zijn.

- **Thuis / Kantoor** – het netwerktype zal altijd Thuis / Kantoor zijn, ongeacht het profiel van het verbonden netwerk. Wanneer dit gebeurt, zullen enkel Firewall-regels voor Thuis / Kantoor of deze die gedefinieerd zijn om op alle netwerktypes te gelden, van toepassing zijn.
- **Openbaar** – het netwerktype zal altijd Openbaar zijn, ongeacht het profiel van het verbonden netwerk. Wanneer dit gebeurt, zullen enkel Firewall-regels voor Openbaar of deze die gedefinieerd zijn om op alle netwerktypes te gelden, van toepassing zijn.

Om uw netwerkadapters te configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **FIREWALL** paneel, klik **Instellingen**.
3. Selecteer het venster **Netwerkadapters**.
4. Selecteer de instellingen die u volgens u van toepassing moeten zijn wanneer u aansluit op de volgende adapters:
   - Wi-Fi
   - Ethernet

Geavanceerde instellingen configureren

Geavanceerde firewall-instellingen configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **FIREWALL** paneel, klik **Instellingen**.
3. Selecteer de **Instellingen** raam.

De volgende functies kunnen geconfigureerd worden:

- **Poortscanbescherming** - detecteert en blokkeert pogingen om uit te vinden welke poorten open zijn.
  Poortscans worden vaak door hackers gebruikt om geopende poorten op uw apparaat te vinden. Als zij een minder veilige of kwetsbare poort vinden kunnen zij inbreken in uw apparaat.
- **Waarschuwingsmodus** - waarschuwingen worden getoond telkens wanneer een app verbinding probeert te maken met het internet. Selecteer **Toestaan** of **Blokkeren**. Als de Waarschuwingsmodus ingeschakeld is, wordt de functie **Profielen** automatisch uitgeschakeld.

De waarschuwingsmodus kan gelijktijdig gebruikt worden met de **Batterijmodus**.

- **Toegang tot domeinnetwerk toestaan** - sta toegang tot hulpbronnen en gedeelde bestanden, gedefinieerd door uw domeincontrollers, toe of blokkeer deze toegang.
- **Stealth-modus** - hiermee kunt u instellen of u door andere apparaten kunt worden gedetecteerd. Klik op **Stealth-instellingen bewerken** om te kiezen wanneer uw apparaat wel of niet zichtbaar moet zijn voor andere apparaten.
- **Standaardgedrag toepassing** - toestaan dat Bitdefender automatische instellingen toepast op toepassingen waarvoor geen regels gedefinieerd zijn. Klik op **Standaardregels configureren** om te kiezen of automatische instellingen moeten worden toegepast of niet.
  - Automatisch - toegang tot toepassingen zal toegestaan of geweigerd worden op basis van de automatische Firewall- en gebruikersregels.
  - Toestaan - toepassingen waarvoor geen Firewall-regel gedefinieerd werd, zullen automatisch toestemming krijgen.
  - Blokkeren - toepassingen waarvoor geen Firewall-regel gedefinieerd werd, zullen automatisch geblokkeerd worden.

1.2.7. Kwetsbaarheid

Een belangrijke stap bij het beschermen van uw apparaat tegen kwaadwillende acties en applicaties is het up-to-date houden van het besturingssysteem en van de applicaties die u regelmatig gebruikt. Bovendien: om ongeoorloofde fysieke toegang tot uw apparaat te voorkomen, moeten sterke wachtwoorden (wachtwoorden die niet makkelijk kunnen geraden worden) geconfigureerd worden voor elke Windows-gebruikersaccount en voor de Wi-Fi-netwerken waarmee u een verbinding maakt.

Bitdefender biedt twee eenvoudige manieren om de kwetsbaarheden van uw systeem op te lossen:

- U kunt uw systeem scannen op kwetsbaarheden en ze stapsgewijs repareren met de optie **Kwetsbaarheidscan**.

- Met de automatische kwetsbaarheidsbewaking kunt u de gedetecteerde kwetsbaarheden controleren en oplossen in het venster **Kennisgevingen**.

Het is aanbevolen de systeemkwetsbaarheden om de week of twee weken te controleren en op te lossen.

Uw systeem scannen op kwetsbaarheden

Om kwetsbaarheden in het systeem te detecteren, vereist Bitdefender een actieve internetverbinding.

Om uw systeem op kwetsbaarheden te scannen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **KWETSBAARHEID** op **Openen**.
3. Klik in het tabblad **Kwetsbaarheidsscan** op **Scan starten** en wacht tot Bitdefender uw systeem controleert op kwetsbaarheden. De gedetecteerde kwetsbaarheden worden gegroepeerd in drie categorieën:

   - **BESTURINGSSYSTEEM**

     - **Beveiliging van het besturingssysteem**
       Gewijzigde systeeminstellingen die uw apparaat en gegevens zouden kunnen aantasten, zoals het niet weergeven van waarschuwingen wanneer uitgevoerde bestanden zonder uw toestemming wijzigingen uitvoeren op uw systeem, of wanneer MTP-apparaten zoals telefoons of camera's verbinding maken en verschillende bewerkingen uitvoeren zonder uw medeweten.

     - **Kritieke Windows updates**
       Er wordt een lijst weergegeven met kritieke Windows-updates die niet geïnstalleerd zijn op uw computer. Het is mogelijk dat u het systeem opnieuw moet opstarten, zodat Bitdefender de installatie kan voltooien. Het kan even duren voordat de updates geïnstalleerd zijn.

     - **Zwakke Windows-accounts**
       U ziet de lijst van Windows gebruikersaccounts die zijn geconfigureerd op uw apparaat en de beschermingsniveaus van de wachtwoorden. U kunt kiezen om de gebruiker te vragen het wachtwoord te wijzigen bij de volgende aanmelding of u kunt het wachtwoord zelf onmiddellijk wijzigen. Om een

nieuw wachtwoord in te stellen voor uw systeem, selecteert u **Wachtwoord nu wijzigen**.

Om een sterk wachtwoord te maken, raden we aan dat u een combinatie gebruikt van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, $ of @).

- **TOEPASSINGEN**
  - **Browserbeveiliging**

    Wijziging in de instellingen van uw apparaat, waardoor bestanden en programma's die zijn gedownload via Internet Explorer zonder integriteitsvalidering kunnen worden uitgevoerd. Dit kan ervoor zorgen dat uw apparaat wordt aangetast.
  - **Toepassingsupdates**

    Om informatie te zien over de toepassing die moet worden bijgewerkt, klikt u erop in de lijst.

    Als een toepassing niet up-to-date is, klikt u op **NIEUWE VERSIE DOWNLOADEN** om de laatste versie te downloaden.
- **NETWERK**
  - **Netwerk en Inloggegevens**

    Gewijzigde systeeminstellingen zoals het automatisch verbinden met open hotspot-netwerken zonder uw medeweten of het niet afdwingen van versleuteling van uitgaand beveiligd verkeer.
  - **Wi-Fi-netwerken en routers**

    Om meer te weten over het draadloze netwerk en de router waarmee u verbinding hebt gemaakt, klikt u erop in de lijst. Als het aanbevolen wordt dat u voor uw thuisnetwerk een sterker wachtwoord kiest, zorg dan dat u onze instructies volgt, zodat u verbonden kunt blijven zonder dat u zich zorgen hoeft te maken over uw privacy.

    Wanneer andere aanbevelingen beschikbaar zijn, volt u de instructies zodat u zeker bent dat uw thuisnetwerk veilig blijft tegen de indiscrete blikken van hackers.

De automatische kwetsbaarheidsbewaking gebruiken

Bitdefender scant uw systeem regelmatig op de achtergrond op kwetsbaarheden en houdt gegevens bij van de gevonden problemen in het venster **Kennisgevingen**.

Zo kunt u de opgespoorde problemen controleren en verhelpen:

1. Klik **Meldingen** in het navigatiemenu op de Bitdefender-interface.
2. In het tabblad **Alle** selecteert u de kennisgeving betreffende de Kwetsbaarheidsscan.
3. U kunt gedetailleerde informatie betreffende de gedetecteerde kwetsbaarheden van het systeem zien. Afhankelijk van het probleem, gaat u als volgt te werk om een specifieke kwetsbaarheid te herstellen:
   - Klik op **Installeren** als er Windows-updates beschikbaar zijn.
   - Indien automatische Windows Update geïnactiveerd is klikt u op **Activeren**.
   - Als een toepassing verouderd is, klikt u op **Nu updaten** om een link te zoeken naar de webpagina van de verkoper, vanaf waar u de nieuwste versie van die toepassing kunt installeren.
   - Als een Windows-gebruikersaccount een zwak wachtwoord heeft, klikt u op **Wachtwoord veranderen** om de gebruiker te forceren het wachtwoord te wijzigen bij de volgende aanmelding of wijzigt u zelf het wachtwoord. Voor een sterk wachtwoord gebruikt u een combinatie van hoofdletters en kleine letters, getallen en speciale tekens (zoals #, $ of @).
   - Als de Windows-functie Autorun is ingeschakeld, klikt u op **Verhelpen** om de functie uit te schakelen.
   - Indien de router die u hebt geconfigureerd een zwak wachtwoord heeft ingesteld, klikt u op **Wachtwoord wijzigen** om naar de interface te gaan, waar u een sterk wachtwoord kunt instellen.
   - Klik op **Wifi-instellingen wijzigen** indien het netwerk waarmee u verbonden bent, kwetsbaarheden heeft die uw systeem in gevaar kunnen brengen.

De controle-instellingen voor kwetsbaarheid configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.

2. In de **KWETSBAARHEID** paneel, klik **Open**.

   > **Belangrijk**
   > Om automatisch op de hoogte te worden gebracht over kwetsbaarheden van het systeem of de toepassing, moet u de optie **Kwetsbaarheid** ingeschakeld houden.

3. Ga naar het tabblad **INSTELLINGEN**
4. Kies de systeemkwetsbaarheden die u regelmatig wilt controleren met de overeenkomende schakelaars.

   Windows updates

   Controleer of uw Windows-besturingssysteem over de laatste kritieke beveiligingsupdates van Microsoft beschikt.

   Applicatie-updates

   Controleer of toepassingen geïnstalleerd op uw systeem up-to-date zijn. Verouderde toepassingen kunnen door kwaadaardige software worden misbruikt, waardoor uw PC kwetsbaar wordt voor aanvallen van buitenaf.

   Gebruikerswachtwoorden

   Controleer of de wachtwoorden van de Windows-accounts en routers die op het systeem zijn geconfigureerd, gemakkelijk te raden zijn. Het instellen van moeilijk te raden wachtwoorden (sterke wachtwoorden) maakt het bijzonder moeilijk voor hackers om in uw systeem in te breken. Een sterk wachtwoord bevat hoofdletters en kleine letters, cijfers en speciale tekens (zoals #, $ of @).

   Autoplay

   Controleer de status van de Windows-functie Autorun. Met deze functie kunnen toepassingen automatisch worden gestart vanaf cd's, dvd,'s, USB-stations of andere externe apparaten.

   Sommige types bedreigingen gebruiken Autorun om zich automatisch te verspreiden van de verwisselbare media naar de PC. Daarom is het aanbevolen deze Windows-functie uit te schakelen.

   Wi-Fi Security Advisor

   Controleer of het draadloze thuisnetwerk waarmee u verbonden bent al dan niet veilig is en of er kwetsbaarheden zijn. Controleer ook of het wachtwoord van uw thuisrouter sterk genoeg is en hoe u het veiliger kunt maken.

De meeste onbeveiligde draadloze netwerken zijn niet veilig, waardoor de indiscrete ogen van hackers toegang krijgen tot uw persoonlijke activiteiten.

Opmerking
Als u de bewaking van een specifieke kwetsbaarheid uitschakelt, worden verwante problemen niet langer opgenomen in het venster Kennisgevingen.

Wi-Fi Security Advisor

Als u onderweg bent, in een coffee shop gaat werken of in de luchthaven wacht, kan het de snelste oplossing zijn om een verbinding te maken met een openbaar draadloos netwerk om betalingen te doen, e-mails te lezen of sociale netwerkaccounts te raadplegen. Maar er kunnen nieuwsgierige ogen zijn, die uw persoonlijke gegevens proberen te stelen en kijken hoe de informatie door het netwerk heen druppelt.

Persoonlijke gegevens zijn de wachtwoorden en gebruikersnamen die u gebruikt om naar uw online accounts te gaan, zoals e-mails, bankrekeningen, sociale media-accounts, maar ook de berichten die u verzendt.

Gewoonlijk zijn openbare draadloze netwerken niet veilig, aangezien ze geen wachtwoord vragen om u aan te melden, en als dat wel het geval is, kan het wachtwoord ter beschikking gesteld worden van iedereen die een verbinding wil maken. Bovendien kunnen er kwaadaardige of honingpotnetwerken zijn, die een doelwit vormen voor cybercriminelen.

De Bitdefender Wi-Fi Security Advisor geeft u informatie over:

- **Thuis-wifi-netwerken**
- **Wifi-netwerken op kantoor**
- **Openbare wifi-netwerken**

De meldingen van Wi-Fi Security Advisor aan- of uitzetten

Om de meldingen van Wi-Fi Security Advisor aan of uit te zetten:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **KWETSBAARHEID** paneel, klik **Open**.

3. Ga naar het venster **Instellingen** en schakel de optie **Wifi Beveiligingsadviseur** in of uit.

Thuis-Wi-Fi-netwerk configureren

Uw thuisnetwerk beginnen configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **KWETSBAARHEID** paneel, klik **Open**.
3. Ga naar het venster **Wifi Beveiligingsadviseur** en klik op **Thuis-wifi**.
4. Klik in het tabblad **Thuis-wifi** op **THUIS-WIFI SELECTEREN**.
   Er wordt een lijst weergegeven met de draadloze netwerken waarmee u tot nu toe een verbinding hebt gemaakt.
5. Duid uw thuisnetwerk aan en klik daarna op **SELECTEREN**.

Indien een thuisnetwerk als onbeveiligd of onveilig wordt beschouwd, worden configuratieaanbevelingen weergegeven om de beveiliging te verbeteren.

Om het draadloze netwerk dat u als thuisnetwerk hebt ingesteld, te verwijderen, klikt u op de knop **VERWIJDEREN**.

Om een nieuw draadloos netwerk als thuis-wifi toe te voegen, klikt u op **Nieuwe thuis-wifi selecteren**.

Wifinetwerk op kantoor configureren

Om uw kantoornetwerk te configureren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **KWETSBAARHEID** paneel, klik **Open**.
3. Ga naar het venster **Wifi Beveiligingsadviseur** en klik op **Kantoor-wifi**.
4. Klik in het tabblad **Kantoor-wifi** op **KANTOOR-WIFI SELECTEREN**.
   Er wordt een lijst weergegeven met de draadloze netwerken waarmee u tot nu toe verbinding hebt gemaakt.
5. Duid het netwerk van uw kantoor aan en klik op **SELECTEREN**.

Indien een netwerk voor kantoor als onbeveiligd of onveilig wordt beschouwd, worden configuratieaanbevelingen weergegeven om de beveiliging ervan te verbeteren.

Om het draadloze netwerk dat u als netwerk voor kantoor hebt ingesteld, te verwijderen, klikt u op **VERWIJDEREN**.

Om een nieuw draadloos netwerk als kantoor-wifi toe te voegen, klikt u op **Nieuwe kantoor-wifi selecteren**.

Openbare Wifi

Terwijl u met een onbeveiligd of onveilig draadloos netwerk verbonden bent, wordt het openbare Wi-Fi-profiel geactiveerd. Terwijl u in dit profiel werkt, is Bitdefender Ultimate Security ingesteld om automatisch de volgende programma-instellingen uit te voeren:

- Advanced Threat Defense is ingeschakeld
- De volgende instellingen van Online Threat Prevention zijn ingeschakeld:
  - Versleutelde webscan
  - Bescherming tegen fraude
  - Bescherming tegen phishing
- Er is een knop beschikbaar die Bitdefender Safepay™ opent. In dit geval is de Hotspot-bescherming voor onbeveiligde netwerken standaard geactiveerd.

Informatie controleren over Wi-Fi-netwerken

Om informatie te controleren over de draadloze netwerken, verbindt u zich gewoonlijk met:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **KWETSBAARHEID** paneel, klik **Open**.
3. Ga naar het venster **Wifi Beveiligingsadviseur**.
4. Afhankelijk van de informatie die u nodig hebt, selecteert u een van de drie tabbladen, **Thuis-wifi**, **Kantoor-wifi** of **Openbare wifi**.
5. Klik op **Details bekijken** naast het netwerk waar u meer informatie over wenst.

Er zijn drie types draadloze netwerken gefilterd naargelang belang. Elk type wordt aangeduid door een specifiek pictogram:

Wifi is onveilig - betekent dat het beveiligingsniveau van het netwerk laag is. Dit betekent dat er een hoog risico bestaat als u

het gebruikt en het is niet aanbevolen om betalingen uit te voeren of bankrekeningen te controleren zonder extra bescherming. In dergelijke situaties bevelen wij u aan om Bitdefender Safepay™ met Hotspot-bescherming voor onveilige netwerken geactiveerd te gebruiken.

Wifi is niet veilig - betekent dat het beveiligingsniveau van het netwerk matig is. Dit betekent dat het kwetsbaarheden kan bevatten, en het niet aanbevolen is om betalingen uit te voeren of bankrekeningen te controleren zonder extra bescherming. In dergelijke situaties bevelen wij u aan om Bitdefender Safepay™ met Hotspot-bescherming voor onveilige netwerken geactiveerd te gebruiken.

Wifi is veilig - betekent dat het netwerk dat u gebruikt, veilig is. In dit geval kunt gevoelige gegevens gebruiken om online bewerkingen uit te voeren.

Als u op de koppeling **Informatie bekijken** in het gebied van elk netwerk klikt, worden de volgende gegevens weergegeven:

- **Beveiligd** - hier kunt u bekijken of het geselecteerde netwerk al dan niet beveiligd is. Onbeveiligde netwerken kunnen de gegevens die u gebruikt, toegankelijk laten.
- **Type versleuteling** - hier kunt u bekijken welk type versleuteling wordt gebruikt door het geselecteerde netwerk. Bepaalde versleutelingstypes zijn mogelijk niet veilig. Daarom bevelen we u sterk aan om informatie over het weergegeven versleutelingstype te controleren, zodat u zeker bent dat u beschermd bent terwijl u op het internet surft.
- **Kanaal/Frequentie** - hier kunt u de frequentie van het kanaal bekijken dat het geselecteerde netwerk gebruikt.
- **Wachtwoordkwaliteit** - hier kunt u bekijken hoe sterk het wachtwoord is. Merk op dat de netwerken met een zwak wachtwoord een doelwit vormen voor cybercriminelen.
- **Type aanmelding** - hier kunt u bekijken of het geselecteerde netwerk al dan niet beschermd is met een wachtwoord. Het is sterk aanbevolen om enkel een verbinding te maken met netwerken die een sterk wachtwoord hebben.
- **Type authentificatie** - hier kunt u bekijken welk type authentificatie wordt gebruikt door het geselecteerde netwerk.

1.2.8. Video- & audiobeveiliging

Steeds meer dreigingen zijn ontworpen om toegang te krijgen tot ingebouwde webcams en microfoons. Om onbevoegde toegang tot uw webcam te voorkomen en u te informeren over welke niet-vertrouwde toepassingen toegang hebben tot de microfoon van uw apparaat, en wanneer, heeft Bitdefender Video & Audio het volgende opgenomen:

- **Webcambeveiliging**
- **Microfoonmonitor**

Webcambeveiliging

Dat hackers uw webcam kunnen overnemen om u te bespioneren is geen nieuwigheid meer, en oplossingen om deze te beschermen, zoals het intrekken van de privileges van apps, het uitschakelen van de ingebouwde camera van het apparaat of het afdekken ervan zijn niet erg praktisch. Om verdere pogingen om toegang te krijgen tot uw privacy te voorkomen, controleert Bitdefender Webcam Protection permanent de apps die toegang proberen te krijgen tot uw camera en blokkeert deze die niet als vertrouwd gelabeld zijn.

Als veiligheidsmaatregel wordt u op de hoogte gebracht telkens een niet-vertrouwde toepassing uw camera probeert te gebruiken.

Uw Webcambeveiliging in- of uitschakelen

1. Klik in het navigatiemenu in de **Bitdefender-interface** op **Privacy**.
2. Klik in het **VIDEO- & AUDIOBEVEILIGING**-venster op **Instellingen**.
3. Ga nu naar het venster **Instellingen** en schakel de overeenkomstige schakelaar in of uit.

Webcambeveiliging configureren

U kunt instellen welke regels er moeten toegepast worden wanneer een toepassing probeert om zich toegang te verschaffen tot uw camera. Volg hiervoor deze stappen:

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
2. In de **VIDEO- & AUDIOBESCHERMING** paneel, klik **Instellingen**.
3. Ga naar de **Instellingen** tabblad.

De volgende opties zijn beschikbaar:

Regels voor het blokkeren van toepassingen

- **Alle toegang tot de webcam blokkeren** - geen enkele toepassing zal toegang krijgen tot uw webcam.
- **De toegang van browsers tot de webcam blokkeren** - geen enkele webbrowser behalve Internet Explorer en Microsoft Edge krijgt toegang tot uw webcam. Vanwege de procedure van Windows Store Apps om in een enkel proces te draaien, kunnen Internet Explorer en Microsoft Edge niet door Bitdefender worden gedetecteerd als webbrowsers en zijn ze daarom uitgezonderd van deze instelling.
- **Toelatingen voor toepassingen instellen volgens de voorkeuren van de gemeenschap** - indien de meerderheid van de Bitdefender-gebruikers een populaire toepassing als schadeloos beschouwen, zal de toegang tot de webcam automatisch ingesteld worden op Toestaan. Indien een populaire toepassing door de meesten als gevaarlijk wordt beschouwd, zal de toegang automatisch ingesteld worden op Geblokkeerd.

Notificaties

- **Waarschuwen wanneer toegestane toepassingen de webcam gebruiken** - u wordt op de hoogte gebracht wanneer een toegestane toepassing uw webcam gebruikt.

Toepassingen toevoegen tot de lijst van Webcambeveiliging

Toepassingen die proberen om een verbinding te maken met uw webcam worden automatisch opgespoord en afhankelijk van hun gedag en de keuze van de gemeenschap, wordt hun toegang toegestaan of geweigerd. U kunt echter zelf manueel beginnen configureren welke actie moet worden ondernomen. Volg hiervoor de volgende stappen:

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
2. In de **VIDEO- & AUDIOBESCHERMING** paneel, klik **Instellingen**.
3. Ga naar het venster **Webcambescherming**.
4. Klik op het venster **Toepassing toevoegen**.
5. Klik op de gewenste link:

- **Vanuit Windows Store** - er wordt een lijst met de gedetecteerde Windows Store-apps weergegeven. Zet de schakelaars naast de toepassingen die u wilt toevoegen aan de lijst, aan.
- **Vanuit uw apps** - ga naar het bestand .exe dat u aan de lijst wilt toevoegen, en klik vervolgens op **OK**.

Om te zien wat de gebruikers van Bitdefender gekozen hebben om te doen met de geselecteerde app, klikt u op het pictogram.

De toepassingen die toegang tot uw camera vragen verschijnt in dit venster, samen met het tijdstip van laatste activiteit.

U wordt op de hoogte gebracht telkens een van de toegestane toepassingen door de Bitdefender-gebruikers wordt geblokkeerd.

Om de toegang van een toegevoegde app tot uw webcam te stoppen, klikt u op het pictogram.

Het pictogram verandert naar, wat betekent dat de geselecteerde toepassingen geen toegang hebben tot uw webcam.

Microfoonmonitor

Corrupte toepassingen kunnen zonder uw toestemming toegang verkrijgen tot uw ingebouwde microfoon. Om u bewust te maken van mogelijke schadelijke exploits, geeft Bitdefender Microfoonmonitor u in dergelijke situaties kennisgevingen. Zo krijgt geen enkele toepassing toegang tot uw microfoon, zonder dat u daarbij de touwtjes in handen hebt.

Microfoonmonitor in- en uitschakelen

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
2. In de **VIDEO- & AUDIOBESCHERMING** paneel, klik **Instellingen**.
3. Selecteer de **Instellingen** raam.
4. In het venster **Instellingen** schakelt u de schakelaar voor **Microfoonmonitor** in of uit.

Notificaties configureren voor Microfoonmonitor

Om te configureren welke notificaties moeten verschijnen wanneer toepassingen toegang proberen te verkrijgen tot uw microfoon, volgt u deze stappen:

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
2. In de **VIDEO- & AUDIOBESCHERMING** paneel, klik **Instellingen**.
3. Ga naar de **Instellingen** raam.

Meldingen

- **Notificatie geven wanneer een toepassing de microfoon probeert te openen**
- **Notificatie geven wanneer browsers de microfoon openen**
- **Notificatie geven wanneer niet-vertrouwde toepassingen uw microfoon openen**
- **Notificatie weergeven op basis van voorkeuren van Bitdefender-gebruiker**

Toepassingen toevoegen aan de lijst Microfoonmonitor

Toepassingen die verbinding proberen te maken met uw microfoon worden automatisch gedetecteerd en toegevoegd aan de lijst met Notificaties. Maar u kunt ook zelf, handmatig en aan de hand van de volgende stappen configureren of een notificatie wel of niet moet worden weergegeven:

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
2. In de **VIDEO- & AUDIOBESCHERMING** paneel, klik **Instellingen**.
3. Ga naar het venster **Audiobeveiliging**.
4. Klik **Applicatie toevoegen** raam.
5. Klik op de gewenste link:
   - **Van Windows Store** - er wordt een lijst met de gedetecteerde Windows Store-apps weergegeven. Schakel de schakelaars in naast de apps die u aan de lijst wilt toevoegen.
   - **Van je apps** - ga naar het .exe-bestand dat u aan de lijst wilt toevoegen en klik vervolgens op **OK**.

Om te bekijken wat de Bitdefender-gebruikers hebben gekozen om te doen met de geselecteerde app, klikt u op de icoon.

De toepassingen die toegang tot uw microfoon vragen, verschijnen in dit venster, samen met het tijdstip van de laatste activiteit.

Om geen notificaties meer te ontvangen over de activiteit van een toegevoegde app, klikt u op het pictogram .

Het pictogram wordt , wat betekent dat geen Bitdefender-notificaties worden weergegeven wanneer de geselecteerde toepassing uw microfoon probeert te gebruiken.

1.2.9. Ransomware-remediëring

Ransomware-remediëring van Bitdefender maakt een back-up van uw bestanden zoals documenten, afbeeldingen, video's of muziek, om te verzekeren dat ze worden beschermd tegen schade of verlies in geval van versleuteling door ransomware. Telkens een ransomware-aanval wordt gedetecteerd, blokkeert Bitdefender alle processen die in de aanval zijn betrokken en start het remediëringsproces op. Zo kunt u de inhoud van al uw bestanden herstellen, zonder het gevraagde losgeld te moeten betalen

De Ransomware-remediëring in- of uitschakelen

Om de Ransomware-remediëring in of uit te schakelen:

1. 1. Klik in het navigatiemenu in de **Bitdefender-interface** op **Bescherming**.
2. Schakel de schakelaar in het paneel **RANSOMWARE-REMEDIËRING** in of uit.

> **Opmerking**
> Om te verzekeren dat uw bestanden tegen ransomware worden beschermd, raden we aan dat u Ransomware-remediëring ingeschakeld laat.

Automatisch herstellen in- of uitschakelen

Automatisch herstellen zorgt ervoor dat uw bestanden automatisch worden hersteld in geval van versleuteling door ransomware.

Om automatisch herstellen in of uit te schakelen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **RANSOMWARE-REMEDIËRING** op **Beheren**.
3. In het venster Instellingen schakelt u de schakelaar voor **Automatisch herstellen** in of uit.

Bestanden bekijken die automatisch werden hersteld

Wanneer de optie **Automatisch herstellen** ingeschakeld is, herstelt Bitdefender automatisch de bestanden die door ransomware werden versleuteld. Zo kunt u zorgeloos genieten van uw apparaat, want u weet dat uw bestanden veilig zijn.

Om bestanden te bekijken die automatisch werden hersteld:

1. Klik **Meldingen** in het navigatiemenu op de Bitdefender-interface.
2. In het tabblad **Alle** selecteert u de notificatie betreffende het ransomware-gedrag dat als laatste werd geremedieerd en klikt u op **Herstelde bestanden**.
   De lijst met herstelde bestanden wordt weergegeven. Hier kunt u ook de locatie waar uw bestanden werden hersteld, bekijken.

Versleutelde bestanden handmatig herstellen

Volg deze stappen indien u de bestanden die door ransomware werden versleuteld handmatig wilt herstellen:

1. Klik **Meldingen** in het navigatiemenu op de Bitdefender-interface.
2. In het tabblad **Alle** selecteert u de notificatie betreffende het ransomware-gedrag dat als laatste werd gedetecteerd en klikt u op **Versleutelde bestanden**.
3. De lijst met versleutelde bestanden wordt weergegeven.
   Klik op **Bestanden herstellen** om verder te gaan.
4. Indien een deel van of het gehele herstelproces mislukt, moet u de locatie kiezen waar de ontcijferde bestanden moeten worden bewaard. Klik op **LOCATIE VOOR HET HERSTEL** en kies een locatie op uw pc.
5. Er wordt een bevestigingsvenster weergegeven.
   Klik op **VOLTOOIEN** om het herstelproces te beëindigen.

Bestanden met de onderstaande extensies kunnen worden hersteld, indien ze worden versleuteld:

.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;

Toepassingen aan uitzonderingen toevoegen

U kunt de uitzonderingsregels voor vertrouwde toepassingen configureren zodat de functie Ransomware-remediëring deze niet blokkeert wanneer ze handelingen uitvoeren die op ransomware lijken.

Om toepassingen toe te voegen aan de uitzonderingenlijst van Ransomware-remediëring:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **RANSOMWARE-OPLOSSING** paneel, klik **Beheren**.
3. Ga naar het venster **Uitzonderingen** en klik op **+Een uitzondering toevoegen**.

1.2.10. Cryptomining Protection

Wat is Cryptomining-bescherming?

Met het gebruik van cryptomining kunnen aanvallers financieel profiteren zonder de bijbehorende kosten en juridische gevolgen te dragen.

De Cryptomining Protection-functie van Bitdefender verdedigt Windows-computers tegen de groeiende dreiging van ongeautoriseerde cryptomining-activiteiten, een kwaadaardige praktijk die de bronnen en elektriciteit van een gebruiker exploiteert om inkomsten voor aanvallers te genereren.

> **Opmerking**
> Cryptomining-bescherming is afhankelijk van:
>
> - Bitdefender-schild
> - Preventie van webaanvallen
>
> Om Cryptomining Protection te kunnen gebruiken, moeten beide functies ook zijn ingeschakeld.

Cryptomining-beveiliging inschakelen

De functie Cryptomining Protection bevindt zich op het tabblad Bescherming.

Om dit in te schakelen, schakelt u eenvoudigweg de bijbehorende schakelaar om.

> **Opmerking**
> Cryptomining-beveiliging is standaard uitgeschakeld, zodat gebruikers controle hebben over de activering ervan.

Bedrijfsmodi

Eenmaal ingeschakeld, werkt de functie Cryptomining Protection in 2 verschillende statussen, elk afgestemd op de voorkeuren van de gebruiker:

1. **Blokkeer alle Cryptomining-activiteiten.** (blokkeert automatisch alle cryptomining-activiteiten en onderneemt de nodige acties om verdere ongeautoriseerde pogingen te voorkomen)
   Deze modus is ideaal voor gebruikers die niet van plan zijn zich bezig te houden met cryptomining-activiteiten.
2. **Detecteer Cryptomining-activiteiten.** (geeft waarschuwingen wanneer er een cryptomining-activiteit wordt gedetecteerd en vereist gebruikersinvoer om de juiste actie te bepalen)
   Deze modus is geschikt voor gebruikers die actief betrokken zijn bij hun eigen cryptomining-activiteiten, maar ongeoorloofde pogingen willen monitoren en controleren.

Beheer uitzonderingen

Uitzonderingen kunnen worden gespecificeerd voor toepassingen, met de extra mogelijkheid om specifieke opdrachtregels te definiëren. Er kunnen echter ook uitzonderingen worden gemaakt zonder de noodzaak om dergelijke gedetailleerde parameters op te geven, waardoor een evenwicht wordt geboden tussen maatwerk en eenvoud.

Om een uitzondering toe te voegen:

1. Klik**Bescherming**in het menu aan de linkerkant van de Bitdefender-interface.

2. In de**Bescherming tegen cryptomining**paneel, klik**Instellingen**.
3. Klik op de**Beheer uitzonderingen**keuze.
4. Klik vervolgens op de**Voeg een uitzondering toe**knop.
5. Er wordt een nieuw venster geopend. U kunt applicaties, URL's en IP-adressen handmatig uitsluiten.
6. Klik ten slotte**Redden**. De nieuwe regel is toegevoegd aan de uitzonderingenlijst voor Cryptomining Protection.

> **Opmerking**
> Om een uitzondering te verwijderen, klikt u eenvoudig op het prullenbakpictogram ernaast.

1.2.11. Scam Copilot voor Windows

Scam Copilot is de door AI aangedreven oplichtingsdetector van Bitdefender.

Door het te gebruiken, kunt u alle lastige sms'jes, e-mails, berichten op sociale media, links of zelfs QR-codes verzenden die u hebt ontvangen en waarvan u achterdochtig bent, om onmiddellijk een analyse te krijgen van hun veiligheid en legitimiteit.

Om Scam Copilot in te stellen:

1. Open Bitdefender.
2. Open het tabblad Bescherming in het menu aan de linkerkant van het Bitdefender-venster.
3. Klik op de **Ga aan de slag** knop.
4. Volg vanaf hier alle instructies op het scherm om alle componenten van de Scam Copilot-module in te schakelen.

Scam Copilot wordt dan succesvol ingesteld op uw apparaat!

In het Scam Copilot-dashboard kunt u zien hoeveel geverifieerde en gedetecteerde berichten, e-mails en links u ontvangt en die voortdurend door Bitdefender worden gecontroleerd, evenals het aantal mogelijke oplichting dat tot nu toe is gecontroleerd en gedetecteerd.

In hetzelfde dashboard heb je ook de mogelijkheid om te chatten met Scam Copilot, wanneer je het gevoel hebt dat je het doelwit bent van een poging tot oplichting of phishing.

1.2.12. Anti-tracker

Vele websites die u bezoekt, gebruiken trackers om informatie te verzamelen over uw gedrag. Ze kunnen deze informatie vervolgens delen met derden of ze kunnen de informatie gebruiken om u advertenties te laten zien die voor u relevanter zijn. Eigenaars van websites verdienen zo geld, om u gratis inhoud te kunnen bieden of om draaiende te blijven. Naast het verzamelen van informatie, kunnen trackers uw surfervaring vertragen of uw bandbreedte opgebruiken.

Als de Bitdefender Anti-tracker-extensie geactiveerd is in uw webbrowser, vermijdt u deze tracking, zorgt u dat uw gegevens privé blijven terwijl u online surft en wordt de laadtijd voor websites versneld.

De Bitdefender-extensie is compatibel met de volgende webbrowsers:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

De trackers die we detecteren worden in de volgende categorieën gegroepeerd:

- **Reclame** - wordt gebruikt voor de analyse van patronen in websiteverkeer, het gedrag van gebruikers of het verkeer van bezoekers.
- **Klanteninteractie** - wordt gebruikt om de interactie van gebruikers met verschillende invoervormen, zoals chat of ondersteuning, te meten.
- **Essentieel** - wordt gebruikt om de kritieke functionaliteiten van webpagina's te monitoren.
- **Website-analytics** - wordt gebruikt om gegevens over het gebruik van webpagina's te verzamelen.
- **Sociale Media** - wordt gebruikt voor de monitoring van het sociale publiek, de activiteiten en het gebruikersengagement met verschillende sociale mediaplatformen.

Interface van Anti-tracker

Wanneer de Bitdefender Anti-tracker-extensie is geactiveerd, verschijnt het symbool naast de zoekbalk in uw webbrowser. Telkens wanneer u

een website bezoekt, kunt u op het symbool een teller zien die verwijst naar de gedetecteerde en geblokkeerde trackers. Om meer details over de geblokkeerde trackers te bekijken, klikt u op het symbool om de interface te openen. Naast het aantal geblokkeerde trackers kunt u de tijd zien die nodig is om de pagina te laden en de categorieën waartoe de gedetecteerde trackers behoren. Om de lijst met websites die tracken te bekijken, klikt u op de gewenste categorie.

Om de blokkering van trackers door Bitdefender op te heffen voor de website die u momenteel bezoekt, klikt u op **Bescherming op deze website pauzeren**. Deze instelling is enkel van toepassing zolang u de website open hebt staan en gaat terug naar zijn initiële staat zodra u de website verlaat.

Om toe te staan dat trackers van een specifieke categorie uw activiteiten volgen, klikt u op de gewenste activiteit en vervolgens op de bijhorende knop. Indien u zich bedenkt, klikt opnieuw op dezelfde knop.

Bitdefender Anti-tracker uitschakelen

Om de Bitdefender Anti-tracker uit te schakelen:

- Vanuit uw webbrowser:
  1. Open uw webbrowser.
  2. Klik op het symbool naast de adresbalk in uw webbrowser.
  3. Klik op het symbool in de rechterbovenhoek.
  4. Gebruik de bijhorende schakelaar om uit te schakelen.
     Het Bitdefender-pictogram wordt dan grijs.

- Vanuit deBitdefender-interface:
  1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
  2. Klik in het deelvenster **ANTI-TRACKER** op **Instellingen**.
  3. Schakel de overeenstemmende schakelaar uit naast de webbrowser waarvoor u de extensie wenst uit te schakelen.

Toestaan dat een website aan tracking doet

Wilt u dat tracking wordt toegepast wanneer u een bepaalde website bezoekt, kunt u dit adres als volgt toevoegen aan de uitzonderingen:

1. Open uw webbrowser.
2. Klik op het symbool naast de zoekbalk.
3. Klik op de pictogram in de rechterbovenhoek.
4. Bent u op de website die u wilt toevoegen aan de uitzonderingen, klikt u op **Huidige website aan lijst toevoegen**.
   Wilt u een andere website toevoegen, voert u het adres in het bijhorende veld in en klikt u op .

1.2.13. Safepay beveiliging voor online transacties

De computer wordt in snel tempo het hoofdhulpmiddel voor winkelen en bankieren. Facturen betalen, geld overmaken, bijna alles wat u zich maar voor kunt stellen kopen, dat alles is nooit sneller en gemakkelijker geweest.

Dit houdt in het verzenden via Internet van persoonlijke gegevens, account- en creditcardgegevens, wachtwoorden en andere soorten privégegevens, met andere woorden, precies het soort gegevensstroom waar cybercriminelen graag gebruik van maken. Hackers zijn meedogenloos in hun pogingen deze gegevens te stelen, dus u kunt nooit voorzichtig genoeg zijn als het om het beveiligen van online transacties gaat.

Bitdefender ™ is in de eerste plaats een beveiligde browser, een verzegelde omgeving, ontworpen om uw internetbankieren, e-shopping en andere soorten online transacties privé en veilig te houden.

Bitdefender Safepay™ biedt de volgende functies:

- Het blokkeert de toegang tot uw desktop en elke poging snapshots van uw scherm te maken.
- Het verschaft een virtueel toetsenbord dat het, als het wordt gebruikt, onmogelijk maakt voor hackers uw aanslagen te lezen.
- Het is volledig onafhankelijk van uw andere browsers.
- Het biedt een ingebouwde hotspotbeveiliging die kan worden gebruikt wanneer uw apparaat is verbonden met onbeveiligde Wi-Fi-netwerken.
- Het ondersteunt bookmarks en stelt u in staat om te surfen tussen uw favoriete bank/winkelsites.

- Het is niet beperkt tot bankieren en online winkelen. Elke website kan worden geopend in Bitdefender Safepay™.

Bitdefender Safepay™ gebruiken

Standaard detecteert Bitdefender wanneer u naar een online banksite of online winkel in een willekeurige browser op uw apparaat surft en het vraagt u deze site te starten in Bitdefender Safepay™.

Om naar de hoofdinterfae van Bitdefender Safepay™ te gaan, gebruikt u een van de volgende manieren:

- Vanuit de **Bitdefender-interface**:
  1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
  2. Klik in het deelvenster **SAFEPAY** op **Instellingen**.
  3. Klik in het venster **Safepay** op **Safepay starten**.

- Voor Windows:
  - In **Windows 7**:
    1. Klik op **Start** en ga naar **Alle Programma's**.
    2. Klik op **Bitdefender**.
    3. Klik op **Bitdefender Safepay™**.
  - In **Windows 8** en **Windows 8.1**:
    Zoek Bitdefender Safepay™ vanuit het Windows-startscherm (u kunt bijvoorbeeld beginnen met het typen van "Bitdefender Safepay™", rechtstreeks in het startscherm) en klik op het pictogram.
  - In **Windows 10** en **Windows 11**:
    Voer "Bitdefender Safepay™" in het zoekveld in de taakbalk in en klik op de icoon ervan.

Indien u gewend bent aan webbrowsers, zult u geen moeite hebben Bitdefender Safepay te gebruiken ™- het ziet eruit en gedraagt zich als een gewone browser:

- geef de URL's op in de adresbalk van de sites waar u heen wilt gaan.

- voeg tabs toe om meerdere websites te bezoeken in het Bitdefender Safepay™-venster door te klikken op ⊞.
- surf terug en vooruit en vernieuw pagina's met gebruikmaking van respectievelijk ← → ↻.
- ga naar BitdefenderSafepay™ **instellingen** door te klikken op en te kiezen voor **Instellingen**.
- beheer uw **favorieten** door te klikken op ☆ naast de adresbalk.
- open het virtuele toetsenbord door te klikken op .
- vergroot of verklein de browserafmetingen door gelijktijdig te drukken op de toetsen **Ctrl** en **+/-** op het numerieke toetsenbord.
- bekijk informatie over uw Bitdefender-product door te klikken op ⋯ en **Over** te kiezen.
- druk belangrijke informatie af door te klikken op ⋯ en **Afdrukken** te kiezen.

> **Opmerking**
> Om tussen Bitdefender Safepay™ en Windows-bureaublad te wisselen, drukt u op de toetsen **Alt+Tab** of klikt u in de linkerbovenhoek van het venster op de optie **Wisselen naar Bureaublad**.

Instellingen configureren

Klik op ⋯ en kies **Settings** om Bitdefender Safepay™ te configureren:

Regels voor Bitdefender Safepay toepassen voor domeinen die worden geopend

De websites die u hebt toegevoegd aan **Bladwijzers** met de optie **Automatisch openen in Safepay** ingeschakeld, verschijnen hier. Wilt u het automatisch openen met Bitdefender Safepay™ opheffen voor een website uit de lijst, klikt u op × naast het gewenste item in de kolom **Verwijderen**.

Pop-ups blokkeren

U kunt ervoor kiezen om pop-ups te blokkeren door te klikken op de overeenkomende schakelaar.

U kunt ook een lijst aanmaken met websites waarvan u pop-ups toestaat. De lijst mag websites bevatten die u volledig vertrouwt.

Om een site toe te voegen aan de lijst, geeft u het adres van de site op in het overeenkomende veld en klikt u op **Domein toevoegen**.

Om een website uit de lijst te verwijderen, selecteert u het X-je bij het gewenste gegeven.

Plug-ins beheren

U kunt kiezen of u specifieke plug-ins in Bitdefender Safepay™ wenst te activeren of inactiveren.

Certificaten beheren

U kunt certificaten van uw systeem importeren naar een certificatenwinkel.

Klik op **IMPORTEREN** en volg de wizard om de certificaten te gebruiken in Bitdefender Safepay™.

Virtueel toetsenbord gebruiken

Het Virtuele toetsenbord verschijnt automatisch wanneer een wachtwoordveld wordt geselecteerd.

Gebruik de bijhorende schakelaar om de functie te activeren of inactiveren.

Bevestiging afdrukken

Activeer deze optie indien u uw bevestiging wenst te geven voordat het afdrukproces start.

Favorieten beheren

Indien u de automatische detectie van sommige of alle websites hebt uitgeschakeld, of Bitdefender detecteert bepaalde websites eenvoudigweg niet, dan kunt u favorieten toevoegen aan Bitdefender Safepay™ zodat u favoriete websites in de toekomst eenvoudig kunt starten.

Volg deze stappen om een URL toe te voegen aan Bitdefender Safepay™-favorieten:

1. Klik op ⋯ en kies **Favorieten** om de pagina met favorieten te openen.

Opmerking
De pagina met favorieten is standaard geopend als u Bitdefender Safepay™ start.

2. Klik op de knop **+** om een nieuwe favoriete pagina toe te voegen.
3. Geef de URL en de titel van de bladwijzer in en klik vervolgens op **AANMAKEN**. Vink de optie **Automatisch openen in Safepay** aan indien u de gemarkeerde pagina wilt openen met Bitdefender Safepay™, telkens als u er naartoe gaat. De URL wordt ook toegevoegd aan de Domeinenlijst op de instellingen-pagina.

Safepay-notificaties uitschakelen

Bitdefender-product is zo ingesteld dat u via een pop-up op de hoogte wordt gebracht wanneer een website voor internetbankieren wordt gedetecteerd.

Om Safepay-notificaties uit te schakelen:

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
2. In de **VEILIG** paneel, klik **Instellingen**.
3. In het venster **Instellingen** schakelt u de schakelaar naast **Safepay-notificaties** in.

1.2.14. Ouderlijk Toezicht

Met Ouderlijk Toezicht van Bitdefender kunt u de online activiteiten van uw kinderen beheren en beschermen. Zodra u Ouderlijk Toezicht van Bitdefender hebt geconfigureerd, kunt u gemakkelijk te weten komen wat uw kinderen doen op de apparaten die ze gebruiken en waar ze de afgelopen 24 uur zijn geweest. Om u te helpen beter te weten wat uw kinderen doen, geeft de functie u bovendien statistieken over hun activiteiten en interesses.

Uw Bitdefender-abonnement bevat de volgende functies:

- Op Windows-, macOS- en Android-apparaten:
  - Ongeschikte webpagina's te blokkeren.
  - Toepassingen zoals spelletjes, chat, programma's die bestanden uitwisselen en andere programma's blokkeren.

- Het gebruik van het apparaat dat wordt gecontroleerd, blokkeren.
- De toegang tot het internet gedurende bepaalde periodes (bijvoorbeeld tijdens lessen) te blokkeren.
- Tijdsbeperkingen instellen voor het gebruik van de apparaten.
- Weergeven hoeveel tijd uw kinderen gemiddeld hun apparaten gebruiken.
- Een rapport weergeven met de toepassingen die in de voorbije 30 dagen zijn gebruikt op het gecontroleerde apparaat.
- Afgeschermde gebieden in te stellen.
- De locatie van het Android-apparaat van uw kind vinden.

U hebt toegang nodig tot uw Bitdefender-account om de online activiteiten van uw kinderen te controleren, de apparaten te beheren die uw kinderen gebruiken of de instellingen van Ouderlijk toezicht te wijzigen.

Er zijn twee mogelijkheden om toegang te krijgen tot uw Bitdefender-account, ofwel via een webbrowser door naar https://central.bitdefender.com te gaan, ofwel via de Bitdefender Central app, die kan worden geïnstalleerd op Android- en iOS-apparaten.

Opmerking
In dit materiaal leest u de opties en instructies die op het webplatform beschikbaar zijn.

Naar Ouderlijk toezicht gaan - Mijn kinderen

Zodra u het gedeelte Ouderlijk toezicht opent, is het venster **Mijn kinderen** beschikbaar. Hier kunt u profielen aanmaken voor uw kinderen. U kunt deze later ook bekijken en bewerken. Eens de profielen zijn aangemaakt, worden ze weergegeven als profielkaarten zodat u ze snel kunt beheren en hun status in een oogopslag kunt controleren.

Zodra u een profiel creëert, kunt u meer gedetailleerde instellingen aanpassen om de toegang tot het internet en tot specifieke applicaties voor uw kinderen controleren.

U krijgt vanaf Bitdefender Central toegang tot de instellingen van Ouderlijk toezicht vanop elke computer of mobiel apparaat met een internetverbinding.

Ga naar uw Bitdefender-account:

- Op elk apparaat met internettoegang:
  1. Toegang Bitdefender Centraal.
  2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
  3. Selecteer het paneel **Ouderlijk toezicht**.
  4. In het venster dat verschijnt, kunt u de profielen van Ouderlijk Toezicht voor elk apparaat configureren.

- Vanuit uw Bitdefender-interface:
  1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
  2. Klik in het deelvenster **OUDERLIJK TOEZICHT** op **Configureren**.
     U wordt afgeleid naar de Bitdefender-account webpagina. Zorg ervoor dat u aangemeld bent met uw gegevens.
  3. Selecteer de functie **Ouderlijk toezicht**.
  4. In het venster dat verschijnt, kunt u de profielen voor ouderlijk toezicht voor elk apparaat beheren en configureren.

> **Opmerking**
> Zorg dat u bij de apparaat bent aangemeld met een beheerdersaccount. Alleen gebruikers met beheerdersrechten (administrators) op het systeem kunnen Ouderlijk Toezicht openen en configureren.

Profielen voor uw kinderen aanmaken

Om de online activiteiten van uw kinderen te beginnen volgen, moet u profielen configureren en de app Ouderlijk Toezicht van Bitdefender installeren op de apparaten die ze gebruiken.

Om een kindprofiel aan te maken:

1. Toegang Bitdefender Centraal.
2. Selecteer de Ouderlijk toezicht paneel.
3. Klik op **KINDPROFIEL TOEVOEGEN** in het venster **Mijn kinderen**.
4. Stel specifieke informatie in, zoals naam, geboortedatum of geslacht. Om een foto aan het profiel van uw kind toe te voegen,

klikt u op het pictogram rechtsonder bij de optie **Profielfoto**. Klik op **OPSLAAN** om door te gaan.

Op basis van normen voor de ontwikkeling van kinderen, laadt de geboortedatum van het kind instellingen voor het doorzoeken van het internet die als geschikt geacht worden voor deze leeftijdcategorie.

5. Klik op **LATEN WE EEN APPARAAT TOEVOEGEN**.
6. Indien er al een Bitdefender-product op het apparaat van uw kind geïnstalleerd is, selecteert u dit apparaat uit de beschikbare lijst en selecteert u de account die u wenst te controleren. Klik op **TOEWIJZEN**.

   Belangrijk

   Op Windows- en macOS-apparaten waarop geen Bitdefender-product is geïnstalleerd, wordt de tracker van Ouderlijk Toezicht van Bitdefender geïnstalleerd, zodat u de online activiteiten van uw kinderen kunt volgen.

   Op Android- en iOS-apparaten wordt de app Ouderlijk Toezicht van Bitdefender gedownload en geïnstalleerd.

Om andere apparaten toe te wijzen, klikt u op **APPARAAT TOEVOEGEN** naast het profiel van het kind. Volg de instructies vanaf stap 6 in dit hoofdstuk.

De online activiteiten van uw kind bekijken

Ouderlijk Toezicht van Bitdefender helpt u bij te houden wat uw kinderen online doen. Zo kunt u altijd precies nagaan bij welke activiteiten ze betrokken waren terwijl ze tijd doorbrachten op de toegewezen apparaten.

Afhankelijk van de instellingen die u invoert, levert Bitdefender u verslagen die gedetailleerde informatie kunnen bevatten voor elke gebeurtenis, bijvoorbeeld:

- De status van de gebeurtenis.
- De ernst van de kennisgeving.
- De apparaatnaam.
- De datum en het tijdstip waarop de gebeurtenis is opgetreden.

Om het internetverkeer, de gebruikte toepassingen of de online activiteiten van uw kinderen te monitoren:

1. Toegang Bitdefender Centraal.
2. Selecteer de Ouderlijk toezicht paneel.
3. Selecteer een kindprofiel.
   In het venster **Activiteit** kunt u de informatie bekijken die u interesseert.

De Rapportinstellingen configureren

Wanneer Ouderlijk toezicht is ingeschakeld, worden de online van uw activiteiten standaard gelogd.

Om e-mailnotificaties te ontvangen over de online activiteiten van uw kinderen:

1. Toegang Bitdefender Centraal.
2. Selecteer de Ouderlijk toezicht paneel.
3. Klik op **RAPPORTINSTELLINGEN**.
4. Schakel de overeenkomende schakelaar in om activiteitsverslagen te ontvangen.
5. Voer het e-mailadres in waarnaar de e-mailmeldingen moeten worden verzonden.
6. Pas de frequentie aan door dagelijks, wekelijks of maandelijks te selecteren, en klik vervolgens op **OPSLAAN**.

U kunt er ook voor kiezen om notificaties te ontvangen in uw Bitdefender-account, in de onderstaande situaties:

- Telkens uw kinderen toegang proberen te verkrijgen tot geblokkeerde toepassingen (op Windows, macOS en Android).
- Telkens uw kinderen oproepen ontvangen van geblokkeerde/onbekende telefoonnummers (op iOS).
- Telkens uw kinderen de veilige gebieden verlaten of verboden gebieden binnengaan
- Telkens uw kinderen inchecken als Veilig.

Een profiel bewerken

Om een bestaand profiel te bewerken:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Ouderlijk toezicht** paneel.
3. Klik op de gewenste profielkaart op **OPTIES** en selecteer vervolgens **Profiel bewerken**.
4. Nadat u de gewenste instellingen hebt aangepast, selecteert u **OPSLAAN**.

Een profiel verwijderen

Om een bestaand profiel te verwijderen:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Ouderlijk toezicht** paneel.
3. Selecteer het kindprofiel.
4. Klik op de knop **OPTIES** en selecteer vervolgens **Profiel verwijderen**.
5. Bevestig uw keuze.

Profielen in Ouderlijk toezicht configureren

Om uw kinderen te beginnen volgen, moet u een profiel toewijzen aan de apparaten waarop de functie of de app Ouderlijk Toezicht van Bitdefender is geïnstalleerd.

Nadat u een profiel hebt aangemaakt, kunt u meer gedetailleerde instellingen aanpassen om de toegang tot het internet en specifieke toepassingen te volgen en te controleren.

Om een profiel te beginnen configureren, selecteert u de gewenste profielkaart en klikt u op **OPTIES**.

Klik op een tabblad om de overeenkomende functie van Ouderlijk toezicht voor het apparaat te configureren:

- **Schermtijd** - hier kunt u de toegang tot de apparaten die u in de profielen van uw kinderen hebt aangeduid, blokkeren. De toegang kan wordt beperkt voor bepaalde tijdsintervallen, alsook na cumulatieve dagelijkse limieten.
- **Toepassingen** - hier kunt u de toegang tot bepaalde applicaties, zoals games, berichtensoftware, films enz. blokkeren.
- **Websites** - hier kunt u de webnavigatie filteren.

- **Apparaten weergeven** - hier kunt u de status zien van de apparaten die opgevolgd worden, een nieuw apparaat toewijzen aan het profiel van uw kind of een toegewezen apparaat verwijderen.

Als u de slimme luidspreker Amazon Alexa of de Google Assistant app gebruikt, kunt u spraakopdrachten starten om de locaties of online activiteiten van uw kinderen te controleren. Raadpleeg Spraakopdrachten voor interactie met Bitdefender voor de volledige lijst met spraakopdrachten die u kunt starten.

Activiteit

Het hoofdvenster biedt u gedetailleerde informatie over de online activiteiten van uw kinderen van de afgelopen 24 uur of van de afgelopen 7 dagen, afhankelijk van uw keuze, binnenshuis en buitenshuis. Om de activiteiten van de afgelopen zeven dagen weer te geven, klikt u op **Afgelopen 7 dagen**.

Afhankelijk van de activiteit kan dit venster informatie bevatten over:

- **Websiteactiviteit** - hier vindt u informatie over de categorieën van websites die uw kinderen bezocht hebben. Klik op de link **INSTELLINGEN WIJZIGEN** om specifieke interesses toe te staan of te weigeren.
- **Recent toegevoegde telefooncontacten** - hier kunt u weergeven of er nieuwe contactpersonen zijn toegevoegd aan de apparaten van uw kind. Klik op de link **ALLE TELEFOONCONTACTEN WEERGEVEN** om de contactpersonen te selecteren waarmee uw kinderen in contact mogen zijn of niet.
- **Toepassingen** - hier ziet u welke toepassingen uw kinderen hebben gebruikt. Klik op de link **ALLE TOEPASSINGEN WEERGEVEN** om de toegang tot specifieke toepassingen te blokkeren of toe te staan.
- **Schermtijd** - Hier kunt u zien hoeveel tijd er online is doorgebracht op alle apparaten die aan uw kinderen zijn toegewezen. Klik op de knop **SCHERMTIJD WEERGEVEN** om het venster **Schermtijd** te openen.

toepassingen

Met het venster Toepassingen kunt u toepassingen blokkeren op Windows-, macOS- en Android-apparaten. Games, media en messaging software, maar ook andere categorieën van software kunnen op deze manier worden geblokkeerd.

Hier ziet u ook de toepassingen die de voorbije 30 dagen het vaakst werden gebruikt, samen met info over hoelang uw kinderen de toepassingen hebben gebruikt. Informatie over hoelang de toepassingen werden gebruikt, kan enkel worden opgevraagd voor Windows-, macOS- en Android-apparaten.

Om Toepassingsbeheer voor een specifieke gebruikersaccount te configureren:

1. Er wordt een lijst met toegekende apparaten weergegeven.
   Selecteer de kaart met het apparaat waarvoor u de toegang tot toepassingen wilt beperken.
2. Klik op **De toepassingen van ... beheren**.
   Er wordt een lijst met geïnstalleerde toepassingen weergegeven.
3. Selecteer **Geblokkeerd** naast de toepassingen die u voor uw kind wilt verbieden.
4. Klik op **OPSLAAN** om de nieuwe instelling toe te passen.

U kunt de monitoring van de geïnstalleerde toepassingen opheffen door de optie **Gebruikte Toepassingen Monitoren** in de rechterbovenhoek van het venster uit te schakelen.

Webpagina's

Het venster Websites helpt u websites met ongepaste inhoud te blokkeren, op Windows-, macOS- en Android-apparaten. Websites waarop video's, games, media en messaging-software worden gehoost, maar ook andere categorieën van negatieve inhoud, kunnen op deze manier geblokkeerd worden.

De functie kan geactiveerd of geïnactiveerd worden met de hiertoe bestemde schakelaar.

Afhankelijk van de leeftijd die u voor uw kinderen instelt, wordt de lijst Interesses standaard voorzien van een selectie geactiveerde categorieën. Om de toegang tot een specifieke categorie toe te staan of te weigeren, klikt u erop.

Het pictogram ⊘ dat verschijnt, geeft aan dat uw kind niet in staat zal zijn toegang te verkrijgen tot inhoud gelinkt aan een bepaalde categorie.

Een website toestaan of blokkeren:

Om de toegang tot bepaalde webpagina's te beperken of toe te staan, moet u ze als volgt aan de Uitzonderingenlijst toevoegen:

1. Klik op de knop **BEHEREN**.
2. Tik de webpagina die u wilt toestaan of blokkeren in het overeenkomstige veld in.
3. Selecteer **Toestaan** of **Blokkeren**.
4. Klik op het pictogram **+** om de wijzigingen op te slaan.

> **Opmerking**
> Toegangsbeperkingen voor websites kunnen enkel ingesteld worden voor Windows-, Android- en macOS-apparaten die toegevoegd zijn aan het profiel van uw kind.

Schermtijd

In het venster Schermtijd ziet u hoeveel tijd er vandaag werd doorgebracht op de toegewezen apparaten, hoeveel tijd er overschiet van de dagelijkse limiet en de status van het geselecteerde profiel, actief of gepauzeerd. Vanuit dit venster kunt u ook de tijdsbeperkingen instellen voor verschillende momenten van de dag, zoals bedtijd, huiswerk of privélessen.

Tijdsbeperkingen

Om de tijdsbeperkingen te configureren:

1. Klik op **OPTIES** en selecteer **Schermtijd**.
2. Klik in het gebied **Schema's** op **EEN SCHEMA TOEVOEGEN**.
3. Geef een naam aan het schema dat u wilt instellen (bijvoorbeeld, bedtijd, huiswerk, tennisles enz.).
4. Stel het tijdschema en de dagen voor de beperkingen in en klik op **TOEVOEGEN** om de instellingen op te slaan.

Om een beperking die u hebt ingesteld, te bewerken, gaat u naar de sectie Schema's, wijst u op de beperking die u wilt bewerken en klikt u op de knop **BEWERKEN**.

Om een beperking te verwijderen, gaat u naar het venster Schermtijd, wijst u op de beperking die u wilt bewerken, klikt u op **BEWERKEN** en selecteert u **SCHEMA VERWIJDEREN**.

Dagelijkse limiet

De dagelijkse gebruikslimiet kan worden toegepast op Windows-, macOS- en Android-apparaten. Indien u het profiel laat pauzeren wanneer de limiet wordt bereikt, dan wordt deze instelling toegepast op alle toegewezen apparaten, ongeacht of ze Windows-, macOS-, Android- of iOS-apparaten zijn.

Om een dagelijkse gebruikslimiet in te stellen:

1. Klik op **OPTIES** en selecteer **DAGELIJKSE TIJDSBEPERKINGEN INSTELLEN**.
2. Stel de tijd en de dagen voor de beperkingen in en klik op **WIJZIGINGEN OPSLAAN** om de instellingen op te slaan.

1.2.15. Apparaat antidiefstal

Diefstal van laptops is een groot probleem dat zowel individuen als organisaties treft. Meer nog dan het verlies van de hardware zelf, kunnen de gegevens die ermee verloren gaan aanzienlijke schade aanrichten, zowel financieel als emotioneel.

Toch nemen maar weinig mensen de juiste stappen om hun belangrijke persoonlijke, zakelijke en financiële gegevens te beveiligen in geval van diefstal of verlies.

Bitdefender Antidiefstal helpt u beter voorbereid te zijn op een dergelijke gebeurtenis door u in staat te stellen uw laptop op afstand te lokaliseren of te vergrendelen en zelfs alle gegevens ervan te wissen, mocht u ooit tegen uw wil afstand doen van uw laptop.

Om de functies van Antidiefstal te gebruiken, moet aan de volgende voorwaarden worden voldaan:

- De opdrachten kunnen alleen worden verzonden vanaf het Bitdefender-account.
- De laptop moet verbonden zijn met internet om de opdrachten te ontvangen.

Antidiefstalfuncties werken op de volgende manier:

bevind zich

Bekijk de locatie van uw apparaat op Google Maps.

De nauwkeurigheid van de locatie hangt af van hoe Bitdefender deze kan bepalen. De locatie wordt tot op tientallen meters nauwkeurig bepaald als

Wi-Fi is ingeschakeld op uw laptop en er draadloze netwerken binnen het bereik zijn.

Als de laptop is verbonden met een bekabeld LAN zonder beschikbare Wi-Fi-locatie, wordt de locatie bepaald op basis van het IP-adres, dat aanzienlijk minder nauwkeurig is.

Alarm

Stuur een waarschuwing op afstand op het apparaat.

De functie is alleen beschikbaar op mobiele apparaten.

Slot

Vergrendel uw laptop en stel een 4-cijferige pincode in om deze te ontgrendelen. Wanneer u de **Slot** opdracht, start het systeem opnieuw op en is inloggen op Windows alleen mogelijk na het invoeren van de door u ingestelde pincode.

Als u wilt dat Bitdefender foto's maakt van degene die toegang probeert te krijgen tot uw laptop, schakelt u het overeenkomstige selectievakje in. De gemaakte foto's worden gemaakt met de camera aan de voorzijde en samen met het tijdstempel weergegeven in het Anti-Theft-dashboard. Alleen de twee meest recente foto's worden opgeslagen.

Deze actie is alleen beschikbaar voor laptops met een camera aan de voorkant.

Veeg

Verwijder alle gegevens van uw systeem. Wanneer u de **Veeg** opdracht, start de laptop opnieuw op en worden de gegevens op alle partities op de harde schijf gewist.

Toon IP

Toont het laatste IP-adres voor het geselecteerde apparaat. Klik **TOON IP** om het zichtbaar te maken.

Antidiefstal wordt geactiveerd na de installatie en is uitsluitend toegankelijk via uw Bitdefender-account vanaf elk apparaat dat is verbonden met internet, waar dan ook.

Antidiefstalfuncties gebruiken

Gebruik een van de volgende mogelijkheden om toegang te krijgen tot de functies van Antidiefstal:

- Vanuit de hoofdinterface van Bitdefender:
  1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
  2. Klik **GA NAAR CENTRALE**.
     U wordt doorgestuurd naar de Bitdefender Central-pagina. Zorg ervoor dat u bent aangemeld met uw inloggegevens.
  3. Klik in het geopende Bitdefender Central-venster op de gewenste apparaatkaart en selecteer vervolgens **Anti diefstal**.

- Op elk apparaat met internettoegang:
  1. Open een webbrowser en ga naar: https://central.bitdefender.com.
  2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
  3. Selecteer de **Mijn apparaten** paneel.
  4. Klik op de gewenste apparaatkaart en selecteer vervolgens **Anti diefstal**.
  5. Selecteer de functie die u wilt gebruiken:
     bevind zich - geef de locatie van uw apparaat weer op Google Maps.
     Toon IP - geef het laatste IP-adres van uw apparaat weer.
     Alarm - stuur een waarschuwing op het apparaat.
     Slot - vergrendel uw laptop en stel een pincode in om deze te ontgrendelen.
     Veeg - verwijder alle gegevens van uw laptop.

     Belangrijk
     Nadat u een apparaat hebt gewist, werken alle functies van Antidiefstal niet meer.

1.3. Nutsvoorzieningen

1.3.1. profielen

Dagelijkse werkactiviteiten, films kijken of games spelen kan het systeem vertragen, met name wanneer ze tegelijkertijd worden uitgevoerd

met het Windows-updateproces en onderhoudstaken. Met Bitdefender kunt u nu uw voorkeursprofiel kiezen en toepassen. Het maakt systeemafstellingen om de prestaties van specifieke geïnstalleerde toepassingen te verbeteren.

Bitdefender verschaft de volgende profielen:

- werk profiel
- Film profiel
- Spelprofiel
- **Openbaar wifi-profiel**
- Batterijmodusprofiel

Als u besluit om **Profielen** niet te gebruiken, wordt er een standaardprofiel ingeschakeld genaamd **Standaard** dat geen optimalisering verschaft aan uw systeem.

Afhankelijk van uw activiteit worden de volgende productinstellingen toegepast als er Werk-, Film- of Gameprofielen geactiveerd zijn:

- Alle BitDefender waarschuwingen en pop-ups zijn uitgeschakeld.
- Automatische Update wordt uitgesteld.
- Geplande scans zijn uitgesteld.
- **Search Advisor** is uitgeschakeld.
- Meldingen bijzondere aanbiedingen zijn uitgeschakeld

Afhankelijk van uw activiteit worden de volgende systeeminstellingen toegepast als er Werk-, Film- of Gameprofielen geactiveerd zijn:

- Automatische Windows-updates zijn uitgesteld.
- Windows-waarschuwingen en pop-ups zijn uitgeschakeld.
- Onnodige programma's op de achtergrond worden gestaakt.
- Visuele effecten worden afgesteld voor de beste prestaties.
- Onderhoudstaken worden uitgesteld.
- Instellingen voor het vermogen worden aangepast.

Terwijl u in het Openbare Wi-Fi-profiel werkt, is Bitdefender Ultimate Security ingesteld om automatisch de volgende programma-instellingen uit te voeren:

- Geavanceerde bescherming tegen bedreigingen is ingeschakeld
- De volgende instellingen van Online Threat Prevention zijn ingeschakeld:
  - Versleutelde webscan
  - Bescherming tegen fraude
  - Bescherming tegen phishing

Werkprofiel

Meerdere taken uitvoeren op het werk, zoals het verzenden van e-mails, een videogesprek hebben met collega's op afstand of werken met designtoepassingen kan invloed hebben op uw systeemprestaties. Werkprofiel is ontworpen om u te helpen uw werkefficiëntie te verbeteren, door een aantal diensten op de achtergrond en onderhoudstaken uit te schakelen.

Werkprofiel configureren

Om de te ondernemen acties te configureren terwijl u in Werkprofiel zit:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de knop **CONFIGUREREN** in het gebied Werkprofiel.
4. Kies de afstellingen voor het systeem die u wilt toepassen door de volgende opties aan te vinken:
   - Prestaties boosten op werktoepassingen
   - Productinstellingen voor Werkprofiel optimaliseren
   - Programma's op de achtergrond en onderhoudstaken uitstellen
   - Automatische Windows-updates uitstellen
5. Klik op **OPSLAAN** om de wijzigingen op te slaan en het venster te sluiten.

Handmatig toepassingen toevoegen aan de lijst Werkprofiel

Indien Bitdefender niet automatisch naar Werkprofiel overschakelt wanneer u een bepaalde werktoepassing opstart, kunt u de toepassing handmatig toevoegen aan de **Werktoepassingenlijst**.

Om toepassingen handmatig toe te voegen aan de Werktoepassingenlijst in Werkprofiel:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de **CONFIGUREREN** knop in het gebied Werkprofiel.
4. Klik in het venster **Instellingen Werkprofiel** op **Toepassingenlijst**.
5. Klik op **TOEVOEGEN**.
   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de toepassing, selecteer het en klik op **OK** om het aan de lijst toe te voegen.

Filmprofiel

Het weergeven van videocontent in HD-kwaliteit, zoals HD-films, vereist belangrijke systeemvermogens. Filmprofiel stelt het systeem- en de productinstellingen af zodat u kunt genieten van een ononderbroken en vloeiende filmervaring.

Filmprofiel configureren

Om de te nemen handelingen te configureren terwijl u in Filmprofiel bent:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de knop **CONFIGUREREN** in het gebied Filmprofiel.
4. Kies de systeemaanpassingen die u wilt toepassen door de volgende opties aan te vinken:
   - ❍ Prestaties voor videospelers boosten
   - ❍ Productinstellingen voor Filmprofiel optimaliseren

- Stel achtergrondprogramma's en onderhoudstaken uit
- Stel automatische Windows-updates uit
- Instellingen vermogensplan voor films afstellen.

5. Klik **REDDEN** om de wijzigingen op te slaan en het venster te sluiten.

Handmatig videospelers toevoegen aan de lijst Filmprofiel

Indien Bitdefender niet automatisch naar Filmprofiel overschakelt wanneer u een bepaalde videospeler start, kunt u de toepassing handmatig toevoegen aan de **Filmtoepassingenlijst**.

Om videospelers handmatig toe te voegen aan de Filmtoepassingenlijst in Filmprofiel:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de **CONFIGUREREN** knop in het gebied Filmprofiel.
4. Klik in het venster **Instellingen Filmprofiel** op **Spelerslijst**.
5. Klik **TOEVOEGEN**.
   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de app, selecteer het en klik **OK** om het aan de lijst toe te voegen.

Gameprofiel

Genieten van een ononderbroken game-ervaring heeft alles te maken met het verminderen van systeemolaadtijden en het beperken van vertraging. Door gebruik te maken van gedragsheuristiek tegelijk met een lijst van bekende games, kan Bitdefender automatisch uitgevoerde games detecteren en uw systeemvermogen optimaliseren zodat u kunt genieten van uw gametijd.

Gameprofiel configureren

Om de te ondernemen acties te configureren terwijl u in Gameprofiel zit:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.

3. Klik op de knop **Configureren** in het gebied Gameprofiel.
4. Kies de systeemaanpassingen die u wilt toepassen door de volgende opties aan te vinken:
   - Prestaties voor games boosten
   - Productinstellingen voor Gameprofiel optimaliseren
   - Stel achtergrondprogramma's en onderhoudstaken uit
   - Stel automatische Windows-updates uit
   - Instellingen vermogensplan voor games afstellen.
5. Klik **REDDEN** om de wijzigingen op te slaan en het venster te sluiten.

Handmatig games aan de Spellijst toevoegen

Indien Bitdefender niet automatisch naar het Gameprofiel overschakelt wanneer u een bepaalde game of toepassing start, kunt u de toepassing handmatig toevoegen aan de **Gametoepassingenlijst**.

Om games handmatig aan de Gametoepassingenlijst toe te voegen in het Gameprofiel:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de **Configureren** knop in het spelprofielgebied.
4. Klik in het venster **Instellingen Gameprofiel** op **Spellijst**.
5. Klik **TOEVOEGEN**.
   Er verschijnt een nieuw venster. Blader naar het uitvoerbare bestand van de game, selecteer het en klik op **OK** om het aan de lijst toe te voegen.

Openbaar Wifi-profiel

E-mailberichten verzenden, gevoelige logingegevens invoeren of online winkelen terwijl u met onveilige draadloze netwerken verbonden bent, kan uw persoonlijke gegevens in gevaar brengen. Openbaar Wifi-profiel past de productinstellingen aan, zodat u online betalingen kunt uitvoeren en gevoelige informatie kunt gebruiken in een beveiligde omgeving.

Openbaar Wi-Fi-profiel configureren

Om Bitdefender te configureren zodat productinstellingen worden toegepast wanneer u verbonden bent met een onveilig draadloos netwerk:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de knop **CONFIGUREREN** in het gebied Openbaar Wi-Fi-profiel.
4. Laat het vakje **Pas de productinstellingen aan om de bescherming te stimuleren bij verbinding met een onveilig openbaar Wi-Fi-netwerk** aangevinkt.
5. Klik **Redden**.

Profiel Accumodus

Het profiel Accumodus is speciaal ontworpen voor laptop- en tabletgebruikers. Het doel ervan is om de invloed op vermogensverbruik van zowel het systeem als Bitdefender te beperken als het accuniveau lager is dan de standaardconsumptie van deze die u selecteert.

Profiel Accumodus aan het configureren

Om het profiel Accumodus te configureren:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Klik op de knop **Configureren** in het gebied Profiel Accumodus.
4. Kies de afstellingen voor het systeem die moeten worden toegepast door de volgende opties aan te vinken:
   - Productinstellingen voor Accumodus optimaliseren.
   - Programma's op de achtergrond en onderhoudstaken uitstellen.
   - Automatische Windows-updates uitstellen.
   - Instellingen vermogensplan voor Accumodus afstellen.
   - Externe apparaten en netwerkpoorten uitschakelen.

5. Klik **REDDEN** om de wijzigingen op te slaan en het venster te sluiten.

Tik een geldige waarde in het vakje in of selecteer er een met de pijltjes omhoog en om laag om in te stellen wanneer het systeem moet beginnen werken in Batterijmodus. Standaard is de modus geactiveerd als het accuniveau onder de 30% komt.

De volgende productinstellingen worden toegepast als Bitdefender in het profiel Accumodus handelt:

- Bitdefender Automatic Update is uitgesteld.
- Geplande scans worden uitgesteld.

Bitdefender detecteert wanneer uw laptop overschakelt op accuvoeding en afhankelijk van het accuniveau gaat het dan automatisch over op de Accumodus. Op dezelfde manier verlaat Bitdefender automatisch de Accumodus, als de laptop niet langer op de accu werkt.

Realtime Optimalisering

Bitdefender Real-Time Optimalisering is een plug-in die uw systeemprestaties geruisloos verbetert, op de achtergrond, en garandeert dat u niet wordt onderbroken terwijl u in een profielmodus bent. Afhankelijk van de CPU-belasting bewaakt de plug-in alle processen en richt zich op die processen die een hogere belasting aannemen om ze aan te passen aan uw behoeften.

Om Realtime-optimalisatie in of uit te schakelen:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. In de **profielen** tabblad, klik **Instellingen**.
3. Verrol naar beneden tot u de optie Optimalisatie in reële tijd ziet, en gebruik vervolgens de bijhorende schakelaar om deze in of uit te schakelen.

1.3.2. OneClick-optimalisatie

Problemen zoals defecte harde schijven, overgebleven registerbestanden en browsergeschiedenis kunnen uw werk vertragen, wat vervelend voor u kan worden. Al deze problemen kunnen nu met één enkele klik op de knop worden opgelost.

Met OneClick Optimizer kunt u nutteloze bestanden identificeren en verwijderen door meerdere opschoontaken tegelijkertijd uit te voeren.

Om het OneClick Optimizer-proces te starten:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. Klik op de **Optimaliseren** knop.
   a. **Analyseren**
   Wacht tot Bitdefender klaar is met zoeken naar systeemproblemen.
      - Schijfopruiming - identificeert onnodige bestanden en mappen.
      - Registeropruiming - identificeert ongeldige of verouderde referenties in het Windows-register.
      - Privacy Cleanup - identificeert tijdelijke internetbestanden en cookies, browsercache en geschiedenis.

   Het aantal gevonden problemen wordt weergegeven. Klik op de link Bekijk details om ze te bekijken voordat u doorgaat met het opschoonproces. Klik op Optimaliseren om door te gaan.

   b. **optimaliseren**
   Wacht tot Bitdefender klaar is met het optimaliseren van uw systeem.

   c. **Problemen**
   Hier kunt u het resultaat van de operatie bekijken.
   Als u uitgebreide informatie over het optimalisatieproces wilt, klikt u op de **Bekijk gedetailleerd rapport** knop.

1.3.3. Data bescherming

Bestanden definitief verwijderen

Wanneer u een bestand verwijdert, is het niet langer toegankelijk met de normale middelen. Het bestand blijft echter opgeslagen op de harde schijf tot het wordt overschreven wanneer nieuwe bestanden worden gekopieerd.

De Bitdefender File Shredder helpt u gegevens permanent te verwijderen door ze fysiek van uw harde schijf te verwijderen.

Volg deze stappen om bestanden of mappen snel permanent verwijderen van uw apparaat via het contextmenu van Windows:

1. Klik met de rechtermuisknop op het bestand of de map die u permanent wilt verwijderen.
2. Selecteer **Bitdefender > Bestandsvernietiging** in het contextmenu dat verschijnt.
3. Klik op **PERMANENT VERWIJDEREN** en bevestig dat u het proces wilt voortzetten.
   Wacht tot Bitdefender klaar is met het versnipperen van de bestanden.
4. De resultaten worden weergegeven. Klik op **BEËINDIGEN** om de wizard te verlaten.

U kunt bestanden ook vernietigen via de Bitdefender-interface, als volgt:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **Gegevensbeveiliging** op **Bestandsvernietiging**.
3. Volg de wizard Bestandsvernietiging:
   a. Klik op de knop **MAPPEN TOEVOEGEN** om de bestanden of mappen die u permanent wenst te verwijderen, toe te voegen.
      U kunt deze bestanden of mappen ook naar dit venster slepen.
   b. Klik op **PERMANENT VERWIJDEREN** en bevestig dat u het proces wilt voortzetten.
      Wacht tot Bitdefender klaar is met het versnipperen van de bestanden.
   c. **Overzicht van resultaten**
      De resultaten worden weergegeven. Klik **Finish** om de wizard af te sluiten.

1.4. Zo werkt het

1.4.1. Installatie

Hoe installeer ik Bitdefender op een tweede apparaat?

Indien de abonnement dat u hebt gekocht meer dan één apparaat dekt, kunt u uw Bitdefender-account gebruiken om een tweede pc te activeren.

Om Bitdefender op een tweede apparaat te installeren:

1. Klik op **Installeren op ander apparaat** in de linkerbenedenhoek van de **Bitdefender-interface**.
   Er verschijnt een nieuw venster op uw scherm.
2. Klik **DEEL DE DOWNLOADLINK**.
3. Volg de aanwijzingen op het scherm om Bitdefender te installeren.

Het nieuwe apparaat waarop u het Bitdefender-product hebt geïnstalleerd, zal op uw Bitdefender Central-bedieningspaneel verschijnen.

Hoe kan ik Bitdefender opnieuw installeren?

Typische situaties waarin u Bitdefender opnieuw moet installeren, zijn ondermeer de volgende:

- u hebt het besturingssysteem opnieuw geïnstalleerd..
- u wilt problemen oplossen die mogelijk voor vertragingen en crashes hebben gezorgd
- uw Bitdefender-product start of werkt niet naar behoren.

In het geval dat een van de vermelde situaties op u van toepassing is, volg dan deze stappen:

- In **Windows 7**:
  1. Klik **Begin** en ga naar **Alle programma's**.
  2. Zoek *Bitdefender Ultimate Security* en selecteer **De-installeren**.
  3. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
  4. U moet de apparaat opnieuw opstarten om het proces te voltooien.

- In **Windows 8** En **Windows 8.1**:
  1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  2. Klik op een programma **De-installeren** of **Programma's en Functies**.
  3. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
  4. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
  5. U moet het apparaat opnieuw opstarten om het proces te voltooien.

- In **Windows 10** En **Windows 11**:
  1. Klik op **Start**, klik dan op **Instellingen**.
  2. Klik op het **Systeem**-pictogram in Instellingen, selecteer dan **Apps & functies**.
  3. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
  4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
  5. Klik op **HERINSTALLEREN**.
  6. U moet het apparaat opnieuw opstarten om het proces te voltooien.

  Opmerking
  Als u deze procedure voor opnieuw installeren volgt, worden persoonlijke instellingen opgeslagen, die in het nieuw geïnstalleerde product ook beschikbaar blijven. Andere instellingen kunnen teruggesteld worden naar hun fabrieksconfiguratie.

Waar kan ik mijn Bitdefender-product downloaden?

U kunt Bitdefender installeren vanaf de installatiedisk of via de web installer die u naar uw computer kunt downloaden vanaf uw apparaat via het Bitdefender Central-platform.

> **Opmerking**
> Voordat u de kit uitvoert, raden we aan om beveiligingsoplossingen die op uw systeem zijn geïnstalleerd, te verwijderen. Wanneer u meer dan één beveiligingsoplossing op dezelfde apparaat gebruikt, wordt het systeem onstabiel.

Om Bitdefender te installeren vanuit Bitdefender Central:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel en klik vervolgens op **INSTALLEER BESCHERMING**.
3. Kies een van de twee beschikbare opties:
   - **Bescherm dit apparaat**
     Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.
   - **Bescherm andere apparaten**
     Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.
     Klik **STUUR DOWNLOADLINK**. Typ een e-mailadres in het overeenkomstige veld en klik **STUUR E-MAIL**. Houd er rekening mee dat de gegenereerde downloadlink alleen de komende 24 uur geldig is. Als de link verloopt, moet u een nieuwe genereren door dezelfde stappen te volgen.
     Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailaccount dat u hebt ingevoerd en klik vervolgens op de overeenkomstige downloadknop.
4. Start het gedownloade Bitdefender-programma.

Hoe gebruik ik mijn Bitdefender-abonnement na een Windows-upgrade?

Deze situatie doet zich voor wanneer u uw besturingssysteem upgrade en verder wilt gaan met het gebruik van uw Bitdefender-abonnement.

Als u een vorige Bitdefender-versie gebruikt, kunt u gratis upgraden naar de nieuwste Bitdefender, als volgt:

- Van een vorige Bitdefender Antivirusversie naar de nieuwste Bitdefender Antivirus die beschikbaar is.
- Van een vorige Bitdefender Internet Security versie naar de nieuwste Bitdefender Internet Security die beschikbaar is.
- Van een vorige Bitdefender Total Security versie naar de nieuwste Bitdefender Total Security die beschikbaar is.

Er kunnen zich twee gevallen voordoen:

- U hebt het besturingssysteem bijgewerkt met gebruikmaking van Windows Update en u merkt dat Bitdefender niet langer werkt.
  Installeer het product in dit geval opnieuw door de volgende stappen te volgen:
  - In **Windows 7**:
    1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
    2. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
    3. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
    4. Wacht tot het verwijderen is voltooid en start vervolgens uw systeem opnieuw op.
       Open de interface van uw nieuw geïnstalleerde Bitdefender-product om toegang te krijgen tot de functies ervan.
  - In **Windows 8** En **Windows 8.1**:
    1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
    2. Klik op **Een programma de-installeren** of **Programma's en Functies**.
    3. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
    4. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
    5. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

Open de interface van uw nieuw geïnstalleerde Bitdefender-product om toegang te krijgen tot de functies ervan.

- In **Windows 10** En **Windows 11**:
  1. Klik **Begin**, dan klikken **Instellingen**.
  2. Klik in het gebied Instellingen op het pictogram **Systeem** en selecteer dan **Apps**.
  3. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
  4. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.
  5. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
  6. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.
     Open de interface van uw nieuw geïnstalleerde Bitdefender-product om toegang te krijgen tot de functies ervan.

  > **Opmerking**
  > Door deze herinstallatieprocedure te volgen, worden aangepaste instellingen opgeslagen en beschikbaar in het nieuw geïnstalleerde product. Andere instellingen kunnen worden teruggeschakeld naar hun standaardconfiguratie.

- U hebt uw systeem gewijzigd en u wilt doorgaan met het gebruik van de beveiliging van Bitdefender. Daarvoor moet u het product opnieuw installeren met gebruikmaking van de nieuwste versie.
  Om dit probleem op te lossen:
  1. Download het installatiebestand:
     a. Toegang Bitdefender Centraal.
     b. Selecteer de **Mijn apparaten** paneel en klik vervolgens op **INSTALLEER BESCHERMING**.
     c. Kies een van de twee beschikbare opties:
        - **Bescherm dit apparaat**
          Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.

- **Een ander apparaat beschermen**
  Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.
  Klik **STUUR DOWNLOADLINK**. Typ een e-mailadres in het overeenkomstige veld en klik **STUUR E-MAIL**. Houd er rekening mee dat de gegenereerde downloadlink alleen de komende 24 uur geldig is. Als de link verloopt, moet u een nieuwe genereren door dezelfde stappen te volgen.
  Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailaccount dat u hebt ingevoerd en klik vervolgens op de overeenkomstige downloadknop.

2. Voer het Bitdefender-product uit dat u hebt gedownload.

Raadpleeg Uw Bitdefender-product installeren (pagina 6) voor meer informatie over het Bitdefender-installatieproces.

Hoe kan ik upgraden naar de recentste Bitdefender-versie?

Vanaf nu kunt u naar de nieuwste versie upgraden zonder de handmatige de-installatie- en installatie-procedures te volgen. Het nieuwe product, wordt meer bepaald samen met nieuwe functies en ingrijpende verbeteringen in het product, geleverd via productupdate en als u al een actieve Bitdefender-abonnement hebt, wordt het product automatisch geactiveerd.

Indien u de versie van 2020 gebruikt, kunt u naar de nieuwste versie upgraden aan de hand van de volgende stappen:

1. Klik op **NU OPNIEUW OPSTARTEN** in de kennisgeving die u ontvangt met de upgrade-informatie. Als u deze gemist hebt, ga naar het venster **Kennisgevingen**, ga naar de recentste update en klik vervolgens op de knop **NU OPNIEUW OPSTARTEN**. Wacht totdat het apparaat opnieuw is opgestart.
   Het venster **Wat is er nieuw** verschijnt, met informatie over de verbeterde en nieuwe functies.
2. Klik op de koppelingen **Meer weten** om doorgestuurd te worden naar de specifieke pagina, met meer informatie en nuttige artikels.

3. Sluit het venster **Wat is er nieuw** om naar de interface van de nieuw geïnstalleerde versie te gaan.

Gebruikers die gratis willen upgraden van Bitdefender 2016 of een lagere versie naar de nieuwste Bitdefender-versie moeten hun huidige versie verwijderen uit het controlepaneel en vervolgens het recentste installatiebestand downloaden via de Bitdefender-website op het volgende adres: https://www.bitdefender.com/Downloads/. De activatie is enkel mogelijk met een geldig abonnement.

1.4.2. Bitdefender Centraal

Hoe meldt u zich met een andere account aan voor Bitdefender-account?

U hebt een nieuwe Bitdefender-account aangemaakt en u wilt deze van nu af aan gebruiken.

Om succesvol in te loggen met een andere Bitdefender-account:

1. Klik op uw accountnaam in het bovenste gedeelte van de **Bitdefender-interface**.
2. Klik in de rechterbovenhoek van het scherm op **Account wisselen** om de account gelinkt aan de apparaat te wisselen.
3. Typ het e-mailadres in het overeenkomstige veld en klik vervolgens op **VOLGENDE**.
4. Typ uw wachtwoord en klik vervolgens op **AANMELDEN**.

> **Opmerking**
> Het Bitdefender-product van uw toestel verandert automatisch volgens het abonnement dat verbonden is met de nieuwe Bitdefender-account. Als er geen beschikbaar abonnement gekoppeld is aan de Bitdefender-account, of als u deze wilt overzetten naar de vorige account, kunt u contact opnemen met Bitdefender voor ondersteuning, zoals beschreven in deel Hulp vragen (pagina 307).

Hoe schakel ik Bitdefender Central-hulpberichten uit?

Om u te helpen begrijpen waar elke optie in Bitdefender Central nuttig voor is, worden hulpberichten op de overzichtspagina weergegeven.

Indien u deze berichten niet meer wil zien:

1. Toegang Bitdefender Centraal.
2. Klik op de pictogram in de rechterbovenhoek van het scherm.
3. Klik op **Mijn account** in het schuifmenu.
4. Klik op **Instellingen** in het schuifmenu.
5. Schakel de optie **Hulpberichten in/uitschakelen** uit.

Ik ben het wachtwoord dat ik voor mijn Bitdefender-account heb gekozen, vergeten. Hoe kan ik het terugstellen?

Er zijn twee mogelijkheden om een nieuw wachtwoord in te stellen voor uw Bitdefender-account:

- Van de Bitdefender-interface:
  1. Klik **Mijn rekening** in het navigatiemenu op de Bitdefender-interface.
  2. Klik in de rechterbovenhoek van het scherm op **Account wisselen**.
     Er verschijnt een nieuw venster.
  3. Voer uw e-mailadres in en klik op **VOLGENDE**.
     Er verschijnt een nieuw venster.
  4. Klik **Wachtwoord vergeten?**.
  5. Klik op **VOLGENDE**.
  6. Controleer uw e-mailaccount, typ de beveiligingscode die u hebt ontvangen en klik vervolgens op **VOLGENDE**.
     U kunt ook klikken **Verander wachtwoord** in de e-mail die we u hebben gestuurd.
  7. Typ het nieuwe wachtwoord dat u wilt instellen en typ het nogmaals. Klik **REDDEN**.

- Vanuit uw webbrowser:
  1. Ga naar: https://central.bitdefender.com.
  2. Klik op **AANMELDEN**.
  3. Typ uw e-mailadres en klik vervolgens op **VOLGENDE**.
  4. Klik **Wachtwoord vergeten?**.
  5. Klik **VOLGENDE**.

6. Controleer uw e-mailaccount en volg de instructies om een nieuw wachtwoord in te stellen voor uw Bitdefender-account.

Om naar uw Bitdefender-account te gaan tikt u voortaan uw e-mailadres en het wachtwoord in dat u net ingesteld hebt.

Hoe kan ik de aanmeldsessies van mijn Bitdefender-account beheren?

In uw Bitdefender-account kunt u de recentste inactieve en actieve aanmeldsessies op de apparaten van uw account bekijken. Bovendien kunt u van op afstand afmelden via deze stappen:

1. Toegang Bitdefender Centraal.
2. Klik op de pictogram in de rechterbovenhoek van het scherm.
3. Klik op **Instellingen** in het schuifmenu.
4. Selecteer in het gebied **Actieve sessies** de optie **AFMELDEN** naast het apparaat waar u de aanmeldsessie wenst stop te zetten.

1.4.3. Scannen met BitDefender

Een bestand of map scannen

De eenvoudigste manier om een bestand of map te scannen is klikken met de rechtermuisknop op het object dat u wilt scannen, Bitdefender aanwijzen en **Scannen met Bitdefender** te selecteren in het menu.

Volg de Antivirusscanwizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden.

Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen.

Typische situaties voor het gebruik van deze scanmethode zijn ondermeer de volgende:

- U vermoedt dat een specifiek bestand of een specifieke map geïnfecteerd is.
- Wanneer u bestanden waarvan u denkt dat ze mogelijk gevaarlijk zijn, downloadt van Internet.

- Scan een netwerkshare voordat u bestanden naar uw apparaat kopieert.

Hoe kan ik mijn systeem scannen

Om een volledige scan van het systeem uit te voeren:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik op de knop **Scan uitvoeren** naast **Systeemscan**.
4. Volg de Systeemscanwizard om de scan te voltooien. Bitdefender zal automatisch de aanbevolen acties ondernemen op de gedetecteerde bestanden.
   Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen. Zie voor meer informatie.

Hoe plan ik een scan?

U kunt uw Bitdefender-product instellen om belangrijke systeemlocaties te beginnen scannen wanneer u niet voor de apparaat zit.

Een scan plannen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het onderste gedeelte van de interface op ⋯ naast het scantype dat u wilt inplannen, Systeemscan of Snelle scan, en selecteer vervolgens **Bewerken**.
   U kunt ook een scantype maken dat bij uw noden past, door te klikken op **+Scan aanmaken** naast **Scans beheren**.
4. Pas de scan aan in overeenkomst met uw noden, en klik op **Volgende**.
5. Vink het vakje naast **Kiezen wanneer deze taak wordt ingepland** aan. Selecteer een van de overeenkomstige opties om een planning in te stellen:
   - Bij het opstarten van het systeem
   - Dagelijks
   - Wekelijks

- Maandelijks

  Als u Dagelijks, Maandelijks of Wekelijks kiest, sleept u de schuifregelaar langs de schaal om de gewenste periode in te stellen wanneer de geplande scan moet starten.

Het venster **Scantaak** verschijnt als u ervoor kiest een nieuwe aangepaste scan aan te maken. Hier kunt u de locaties selecteren die u wilt laten scannen.

Een aangepaste scantaak maken

Als u specifieke locaties wilt scannen op uw apparaat of de scanopties wilt configureren, kunt u een aangepaste scantaak configureren en uitvoeren.

Ga als volgt te werk om een aangepaste scantaak te maken:

1. In de **ANTIVIRUS** paneel, klik **Open**.
2. Klik op **+Scan aanmaken** naast **Scans beheren**.
3. Voer in het veld Taaknaam een naam in voor de scan, selecteer vervolgens de locaties die u wilt laten scannen en klik op **VOLGENDE**.
4. Configureer deze algemene opties:
   - **Scan alleen toepassingen**. U kunt Bitdefender instellen om alleen geopende apps te scannen.
   - **Prioriteit scantaak**. U kunt kiezen welke impact een scanprocedure mag hebben op de prestaties van uw systeem.
     - Auto - De prioriteit van het scanproces hangt af van de systeemactiviteit. Om ervoor te zorgen dat het scanproces geen invloed heeft op de systeemactiviteit, zal Bitdefender beslissen of het scanproces met hoge of lage prioriteit moet worden uitgevoerd.
     - Hoog - De prioriteit van het scanproces is hoog. Door deze optie te kiezen, laat u andere programma's langzamer werken en verkort u de tijd die nodig is om het scanproces te voltooien.
     - Laag - De prioriteit van het scanproces is laag. Door deze optie te kiezen, kunt u andere programma's sneller laten werken en zal het scanproces langer duren.
   - **Acties na het scannen**. Kies welke actie Bitdefender moet ondernemen als er geen bedreigingen zijn gevonden:

- Samenvattingsvenster tonen
- Apparaat uitschakelen
- Sluit het scanvenster

5. Als u de scanopties in detail wilt configureren, klikt u op **Geavanceerde opties weergeven**.
   Klik **Volgende**.
6. U kunt de optie **Scantaak inplannen** inschakelen als u dat wenst. Vervolgens kiest u wanneer de aangepaste taak die u hebt gemaakt, moet worden gestart.
   - Bij het opstarten van het systeem
   - Dagelijks
   - Maandelijks
   - Wekelijks

   Als u Dagelijks, Maandelijks of Wekelijks kiest, sleept u de schuifregelaar langs de schaal om de gewenste periode in te stellen wanneer de geplande scan moet starten.
7. Klik **Redden** om de instellingen op te slaan en het configuratievenster te sluiten.
   Afhankelijk van de te scannen locaties kan de scan even duren. Als er tijdens het scanproces bedreigingen worden gevonden, wordt u gevraagd om de acties te kiezen die op de gedetecteerde bestanden moeten worden ondernomen.

Als u dat wenst, kunt u snel een eerdere aangepaste scan opnieuw uitvoeren door in de beschikbare lijst te klikken.

Hoe sluit ik een map uit van de scan?

Met Bitdefender kunt u specifieke bestanden, mappen of bestandsextensies uitsluiten van het scannen.

Uitsluitingen zijn bedoeld voor gebruikers met een gevorderde computerkennis en alleen in de volgende situaties:

- U hebt een grote map op uw systeem waarin u films en muziek bewaart.

- U hebt een groot archief op uw systeem waarin u verschillende gegevens bewaart.
- U bewaart een map waarin u verschillende types software en toepassingen installeert voor testdoeleinden. Het scannen van de map kan resulteren in het verlies van bepaalde gegevens.

Om een map toe te voegen aan de Uitzonderingenlijst:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik op het tabblad **Instellingen**.
4. Klik op **Uitzonderingen beheren**.
5. Klik **+Voeg een uitzondering toe**.
6. Voer het pad in van de map die u wilt uitsluiten van scannen in het overeenkomstige veld.
   U kunt ook naar de map navigeren door op de bladerknop aan de rechterkant van de interface te klikken, deze te selecteren en op te klikken **OK**.
7. Zet de schakelaar aan naast de beveiligingsfunctie die de map niet mag scannen. Er zijn drie opties:
   - Antivirus
   - Preventie van online bedreigingen
   - Geavanceerde bescherming tegen bedreigingen
8. Klik **Redden** om de wijzigingen op te slaan en het venster te sluiten.

Wat moet ik doen wanneer Bitdefender een schoon bestand als geïnfecteerd beschouwt?

Er kunnen zich gevallen voordoen waarin Bitdefender een legitiem bestand ten onrechte als een bedreiging labelt (een vals positief). Om deze fout te corrigeren, voegt u het bestand toe aan het gebied van de Bitdefender-uitzonderingen:

1. Schakel de real time-antivirusbeveiliging van Bitdefender uit.
   a. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.

b. In de **ANTIVIRUS** paneel, klik **Open**.

c. Schakel in het venster **Geavanceerd Bitdefender Shield** uit.
Er verschijnt een waarschuwingsvenster. U moet uw keuze bevestigen door in het menu te selecteren hoelang u de real time-beveiliging wilt uitschakelen. U kunt de real time-beveiliging uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot een systeem opnieuw wordt opgestart.

2. Verborgen objecten weergeven in Windows. Om te weten hoe u dit kunt doen, ga naar Verborgen objecten weergeven in Windows (pagina 130).
3. Het bestand herstellen vanaf het quarantainegebied:
   a. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
   b. In de **ANTIVIRUS** paneel, klik **Open**.
   c. Ga naar het venster **Instellingen** op klik op **Quarantaine beheren**.
   d. Selecteer het bestand en klik op **HERSTEL**.
4. Voeg het bestand toe aan de Uitzonderingenlijst.
5. Schakel de real time antivirusbeveiliging van Bitdefender in.
6. Neem contact op met de medewerkers van onze ondersteuningsdienst zodat wij de detectie van de update van de bedreigingsinformatie kunnen verwijderen. Om te weten hoe u dit kunt doen, ga naar Hulp vragen (pagina 307).

Hoe kan ik controleren welke bedreigingen Bitdefender heeft gedetecteerd?

Telkens wanneer een scan wordt uitgevoerd, wordt een scanlogboek gemaakt en registreert Bitdefender de verwijderde problemen.

Het scanlog bevat gedetailleerde informatie over het gevolgde scanproces, zoals de scanopties, het scandoel, de gevonden bedreigingen en de hierop uitgevoerde acties.

U kunt het scanlogboek rechtstreeks vanuit de scanwizard openen, zodra de scan is voltooid, door op te klikken **TOON LOGBOEK**.

Een scanlogboek of een gedetecteerde infectie op een later tijdstip controleren:

1. Klik **Meldingen** in het navigatiemenu op de Bitdefender-interface.
2. In de **Alle** selecteer op het tabblad de melding over de laatste scan.
   Hier kunt u alle bedreigingsscangebeurtenissen vinden, inclusief bedreigingen die zijn gedetecteerd door scannen bij toegang, door de gebruiker gestarte scans en statuswijzigingen voor automatische scans.
3. In de notificatielijst kunt u zien welke scans recentelijk zijn uitgevoerd. Klik op een melding om er details over te bekijken.
4. Klik op **Logboek weergeven** om het scanlogboek te openen.

1.4.4. Ouderlijk toezicht

Mijn kinderen beschermen tegen online bedreigingen

Met Ouderlijk Toezicht van Bitdefender kunt u de toegang tot het internet en specifieke toepassingen beperken en voorkomen dat uw kinderen ongepaste inhoud bekijken wanneer u niet in de buurt bent.

Om Ouderlijk Toezicht te configureren:

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
2. In de **OUDERLIJK TOEZICHT** paneel, klik **Configureren**.
   U wordt doorgestuurd naar de Bitdefender-accountwebpagina. Zorg ervoor dat u bent aangemeld met uw inloggegevens.
3. Het dashboard van Ouderlijk toezicht wordt geopend. Hier kunt u de instellingen voor Ouderlijk toezicht controleren en configureren.
4. Klik op **KINDPROFIEL TOEVOEGEN**.
5. Stel specifieke informatie in, zoals naam, geboortedatum of geslacht. Om een foto toe te voegen aan het profiel van uw kind, klikt u op de pictogram in de rechterbenedenhoek van het **Profielfoto** keuze. Klik **REDDEN** doorgaan.
   Gebaseerd op de ontwikkelingsnormen van kinderen, worden door het instellen van de geboortedatum van het kind automatisch instellingen geladen voor zoeken op internet die geschikt worden geacht voor zijn leeftijdscategorie.
6. Klik **LATEN WE EEN APPARAAT TOEVOEGEN**.
7. Als op het apparaat van uw kind al een Bitdefender-product is geïnstalleerd, selecteert u zijn apparaat in de beschikbare lijst en

selecteert u vervolgens het account dat u wilt controleren. Klik **TOEWIJZEN**.

Belangrijk

Op Windows- en macOS-gebaseerde apparaten waarop geen Bitdefender-product is geïnstalleerd, wordt de Bitdefender Parental Control monitoring-tracker geïnstalleerd zodat u de online activiteiten van uw kinderen kunt volgen.

Op Android- en iOS-apparaten wordt de app Ouderlijk toezicht van Bitdefender gedownload en geïnstalleerd.

Hoe blokkeer ik de toegang van mijn kind tot een website?

Via Ouderlijk Toezicht van Bitdefender kunt u de inhoud die uw kind bekijkt met zijn of haar apparaat controleren en de toegang tot een website blokkeren.

Om de toegang tot een website te blokkeren, moet u deze als volgt toevoegen aan de Uitzonderingenlijst:

1. Ga naar: https://central.bitdefender.com.
2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Klik op **Ouderlijk toezicht** om het dashboard te openen.
4. Selecteer het profiel van uw kind.
5. Klik op het tabblad **OPTIES** en selecteer **Websites**.
6. Klik op **BEHEREN**.
7. Voer de website die u wilt blokkeren in het overeenkomstige veld in.
8. Selecteer **Blokkeren**.
9. Klik op het pictogram om de wijzigingen op te slaan en klik dan op **GEREED**.

Opmerking

Er kunnen enkel beperkingen voor Android-, macOS- en Windows-apparaten worden ingesteld.

Hoe vermijd ik dat mijn kind bepaalde toepassingen gebruikt?

Met Ouderlijk Toezicht van Bitdefender hebt u het beheer over de inhoud waar uw kinderen toegang toe hebben met hun apparaten.

Om de toegang tot een toepassing te blokkeren:

1. Ga naar: https://central.bitdefender.com.
2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Klik **Ouderlijk toezicht** om toegang te krijgen tot het dashboard.
4. Selecteer een kinderprofiel.
5. Klik op **OPTIES** en selecteer **Toepassingen**.
6. Er wordt een lijst met de toegewezen apparaten weergegeven. Selecteer de kaart met het apparaat waarop u de app-toegang wilt beperken.
7. Klik **Beheer de apps die worden gebruikt door...**.
8. Selecteer **Geblokkeerd** naast de apps waarvan je wilt dat je kind stopt met gebruiken.
9. Klik **REDDEN** om de nieuwe instelling toe te passen.

> **Opmerking**
> Beperkingen kunnen alleen worden ingesteld voor Android-, macOS- en Windows-apparaten.

Hoe kan ik een lokatie als veilig of beperkt instellen voor mijn kind?

Met Ouderlijk Toezicht van Bitdefender kunt u een locatie als veilig of beperkt instellen voor uw kind.

Een locatie instellen:

1. Ga naar: https://central.bitdefender.com.
2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Klik **Ouderlijk toezicht** om toegang te krijgen tot het dashboard.
4. Selecteer het profiel van uw kind.
5. Klik op **OPTIES** en selecteer **Locatie kind**.

6. Klik op **Apparaten** in het rooster van het **Locatie kind**-venster.
7. Klik op het apparaat dat u wilt configureren.
8. In de **Gebieden** venster, klik op de **GEBIED TOEVOEGEN** knop.
9. Kies het type locatie, **VEILIG** of **BEPERKT**.
10. Tik een geldige naam in voor het gebied waar uw kind al dan niet toegang toe heeft.
11. Stel het bereik in dat moet worden toegepast voor monitoring vanaf de **Straal** schuifbalk.
12. Klik op **GEBIED TOEVOEGEN** om uw instellingen op te slaan.

Wanneer u een beperkte locatie als veilig wilt instellen, of een veilige locatie als beperkt, klikt u erop en kiest u vervolgens de knop **GEBIED BEWERKEN**. Afhankelijk van de wijziging die u wilt aanbrengen, selecteert u de optie **VEILIG** of de optie **BEPERKT** en klikt u vervolgens op **GEBIED UPDATEN**.

Hoe blokkeer ik voor mijn kind de toegang tot toegekende apparaten tijdens dagelijkse activiteiten?

Via Ouderlijk Toezicht van Bitdefender kunt u voor uw kind de toegang tot toegekende apparaten beperken tijdens dagelijkse activiteiten, zoals schooluren, wanneer uw kind huiswerk zou moet maken of wanneer uw kind zou moeten slapen.

Om nieuwe tijdsbeperkingen toe te voegen:

1. Ga naar: https://central.bitdefender.com.
2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Klik **Ouderlijk toezicht** om toegang te krijgen tot het dashboard.
4. Selecteer het profiel van het kind waarvoor u beperkingen wilt instellen.
5. Klik **OPTIES** en selecteer **Scherm tijd**.
6. Klik in het gebied **Schema's** op **Een schema toevoegen**.
7. Geef een naam aan de beperking die u wilt instellen (bijvoorbeeld, bedtijd, huiswerk, tennisles enz.).

8. Stel het tijdsbestek en de dagen in waarop de beperkingen moeten worden toegepast en klik vervolgens op **SCHEMA TOEVOEGEN** om de instellingen op te slaan.

Hoe blokkeer ik voor mijn kind de toegang tot de toegekende apparaten 's nachts of overdag?

Via Ouderlijk toezicht van Bitdefender kunt u voor uw kind de toegang tot de toegekende apparaten op verschillende momenten gedurende de dag beperken.

Om een beperking voor dagelijks gebruik in te stellen:

1. Ga naar: https://central.bitdefender.com.
2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Klik **Ouderlijk toezicht** om toegang te krijgen tot het dashboard.
4. Selecteer het profiel van het kind waarvoor u beperkingen wilt instellen.
5. Klik **OPTIES** en selecteer **Scherm tijd**.
6. Klik in het gebied **Dagelijkse tijdsbeperkingen** op **DAGELIJKSE TIJDSBEPERKINGEN INSTELLEN**.
7. Stel de tijd en dagen in waarop de beperkingen moeten worden toegepast en klik vervolgens op **WIJZIGINGEN OPSLAAN** om de instellingen op te slaan.

Hoe kan een kindprofiel worden verwijderd

Indien u een bestaand kindprofiel wenst te verwijderen:

1. Ga naar: https://central.bitdefender.com.
2. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
3. Klik **Ouderlijk toezicht** om toegang te krijgen tot het dashboard.
4. Selecteer het kindprofiel dat u wilt verwijderen.
5. Klik op **OPTIES** en selecteer **Profiel verwijderen**.
6. Bevestig uw keuze.

1.4.5. Privacybeheer

Hoe kan ik controleren of mij online transactie beveiligd is?

Als u wilt controleren of uw online bewerkingen privé blijven, kunt u de browser die door Bitdefender is geleverd, gebruiken voor het beschermen van uw transacties en toepassingen voor thuisbankieren.

Bitdefender Safepay™ is een beveiligde browser die is ontwikkeld om uw creditcardgegevens, accountnummer of enige andere vertrouwelijke gegevens die u mogelijk invoert wanneer u verschillende online locaties bezoekt, te beschermen.

Uw online activiteit veilig en privé houden:

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.
2. In de **VEILIG** paneel, klik **Instellingen**.
3. In de **Veilig betalen** venster, klik **Start Safepay**.
4. Klik op de knop om het **Virtuele toetsenbord** te openen.
   Gebruik het **virtuele toetsenbord** wanneer u vertrouwelijke informatie, zoals uw wachtwoorden, invoert.

Wat kan ik doen als mijn apparaat gestolen is?

Diefstal van mobiele apparaten, of het nu om een smartphone, tablet of laptop gaat, is een van de belangrijkste problemen tegenwoordig die particulieren en organisaties over de hele wereld treft.

Met Bitdefender Antidiefstal kunt u niet alleen het gestolen apparaat zoeken en vergrendelen, maar kunt u ook alle gegevens wissen om zeker te zijn dat ze niet worden gebruikt door de dief.

Naar de antidiefstalfuncties gaan vanaf uw account:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel.
3. Klik op de gewenste toestelkaart en selecteer vervolgens **Antidiefstal**.
4. Selecteer de functie die u wilt gebruiken:
   - **LOKALISEREN** - geef de lokatie van uw apparaat weer op Google Maps.

Toon IP - geeft het laatste IP-adres voor het geselecteerde apparaat weer.

- **Waarschuwing** - een waarschuwing op het apparaat verzenden.
- **Vergrendelen** - vergrendel uw apparaat en stel een numerieke pincode in om het te ontgrendelen. U kunt ook de overeenstemmende optie inschakelen om Bitdefender toe te staan snapshots te maken van de persoon die toegang probeert te krijgen tot uw apparaat.
- **Wissen** - alle gegevens van uw apparaat verwijderen.

> **Belangrijk**
> Nadat u een apparaat hebt gewist, werken de functies van Anti-Theft niet langer.

Hoe kan ik een bestand definitief verwijderen met Bitdefender?

Als u een bestand definitief van uw systeem wilt verwijderen, moet u de gegevens fysiek verwijderen van uw harde schijf.

Met de Bestandsvernietiger van Bitdefender kunt u bestanden of mappen op uw apparaat snel versnipperen met het contextmenu van Windows, door de volgende stappen te volgen:

1. Klik met de rechtermuisknop op het bestand of de map die u definitief wilt verwijderen, wijs Bitdefender aan en selecteer **Bestandsvernietiging**.
2. Klik **permanent verwijderen**en bevestig vervolgens dat u door wilt gaan met het proces.
   Wacht tot Bitdefender klaar is met het versnipperen van de bestanden.
3. De resultaten worden weergegeven. Klik op **BEËINDIGEN** om de wizard te verlaten.

Hoe zorg ik ervoor dat mijn webcam niet gehackt wordt?

U kunt uw Bitdefender-product zo instellen dat u de toegang van geïnstalleerde toepassingen tot uw webcam kunt weigeren of toestaan. Volg hiervoor deze stappen:

1. Klik **Privacy** in het navigatiemenu op de Bitdefender-interface.

2. In de **VIDEO- & AUDIOBESCHERMING** paneel, klik **Instellingen**.
3. Ga naar het venster **Webcambescherming**. U ziet er een lijst met de apps die toegang tot uw camera hebben verzocht.
4. Wijs op de app die u wilt toestaan of waarvoor u de toegang wilt weigeren, en klik vervolgens op de schakelaar ernaast, voorgesteld door een videocamera.

   Klik op het pictogram om te zien wat de andere Bitdefender-gebruikers met de geselecteerde app hebben gedaan. U wordt gewaarschuwd telkens wanneer een van de vermelde apps wordt geblokkeerd door de Bitdefender-gebruikers.

Om manueel toepassingen aan deze lijst toe te voegen, klikt op de knop **Toepassing toevoegen** en selecteert u een van beide opties.

- Van Windows Store
- Van uw apps

Hoe kan ik versleutelde bestanden handmatig herstellen wanneer het herstelproces faalt?

Indien de versleutelde bestanden niet automatisch worden hersteld, kunt u ze handmatig herstellen aan de hand van de volgende stappen:

1. Klik **Meldingen** in het navigatiemenu op de Bitdefender-interface.
2. In de **Alle** Selecteer op het tabblad de melding over het laatste gedetecteerde ransomware-gedrag en klik vervolgens op **Versleutelde bestanden**.
3. De lijst met de versleutelde bestanden wordt weergegeven.
   Klik op **BESTANDEN HERSTELLEN** om verder te gaan.
4. Als het gehele of een deel van het herstelproces mislukt, moet u de locatie kiezen waar de gedecodeerde bestanden moeten worden opgeslagen. Klik **Locatie herstellen**en kies vervolgens een locatie op uw pc.
5. Er verschijnt een bevestigingsvenster.
   Klik **Finish** om het herstelproces te beëindigen.

Bestanden met de volgende extensies kunnen worden hersteld als ze versleuteld worden:

.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;

1.4.6. Optimalisatietools

Hoe verbeter ik mijn systeemprestaties?

De systeemprestaties zijn niet alleen afhankelijk van de hardwareconfiguratie, zoals de CPU-belasting, het geheugengebruik en de ruimte op de harde schijf. Het staat ook direct in verbinding met uw softwareconfiguratie en met uw databeheer.

Dit zijn de belangrijkste acties die u met Bitdefender kunt ondernemen om de snelheid en prestaties van uw systeem te verbeteren:

- ❍ Optimaliseer uw systeemprestaties met een enkele klik (pagina 123)
- ❍ Scan uw systeem regelmatig (pagina 123)

Optimaliseer uw systeemprestaties met een enkele klik

De OneClick Optimizer-optie bespaart u waardevolle tijd wanneer u een snelle manier wilt om uw systeemprestaties te verbeteren door nutteloze bestanden snel te scannen, detecteren en opschonen.

Om het OneClick Optimizer-proces te starten:

1. Klik **Nutsvoorzieningen** in het navigatiemenu op de Bitdefender-interface.
2. Klik op de **Optimaliseren** knop.
3. Laat Bitdefender zoeken naar bestanden die kunnen worden verwijderd en klik vervolgens op de **Optimaliseren** knop om het proces te beëindigen.

Scan uw systeem regelmatig

Uw systeemsnelheid en het algemene gedrag ervan kunnen ook worden beïnvloed door bedreigingen.

Zorg ervoor dat u uw systeem regelmatig scant, minstens één keer per week.

Het wordt aanbevolen om de systeemscan te gebruiken, omdat deze scant op alle soorten bedreigingen die de veiligheid van uw systeem in gevaar brengen en ook binnen archieven scant.

De systeemscan starten:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik **Scan uitvoeren** naast **Systeem scan**.
4. Volg de stappen van de wizard.

1.4.7. Nuttige informatie

Hoe test ik mijn beveiligingsoplossing?

Om er zeker van te zijn dat uw Bitdefender-product correct werkt, raden we u aan de Eicartest te gebruiken.

Met de Eicartest kunt u uw beveiligingsoplossing controleren met een veilig bestand dat hiervoor is ontwikkeld.

Om uw beveiligingsoplossing te testen:

1. Download de test van de officiële webpagina van de EICAR-organisatie http://www.eicar.org/.
2. Klik op de tab **Antimalware Testbestand**.
3. Klik in het menu aan de linkerzijde op **Downloaden**.
4. Vanuit **Downloadgedeelte met gebruikmaking van standaardprotocol http** klikt u op het testbestand **eicar.com**.
5. U zult worden geïnformeerd dat de pagina die u probeert te bezoeken het EICAR-Testbestand bevat (geen bedreiging).
   Indien u klikt op **Ik begrijp de risico's, breng me er toch heen**, dat start de download van de test en een Bitdefender-pop-up informeert u dat er een bedreiging is gedetecteerd.
   Klik op **Meer details** om meer informatie over deze handeling te krijgen.

Indien u geen Bitdefender-waarschuwing wilt ontvangen, raden we u aan om contact op te nemen met Bitdefender voor ondersteuning zoals beschreven in deel Hulp vragen (pagina 307).

Hoe kan ik Bitdefender verwijderen?

Als u uw {1}{2} wilt verwijderen:

- In **Windows 7**:
  1. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
  2. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
  3. Klik op **VERWIJDEREN** in het venster dat verschijnt.
  4. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 8** En **Windows 8.1**:
  1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
  2. Klik **Een programma verwijderen** of **Programma's en functies**.
  3. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
  4. Klik **VERWIJDEREN** in het venster dat verschijnt.
  5. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 10** En **Windows 11**:
  1. Klik op {1}Start{2}, klik dan op Instellingen.
  2. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Apps**.
  3. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
  4. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.
  5. Klik **VERWIJDEREN** in het venster dat verschijnt.
  6. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

> **Opmerking**
> Deze procedure voor opnieuw installeren verwijdert uw persoonlijke instellingen permanent.

Hoe kan ik Bitdefender VPN verwijderen?

De procedure om Bitdefender VPN te verwijderen, is vergelijkbaar met de procedure om andere programma's van uw computer te verwijderen:

- In **Windows 7**:
  1. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
  2. Zoek **Bitdefender VPN** en selecteer **De-installeren**.
     Wacht tot de de-installatieproces is voltooid.
- In **Windows 8** En **Windows 8.1**:
  1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
  2. Klik **Verwijderen** een programma of **Programma's en functies**.
  3. Vinden **Bitdefender-VPN** en selecteer **Verwijderen**.
     Wacht tot het verwijderingsproces is voltooid.
- In **Windows 10** En **Windows 11**:
  1. Klik **Begin**en klik vervolgens op Instellingen.
  2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  3. Vinden **Bitdefender-VPN** en selecteer **Verwijderen**.
  4. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.
     Wacht tot het verwijderingsproces is voltooid.

Hoe verwijder ik de extensie Anti-tracker van Bitdefender?

Afhankelijk van de webbrowser die u gebruikt, volgt u deze stappen om de extensie Anti-tracker van Bitdefender te de-installeren:

- Internet Explorer
  1. Klik op naast de zoekbalk en selecteer Uitbreidingen beheren. Er verschijnt een lijst van de geïnstalleerde extensies.
  2. Klik op Anti-tracker van Bitdefender.

3. Klik rechtsonder op **Uitschakelen**.

- Google Chrome

  1. Klik op ⋮ naast de zoekbalk.
  2. Selecteer **Meer extra** en vervolgens **Extensies**.
     Er verschijnt een lijst van de geïnstalleerde extensies.
  3. Klik op **Verwijderen** in de kaart Anti-tracker van Bitdefender.
  4. Klik op **Verwijderen** in de pop-up die verschijnt.

- Mozilla Firefox

  1. Klik ≡ naast de zoekbalk.
  2. Selecteer **Uitbreidingen** en vervolgens **Extensies**.
     Er verschijnt een lijst met de geïnstalleerde extensies.
  3. Klik op ··· en selecteer **Verwijderen**.

Hoe kan ik de apparaat automatisch afsluiten nadat het scannen is voltooid?

Bitdefender biedt meerdere scantaken die u kunt gebruiken om zeker te zijn dat uw systeem niet is geïnfecteerd door bedreigingen. Het scannen van de volledige apparaat kan langer duren, afhankelijk van de hardware- en softwareconfiguratie van uw systeem.

Omwille van deze reden biedt Bitdefender u de mogelijkheid om uw product te configureren om uw systeem af te sluiten zodra het scannen is voltooid.

Overweeg dit voorbeeld: u bent klaar met uw werk en wilt naar bed. U wilt dat Bitdefender uw volledig systeem controleert op bedreigingen.

Om de apparaat uit te schakelen wanneer Snelle scan of Systeemscan zijn voltooid:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik in het venster **Scans** op ··· naast Snelle scan of Systeemscan en selecteer **Bewerken**.

4. Pas de scan aan in overeenkomst met uw noden en klik op **Volgende**.
5. Vink het vakje naast **Kiezen wanneer deze taak wordt ingepland** aan en kies vervolgens wanneer de taak moet worden gestart.
   Als u Dagelijks, Maandelijks of Wekelijks kiest, sleept u de schuifregelaar langs de schaal om de gewenste periode in te stellen wanneer de geplande scan moet starten.
6. Klik **Redden**.

Om het apparaat uit te schakelen wanneer een aangepaste scan is voltooid:

1. Klik op ··· naast de aangepaste scan die u hebt aangemaakt.
2. Klik op **Volgende** en klik dan opnieuw op **Volgende**.
3. vink het vakje naast **Kiezen wanneer deze taak wordt ingepland** aan en kies vervolgens wanneer de taak moet worden gestart.
4. Klik **Redden**.

Als er geen bedreigingen zijn gevonden, wordt de apparaat uitgeschakeld.

Als er niet opgeloste bedreigingen achterblijven, wordt u gevraagd de acties te kiezen die moeten worden ondernomen. Zie Antivirusscanwizard (pagina 24) voor meer informatie.

Hoe kan ik Bitdefender configureren om een proxy-internetverbinding te gebruiken?

Als uw apparaat een internetverbinding maakt via een proxyserver, moet u Bitdefender configureren met de proxy-instellingen. Bitdefender zal standaard de proxy-instellingen van uw systeem automatisch detecteren en importeren.

> **Belangrijk**
> Internetverbindingen bij u thuis gebruiken doorgaans geen proxyserver. Als vuistregel is het aanbevolen de proxyverbindingsinstellingen van uw Bitdefender-programma te controleren en te configureren wanneer de updates niet werken. Als Bitdefender een update kan uitvoeren, dan is de toepassing correct geconfigureerd voor het maken van een internetverbinding.

Uw proxy-instellingen beheren:

1. Klik **Instellingen** in het navigatiemenu op de Bitdefender-interface.

2. Selecteer de **Geavanceerd** tabblad.
3. Schakel **Proxyserver** in.
4. Klik op **Proxywijziging**.
5. Er zijn twee opties voor het instellen van de proxy-instellingen:
   - **Proxy-instellingen van de standaardbrowser importeren** - proxy-instellingen van de huidige gebruiker, opgehaald van de standaardbrowser. Als de proxyserver een gebruikersnaam en wachtwoord vereist, moet u deze gegevens opgeven in de overeenkomende velden.

     > **Opmerking**
     > Bitdefender kan proxy-instellingen van de populairste browsers importeren, inclusief de nieuwste versies van Microsoft Edge, Internet Explorer, Mozilla Firefox en Google Chrome.

   - **Proxy-instellingen aanpassen** - proxy-instellingen die u zelf kunt configureren.
     U moet de volgende instellingen definiëren:
     - **Adres** - voer het IP-adres van de proxyserver in.
     - **Poort** – voer de poort in die Bitdefender gebruikt om verbinding te maken met de proxyserver.
     - **Gebruikersnaam** – voer een gebruikersnaam in die wordt herkend door de proxy.
     - **Wachtwoord** – voer het geldige wachtwoord voor de eerder opgegeven gebruiker in.
6. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Bitdefender gebruikt de beschikbare proxy-instellingen tot er een internetverbinding kan worden gemaakt.

Gebruik ik een 32- of 64-bits versie van Windows?

Nagaan of u een besturingssysteem van 32 bits of 64 bits hebt:

- In **Windows 7**:
  1. Klik op **Start**.

2. Zoek **Computer** in het menu **Start**.
3. Klik met de rechtermuisknop op **Computer** en selecteer **Eigenschappen**.
4. Kijk onder **Systeem** om de informatie over uw systeem te controleren.

- In **Windows 8**:
  1. Zoek vanuit het Windows-startscherm **Computer** (u kunt bijvoorbeeld starten met het typen van "computer", rechtstreeks in het startscherm) en rechterklik op het pictogram ervan.
  2. Selecteer **Eigenschappen** in het onderste menu.
  3. Kijk in Systeem om uw systeemtype te zien.

- In **Windows 10** En **Windows 11**:
  1. Typ "Systeem" in het zoekveld in de taakbalk en klik op het pictogram ervan.
  2. Kijk bij Systeem om informatie over uw systeemtype te vinden.

Verborgen objecten weergeven in Windows

Deze stappen zijn nuttig in de gevallen waarin u te maken krijgt met een bedreiging en u de geïnfecteerde bestanden die kunnen verborgen zijn, moet vinden en verwijderen.

Volg deze stappen om verborgen objecten weer te geven in Windows.

1. Klik op **Start**, ga naar **Configuratiescherm**.
   In **Windows 8** en **Windows 8.1**: Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
2. Selecteer **Mapopties**.
3. Ga naar het tabblad **Weergave**.
4. Selecteer **Verborgen bestanden en mappen weergeven**.
5. Vink **Extensies voor bekende bestandstypen verbergen** uit.

6. Schakel het selectievakje **Beveiligde besturingssysteembestanden verbergen** in.
7. Klik op **Toepassen**, klik daarna op **OK**.

In **Windows 10** En **Windows 11**:

1. Typ "Verborgen bestanden en mappen tonen" in het zoekveld in de taakbalk en klik op het pictogram ervan.
2. Selecteer **Verborgen bestanden, mappen en drives tonen**.
3. Duidelijk **Verberg extensies voor bekende bestandstypen**.
4. Duidelijk **Verberg beveiligde besturingssysteembestanden**.
5. Klik **Toepassen**, dan klikken **OK**.

Andere beveiligingsoplossingen verwijderen

De hoofdreden voor het gebruik van een beveiligingsoplossing is het bieden van bescherming en veiligheid voor uw gegevens. Maar wat gebeurt er als er meerdere beveiligingsproducten aanwezig zijn op hetzelfde systeem?

Wanneer u meer dan één beveiligingsoplossing op dezelfde apparaat Bitdefender Ultimate Securitygebruikt, wordt het systeem onstabiel. Het installatieprogramma van detecteert automatisch andere beveiligingsprogramma's en biedt u de mogelijkheid om ze te verwijderen.

Indien u de andere beveiligingsoplossingen niet hebt verwijderd tijdens de eerste installatie:

- In **Windows 7**:
  1. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
  2. Wacht enkele ogenblikken tot de lijst met geïnstalleerde software wordt weergegeven.
  3. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
  4. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.
- In **Windows 8** En **Windows 8.1**:

1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
2. Klik **Een programma verwijderen** of **Programma's en functies**.
3. Wacht even totdat de lijst met geïnstalleerde software wordt weergegeven.
4. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
5. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10** En **Windows 11**:
  1. Klik **Begin**en klik vervolgens op Instellingen.
  2. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Apps**.
  3. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.
  4. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.
  5. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

Als u de andere beveiligingsoplossing niet van uw systeem kunt verwijderen, kunt u het hulpprogramma voor het verwijderen ophalen van de website van de verkoper of direct met hem contact opnemen voor richtlijnen betreffende het verwijderen.

Opnieuw opstarten in Veilige modus

De Veilige modus is een diagnostische gebruiksmodus die hoofdzakelijk wordt gebruikt om problemen op te lossen die de normale werking van Windows beïnvloeden. Dergelijke problemen kunnen lopen van conflicterende stuurprogramma's tot bedreigingen die verhinderen dat Windows normaal wordt gestart. In de Veilige modus werken slechts enkele toepassingen en laadt Windows alleen de basisbesturingsprogramma's en een minimum aan componenten van het besturingssysteem. Daarom zijn de meeste bedreigingen inactief wanneer Windows in de Veilige modus wordt gebruikt en kunnen ze gemakkelijk worden verwijderd.

Windows in Veilige modus starten:

- In **Windows 7**:
  1. Start uw apparaat opnieuw op.
  2. Druk meerdere keren op de **F8**-toets voordat Windows wordt gestart om toegang te krijgen tot het opstartmenu.
  3. Selecteer **Veilige modus** in het opstartmenu of **Veilige modus met netwerkmogelijkheden** als u internettoegang wenst.
  4. Druk op **Enter** en wacht terwijl Windows wordt geladen in Veilige modus.
  5. Dit proces eindigt met een bevestigingsbericht. Klik op **OK** om te bevestigen.
  6. Om Windows normaal te starten, hoeft u alleen het systeem opnieuw op te starten.

- In **Windows 8**, **Windows 8.1**, **Windows 10** en **Windows 11**:
  1. Lanceer **Systeemconfiguratie** in Windows door tegelijk op de toetsen **Windows + R** op uw keyboard te drukken.
  2. Schrijf **msconfig** in het dialoogvenster **Openen** en klik daarna op **OK**.
  3. Selecteer het tabblad **Opstarten**.
  4. In het gebied **Opstartopties** vinkt u het vakje **Veilig opstarten** aan.
  5. Klik op **Netwerk** en vervolgens op **OK**.
  6. Klik op **OK** in het venster **Systeemconfiguratie** dat u vertelt dat het systeem opnieuw moet worden opgestart om de wijzigingen die u hebt ingesteld, door te voeren.
     Uw systeem wordt opnieuw opgestart in Veilige modus met Netwerk.

Om opnieuw op te starten in normale modus, zet u de instellingen terug door de **Systeemoperatie** opnieuw te lanceren en het vakje **Veilig opstarten** terug uit te vinken. Klik op **OK** en daarna op **Opnieuw opstarten**. Wacht tot de nieuwe instellingen toegepast zijn.

1.5. Problemen oplossen

1.5.1. Algemene problemen oplossen

Dit hoofdstuk beschrijft enkele problemen die zich kunnen voordoen terwijl u BitDefender gebruikt en biedt u mogelijke oplossingen voor deze problemen. De meeste problemen kunnen worden opgelost door de juiste configuratie van de productinstellingen.

- Mijn systeem lijkt traag (pagina 134)
- Het scannen start niet (pagina 136)
- Ik kan een bepaalde toepassing niet meer gebruiken (pagina 138)
- Wat moet u doen wanneer Bitdefender een website, domein, IP-adres of online toepassing blokkeert die veilig is (pagina 139)
- Bitdefender updaten bij een langzame internetverbinding (pagina 144)
- De Bitdefender-services reageren niet (pagina 145)
- Het verwijderen van Bitdefender is mislukt (pagina 150)
- Mijn systeem start niet op na het installeren van Bitdefender (pagina 151)

Als u het probleem hier niet kunt vinden of als de voorgestelde oplossingen niet werken, kunt u contact opnemen met vertegenwoordigers van de technische ondersteuning van BitDefender zoals beschreven in hoofdstuk Hulp vragen (pagina 307).

Mijn systeem lijkt traag

Na het installeren van beveiligingssoftware kan er doorgaans een lichte vertraging van het systeem merkbaar zijn. Dit is normaal tot in zekere mate.

Als u een aanzienlijke vertraging opmerkt, kan dit probleem verschijnen door de volgende redenen:

- **Bitdefender is niet het enige beveiligingsprogramma dat op uw systeem is geïnstalleerd.**
  Hoewel Bitdefender de beveiligingsprogramma's verwijdert die tijdens de installatie zijn gevonden, is het aanbevolen elke andere beveiligingsoplossing die u mogelijk gebruikt voordat u Bitdefender

installeert, te verwijderen. Zie Andere beveiligingsoplossingen verwijderen (pagina 131) voor meer informatie.

- **Er is niet voldaan aan de systeemvereisten voor het uitvoeren van Bitdefender.**
  Als uw apparaat niet voldoet aan de systeemvereisten wordt de computer trager, vooral wanneer er meerdere toepassingen tegelijk actief zijn. Zie Systeemvereisten (pagina 4) voor meer informatie.
- **U hebt toepassingen geïnstalleerd die u niet gebruikt.**
  Elk apparaat heeft programma's of toepassingen die niet worden gebruikt. En veel ongewenste programma's worden op de achtergrond uitgevoerd en nemen schijfruimte en geheugen in. De-installeer een programma als u het niet gebruikt. Dit geldt ook voor andere vooraf geïnstalleerde software of evaluatietoepassingen die u hebt vergeten te verwijderen.

  > **Belangrijk**
  > Indien u vermoedt dat een programma of toepassing een essentieel deel van uw besturingssysteem uitmaakt, verwijder het dan niet en neem contact op met Bitdefender-klantenservice voor hulp.

- **Uw systeem is mogelijk geïnfecteerd.**
  De snelheid en het algemene gedrag van uw systeem kan ook worden beïnvloed door dreigingen. Spyware, malware, Trojaanse paarden en adware eisen allemaal hun tol op de prestaties van uw computer. Zorg dat u uw systeem periodiek scant, maar minstens eenmaal per week. Het wordt aanbevolen om Bitdefender Systeemscan te gebruiken want deze scant op alle types dreigingen die de veiligheid van uw systeem in gevaar brengen.
  De Systeemscan starten:

  1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
  2. In de **ANTIVIRUS** paneel, klik **Open**.
  3. Klik in het venster **Scans** op de **Scan uitvoeren** knop naast **Systeemscan**.
  4. Volg de stappen van de wizard.

Het scannen start niet

Dit probleemtype kan twee hoofdoorzaken hebben:

- **Een eerder installatie van Bitdefender die niet volledig werd verwijderd of een ongeldige Bitdefender-installatie.**
  Installeer Bitdefender in dat geval opnieuw:
  - In **Windows 7**:
    1. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
    2. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
    3. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
    4. Wacht tot het herinstalleren is voltooid en start vervolgens uw systeem opnieuw op.
  - In **Windows 8** En **Windows 8.1**:
    1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
    2. Klik **Verwijderen** een programma of **Programma's en functies**.
    3. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
    4. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
    5. Wacht tot het herinstallatieproces is voltooid en start vervolgens uw systeem opnieuw op.
  - In **Windows 10** En **Windows 11**:
    1. Klik **Begin**, dan klikken **Instellingen**.
    2. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Geïnstalleerde apps**.
    3. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
    4. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.

5. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
6. Wacht tot het herinstallatieproces is voltooid en start vervolgens uw systeem opnieuw op.

> **Opmerking**
> Door deze herinstallatieprocedure te volgen, worden aangepaste instellingen opgeslagen en beschikbaar in het nieuw geïnstalleerde product. Andere instellingen kunnen worden teruggezet naar hun standaardconfiguratie.

- **Bitdefender is niet het enige beveiligingsoplossing die op uw systeem is geïnstalleerd.**
  In dit geval:
  1. Verwijder de andere beveiligingsoplossing. Zie Andere beveiligingsoplossingen verwijderen (pagina 131) voor meer informatie.
  2. Bitdefender opnieuw installeren:
     - In **Windows 7**:
       a. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
       b. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
       c. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.
       d. Wacht tot het herinstallatieproces is voltooid en start vervolgens uw systeem opnieuw op.
     - In **Windows 8** En **Windows 8.1**:
       a. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
       b. Klik **Verwijderen** een programma of **Programma's en functies**.
       c. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.

d. Klik **OPNIEUW INSTALLEREN** in het venster dat verschijnt.

e. Wacht tot het herinstallatieproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10** En **Windows 11**:

a. Klik **Begin**, dan klikken **Instellingen**.

b. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Geïnstalleerde apps**.

c. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.

d. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.

e. Klik op **OPNIEUW INSTALLEREN** in het venster dat verschijnt

f. Wacht tot het herinstallatieproces is voltooid en start vervolgens uw systeem opnieuw op.

> **Opmerking**
> Door deze herinstallatieprocedure te volgen, worden aangepaste instellingen opgeslagen en beschikbaar in het nieuw geïnstalleerde product. Andere instellingen kunnen worden teruggezet naar hun standaardconfiguratie.

Als deze informatie niet nuttig was, kunt u contact opnemen met BitDefender voor ondersteuning, zoals beschreven in de sectie Hulp vragen (pagina 307).

Ik kan een bepaalde toepassing niet meer gebruiken

Dit probleem doet zich voor wanneer u probeert een programma te gebruiken dat normaal werkte vóór de installatie van Bitdefender.

Na installatie van Bitdefender kunt u een van deze situaties tegenkomen:

- U kunt van Bitdefender een bericht ontvangen met de melding dat het programma probeert een wijziging aan te brengen aan het systeem.
- U kunt een foutbericht ontvangen van het programma dat u probeert te gebruiken.

Dit type situatie doet zich voor wanneer Advanced Threat Defense per vergissing toepassingen als schadelijk beschouwt.

Advanced Threat Defense is een Bitdefender-functie die constant toezicht houdt op de toepassingen die op uw systeem draaien en verslag uitbrengt over deze die potentieel schadelijk gedrag vertonen. Omdat deze functie op een heuristisch systeem is gebaseerd, kunnen er gevallen zijn waarbij rechtmatige toepassingen worden gerapporteerd door Advanced Threat Defense.

Wanneer deze situatie zich voordoet, kunt u de respectievelijke toepassing uitsluiten, zodat deze niet wordt gemonitord door Advanced Threat Defense.

Om het programma toe te voegen aan de lijst met uitsluitingen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **GEAVANCEERDE BEDREIGINGSVERDEDIGING** paneel, klik **Open**.
3. In de **Instellingen** venster, klik **Uitzonderingen beheren**.
4. Klik **+Voeg een uitzondering toe**.
5. Voer in het overeenkomende veld het pad van het uitvoerbare bestand in dat u wilt uitsluiten van het scannen.
   U kunt ook naar het uitvoerbare bestand navigeren door op de bladerknop aan de rechterkant van de interface te klikken, het te selecteren en op te klikken **OK**.
6. Zet de schakelaar ernaast aan **Geavanceerde bescherming tegen bedreigingen**.
7. Klik **Redden**.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning zoals beschreven in sectie Hulp vragen (pagina 307).

Wat moet u doen wanneer Bitdefender een website, domein, IP-adres of online toepassing blokkeert die veilig is

Bitdefender biedt een veilige websurfervaring door al het webverkeer te filteren en alle kwaadaardige content te blokkeren. Het is echter mogelijk dat Bitdefender een website, domein, IP-adres of online toepassing die veilig is, als onveilig beschouwt, waardoor het scannen van HTTP-verkeer door Bitdefender deze onterecht gaat blokkeren.

Als dezelfde pagina of online toepassing of hetzelfde domein of IP-adres herhaaldelijk wordt geblokkeerd, kunt u deze toevoegen aan de uitzonderingen zodat ze niet worden gescand door de engines van Bitdefender, wat een vlottere surfervaring garandeert.

Om een website toe te voegen aan **Uitzonderingen**:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ONLINE BEDREIGINGSPREVENTIE** paneel, klik **Instellingen**.
3. Klik **Beheer uitzonderingen**.
4. Klik **+Voeg een uitzondering toe**.
5. Typ in het overeenkomstige veld de naam van de website, de naam van het domein of het IP-adres dat u aan uitzonderingen wilt toevoegen.
6. Klik op de schakelaar ernaast **Preventie van online bedreigingen**.
7. Klik **Redden** om de wijzigingen op te slaan en het venster te sluiten.

U dient enkel websites, domeinen, IP-adressen en toepassingen die u volledig vertrouwt, toe te voegen aan deze lijst. Ze worden uitgesloten van het scannen door de volgende engines: bedreiging, phishing en fraude.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning zoals beschreven in sectie Hulp vragen (pagina 307).

Ik kan geen verbinding maken met het internet

Het is mogelijk dat een programma of een webbrowser, na het installeren van Bitdefender, geen verbinding meer kan maken met Internet of geen toegang meer krijgt tot de netwerkdiensten.

In dat geval is de beste oplossing het configureren van Bitdefender om verbindingen naar en van de respectieve softwaretoepassing automatisch toe te staan.

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **FIREWALL** paneel, klik **Instellingen**.
3. In de **Reglement** venster, klik **Regel toevoegen**.
4. Er verschijnt een nieuw venster waarin u de details kunt toevoegen. Zorg ervoor dat u alle beschikbare netwerktypes selecteert en in de **Machtiging** sectie **Toestaan** selecteert.

Sluit Bitdefender, open de softwaretoepassing en probeert opnieuw een verbinding te maken met internet.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning zoals beschreven in sectie Hulp vragen (pagina 307).

Ik kan geen toegang krijgen tot een apparaat op mijn netwerk.

Afhankelijk van het netwerk waarmee u verbonden bent, kan de Bitdefender-firewall de verbinding tussen uw systeem en een ander apparaat (zoals een andere pc of printer) blokkeren. Hierdoor zult u mogelijk niet langer bestanden kunnen delen of afdrukken.

In dit geval is de beste oplossing om Bitdefender zo te configureren dat het verbindingen naar en van het betreffende apparaat automatisch toestaat, op de volgende manier:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **FIREWALL** paneel, klik **Instellingen**.
3. In de **Reglement** venster, klik **Regel toevoegen**.
4. Schakel de optie **Deze regel toepassen op alle toepassingen** in.
5. Klik op de knop **Geavanceerde instellingen**.
6. Tik in het vakje **Aangepast afstandsadres** het IP-adres in van de computer of de printer waar u onbeperkte toegang toe wenst.

Als u nog steeds geen verbinding kunt maken met het apparaat, wordt het probleem mogelijk niet veroorzaakt door Bitdefender.

Controleer op andere potentiële oorzaken, zoals hieronder:

- De firewall op het andere apparaat blokkeert mogelijk het delen van bestanden en printers met uw pc.
  - Als de Windows Firewall wordt gebruikt, kan deze worden geconfigureerd om het delen van bestanden en printers als volgt toe te staan:
    - In **Windows 7**:
      1. Klik op **Start**, ga naar **Configuratiescherm** en selecteer **Systeem en beveiliging**.

2. Ga naar **Windows Firewall** en klik daarna op **Een programma toestaan via Windows Firewall**.
3. Selecteer het vakje **Bestands- en printerdeling**.

- In **Windows 8** En **Windows 8.1**:
  1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
  2. Klik op **Systeem en Beveiliging**, ga naar **Windows Firewall** en selecteer **Een app toegang geven via Windows Firewall**.
  3. Selecteer het vakje **Bestands- en printerdeling** en klik daarna op **OK**.

- In **Windows 10** En **Windows 11**:
  1. Typ "Een app via Windows Firewall toestaan" in het zoekveld in de taakbalk en klik op het pictogram ervan.
  2. Klik op **Instellingen wijzigen**.
  3. In de lijst **Toegestane apps en functies** selecteert u het vakje **Delen van Bestand en Printer** en klikt u daarna op **OK**.

- Als er een ander firewall-programma wordt gebruikt, moet u de documenten of het Help-bestand van dit programma raadplegen.

- Algemene omstandigheden die het gebruik van of verbinden met de gedeelde printer kunnen verhinderen:
  - U moet zich mogelijk aanmelden bij een Windows-beheerdersaccount om toegang te krijgen tot de gedeelde printer.
  - Er zijn machtigingen ingesteld voor de gedeelde printer om de toegang alleen toe te staan tot specifieke apparaten en gebruikers. Als u uw printer deelt, moet u de bevoegdheden controleren die voor de printer zijn ingesteld om te zien of de gebruiker op de andere apparaat toegang heeft tot de printer. Als u probeert een verbinding te maken met een gedeelde printer,

moet u bij de gebruiker op de andere apparaat controleren of u de machtiging hebt om een verbinding te maken met de printer.

- De printer verbonden met uw apparaat of met het andere apparaat is niet gedeeld.
- De gedeelde printer is niet toegevoegd aan de apparaat.

> **Opmerking**
> Om te leren hoe u het delen van printers kunt beheren (een printer delen, machtigingen voor een printer instellen of verwijderen, verbinden met een netwerkprinter of met een gedeelde printer), gaat u naar Windows Help en ondersteuning (klik in het menu Start op **Help en ondersteuning**).

- De toegang tot de netwerkprinter is mogelijk beperkt tot specifieke apparaaten of gebruikers. Raadpleeg de netwerkbeheerder om uit te vinden of u de machtiging hebt om een verbinding te maken met die printer.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning zoals beschreven in sectie Hulp vragen (pagina 307).

Mijn internetverbinding is langzaam

Deze situatie kan zich voordoen nadat u Bitdefender hebt geïnstalleerd. Het probleem kan zijn veroorzaakt door fouten in de Bitdefender-firewallconfiguratie.

Om deze problemen op te lossen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Schakel de schakelaar in het venster **FIREWALL** uit om de functie uit te schakelen.
3. Controleer of uw internetverbinding verbetert wanneer de Bitdefender-firewall is uitgeschakeld.
   - Als u nog steeds een langzame internetverbinding kunt maken, wordt het probleem mogelijk niet veroorzaakt door Bitdefender. Neem contact op met uw internetprovider om te controleren of de verbinding werkt aan hun kant.
     Als u van uw internet-provider de bevestiging ontvangt dat de verbinding aan hun zijde werkt en het probleem zich blijft

voordoen, neemt u contact op met Bitdefender zoals beschreven in sectie Hulp vragen (pagina 307).

- Als de internetverbinding is verbeterd na het uitschakelen van de Bitdefender-firewall:

  a. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.

  b. In de **FIREWALL** paneel, klik **Instellingen**.

  c. Ga naar het tabblad **Netwerkadapters** en stel uw internetverbinding in op **Thuis/Kantoor**.

  d. Schakel in het tabblad **Instellingen** de **Poortscanbescherming** uit.
  Klik in het gebied **Stealth-modus** op **Stealth-instellingen bewerken**. Schakel de stealth-modus in voor de netwerkadapter waarmee u verbonden bent.

  e. Sluit Bitdefender, start het systeem opnieuw op en controleer de snelheid van de internetverbinding.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning zoals beschreven in sectie Hulp vragen (pagina 307).

Bitdefender updaten bij een langzame internetverbinding

Als u een langzame internetverbinding hebt (zoals een inbelverbinding), kunnen er fouten optreden tijdens het updaten.

Om uw systeem up to date houden met de nieuwste Bitdefender-informatie-database voor bedreigingen:

1. Klik **Instellingen** in het navigatiemenu op de Bitdefender-interface.
2. Selecteer de **Update** tabblad.
3. Schakel de schakelaar **Stille update** uit.
4. Wanneer een volgende update beschikbaar is, zal u worden gevraagd welke update u wilt downloaden. Selecteer enkel **Handtekeningen update**.
5. Bitdefender downloadt en installeert enkel de informatie-database voor bedreigingen.

De Bitdefender-services reageren niet

Dit artikel helpt u bij het oplossen van de foutmelding **BitDefender-services reageren niet**. U kunt deze fout aantreffen als volgt:

- Het Bitdefender-pictogram in het **systeemvak** wordt grijs weergegeven en u wordt gemeld dat de Bitdefender-services niet reageren.
- Het BitDefender-venster geeft aan dat de BitDefender-services niet reageren.

De fout kan worden veroorzaakt door een van de volgende omstandigheden:

- tijdelijke communicatiefouten tussen de BitDefender-services.
- sommige BitDefender-services zijn gestopt.
- andere beveiligingsoplossingen worden op hetzelfde ogenblik als Bitdefender uitgevoerd.

Probeer de volgende oplossingen om deze fouten op te lossen:

1. Wacht enkele ogenblikken en kijk of er iets verandert. De fout kan tijdelijk zijn.
2. Start de apparaat opnieuw op en wacht enkele ogenblikken tot Bitdefender is geladen. Open BitDefender om te zien of de fout blijft bestaan. Het probleem wordt doorgaans opgelost door de apparaat opnieuw op te starten.
3. Controleer of er een andere beveiligingsoplossing is geïnstalleerd. Dit kan de normale werking van BitDefender verstoren. Als dat het geval is, raden wij u aan alle andere beveiligingsoplossingen te verwijderen en vervolgens BitDefender opnieuw te installeren.
   Zie Andere beveiligingsoplossingen verwijderen (pagina 131) voor meer informatie.

Als de fout zich blijft voordoen, moet u contact opnemen met onze experts voor hulp, zoals beschreven in deel Hulp vragen (pagina 307).

De antispamfilter werkt niet goed

Dit artikel helpt u bij het oplossen van de volgende problemen met betrekking tot de werking van de antispamfilter van BitDefender:

- **Een aantal rechtmatige e-mailberichten wordt gemarkeerd als [spam].**
- **Talrijke spamberichten worden niet als dusdanig gemarkeerd door de antispam-filter.**
- **De antispam-filter detecteert geen enkel spambericht.**

Rechtmatige berichten worden gemarkeerd als [spam]

Legitieme berichten worden gemarkeerd als [spam] omdat ze er voor de Bitdefender antispam-filter uitzien als spam. Normaal gesproken kunt u dit probleem oplossen door het Antispam-filter adequaat te configureren.

Bitdefender voegt de ontvangers van uw e-mailberichten automatisch toe aan een Vriendenlijst. De e-mailberichten die u ontvangt van de contactpersonen in de Vriendenlijst worden als legitiem beschouwd. Ze worden niet gecontroleerd door de antispam-filter en worden dus nooit gemarkeerd als [spam].

De automatische configuratie van de vriendenlijst verhindert niet dat er detectiefouten optreden in deze situaties:

- U ontvangt veel gevraagde commerciële e-mail omdat u zich op verschillende websites hebt geabonneerd. In dit geval bestaat de oplossing eruit de e-mailadressen waarvan u dergelijke e-mailberichten ontvangt, toe te voegen aan de vriendenlijst.
- Een belangrijk deel van uw rechtmatige e-mail komt van mensen naar wie u nog nooit een e-mail hebt gestuurd, zoals klanten, potentiële zakenpartners en anderen. In dit geval zijn andere oplossingen vereist.

Als u een van de e-mailclients gebruikt waarin Bitdefender wordt geïntegreerd, **worden de detectiefouten aangegeven**.

> **Opmerking**
> Bitdefender kan worden geïntegreerd in de meest gebruikte e-mailclients via een gebruiksvriendelijke antispamwerkbalk. Raadpleeg voor een volledige lijst met ondersteunde e-mailclients Ondersteunde e-mailclients en protocollen (pagina 43).

Contactpersonen toevoegen aan de vriendenlijst

Als u een ondersteunde e-mailclient gebruikt, kunt u de afzenders van rechtmatige berichten gemakkelijk toevoegen aan de vriendenlijst. Volg deze stappen:

1. Selecteer in uw e-mailclient een e-mailbericht van de afzender die u wilt toevoegen aan de vriendenlijst.
2. Klik op de knop **Vriend toevoegen** op de Bitdefender antispamwerkbalk.
3. U wordt gevraagd de adressen die aan de vriendenlijst zijn toegevoegd, te bevestigen. Selecteer **Dit bericht niet meer weergeven** en klik op **OK**.

U ontvangt alle e-mailberichten van dit adres, ongeacht hun inhoud.

Als u een andere e-mailclient gebruikt, kunt u contactpersonen toevoegen aan de vriendenlijst vanaf de BitDefender-interface. Volg deze stappen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik in het deelvenster **ANTISPAM** op **Vrienden beheren**.
   Er wordt een configuratievenster weergegeven.
3. Voer het e-mailadres in waarvan u altijd e-mailberichten wilt ontvangen en klik daarna op **TOEVOEGEN**. U kunt zoveel e-mailadressen toevoegen als u wilt.
4. Klik **OK** om de wijzigingen op te slaan en het venster te sluiten.

Detectiefouten aangegeven

Als u een ondersteunde e-mailclient gebruikt, kunt u de antispamfilter gemakkelijk corrigeren (door aan te geven welke e-mailberichten niet als [spam] aangemerkt moeten worden). Hierdoor helpt u de efficiëntie van de antispamfilter te verbeteren. Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map met ongewenste e-mail waar spamberichten naartoe worden verplaatst.
3. Selecteer het rechtmatige bericht dat door Bitdefender verkeerdelijk is gemarkeerd als [spam].
4. Klik op de knop **Vriend toevoegen** op de antispamwerkbalk van Bitdefender om de afzender van de geselecteerde e-mail toe aan de vriendenlijst. Mogelijk moet u op **OK** klikken om te bevestigen. U zult altijd e-mailberichten van dit adres ontvangen, ongeacht de inhoud ervan.
5. Klik op de **Geen spam** op de antispamwerkbalk van Bitdefender (normaal gesproken in het bovenste gedeelte van het venster van de

e-mailclient). Het e-mailbericht wordt verplaatst naar de map Postvak IN.

Veel spamberichten worden niet gedetecteerd

Als u veel spamberichten ontvangt die niet als [spam] zijn gemarkeerd, moet u de antispamfilter van BitDefender configureren om de efficiëntie te verbeteren.

Probeer de volgende oplossingen:

1. Als u een van de e-mailprogramma's gebruikt waarin Bitdefender wordt geïntegreerd, moet u **niet-gedetecteerde spamberichten aangegeven**.

   > **Opmerking**
   > Bitdefender kan worden geïntegreerd in de meest gebruikte e-mailclients via een gebruiksvriendelijke antispamwerkbalk. Raadpleeg voor een volledige lijst met ondersteunde e-mailclients Ondersteunde e-mailclients en protocollen (pagina 43).

2. **Spammers toevoegen aan de Spammerslijst.** De e-mailberichten die worden ontvangen van adressen in de Spammerslijst worden automatisch gemarkeerd als [spam].

Niet-gedetecteerde spamberichten aangeven

Als u een ondersteunde e-mailclient gebruikt, kunt u eenvoudig aangeven welke e-mailberichten als spam moeten worden gedetecteerd. Dit helpt de efficiëntie van het antispamfilter te verbeteren. Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map Postvak IN.
3. Selecteer de niet-gedetecteerde spamberichten.
4. Klik op de knop **Is spam** in de antispamwerkbalk van Bitdefender (bevindt zich normaal in het bovenste gedeelte van het venster van de e-mailclient). Ze worden onmiddellijk als [spam] gemarkeerd en naar de map met ongewenste e-mail verplaatst.

Spammers toevoegen aan de spammerslijst

Als u een ondersteunde e-mailclient gebruikt, kunt u de afzenders van de spamberichten gemakkelijk toevoegen aan de spammerslijst. Volg deze stappen:

1. Open uw e-mailclient.
2. Ga naar de map met ongewenste e-mail waar spamberichten naartoe worden verplaatst.
3. Selecteer de berichten die door BitDefender zijn gemarkeerd als [spam].
4. Klik op de knop **Spammer toevoegen** op de Bitdefender antispamwerkbalk.
5. U wordt gevraagd de adressen die aan de spammerslijst zijn toegevoegd, te bevestigen. Selecteer **Dit bericht niet meer weergeven** en klik op **OK**.

Als u een ander e-mailprogramma gebruikt, kunt u spammers handmatig toevoegen aan de spammerslijst vanaf de Bitdefender-interface. Het is handig om dit alleen te doen wanneer u meerdere spamberichten hebt ontvangen van hetzelfde e-mailadres. Volg deze stappen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTI SPAM** paneel, klik **Instellingen**.
3. Ga naar het venster **Spammers beheren**.
4. Voer het e-mailadres van de scanner in en klik daarna op **Toevoegen**. U kunt zoveel e-mailadressen toevoegen als u wilt.
5. Klik **OK** om de wijzigingen op te slaan en het venster te sluiten.

De antispamfilter detecteert geen enkel spambericht

Als er een spambericht als [spam] is gemarkeerd, kan er een probleem zijn met de antispamfilter van BitDefender. Voordat u dit probleem probeert op te lossen, moet u controleren of het niet wordt veroorzaakt door een van de volgende omstandigheden:

- De antispambeveiliging wordt mogelijk uitgeschakeld. Klik op **Bescherming** in het navigatiemenu in de **Bitdefender-interface** om de status van de antispambescherming te controleren. Kijk in het venster **Antispam** of de functie geactiveerd is.

  Als Antispam is uitgeschakeld, is dit de oorzaak van uw probleem. Klik op de bijhorende schakelaar om uw Antispambescherming in te schakelen.

- De antispambeveiliging van BitDefender is alleen beschikbaar voor e-mailclients die geconfigureerd zijn om e-mailberichten te ontvangen via het POP3-protocol. Dit betekent het volgende:
  - E-mailberichten die zijn ontvangen via op het web gebaseerde e-mailservices (zoals Yahoo, Gmail, Hotmail of andere), worden op spam gefilterd door Bitdefender.
  - Als uw e-mailclient is geconfigureerd om e-mailberichten te ontvangen met een ander protocol dan POP3 (bijv. IMAP4), controleert de antispamfilter van Bitdefender deze berichten niet op spam.

    Opmerking
    POP3 is een van de op grootste schaal gebruikte protocollen voor het downloaden van e-mailberichten van een e-mailserver. Als u het protocol dat uw e-mailclient gebruikt om e-mailberichten te downloaden niet kent, kunt u dat vragen aan de persoon die uw e-mailclient heeft geconfigureerd.
- Bitdefender Ultimate Security scant geen POP3-verkeer van Lotus Notes.

Een mogelijke oplossing is het repareren of opnieuw installeren van het product. Het is echter mogelijk dat u contact wilt opnemen met BitDefender voor ondersteuning, zoals beschreven in sectie Hulp vragen (pagina 307).

Het verwijderen van Bitdefender is mislukt

Indien u uw Bitdefender-product wilt verwijderen en u merkt dat het proces blijft hangen of het systeem bevriest, klik dan op **Annuleren** om de handeling af te breken. Start het systeem opnieuw op als dit niet werkt.

Als het verwijderen mislukt, kunnen er enkele registersleutels en bestanden van Bitdefender achterblijven op uw systeem. Dergelijke herinneringen kunnen een nieuwe installatie van Bitdefender verhinderen. Ze kunnen ook de prestaties en stabiliteit van het systeem beïnvloeden.

Om Bitdefender helemaal van uw systeem te verwijderen:

- In **Windows 7**:
  1. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.

2. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
3. Klik **VERWIJDEREN** in het venster dat verschijnt.
4. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 8** En **Windows 8.1**:
  1. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
  2. Klik **Een programma verwijderen** of **Programma's en functies**.
  3. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
  4. Klik **VERWIJDEREN** in het venster dat verschijnt.
  5. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10** En **Windows 11**:
  1. Klik **Begin**en klik vervolgens op Instellingen.
  2. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Geïnstalleerde apps**.
  3. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
  4. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.
  5. Klik **VERWIJDEREN** in het venster dat verschijnt.
  6. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

Mijn systeem start niet op na het installeren van Bitdefender

Als u Bitdefender net hebt geïnstalleerd en het systeem niet langer opnieuw kunt opstarten in de normale modus, kunnen er verschillende redenen zijn voor dit probleem.

Dit wordt zee waarschijnlijk veroorzaakt door een eerdere installatie van Bitdefender die niet goed werd verwijderd of door een andere beveiligingsoplossing die nog steeds op het systeem aanwezig is.

U kunt elke situatie op de volgende manier aanpakken:

- **U had eerder een versie van Bitdefender en hebt deze niet correct verwijderd.**
  Om dit probleem op te lossen:

  1. Start uw systeem opnieuw op en ga naar de Veilige modus. Om te weten hoe u dit kunt doen, ga naar Opnieuw opstarten in Veilige modus (pagina 132).
  2. Bitdefender verwijderen van uw systeem:
     - In **Windows 7**:
       a. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.
       b. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
       c. Klik **VERWIJDEREN** in het venster dat verschijnt.
       d. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.
       e. Start uw systeem opnieuw op in normale modus.
     - In **Windows 8** En **Windows 8.1**:
       a. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.
       b. Klik **Een programma verwijderen** of **Programma's en functies**.
       c. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.
       d. Klik **VERWIJDEREN** in het venster dat verschijnt.
       e. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.
       f. Start uw systeem opnieuw op in de normale modus.
     - In **Windows 10** En **Windows 11**:
       a. Klik **Begin**en klik vervolgens op Instellingen.

b. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Geïnstalleerde apps**.

c. Vinden **Bitdefender Ultimate Security** en selecteer **Verwijderen**.

d. Klik **Verwijderen** nogmaals om uw keuze te bevestigen.

e. Klik **VERWIJDEREN** in het venster dat verschijnt.

f. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

g. Start uw systeem opnieuw op in de normale modus.

3. Uw Bitdefender-product herinstalleren.

- **U had eerder een andere beveiligingsoplossing en u hebt deze niet correct verwijderd.**
  Om dit op te lossen:

  1. Start uw systeem opnieuw op en ga naar Veilige modus. Raadpleeg voor meer informatie over hoe u dit doet Opnieuw opstarten in Veilige modus (pagina 132).
  2. Verwijder de andere beveiligingsoplossing van uw systeem:
     - In **Windows 7**:

       a. Klik **Begin**, ga naar **Controlepaneel** en dubbelklik **Programma's en functies**.

       b. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.

       c. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

     - In **Windows 8** En **Windows 8.1**:

       a. Zoek vanuit het startscherm van Windows **Controlepaneel** (u kunt bijvoorbeeld "Configuratiescherm" rechtstreeks in het startscherm typen) en vervolgens op het bijbehorende pictogram klikken.

       b. Klik **Een programma verwijderen** of **Programma's en functies**.

c. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.

d. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

- In **Windows 10** En **Windows 11**:

  a. Klik **Begin**en klik vervolgens op Instellingen.

  b. Klik op de **Systeem** pictogram in het gebied Instellingen en selecteer vervolgens **Geïnstalleerde apps**.

  c. Zoek de naam van het programma dat u wilt verwijderen en selecteer **Verwijderen**.

  d. Wacht tot het verwijderingsproces is voltooid en start vervolgens uw systeem opnieuw op.

Om andere software correct te verwijderen, gaat u naar de betreffende website en voert u het hulpprogramma voor het verwijderen uit of neemt u contact op met ons voor de richtlijnen voor het verwijderen.

3. Start uw systeem opnieuw op in de normale modus en installeer Bitdefender opnieuw.

U hebt de bovenstaande stappen al gevolgd en de situatie is niet opgelost.

Om dit op te lossen:

1. Start uw systeem opnieuw op en ga naar Veilige modus. Raadpleeg voor meer informatie over hoe u dit doet Opnieuw opstarten in Veilige modus (pagina 132).
2. Gebruik de optie Systeemherstel van Windows om de apparaat te herstellen naar een eerdere datum voordat u het product Bitdefender installeert.
3. Start het systeem opnieuw op in de normale modus en neem contact op met onze experts voor hulp, zoals beschreven in deel Hulp vragen (pagina 307).

1.5.2. Bedreigingen van uw systeem verwijderen

Bedreigingen kunnen uw systeem op heel wat verschillende manieren beïnvloeden en de benadering van Bitdefender is afhankelijk van het

type bedreiging. Omdat bedreigingen vaak hun gedrag veranderen, is het moeilijk een patroon vast te stellen voor hun gedrag en hun acties.

Er zijn situaties wanneer Bitdefender de bedreigingsinfectie niet automatisch kan verwijderen van uw systeem. In dergelijke gevallen is uw tussenkomst vereist.

- Reddingsomgeving (pagina 155)
- Wat moet u doen als Bitdefender dreigingen vindt op uw apparaat? (pagina 156)
- Een bedreiging in een archief opruimen (pagina 158)
- Een bedreiging in een e-mailarchief opruimen (pagina 159)
- Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is? (pagina 160)
- Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek? (pagina 160)
- Wat zijn de overgeslagen items in het scanlogboek? (pagina 161)
- Wat zijn de overgecomprimeerde bestanden in het scanlogboek? (pagina 161)
- Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd? (pagina 161)

Als u uw probleem hier niet kunt vinden, of als de gepresenteerde oplossingen het niet oplossen, kunt u contact opnemen met de vertegenwoordigers van de technische ondersteuning van Bitdefender, zoals weergegeven in hoofdstuk Hulp vragen (pagina 307).

Reddingsomgeving

Helpmodus is een Bitdefender-functie waarmee u alle bestaande harde schijfpartities binnen en buiten uw besturingssysteem kunt scannen en desinfecteren.

Bitdefender Noodomgeving is geïntegreerd met Windows RE.

Uw systeem starten in de Helpmodus

U kunt enkel op de volgende manier van uw Bitdefender-product naar de Rescue Environment gaan:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. In de **ANTIVIRUS** paneel, klik **Open**.
3. Klik op **Openen** naast **Noodomgeving**.
4. Klik op **Herstarten** in het venster dat verschijnt.
   Bitdefender Noodomgeving wordt binnen enkele ogenblikken geladen.

Uw systeem scannen in de Noodomgeving

Om uw systeem te scannen in de Noodomgeving:

1. Ga naar de Rescue Environment, zoals beschreven in Uw systeem starten in de Helpmodus (pagina 155).
2. Het Bitdefender-scanproces start automatisch zodra het systeem is geladen in Rescue Environment.
3. Wacht tot de scan is voltooid. Volg de instructies om een gedetecteerde bedreiging te verwijderen.
4. Om Rescue Environment te verlaten, klikt u op de knop SLUITEN in het venster met de scanresultaten.

Wat moet u doen als Bitdefender dreigingen vindt op uw apparaat?

U ontdekt op een van de volgende manieren dat er een dreiging aanwezig is op uw apparaat:

- U hebt uw apparaat gescand en Bitdefender heeft geïnfecteerde items gevonden.
- Een bedreigingswaarschuwing laat u weten dat Bitdefender een of meerdere bedreigingen op uw apparaat heeft geblokkeerd.

Voer in dergelijke gevallen een update uit van Bitdefender om zeker te zijn dat u over de laatste informatiedatabase over bedreigingen beschikt en voer een systeemscan uit om het systeem te analyseren.

Selecteer de gewenste actie (desinfecteren, verwijderen, naar quarantaine verplaatsen) voor de geïnfecteerde items zodra de systeemscan is voltooid.

Waarschuwing

Als u vermoedt dat het bestand deel uitmaakt van het Windows-besturingssysteem of dat het geen geïnfecteerd bestand is, volgt u deze stappen niet en neemt u zo snel mogelijk contact op met de klantendienst van Bitdefender.

Als de geselecteerde actie niet kan worden ondernemen en het scanlogboek een infectie meldt die niet kan worden verwijderd, moet u de bestanden handmatig verwijderen.

De eerste methode kan worden gebruikt in de normale modus:

1. Schakel de real-time antivirusbescherming van Bitdefender uit:
   a. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
   b. In de **ANTIVIRUS** paneel, klik **Open**.
   c. In de **Geavanceerd** venster, uitschakelen **Bitdefender-schild**.
2. Geef verborgen objecten weer in Windows. Raadpleeg voor meer informatie over hoe u dit doet Verborgen objecten weergeven in Windows (pagina 130).
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Schakel de real-time antivirusbescherming van Bitdefender in.

Indien de eerste methode niet werkte om de infectie te verwijderen:

1. Start uw systeem opnieuw op en ga naar Veilige modus. Raadpleeg voor meer informatie over hoe u dit doet Opnieuw opstarten in Veilige modus (pagina 132).
2. Geef verborgen objecten weer in Windows. Raadpleeg voor meer informatie over hoe u dit doet Verborgen objecten weergeven in Windows (pagina 130).
3. Blader naar de locatie van het geïnfecteerde bestand (controleer het scanlogboek) en verwijder het.
4. Start uw systeem opnieuw op en ga naar de normale modus.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning zoals beschreven in sectie Hulp vragen (pagina 307).

Een bedreiging in een archief opruimen

Een archief is een bestand of een verzameling van bestanden dat is gecomprimeerd onder een speciale indeling om de benodigde schijfruimte voor het opslaan van de bestanden te beperken.

Sommige van deze formaten zijn open formaten. Hierdoor kan Bitdefender binnen deze formaten scannen en de geschikte acties ondernemen om ze te verwijderen.

Andere archiefformaten worden gedeeltelijk of volledig gesloten. Bitdefender kan alleen de aanwezigheid van bedreigingen detecteren, maar kan geen andere acties ondernemen.

Als Bitdefender u meldt dat er een bedreiging is gedetecteerd binnen een archief en er geen actie beschikbaar is, betekent dit dat het niet mogelijk is de bedreiging te verwijderen vanwege beperkingen op de machtigingsinstellingen voor het archief.

Een bedreiging die in een archief is opgeslagen, wordt op de volgende manier opgeruimd:

1. Identificeer het archief dat de bedreiging bevat door een systeemscan uit te voeren.
2. Schakel de real-time antivirusbescherming van Bitdefender uit:
   a. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
   b. In de **ANTIVIRUS** paneel, klik **Open**.
   c. In de **Geavanceerd** venster, uitschakelen **Bitdefender-schild**.
3. Ga naar de locatie van het archief en decomprimeer het met een archiveringstoepassing, zoals WinZip.
4. Identificeer het geïnfecteerde bestand en verwijder het.
5. Verwijder het originele archief zodat u zeker bent dat de infectie volledig is verwijderd.
6. Comprimeer de bestanden in een nieuw archief met een archiveringstoepassing zoals WinZip.
7. Schakel de realtime antivirusbescherming van Bitdefender in en voer een Systeemscan uit om zeker te zijn dat er geen andere infecties op het systeem aanwezig zijn.

> **Opmerking**
> Het is belangrijk dat u weet dat een bedreiging die is opgeslagen in een archief, geen onmiddellijke bedreiging is voor uw systeem, omdat de bedreiging moet worden gedecomprimeerd en uitgevoerd om uw systeem te kunnen infecteren.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning zoals beschreven in sectie Hulp vragen (pagina 307).

Een bedreiging in een e-mailarchief opruimen

Bitdefender kan ook bedreigingen identificeren in de e-maildatabases en e-mailarchieven die op de schijf zijn opgeslagen.

Het is soms nodig het geïnfecteerde bestand te identificeren met de informatie die is opgegeven in het scanrapport en het handmatig te verwijderen.

Een bedreiging die in een e-mailarchief is opgeslagen, wordt op de volgende manier opgeruimd:

1. Scan de e-maildatabase met Bitdefender.
2. Schakel de real-time antivirusbescherming van Bitdefender uit:
   a. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
   b. In de **ANTIVIRUS** paneel, klik **Open**.
   c. In de **Geavanceerd** venster, uitschakelen **Bitdefender-schild**.
3. Open het scanrapport en gebruik de identificatiegegevens (Onderwerp, Van, Aan) van de geïnfecteerde berichten om ze te zoeken in de e-mailclient.
4. De geïnfecteerde bestanden verwijderen. De meeste e-mailclients verplaatsen het verwijderde bericht ook naar een herstelmap van waar het kan worden hersteld. U moet controleren of dit bericht ook uit deze herstelmap is verwijderd.
5. Comprimeer de map die het geïnfecteerde bericht bevat.
   - In Microsoft Outlook 2007: Klik in het menu Bestand op Gegevensbestandsbeheer. Selecteer de bestanden van de

persoonlijke mappen(.pst) die u wilt comprimeren en klik op Instellingen. Klik nu op Compact.

- In Microsoft Outlook 2010 / 2013/ 2016: In het Bestandsmenu klikt u op Info en dan op Accountinstellingen (Accounts toevoegen en verwijderen of bestaande login-instellingen wijzigen). Klik dan op Gegevensbestand, selecteer de bestanden van de persoonlijke mappen (.pst) die u wilt comprimeren en klik op Instellingen. Klik nu op Compact.

6. Schakel de real-time antivirusbescherming van Bitdefender in.

Als deze informatie niet nuttig was, kunt u contact opnemen met Bitdefender voor ondersteuning zoals beschreven in sectie Hulp vragen (pagina 307).

Wat moet ik doen als ik vermoed dat een bestand gevaarlijk is?

U kunt vermoeden dat een bestand in uw systeem gevaarlijk is, ondanks het feit dat uw Bitdefender-product het niet heeft gedetecteerd.

Om ervoor te zorgen dat uw systeem beschermd is:

1. Voer een **Systeemscan** uit met Bitdefender. Om te weten hoe u dit kunt doen, ga naar How do I scan my system?.
2. Als het scanresultaat schoon lijkt, maar u nog steeds twijfels hebt en wilt zeker zijn over het bestand, moet u contact opnemen met onze experts zodat wij u kunnen helpen.
   Om te weten hoe u dit kunt doen, ga naar Hulp vragen (pagina 307).

Wat zijn de wachtwoordbeveiligde bestanden in het scanlogboek?

Dit is slechts een melding die aangeeft dat Bitdefender heeft gedetecteerd dat deze bestanden ofwel door een wachtwoord ofwel door een vorm van codering zijn beveiligd.

De meest gebruikelijke items die door een wachtwoord zijn beveiligd, zijn:

- Bestanden die bij een andere beveiligingsoplossing horen.
- Bestanden die bij het besturingssysteem horen.

Om de inhoud ook daadwerkelijk te scannen, moeten deze bestanden zijn opgehaald of op een andere manier zijn gedecodeerd.

Als deze inhoud zou worden uitgepakt, zou de real time scanner van Bitdefender ze automatisch scannen om uw apparaat beschermd te

houden. Als u die bestanden wilt scannen met Bitdefender, moet u contact opnemen met de productfabrikant voor meer informatie over die bestanden.

Wij raden u aan deze bestanden te negeren omdat ze geen bedreiging vormen voor uw systeem.

Wat zijn de overgeslagen items in het scanlogboek?

Alle bestanden die in het scanrapport als Overgeslagen worden weergegeven, zijn zuiver.

Voor betere prestaties scant Bitdefender geen bestanden die niet werden gewijzigd sinds de laatste scan.

Wat zijn de overgecomprimeerde bestanden in het scanlogboek?

Overgecomprimeerde items zijn elementen die niet kunnen worden opgehaald door de scanengine of elementen waarvoor de decoderingstijd te lang zou zijn waardoor het systeem onstabiel zou kunnen worden.

Overgecomprimeerd betekent dat het Bitdefender het scannen binnen dat archief heeft overgeslagen omdat het uitpakken ervan teveel systeembronnen zou in beslag nemen. De inhoud zal bij real time toegang worden gescand indien dat nodig is.

Waarom heeft Bitdefender een geïnfecteerd bestand automatisch verwijderd?

Als er een geïnfecteerd bestand wordt gedetecteerd, zal Bitdefender automatisch proberen dit te desinfecteren. Als de desinfectie mislukt, wordt het bestand naar quarantaine verplaatst om de infectie in te dammen.

Voor bepaalde soorten bedreigingen is desinfectie niet mogelijk omdat het gedetecteerde bestand volledig kwaadaardig is. In dergelijke gevallen wordt het geïnfecteerde bestand van de schijf verwijderd.

Dit is doorgaans het geval met installatiebestanden die zijn gedownload vanaf onbetrouwbare websites. Als u zelf in een dergelijke situatie terechtkomt, downloadt u het installatiebestand vanaf de website van de fabrikant of een andere vertrouwde website.

2. ANTIVIRUS VOOR MAC

2.1. Wat is Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac is een krachtige antivirusscanner die alle soorten schadelijke software ("bedreigingen") kan detecteren en verwijderen, waaronder:

- ransomware
- adware
- virussen
- spyware
- Trojaanse paarden
- keyloggers
- wormen.

Deze toepassing detecteert en verwijdert niet alleen Mac-bedreigingen, maar ook Windows-bedreigingen. Hierdoor weet u zeker dat u nooit ongemerkt een besmet bestand doorstuurt naar familieleden, vrienden of collega's die een Windows-pc gebruiken.

2.2. Installeren en verwijderen

Dit hoofdstuk bevat de volgende onderwerpen:

2.2.1. Systeemvereisten

U kunt Bitdefender Antivirus for Mac installeren op Macintosh-computers met OS X Yosemite (10.10) of nieuwere versies.

Uw Mac moet ook minstens 1 GB beschikbare ruimte hebben op de harde schijf.

Om Bitdefender Antivirus for Mac te registreren en bij te werken, hebt u een internetverbinding nodig.

Opmerking
Bitdefender Anti-tracker en Bitdefender VPN kunnen enkel op systemen met macOS 10.12 of nieuwere versies geïnstalleerd worden.

Zo vindt u uw macOS-versie en hardware-informatie over uw Mac
Klik op het Apple-symbool in de linkerbovenhoek van het scherm en kies Over **Deze Mac**. In het venster dat verschijnt, ziet u de versie van uw besturingssysteem en andere nuttige informatie. Klik op **Systeemrapport** voor gedetailleerde hardware-informatie.

2.2.2. Bitdefender Antivirus for Mac installeren

De Bitdefender Antivirus for Mac app kan als volgt worden geïnstalleerd vanuit uw Bitdefender-account:

1. Log in als beheerder.
2. Ga naar: https://central.bitdefender.com.
3. Meld u aan bij uw Bitdefender-account met uw e-mailadres en wachtwoord.
4. Selecteer het paneel **Mijn Apparaten** en klik dan op **BESCHERMING INSTALLEREN**.
5. Kies een van de twee beschikbare opties:
   - **Bescherm dit apparaat**
     a. Selecteer deze optie en selecteer dan de eigenaar van het apparaat. Als die apparaat aan iemand anders toebehoort, klik dan op de overeenstemmende knop.
     b. Sla het installatiebestand op.
   - **Bescherm andere apparaten**
     a. Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.
     b. Klik op **DOWNLOADKOPPELING VERZENDEN**.
     c. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL VERZENDEN**.

De gegenereerde downloadlink is slechts 24 uur geldig. Indien de link vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.

d. Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailadres dat u ingevoerd hebt en klik op de overeenkomstige downloadknop.

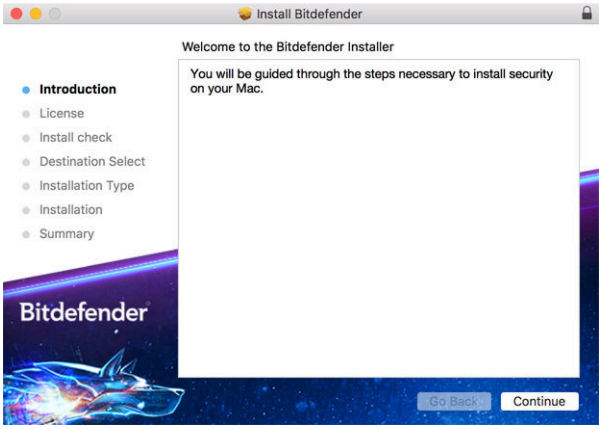
6. Start het gedownloade Bitdefender-programma.
7. Voer de installatiestappen uit.

Installatieprocedure

Om Bitdefender Antivirus for Mac te installeren:

1. Klik op het gedownloade bestand. Hiermee start u het installatieprogramma, dat u begeleidt bij de installatie.
2. Volg de stappen van de installatiewizard.

Stap 1 - Welkomstvenster



Klik op **Doorgaan**.

Stap 2 - Abonnementsovereenkomst lezen

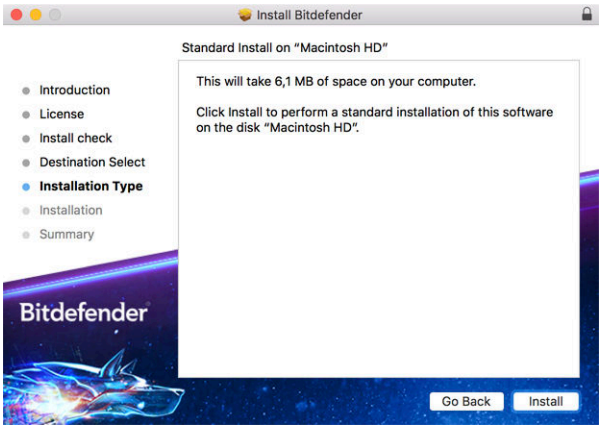
Voordat u verdergaan met de installatie, dient u in te stemmen met de Abonnementsovereenkomst. Lees de Abonnementsovereenkomst grondig door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Antivirus for Mac.

Vanuit dit venster kunt u ook de taal waarin u het product wilt installeren, selecteren.

Klik op **Doorgaan**, en klik dan op **Akkoord**.

> **Belangrijk**
> Als u niet instemt met de voorwaarden in de Licentieovereenkomst, klikt u op **Doorgaan** en vervolgens op **Niet akkoord** om de installatie te annuleren en het installatieprogramma af te sluiten.

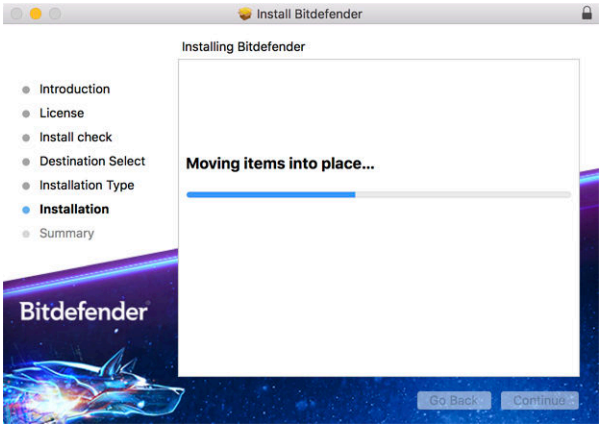
Stap 3 - Installatie starten



Bitdefender Antivirus for Mac wordt geïnstalleerd in Macintosh HD/Library/Bitdefender. Het installatiepad kan niet worden gewijzigd.

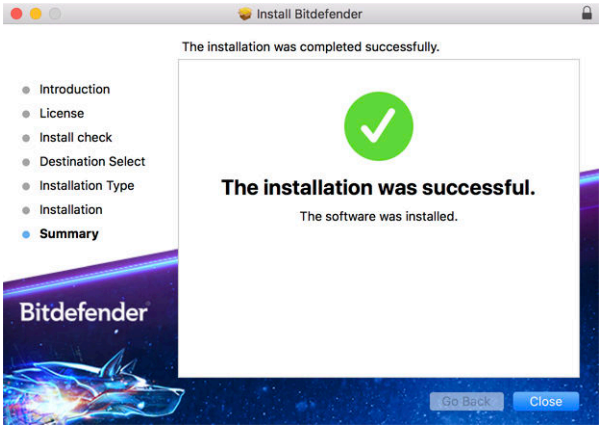
Klik op **Installeren** om de installatie te starten.

Stap 4 - Installeren van Bitdefender Antivirus for Mac



Wacht tot de installatie uitgevoerd is en klik vervolgens op **Doorgaan**.

Stap 5 - Voltooien



Klik op **Sluiten** om het installatie venster te sluiten.

De installatieprocedure is nu voltooid.

Belangrijk

- Als u Bitdefender Antivirus for Mac installeert op macOS High Sierra 10.13.0 of een nieuwere versie, verschijnt de melding **Systeemextensie geblokkeerd**. Deze melding informeert u dat de door Bitdefender ondertekende extensies werden geblokkeerd en handmatig moeten worden ingeschakeld. Klik op OK om door te gaan. Klik in het Bitdefender Antivirus voor Mac-venster dat verschijnt op de koppeling **Beveiliging & Privacy**. Klik op **Toestaan** in het onderste deel van het venster of selecteer de Bitdefender SRL in de lijst en klik vervolgens op **OK**.
- Als u Bitdefender Antivirus for Mac installeert op macOS Mojave 10.14 of een nieuwere versie, verschijnt er een nieuw venster met de mededeling dat u **Bitdefender volledige schijftoegang moet verlenen** en **Bitdefender moet toestaan te laden**. Volg de instructies op het scherm om het product correct te configureren.

2.2.3. Bitdefender Antivirus for Mac verwijderen

Omdat Bitdefender Antivirus for Mac een geavanceerd programma is, kunt u het niet op de gewone manier verwijderen door het programmasymbool van de map **Programma's** naar de Prullenmand te slepen.

Volg deze stappen om Bitdefender Antivirus for Mac te verwijderen:

1. Open een **Finder**-venster en ga naar de map **Programma's**.
2. Open de Bitdefender-map in **Programma's**, en dubbelklik dan op **BitdefenderUninstaller**.
3. Selecteer de verwijderoptie van uw voorkeur.

   Opmerking
   Als u enkel de Bitdefender VPN-app probeert te verwijderen, vink dan alleen **VPN verwijderen** aan.

4. Klik op **Verwijderen** en wacht tot de verwijdering is uitgevoerd.
5. Klik op **Sluiten** om te eindigen.

   Belangrijk
   Als er een fout optreedt, kunt u contact opnemen met het klantenserviceteam van Bitdefender zoals beschreven in Hulp vragen (pagina 307).

2.3. Aan de slag

Dit hoofdstuk bevat de volgende onderwerpen:

2.3.1. Bitdefender Antivirus for Mac openen

Er zijn verschillende manieren om Bitdefender Antivirus for Mac te openen.

- Klik op het symbool van Bitdefender Antivirus for Mac in de Launchpad.
- Klik op het symbool in de menubalk en kies **Antivirus-interface openen**.
- Open een Finder-venster, ga naar Programma's en dubbelklik op het symbool **Bitdefender Antivirus for Mac**.

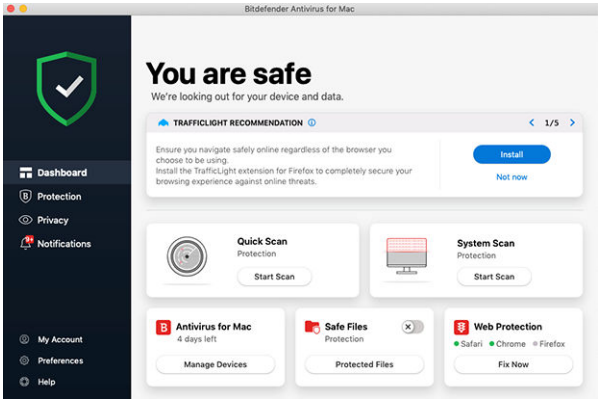
Belangrijk

Wanneer u Bitdefender Antivirus for Mac voor het eerst opent op macOS Mojave 10.14 of een nieuwere versie, verschijnt er een beschermingsaanbeveling. Deze aanbeveling verschijnt omdat we machtigingen nodig hebben om uw hele systeem te scannen op bedreigingen. Om ons deze machtigingen te verlenen, moet u ingelogd zijn als beheerder en de volgende stappen volgen:

1. Klik op de link **Systeemvoorkeuren**.
2. Klik op het symbool, en tik dan uw beheerdersgegevens in.
3. Er verschijnt een nieuw venster. Versleep het bestand **BDLDaemon** naar de lijst met toegestane toepassingen.

2.3.2. Hoofdvenster Toepassing

Bitdefender Antivirus for Mac voldoet niet alleen aan de behoeften van beginnende computergebruikers, maar ook aan de eisen van bijzonder technische gebruikers. De grafische gebruikersinterface is ontworpen zodat elke categorie gebruikers deze probleemloos kunnen gebruiken.



Om door de Bitdefender-interface te gaan, wordt een inleidingswizard getoond met informatie over hoe u moet omgaan met het product en hoe u het moet configureren. Dit wordt in de linkerbovenhoek weergegeven. Selecteer het juiste pijltje om de gids voort te zetten of **Rondleiding overslaan** om de wizard te sluiten.

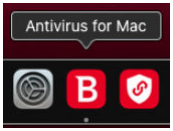
De statusbalk bovenaan het venster informeert u aan de hand van expliciete berichten en suggestieve kleuren over de beveiligingsstatus van het systeem. Indien Bitdefender Antivirus for Mac geen waarschuwingen bevat, is de statusbalk groen. Wanneer er een beveiligingsprobleem werd gedetecteerd, verandert de kleur van de statusbalk naar rood. Raadpleeg Problemen oplossen (pagina 187) voor gedetailleerde informatie over problemen en hoe deze op te lossen.

Bitdefender Autopilot is uw persoonlijke beveiligingsadviseur om u bij al uw activiteiten een effectieve werking en verhoogde bescherming te bieden. Naargelang de activiteiten die u uitvoert, of u nu werkt of online betalingen doet, biedt Bitdefender Autopilot contextuele aanbevelingen op basis van het gebruik en de noden van uw apparaat. Hiermee kunt u de voordelen van de functies die in de toepassing Bitdefender Antivirus for Mac inbegrepen zijn, ontdekken, en ervan genieten.

Vanuit het navigatiemenu aan de linkerkant hebt u toegang tot de Bitdefender-secties voor gedetailleerde configuratie en geavanceerde beheertaken (**Bescherming** en **Privacy** tabbladen), meldingen, uw **Bitdefender-account** en het **Voorkeuren** gedeelte. U kunt ook contact met ons opnemen (**Help** tabblad) voor ondersteuning in het geval u vragen hebt of er iets onverwachts verschijnt.

2.3.3. Dock-symbool toepassing

Het symbool van Bitdefender Antivirus for Mac is te zien in het Dock zodra u het programma opent. Het symbool in het Dock biedt u een eenvoudige manier om bestanden en mappen te scannen op dreigingen. Sleep het bestand of de map gewoon over het Dock-symbool en de scan begint onmiddellijk.



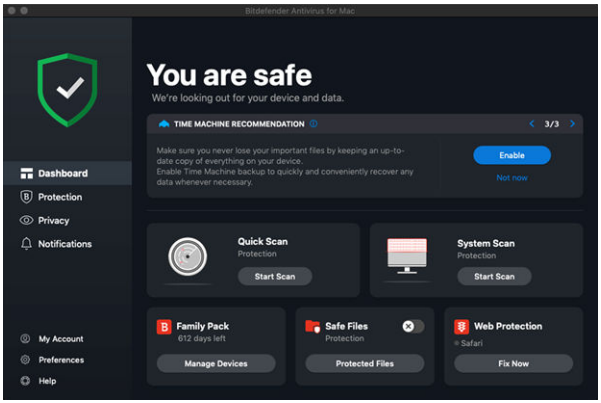
2.3.4. Navigatiemenu

Aan de linkerkant op de Bitdefender-interface staat het navigatiemenu waarmee u snel toegang krijgt tot de functies van Bitdefender voor het gebruik van uw product. Dit zijn de tabbladen die in dit gebied beschikbaar zijn:

- **Dashboard**. Vanuit het Dashboard kunt u beveiligingsproblemen snel oplossen, aanbevelingen op basis van de systeemvereisten en gebruiksprofielen bekijken, snelle acties uitvoeren en naar uw Bitdefender-account gaan om de apparaten die u aan uw Bitdefender-abonnement hebt toegevoegd, te beheren.
- **Bescherming**. Vanuit Bescherming kunt u antivirusscans opstarten, bestanden toevoegen aan de lijst met uitzonderingen, bestanden en toepassingen beschermen tegen ransomware-aanvallen, uw Time Machine back-ups beveiligen en de bescherming tijdens het surfen configureren.
- **Privacy**. Vanaf hier kunt u de Bitdefender VPN-app openen en de Anti-tracker-extensie in uw webbrowser installeren.
- **Meldingen**. Van hieruit kunt u details zien over de acties die op gescande bestanden zijn ondernomen.
- **Mijn Account**. Vanaf hier kunt u zien met welk Bitdefender-account en -abonnement uw apparaat wordt beschermd, en kunt indien nodig van account wisselen.
- **Voorkeuren**. Van hieruit kunt u de Bitdefender-instellingen configureren.
- **Help**. Vanuit Ondersteuning kunt u de afdeling Technische ondersteuning contacteren wanneer u hulp nodig hebt om problemen met uw Bitdefender-product op te lossen. U kunt ons ook feedback sturen om ons te helpen het product te verbeteren.

2.3.5. Donkere modus

Om uw ogen te beschermen tegen verblindend licht wanneer u 's avonds of in het donker werkt, ondersteunt Bitdefender Antivirus for Mac de donkere modus voor Mojave 10.14 en later. De kleuren van de interface werden geoptimaliseerd zodat u uw Mac kunt gebruiken zonder uw ogen te vermoeien. De interface van Bitdefender Antivirus for Mac past zich aan volgens de weergave-instellingen van uw apparaat.



2.4. Bescherming tegen schadelijke software

Dit hoofdstuk bevat de volgende onderwerpen:

2.4.1. Beste praktische toepassingen

Om uw systeem beschermd te houden tegen bedreigingen en te voorkomen dat andere systemen onbedoeld geïnfecteerd worden, gelden de volgende aanbevelingen:

- Houd **Bitdefender Shield** ingeschakeld, zodat systeembestanden automatisch worden gescand door Bitdefender Antivirus for Mac.
- Zorg dat uw Bitdefender Antivirus for Mac-product bijgewerkt blijft met de nieuwste informatie over bedreigingen en productupdates.
- Controleer en herstel regelmatig de problemen die door Bitdefender Antivirus for Mac worden gemeld. Raadpleeg Problemen oplossen (pagina 187) voor gedetailleerde informatie.
- Bekijk de gedetailleerde activiteitenlogboeken van Bitdefender Antivirus for Mac op uw computer. Wanneer er iets belangrijks gebeurt aangaande de beveiliging van uw systeem of gegevens, wordt een nieuw bericht toegevoegd aan het gebied Meldingen van Bitdefender. Raadpleeg Notificaties (pagina 188) voor meer informatie.
- Volg ook de volgende adviezen op:
  - Maak er een gewoonte van om alle bestanden te scannen die u laadt vanaf een extern opslagmedium, zoals een usb-stick of cd. Dit is extra belangrijk als u niet zeker bent van de herkomst van het bestand.
  - Als u een DMG-bestand hebt, moet u dit eerst activeren en vervolgens scant u de inhoud (de bestanden in het geactiveerde volume of de geactiveerde schijfkopie).

  De handigste manier om een bestand, een map of een volume te scannen, is door het object naar het venster of het Dock-symbool van Bitdefender Antivirus for Mac te slepen.

Verder hoeft u niets te doen of in te stellen. Als u dit wilt, kunt u de instellingen en voorkeuren van het programma aan uw wensen aanpassen. Zie Voorkeuren instellen (pagina 191) voor meer informatie.

2.4.2. Uw Mac scannen

De functie **Bitdefender Shield** bewaakt de geïnstalleerde toepassingen op regelmatige basis, zoekt naar gebeurtenissen die op bedreigingen lijken en verhindert dat nieuwe bedreigingen uw systeem kunnen binnendringen, maar u kunt daarnaast ook op elk gewenst moment uw Mac of specifieke bestanden scannen.

De handigste manier om een bestand, een map of een volume te scannen, is door het object naar het venster of het Dock-symbool van Bitdefender

Antivirus for Mac te slepen. De scanwizard wordt gestart en begeleidt u tijdens het scanproces.

U kunt een scan ook op deze manier starten:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Bescherming**.
2. Selecteer het tabblad **Antivirus**.
3. Klik op een van de drie scanknoppen om de gewenste scan uit te voeren.
   - **Snelle scan** - controleert op de aanwezigheid van bedreigingen op de meest kwetsbare locaties van uw systeem (bijvoorbeeld de mappen met documenten, downloads, downloads van e-mails en tijdelijke bestanden van elke gebruiker).
   - **Systeemscan** - voert een uitgebreide controle uit op dreigingen voor het volledige systeem. Ook alle geactiveerde volumes worden gescand.

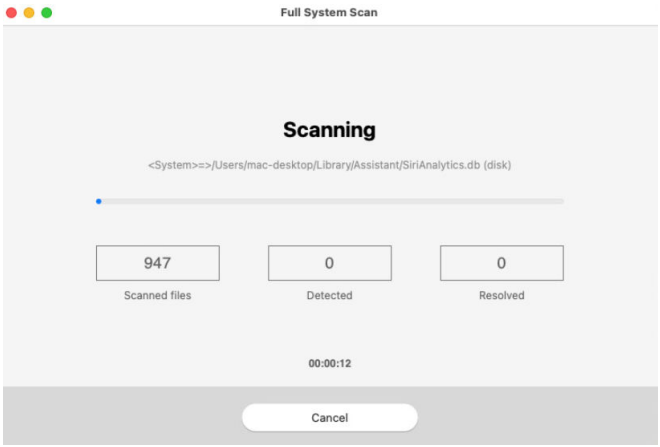
     > **Opmerking**
     > Afhankelijk van de grootte van uw harde schijf kan een scan van het volledige systeem veel tijd in beslag nemen (soms wel een uur, of nog langer). Om de systeemprestaties niet te beïnvloeden, is het aan te raden geen volledige scans te starten terwijl u complexe taken (zoals videobewerking) uitvoert.
     >
     > Als u dat verkiest, kunt u instellen dat bepaalde geactiveerde volumes niet worden gescand, door deze volumes in het venster Bescherming toe te voegen aan de lijst met **Uitzonderingen**.

   - **Aangepaste scan** - hiermee kunt u specifieke bestanden, mappen of volumes scannen op bedreigingen.

U kunt ook een Systeemscan of Snelle Scan starten vanuit het Dashboard.

2.4.3. Scanwizard

Zodra u een scan start, verschijnt de scanwizard van Bitdefender Antivirus for Mac.



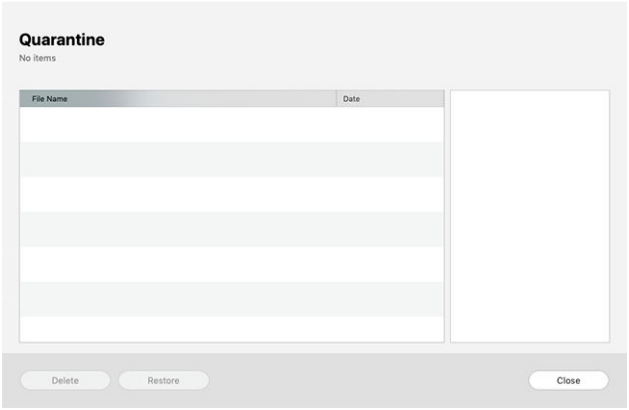
Tijdens elke scan wordt realtime informatie weergegeven over gedetecteerde en verwijderde dreigingen.

Wacht tot Bitdefender Antivirus for Mac klaar is met scannen.

> **Opmerking**
> Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen.

2.4.4. Quarantaine

Bitdefender Antivirus for Mac kan geïnfecteerde of verdachte bestanden verplaatsen naar een speciaal beveiligde map, de zogeheten quarantaine. Wanneer een bedreiging in quarantaine is, kan het geen schade berokkenen, aangezien het niet kan worden uitgevoerd of gelezen.



In de quarantainesectie ziet u alle bestanden die op dit moment zijn geïsoleerd in de quarantainemap.

Als u een bestand uit de quarantaine wilt verwijderen, selecteert u het bestand en klikt u op **Verwijderen**. Als u een bestand uit de quarantaine wilt terugzetten naar de oorspronkelijke locatie, selecteert u het bestand en klikt u op **Terugzetten**.

Om een lijst te zien met alle items in quarantaine:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik op **Openen** in het paneel **Quarantaine**.

2.4.5. Bitdefender Shield (realtime bescherming)

Bitdefender biedt realtime bescherming tegen een brede waaier aan bedreigingen door alle geïnstalleerde toepassingen en hun bijgewerkte versies en nieuwe en gewijzigde bestanden te scannen.

Om de realtime bescherming uit te schakelen:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Voorkeuren**.
2. Schakel **Bitdefender Shield** uit in het venster **Bescherming**.

Waarschuwing

Dit is een kritiek beveiligingsprobleem. Wij raden u aan de real time-beveiliging zo kort mogelijk uit te schakelen. Als de real time-beveiliging is uitgeschakeld, wordt u niet beveiligd tegen bedreigingen.

2.4.6. Scam Copilot voor macOS

Scam Copilot is de door AI aangedreven oplichtingsdetector van Bitdefender.

Door het te gebruiken, kunt u alle lastige sms'jes, e-mails, berichten op sociale media, links of zelfs QR-codes verzenden die u hebt ontvangen en waarvan u achterdochtig bent, om onmiddellijk een analyse te krijgen van hun veiligheid en legitimiteit.

Om Scam Copilot in te stellen:

1. Open Bitdefender Antivirus voor Mac.
2. In het hoofddashboard:
   - Klik op de **Scam Copilot** rechtstreeks op het paneel, of
   - Klik op **Bescherming** in het menu aan de linkerkant en open vervolgens het **Scam Copilot** tab aan de bovenkant.
3. Klik op de **Ga aan de slag** knop.
4. Stel Scam Copilot in.
   U zult zien welke Scam Copilot-componenten al zijn ingeschakeld en welke niet, en u wordt begeleid bij het configureren van de componenten waarvoor extra stappen nodig zijn. Volg de instructies op het scherm om de vereiste machtigingen te verlenen
   - **Bescherming tegen online oplichting:**
     a. Klik op de **Extensie inschakelen** knop.
     b. Installeer de Verkeerslicht (pagina 179) extensie in je browser, als je dat nog niet hebt gedaan.
   - **Nieuwe Scam Wave-waarschuwingen:**

a. Klik op de **Machtiging voor meldingen toestaan** knop om meldingen te ontvangen over nieuwe oplichtingscampagnes in uw regio.

- **E-mailbeveiliging**
  a. Als de e-mailbeveiliging is uitgeschakeld, klikt u op de **E-mailaccount toevoegen** knop.
  b. Kies je e-mailprovider. (Google of Outlook)
  c. Meld u aan met uw Google- of Outlook-e-mailaccount.
  d. Laat Bitdefender uw mailbox scannen.

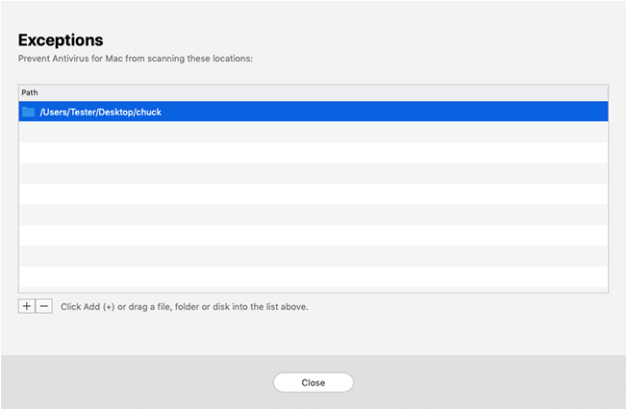
5. Zodra alle Scam Copilot-componenten zijn ingeschakeld, kunt u het instellingenvenster sluiten.

Scam Copilot voor je macOS is nu succesvol geconfigureerd!

2.4.7. Uitzonderingen scannen

Als u wilt, kunt u instellen dat Bitdefender Antivirus for Mac bepaalde bestanden, mappen of zelfs complete volumes overslaat bij het scannen. U kunt bijvoorbeeld de volgende objecten uitsluiten van het scannen:

- Bestanden die tijdens een scan ten onrechte als 'geïnfecteerd' worden aangemerkt (zogeheten fout-positieven)
- Bestanden die fouten veroorzaken tijdens het scannen
- Backup-volumes



De lijst met uitzonderingen bevat de paden die uitgesloten zijn van het scanproces.

Om naar de lijst met uitzonderingen te gaan:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Klik op **Openen** in het paneel **Uitzonderingen**.

U kunt een uitzondering op twee manieren instellen:

- Sleep een bestand, map of volume naar de lijst met uitzonderingen.
- Klik op de knop met het +-teken (+) onder de lijst met uitzonderingen. Kies vervolgens het bestand, de map of het volume dat van het scannen moet worden uitgesloten.

Als u een uitzondering uit de lijst wilt verwijderen, selecteert u deze in de lijst en klikt u onder de lijst met uitzonderingen op de knop met het minteken (-).

2.4.8. Webbeveiliging

Bitdefender Antivirus for Mac gebruikt de TrafficLight-extensies om uw surfervaring volledig te beveiligen. De TrafficLight-extensies filteren, onderscheppen en verwerken al het webverkeer, waarbij schadelijke content wordt geblokkeerd.

De extensies zijn geschikt voor de webbrowsers Mozilla Firefox, Google Chrome en Safari.

TrafficLight-extensies inschakelen

Om de TrafficLight-extensies in te schakelen:

1. Klik op **Nu herstellen** in de kaart **Webbescherming** op het Dashboard.
2. Het venster **Webbescherming** opent.
   De gedetecteerde webbrowser die u op uw systeem geïnstalleerd hebt, verschijnt. Om de TrafficLight-extensie op uw browser te installeren, klikt u op **Extensie downloaden**.
3. U wordt doorgestuurd naar:
   https://bitdefender.nl/solutions/trafficlight.html
4. Selecteer **Gratis Download**.

5. Volg de aanwijzingen om de juiste TrafficLight-extensie voor uw webbrowser te installeren.

Uitbreidingsinstellingen beheren

Er zijn meerdere geavanceerde functies beschikbaar om u tegen allerlei soorten dreigingen te beschermen tijdens het surfen op het web. Om deze te gebruiken, klikt u op het TrafficLight-pictogram naast de instellingen van uw browser. Vervolgens klikt u op de knop ⚙ **Instellingen**:

- **Bitdefender TrafficLight Instellingen**
  - Webbescherming: beschermt u tegen bezoeken aan websites die worden gebruikt voor malware-, phishing- en fraudeaanvallen.
  - Zoekadviseur - waarschuwt u op voorhand over riskante websites die in uw zoekresultaten worden vermeld.

- **Uitzonderingen**
  Bent u op de website die u wilt toevoegen aan de uitzonderingen, klikt u op **Huidige website aan lijst toevoegen**.
  Wilt u een andere website toevoegen, voert u het adres in het bijhorende veld in en klikt u op ⊕.
  Er wordt geen waarschuwing weergegeven wanneer er bedreigingen zijn op de uitgezonderde pagina's. Daarom dient u enkel websites die u volledig vertrouwt toe te voegen aan de lijst.

Paginabeoordelingen en waarschuwingen

Afhankelijk van de beoordeling door TrafficLight van de webpagina die u momenteel bekijkt, worden de volgende pictogrammen weergegeven, in de kleuren van een verkeerslicht:

✅ Dit is een veilige pagina om te bezoeken. U kunt uw werk voortzetten.

⚠ Deze webpagina kan gevaarlijke inhoud bevatten. Ga voorzichtig te werk als u beslist om deze pagina te bezoeken.

⛔ U moet de webpagina onmiddellijk verlaten omdat deze malware of andere dreigingen bevat.

In Safari is de achtergrond van de iconen van TrafficLight zwart.

2.4.9. Anti-tracker

Vele websites die u bezoekt, gebruiken trackers om informatie te verzamelen over uw gedrag. Ze kunnen deze informatie vervolgens delen met derden of ze kunnen de informatie gebruiken om u advertenties te laten zien die voor u relevanter zijn. Eigenaars van websites verdienen zo geld, om u gratis inhoud te kunnen bieden of om draaiende te blijven. Naast het verzamelen van informatie, kunnen trackers uw surfervaring vertragen of uw bandbreedte opgebruiken.

Als de Bitdefender Anti-tracker-extensie geactiveerd is in uw webbrowser, vermijdt u deze tracking, zorgt u dat uw gegevens privé blijven terwijl u online surft en wordt de laadtijd voor websites versneld.

De Bitdefender-extensie is compatibel met de volgende webbrowsers:

- Google Chrome
- Mozilla Firefox
- Safari

De trackers die we detecteren worden in de volgende categorieën gegroepeerd:

- **Reclame** - wordt gebruikt voor de analyse van patronen in websiteverkeer, het gedrag van gebruikers of het verkeer van bezoekers.
- **Klanteninteractie** - wordt gebruikt om de interactie van gebruikers met verschillende invoervormen, zoals chat of ondersteuning, te meten.
- **Essentieel** - wordt gebruikt om de kritieke functionaliteiten van webpagina's te monitoren.
- **Website-analytics** - wordt gebruikt om gegevens over het gebruik van webpagina's te verzamelen.
- **Sociale Media** - wordt gebruikt voor de monitoring van het sociale publiek, de activiteiten en het gebruikersengagement met verschillende sociale mediaplatformen.

Bitdefender Anti-tracker activeren

Om de Bitdefender Anti-tracker-extensie te activeren in uw webbrowser:

1. Klik in het navigatiemenu in de Bitdefender-interface op **Privacy**.
2. Selecteer het tabblad **Anti-tracker**.
3. Klik op **Extensie activeren** naast de webbrowser waarvoor u de extensie wilt activeren.

Interface van Anti-tracker

Wanneer de Bitdefender Anti-tracker-extensie is geactiveerd, verschijnt het symbool naast de zoekbalk in uw webbrowser. Telkens wanneer u een website bezoekt, kunt u op het symbool een teller zien die verwijst naar de gedetecteerde en geblokkeerde trackers. Om meer details over de geblokkeerde trackers te bekijken, klikt u op het symbool om de interface te openen. Naast het aantal geblokkeerde trackers kunt u de tijd zien die nodig is om de pagina te laden en de categorieën waartoe de gedetecteerde trackers behoren. Om de lijst met websites die tracken te bekijken, klikt u op de gewenste categorie.

Om de blokkering van trackers door Bitdefender op te heffen voor de website die u momenteel bezoekt, klikt u op **Bescherming op deze website pauzeren**. Deze instelling is enkel van toepassing zolang u de website open hebt staan en gaat terug naar zijn initiële staat zodra u de website verlaat.

Om toe te staan dat trackers van een specifieke categorie uw activiteiten volgen, klikt u op de gewenste activiteit en vervolgens op de bijhorende knop. Indien u zich bedenkt, klikt opnieuw op dezelfde knop.

Bitdefender Anti-tracker uitschakelen

Om de Bitdefender Anti-tracker uit te schakelen in uw webbrowser:

1. Open uw webbrowser.
2. Klik op het symbool naast de adresbalk in uw webbrowser.
3. Klik op het symbool in de rechterbovenhoek.
4. Gebruik de bijhorende schakelaar om uit te schakelen.
   Het Bitdefender-pictogram wordt dan grijs.

Toestaan dat een website aan tracking doet

Wilt u dat tracking wordt toegepast wanneer u een bepaalde website bezoekt, kunt u dit adres als volgt toevoegen aan de uitzonderingen:

1. Open uw webbrowser.
2. Klik op het symbool naast de zoekbalk.
3. Klik op de pictogram in de rechterbovenhoek.
4. Als u zich op de website bevindt waarop u uitzonderingen wilt toevoegen, klikt u op **Voeg de huidige website toe aan de lijst**.
   Als u nog een website wilt toevoegen, typt u het adres in het overeenkomstige veld en klikt u op .

2.4.10. E-mailbescherming

Uw e-mail is een belangrijk onderdeel van uw digitale leven, en gezien de vele toepassingen in het echte leven, is het een favoriete aanvalsvector geworden voor kwaadwillenden en een van de belangrijkste cyberveiligheidsproblemen van de dagelijkse gebruiker.

E-mailbescherming is een beveiligingsfunctie waarmee u potentieel gevaarlijke inhoud in e-mails die u in uw inbox ontvangt, kunt scannen en identificeren. Deze functie is een pakket van verschillende technologieën die onder dezelfde beveiligingsmodule zijn samengebracht, zoals antiphishing-, antimalware-, antispam-, antifraude- en anti-scamsoftware.

Door een directe verbinding tot stand te brengen tussen Bitdefender en uw e-mailserviceprovider, staat u toe dat de antivirus uw e-mails rechtstreeks scant en elimineert u de beperkingen die ontstaan door het gebruik van verschillende apparaten of e-mailclients.

Opmerking
U kunt maximaal 5 verschillende e-mailaccounts beveiligen.

Uw account configureren

Deze functie is naadloos geïntegreerd in de gebruikersinterface. E-mailbescherming gaan gebruiken:

1. Onder **Bescherming**, Klik op de **E-mailbescherming** tabblad.
2. Kies uw e-mailprovider voor het e-mailaccount dat u wilt beschermen.

> **Opmerking**
> E-mailbeveiliging is momenteel beschikbaar voor Google-accounts, Outlook-accounts en binnenkort ook beschikbaar voor Yahoo Mail.

3. Klik op de **Aanmelden** knop.
   De bewerking wordt vervolgens voortgezet in uw browser.
4. Voer uw e-mailadres in en klik op de **Volgende** knop
5. Om verder te gaan, voert u uw wachtwoord in en klikt u op de **Volgende** knop.
6. Controleer de gevraagde toestemmingen op het scherm en laat Bitdefender uw e-mailaccount beschermen.

Uw e-mailaccount is nu beveiligd en al uw nieuwe inkomende e-mails worden gescand op bedreigingen.

> **Opmerking**
> Elke gescande e-mail wordt gemarkeerd met een label om het veiligheidsniveau aan te geven.

Navigeer door het E-mailbeveiligingsdashboard

Het dashboard toont uw beveiligde e-mails, waaronder:

- configuratiedatum (de datum waarop het account is ingesteld voor E-mailbescherming)
- status (actief of inactief)
- aantal gefilterde e-mails in de afgelopen 30 dagen.
  Hier ziet u een grafiek met het aantal ontvangen veilige e-mails en gevaarlijke e-mails.

Om meerdere e-mailaccounts toe te voegen Klik op de **Voeg nog een account toe** en doorloop voor elk ervan het bovenstaande configuratieproces.

Om het scannen te onderbreken of een account te verwijderen vanuit deze functie klikt u op de drie stippen naast het betreffende account en selecteert u de actie die u wilt uitvoeren.

2.4.11. Safe Files

Ransomoware is een schadelijke software die kwestbare systemen aanvalt door ze te vergrendelen en later om geld te vragen zodat de

gebruiker terug de controle over zijn systeem te krijgen. Deze schadelijke software handelt op een intelligente manier door valse berichten weer te geven zodat de gebruiker panikeert, om hem aan te sporen om de gevraagde betaling uit te voeren.

Gebruik makend van de recentste technologie garandeert Bitdefender systeemintegriteit door kritieke systeemgebieden te beschermen tegen ransomwareaanvallen zonder het systeem te belasten. Mogelijks wilt u echter ook uw persoonlijke bestanden beschermen, zoals documenten, foto's of films tegen ongeoorloofde toegang door onbetrouwbare apps. Met Bitdefender Safe Files kunt u persoonlijke bestanden op een veilige plek bewaren en zelf configureren welke apps toestemming mogen krijgen om wijzigingen aan te brengen in de beschermde bestanden en welke niet.

Om achteraf bestanden toe te voegen aan de beschermde omgeving:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Selecteer het tabblad **Antiransomware**.
3. Klik op **Beschermde bestanden** in het gebied Veilige bestanden.
4. Klik op de knop met het +-teken (+) onder de lijst beschermde bestanden. Kies vervolgens het bestand, de map of het volume dat beschermd moet worden indien tijdens ransomware-aanvallen wordt getracht ze te openen.

Om vertragingen in het systeem te voorkomen, bevelen we u aan om maximaal 30 mappen toe te voegen of om meerdere bestanden in een map op te slaan.

Standaard worden de mappen Afbeeldingen, Documenten, Bureaublad en Downloads beschermd tegen bedreigingsaanvallen.

> **Opmerking**
> Aangepaste mappen kunnen enkel beschermd worden voor huidige gebruikers. Externe schijven, systemen en toepassingsbestanden kunnen niet worden toegevoegd aan de beschermingsomgeving.

Telkens wanneer een ongekend app met een verdacht gedrag probeert om de bestanden die u hebt toegevoegd, te wijzigen, zult u een melding ontvangen. Klik op **Toestaan** of **Blokkeren** en voeg toe aan de lijst **Toepassingen beheren**.

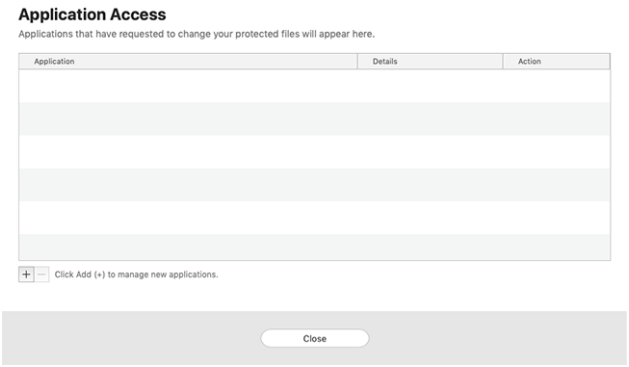
Toegang applicatie

De applicaties die proberen om beschermde bestanden te wijzigen of verwijderen kunnen aangeduid worden als potentieel onveilig en toegevoegd aan de lijst Geblokkeerde applicaties. Indien een applicatie geblokkeerd werd en u zeker bent dat dit normaal gedrag is, kunt u ze toestaan via de volgende stappen:

1. Klik **Bescherming** in het navigatiemenu op de Bitdefender-interface.
2. Selecteer de **Anti-ransomware** tabblad.
3. Klik op **Toegang toepassingen** in het gebied Veilige bestanden.
4. Wijzig de status naast de geblokkeerde toepassing naar Toestaan.

Apps die als Toestaan ingesteld zijn, kunnen ook Geblokkeerd worden.

Gebruik de versleepmethode of klik op het +-teken (+) om meer apps aan de lijst toe te voegen.



2.4.12. Bescherming Time Machine

Bitdefender Time Machine Protection biedt een extra beveiligingslaag voor de bestanden die op uw Time Machine-schijf zijn opgeslagen, doordat externe toegang tot deze backupschijf wordt geblokkeerd. Mochten deze bestanden ooit worden gegijzeld door ransomware, kunt u ze vanaf uw Time Machine-schijf herstellen zonder losgeld te betalen.

Raadpleeg de Apple-ondersteuningspagina voor instructies indien u items van een Time Machine back-up moet herstellen.

Time Machine Protection in- of uitschakelen

Om Time Machine Bescherming in of uit te schakelen:

1. Klik in het navigatiemenu in de **Bitdefender-interface** op **Bescherming**.
2. Selecteer de **Anti-ransomware** tabblad.
3. Schakel de schakelaar **Time Machine Bescherming** in of uit.

2.4.13. Problemen oplossen

Bitdefender Antivirus for Mac detecteert en signaleert automatisch verschillende soorten problemen die van belang zijn voor de veiligheid van uw systeem en uw gegevens. Hierdoor kunt u eventuele veiligheidsrisico's tijdig verhelpen.

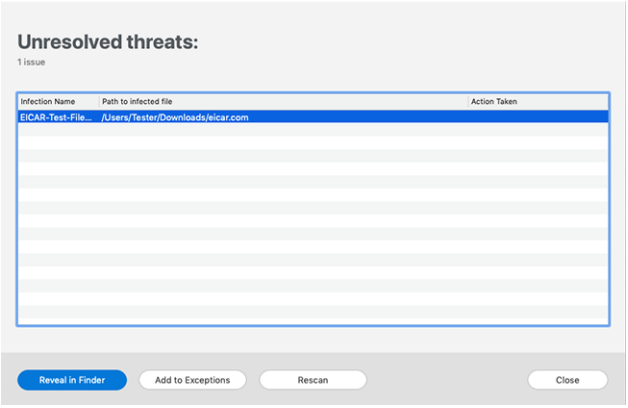
Als u de problemen oplost die door Bitdefender Antivirus for Mac worden gemeld, weet u zeker dat uw systeem en uw gegevens altijd veilig zijn.

Onder andere deze problemen kunnen worden gemeld:

- De nieuwe informatie-update voor bedreigingen werd niet gedownload van onze servers.
- Er werden bedreigingen op uw systeem gedetecteerd en het product kan ze niet automatisch desinfecteren.
- De realtime bescherming is uitgeschakeld.

Zo kunt u controleren of er problemen zijn en deze verhelpen:

1. Als er geen waarschuwingen van Bitdefender zijn, is de statusbalk groen. Als er een beveiligingsprobleem werd gedetecteerd, verandert de kleur van de statusbalk naar rood.
2. Lees de beschrijving voor meer informatie.
3. Wanneer er een probleem wordt gedetecteerd, klikt u op de overeenkomstige knop om een actie te ondernemen.



De lijst met onopgeloste bedreigingen wordt bijgewerkt na elke systeemscan, ongeacht of de scan automatisch werd uitgevoerd of door u werd opgestart.

U kunt op de knoppen in het venster klikken om de volgende maatregelen te nemen voor deze dreigingen:

- **Handmatig verwijderen**. Onderneem deze actie om de infecties handmatig te verwijderen.
- **Toevoegen aan uitzonderingen**. Deze actie is niet beschikbaar voor dreigingen die worden gevonden in archieven.

2.4.14. Notificaties

Bitdefender houdt een gedetailleerd logboek bij van gebeurtenissen met betrekking tot de activiteiten van uw computer. Wanneer er iets gebeurt dat van belang is voor de veiligheid van uw systeem of uw gegevens, wordt er een nieuw bericht toegevoegd aan het gebied Meldingen van Bitdefender, net zoals er nieuwe e-mails verschijnen in uw Postvak IN.

Kennisgevingen zijn een belangrijk hulpmiddel bij het bewaken en beheren van uw Bitdefender-beveiliging. U kunt bijvoorbeeld heel gemakkelijk controleren of een update is geslaagd, of er bedreigingen of kwetsbaarheden op uw computer werden aangetroffen enz. Daarnaast kunt u zo nodig verdere acties ondernemen of acties die door Bitdefender zijn ondernomen, wijzigen.

Klik in het navigatiemenu in de Bitdefender-interface op **Notificaties** om de Notificatielog te bekijken. Telkens wanneer zich een kritiek evenement voordoet, kunt u een teller opmerken op de -icoon.

Afhankelijk van het type en de ernst worden kennisgevingen gegroepeerd in:

- **Kritieke** gebeurtenissen wijzen op kritieke problemen. U moet ze onmiddellijk controleren.
- Gebeurtenissen van het type **Waarschuwing** wijzen op niet-kritieke problemen. U moet ze controleren en herstellen wanneer u tijd hebt.
- Gebeurtenissen van het type **Informatie** duiden op een geslaagde bewerking.

Klik op elke tab om meer details te lezen over de gegenereerde gebeurtenissen. Er wordt beperkte informatie weergegeven als u een keer op elke titel van een gebeurtenis klikt, namelijk: een korte beschrijving, de actie die Bitdefender heeft ondernomen wanneer ze zich voordeed en de datum en tijd van de gebeurtenis. Er kunnen opties worden geboden voor het ondernemen van verdere actie.

Om u te helpen geregistreerde gebeurtenissen gemakkelijker te beheren, biedt het venster Kennisgevingen opties waarmee alle gebeurtenissen in dat deel kunnen worden verwijderd of gemarkeerd als gelezen.

2.4.15. Updates

Er worden dagelijks nieuwe bedreigingen gevonden en geïdentificeerd. Daarom is het erg belangrijk om Bitdefender Antivirus for Mac bij te werken met de nieuwste updates van bedreigingsinformatie.

De updates van de bedreigingsinformatie gebeuren 'on the fly', wat betekent dat de bestanden die moeten worden bijgewerkt, geleidelijk worden vervangen. Zo heeft de update geen gevolgen voor de werking van het product en wordt tegelijkertijd elk zwak punt uitgesloten.

- Als Bitdefender Antivirus for Mac up-to-date is, kunnen ook de nieuwste dreigingen worden gedetecteerd en uit geïnfecteerde bestanden worden verwijderd.
- Als Bitdefender Antivirus for Mac niet up-to-date is, kan het de nieuwste dreigingen die door Bitdefender Labs zijn ontdekt, niet detecteren en verwijderen.

Een update aanvragen

U kunt altijd handmatig een update uitvoeren.

Om te kijken of er nieuwe updates zijn en deze te downloaden, hebt u een actieve internetverbinding nodig.

Zo voert u handmatig een update uit:

1. Klik in de menubalk op de knop **Acties**.
2. Kies **Informatiedatabase bedreigingen updaten**.

U kunt een handmatige update ook uitvoeren door op Command+U te drukken.

Er wordt informatie weergegeven over de voortgang van de update en de gedownloade bestanden.

Updates downloaden via een proxyserver

Bitdefender Antivirus for Mac kan alleen updates downloaden via een proxyserver die géén authenticatie vereist. U hoeft hiervoor verder geen programma-instellingen te wijzigen.

Als u verbinding maakt met het internet via een proxyserver die authenticatie vereist, moet u regelmatig overschakelen naar een rechtstreekse internetverbinding om ervoor te zorgen dat u updates van bedreigingsinformatie ontvangt.

Productupdates

Van tijd tot tijd voeren we een productupdate uit om nieuwe functies en verbeteringen aan het product toe te voegen of om problemen te verhelpen. Het is mogelijk dat u voor deze updates het systeem opnieuw moet opstarten om de installatie van nieuwe bestanden te activeren. Als het voor een productupdate noodzakelijk is het systeem opnieuw op te starten, blijft Bitdefender Antivirus for Mac de oude bestanden gebruiken zolang u de computer nog niet opnieuw hebt opgestart. U kunt dan gewoon doorwerken tijdens het updateproces.

Nadat de productupdate voltooid is, verschijnt een popup-venster met de melding dat het systeem opnieuw moet worden opgestart. Als u deze melding over het hoofd hebt gezien, kunt u in de menubalk op **Opnieuw opstarten voor upgrade** klikken of het systeem handmatig opnieuw opstarten.

Informatie vinden over Bitdefender Antivirus for Mac

Om informatie te vinden over de Bitdefender Antivirus for Mac-versie die u hebt geïnstalleerd, gaat u naar het venster **Over**. Daar vindt u eveneens de Abonnementsovereenkomst, het Privacybeleid en de Open source-licenties.

Om naar het venster Over te gaan:

1. Bitdefender Antivirus for Mac openen.
2. Klik op Bitdefender Antivirus for Mac in de menubalk en kies **Over Antivirus for Mac**.

2.5. Voorkeuren instellen

Dit hoofdstuk bevat de volgende onderwerpen:

- Voorkeuren weergeven (pagina 191)
- Beschermingsvoorkeuren (pagina 191)
- Geavanceerde voorkeuren (pagina 192)
- Speciale aanbieding (pagina 192)

2.5.1. Voorkeuren weergeven

Om het voorkeurenvenster van Bitdefender Antivirus for Mac te openen:

- Voer een van de volgende bewerkingen uit:
  - Klik **Voorkeuren** in het navigatiemenu op de Bitdefender-interface.
  - Klik op Bitdefender Antivirus for Mac in de menubalk en kies **Voorkeuren**.

2.5.2. Beschermingsvoorkeuren

In het venster Beschermingsvoorkeuren kunt u de instellingen voor de malwarescans aanpassen. Naast enkele algemene instellingen kunt u ook instellen wat er moet gebeuren met geïnfecteerde of verdachte bestanden.

- **Bitdefender Shield.** Bitdefender Shield biedt realtime bescherming tegen een brede waaier aan dreigingen door alle geïnstalleerde toepassingen, hun bijgewerkte versies en nieuwe en gewijzigde bestanden te scannen. We raden u aan om Bitdefender Shield niet

uit te schakelen, maar als het toch moet, doe het dan zo kort mogelijk. Als Bitdefender Shield is uitgeschakeld, bent u niet beschermd tegen dreigingen.

- **Alleen nieuwe en gewijzigde bestanden scannen.** Schakel dit selectievakje in om Bitdefender Antivirus for Mac in te stellen om alleen bestanden te scannen die niet eerder zijn gescand of die sinds de laatste scan gewijzigd zijn.
  Als u wilt, kunt u deze instelling negeren voor scans die worden gestart door middel van slepen en neerzetten. Schakel hiervoor het selectievakje uit.
- **Inhoud in back-ups niet scannen.** Schakel dit selectievakje in als u niet wilt dat backup-bestanden worden gescand. Als een geïnfecteerd backup-bestand later wordt teruggezet, wordt dit automatisch door Bitdefender Antivirus for Mac gedetecteerd en zal de juiste actie worden ondernomen.

2.5.3. Geavanceerde voorkeuren

U kunt een algemene actie kiezen voor alle problemen en verdachte items die tijdens de scan gedetecteerd werden.

Actie voor geïnfecteerde objecten

- **Poging tot desinfecteren of verplaatsen naar quarantaine** - Indien er geïnfecteerde bestanden worden gedetecteerd, probeert Bitdefender ze te desinfecteren (schadelijke code verwijderen) of ze naar quarantaine te verplaatsen.
- **Geen actie ondernemen** - Er wordt geen actie ondernomen voor de geïnfecteerde bestanden.

Actie voor verdachte bestanden

- **Bestanden naar quarantaine verplaatsen** - Indien verdachte bestanden worden gedetecteerd, verplaatst Bitdefender ze naar quarantaine.
- **Geen actie ondernemen** - Er wordt geen actie ondernomen op de gedetecteerde bestanden.

2.5.4. Speciale aanbieding

Wanneer er reclameaanbiedingen beschikbaar zijn, is het Bitdefender product zo ingesteld dat u daarvan op de hoogte wordt gesteld via een

pop-upvenster. Dit geeft u de mogelijkheid om te profiteren van voordelige tarieven en om uw apparaten beveiligd te houden gedurende een langere periode.

Om kennisgevingen voor speciale aanbiedingen in of uit te schakelen:

1. Klik **Voorkeuren** in het navigatiemenu op de Bitdefender-interface.
2. Selecteer het tabblad **Andere**.
3. Schakel de schakelaar **Mijn aanbiedingen** in of uit.

> **Opmerking**
> De optie **Mijn aanbiedingen** is standaard ingeschakeld.

2.6. Bitdefender Centraal

Dit hoofdstuk bevat de volgende onderwerpen:

❍

2.6.1. Over Bitdefender CENTRAL

Bitdefender Central is het platform dat u toegang geeft tot de online functies en diensten van het product. Vanuit dit platform kunt u vanop afstand belangrijke taken uitvoeren op de apparaten waarop Bitdefender is geïnstalleerd. U kunt vanaf elke computer en elk mobiel apparaat met een internetverbinding inloggen op uw Bitdefender-account door naar https://central.bitdefender.com te gaan of rechtstreeks vanuit de Bitdefender Central-app op Android- en iOS-apparaten.

Om de Bitdefender Central-toepassing op uw apparaten te installeren:

- **Op Android** - zoek Bitdefender Central op Google Play en download en installeer de toepassing. Volg de nodige stappen om de installatie te voltooien.
- **Op iOS** - zoek Bitdefender Central in de App Store en download en installeer de toepassing. Volg de nodige stappen om de installatie te voltooien.

Zodra u aangemeld bent, kunt u beginnen met het volgende:

- Bitdefender downloaden en installeren op besturingssystemen Windows, macOS, iOS en Android. De producten die beschikbaar zijn om te downloaden, zijn:

- Bitdefender-antivirus voor Mac
- De Bitdefender Windows-productlijn
- Bitdefender Mobile Security for Android
- Bitdefender Mobile Security for iOS

- Uw Bitdefender-abonnementen beheren en vernieuwen.
- Voeg nieuwe apparaten toe aan uw netwerk en beheer deze apparaten, waar u ook bent.

2.6.2. Toegang tot Bitdefender Central

Er bestaan verschillende manieren om naar Bitdefender Central te gaan. Afhankelijk van de taak die u wilt uitvoeren, kunt een van de volgende mogelijkheden gebruiken:

- Vanuit de hoofdinterface van Bitdefender Antivirus for Mac:
  1. Klik rechtsonder in het scherm op de koppeling **Ga naar uw account**.
- Vanuit uw webbrowser:
  1. Open een webbrowser op een computer of mobiel apparaat met internettoegang.
  2. Ga naar: https://central.bitdefender.com.
  3. Log in op uw account met uw e-mailadres en wachtwoord.
- Vanaf uw Android- of iOS-apparaat:
  1. Open de Bitdefender Central-app die u hebt geïnstalleerd.

> **Opmerking**
> Hierin zitten de opties die u ook in de webinterface vindt.

2.6.3. Twee-factorenauthenticatie

De twee-factorenauthenticatiemethode voegt een extra veiligheidslaag toe aan uw Bitdefender account, door een authenticatiecode te vragen bovenop uw aanmeldgegevens. Op deze manier voorkomt u dat uw account wordt overgenomen en houdt u types cyberaanvallen, zoals keyloggers, bruteforce- of woordenlijstaanvallen, af.

Twee-factorenauthenticatie activeren

Door de twee-factorenauthenticatie te activeren, maakt u uw Bitdefender account veel veiliger. Uw identiteit zal gecontroleerd worden telkens u zich aanmeldt via verschillende apparaten, hetzij om één van de Bitdefender producten te installeren, hetzij om de status van uw abonnement te controleren of vanop afstand taken uit te voeren op uw apparaten.

Om de twee-factorenauthenticatie te activeren:

1. Ga naar **Bitdefender Central**.
2. Klik op het pictogram rechtsboven op het scherm.
3. Klik op **Bitdefender Account** in het schuifmenu.
4. Selecteer het tabblad **Wachtwoord en beveiliging**.
5. Kik op **AAN DE SLAG**.
   Kies een van de volgende methodes:
   - **Authenticator App** - gebruik een authenticator app om een code te genereren telkens u zich wilt aanmelden op uw Bitdefender account.
     Als u een authenticator app zou willen, gebruiken, maar u niet zeker weet welke te kiezen, is er een lijst beschikbaar van de authentication apps die we aanbevelen.
     a. Klik op **AUTHENTICATOR APP GEBRUIKEN** om te starten.
     b. Om u aan te melden op een op Android of iOS gebaseerd apparaat, gebruik dat dan om de QR code te scannen.
     Om u aan te melden op een laptop of computer, kunt u de getoonde code manueel toevoegen.
     Klik op **DOORGAAN**.
     c. Voer de code in die de app geeft of deze die weergegeven wordt in de vorige stap, en klik dan op **ACTIVEREN**.
   - **E-mail** - telkens u zich aanmeldt in uw Bitdefender account, zal er een verificatiecode naar het Postvak-IN van uw e-mail worden gestuurd. Controleer de e-mail en gebruik dan de code die u ontving.
     a. Klik op **E-MAIL GEBRUIKEN** om te starten.
     b. Controleer uw e-mail en tik de verstrekte code in.

c. Klik op **ACTIVEREN**.

In het geval u wilt stoppen met het gebruik van de twee-factorenauthenticatie:

1. Klik op **TWEE-FACTORENAUTHENTICATIE UITSCHAKELEN**.
2. Controleer uw app of e-mailaccount en tik de code in die u hebt ontvangen.
   In het geval u ervoor hebt gekozen om de authenticatiecode te ontvangen via e-mail, hebt u vijf minuten om uw e-mailaccount te controleren en de gegenereerde code in te tikken. Als de tijd verstreken is, zult u een nieuwe code moeten genereren volgens dezelfde stappen.
3. Bevestig uw keuze.

2.6.4. Betrouwbare apparaten toevoegen

Om ervoor te zorgen dat alleen u toegang hebt tot uw Bitdefender account, is het mogelijk dat we eerst een veiligheidscode vragen. Als u deze stap zou willen overslaan telkens u verbinding maakt vanaf hetzelfde apparaat, raden we u aan dit te benoemen als een betrouwbaar apparaat.

Om toestellen toe te voegen als betrouwbare apparaten:

1. Toegang Bitdefender Centraal.
2. Klik op de pictogram in de rechterbovenhoek van het scherm.
3. Klik **Bitdefender-account** in het diamenu.
4. Selecteer de **Wachtwoord en veiligheid** tabblad.
5. Klik op **Vertrouwde apparaten**.
6. De lijst van de apparaten waar Bitdefender op geïnstalleerd is, wordt weergegeven. Klik op het gewenste apparaat.

U kunt zo veel apparaten toevoegen als u wilt, op voorwaarde dat Bitdefender erop geïnstalleerd is en uw abonnement geldig is.

2.6.5. Activiteit

In de Activiteitzone hebt u toegang tot informatie over de apparaten waar Bitdefender op geïnstalleerd is.

Wanneer u naar het **Activiteiten**-venster gaat, zijn de volgende kaarten beschikbaar:

- **Mijn apparaten.** Hier kunt u het aantal aangesloten apparaten en hun beschermingsstatus bekijken. Om problemen met de gedetecteerde apparaten op afstand op te lossen, klikt u op **Problemen oplossen** en vervolgens op **SCANNEN EN PROBLEMEN OPLOSSEN**.
  Om details te zien over de gedetecteerde problemen, klikt u op **Problemen bekijken**.
  Informatie over de gedetecteerde bedreigingen kan voor iOS-apparaten niet worden opgehaald.
- **Dreigingen geblokkeerd.** Hier ziet u een grafiek met de algemene statistieken, met inbegrip van informatie over de bedreigingen die de voorbije 24 uur en 7 dagen werden geblokkeerd. De weergegeven informatie wordt opgehaald naargelang het schadelijke gedrag dat in de bestanden, toepassingen en url's werd gedetecteerd.
- **Topgebruikers met geblokkeerde bedreigingen.** Hier ziet u de gebruikers waarbij de meeste bedreigingen werden gevonden.
- **Topapparaten met geblokkeerde bedreigingen.** Hier ziet u de apparaten waarop de meeste bedreigingen werden gevonden.

2.6.6. Mijn abonnementen

Via het Bitdefender Central-platform beheert u heel eenvoudig de abonnementen die u voor uw apparaten hebt aangeschaft.

Controleer beschikbare abonnementen

Zo controleert u uw beschikbare abonnementen:

1. Toegang Bitdefender Centraal.
2. Ga naar het paneel **Mijn abonnementen**.

Hier vindt u informatie over de beschikbaarheid van uw abonnementen en het aantal apparaten dat gebruikmaakt van deze abonnementen.

U kunt een nieuw apparaat aan een abonnement toevoegen of een abonnement verlengen door een abonnementskaart te selecteren.

> **Opmerking**
> U kunt een of meer lidmaatschappen op uw account hebben, op voorwaarde dat ze voor verschillende platforms bestemd zijn (Windows, macOS, iOS of Android).

Abonnement activeren

U kunt een abonnement tijdens het installatieproces activeren via uw Bitdefender-account. De geldigheidsduur van het abonnement begint te lopen vanaf het moment van activering.

Als u een activeringscode hebt ontvangen van een van onze leveranciers, of als u een activeringscode cadeau hebt gekregen, kunt u deze toevoegen aan uw Bitdefender-abonnement.

Volg de onderstaande stappen om een abonnement te activeren met behulp van een activeringscode:

1. Toegang Bitdefender Centraal.
2. Selecteer de **mijn abonnementen** paneel.
3. Klik op de knop **Activeringscode** en typ de code in het bijbehorende veld.
4. Klik op **ACTIVEREN** om door te gaan.

Het abonnement is nu geactiveerd.

Abonnement verlengen

Indien u automatische verlenging voor uw Bitdefender-abonnement hebt uitgeschakeld, kunt u het handmatig verlengen via de volgende stappen:

1. Toegang Bitdefender Centraal.
2. Selecteer de **mijn abonnementen** paneel.
3. Selecteer de gewenste abonnementskaart.
4. Klik op **VERLENGEN** om door te gaan.

In uw webbrowser wordt een webpagina geopend waar u uw Bitdefender-abonnement kunt verlengen.

2.6.7. Mijn apparaten

Vanaf **Mijn apparaten** in uw Bitdefender-account kunt u uw Bitdefender-product installeren, beheren en op afstand gebruiken op al uw apparaten

die zijn ingeschakeld en die verbinding hebben met het internet. De apparaatkaarten geven de naam en de beveiligingsstatus van het apparaat weer en geven weer of er beveiligingsrisico's zijn die de bescherming van uw apparaten beïnvloeden.

Toevoeging van een nieuw apparaat

Indien uw abonnement meer dan één toestel dekt, kunt u een nieuw toestel toevoegen en uw Bitdefender Antivirus for Mac erop installeren, als volgt:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel en tik vervolgens op **INSTALLEER BESCHERMING**.
3. Kies een van de twee beschikbare opties:
   - **Bescherm dit apparaat**
     Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, tikt u op de bijbehorende knop.
   - **Bescherm andere apparaten**
     Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, tikt u op de bijbehorende knop.
     Druk op **DOWNLOADKOPPELING VERZENDEN**. Voer een e-mailadres in het overeenkomstige veld in en klik op **E-MAIL VERZENDEN**. De gegenereerde downloadkoppeling is slechts 24 uur geldig. Indien de koppeling vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.
     Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailaccount dat u hebt ingevoerd en tik vervolgens op de overeenkomstige downloadknop.
4. Wacht tot het downloaden voltooid is en voer het installatieprogramma uit.

Uw apparaten aanpassen

Om uw apparaten beter te kunnen herkennen, kunt u de apparaatnaam aanpassen:

1. Toegang Bitdefender Centraal.
2. Selecteer het paneel **Mijn apparaten**.
3. Klik op de gewenste apparaatkaart en vervolgens op de icoon ⋮ in de rechterbovenhoek van het scherm.
4. Selecteer **Instellingen**.
5. Voer een nieuwe naam in het veld **Naam apparaat** in en klik op **OPSLAAN**.

U kunt een eigenaar aanmaken en toekennen aan elk van uw apparaten, om het beheer te vergemakkelijken:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel.
3. Tik op de gewenste apparaatkaart en vervolgens op ⋮ pictogram in de rechterbovenhoek van het scherm.
4. Selecteer **Profiel**.
5. Klik op **Eigenaar toevoegen** en vul de bijbehorende velden in. Pas het profiel aan: voeg een foto toe, selecteer een geboortedatum en voeg een e-mailadres en geboortedatum toe.
6. Klik op **Toevoegen** om het profiel op te slaan.
7. Selecteer de gewenste eigenaar uit de lijst **Apparaateigenaar** en klik op **TOEWIJZEN**.

Beheer op afstand

Bitdefender van op afstand op een apparaat updaten:

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel.
3. Tik op de gewenste apparaatkaart en vervolgens op ⋮ pictogram in de rechterbovenhoek van het scherm.
4. Selecteer **Update**.

Voor meer acties van op afstand en informatie over uw Bitdefender-product op een specifiek toestel, klik op de gewenste toestelkaart.

Wanneer u op een apparaatkaart klikt, zijn de volgende tabbladen beschikbaar:

- **Dashboard.** In dit venster kunt u de gegevens van het geselecteerde apparaat bekijken, de beschermingsstatus en de Bitdefender VPN-status controleren en nakijken hoeveel bedreigingen de voorbije zeven dagen werden geblokkeerd. De beschermingsstatus is altijd groen (dan zijn er geen problemen voor uw apparaat), geel (dan moet u het apparaat controleren) of rood (dan loopt uw apparaat een risico). Wanneer er problemen zijn met uw apparaat, klik dan op het uitklappijltje in het bovenste statusgebied voor meer details. Hier kunt u
- **Bescherming.** In dit tabblad kunt u op afstand een snelle of systeemscan uitvoeren op uw apparaten. Klik op de knop **Scan** om de scan te starten. U kunt ook zien wanneer de laatste scan op het apparaat is uitgevoerd en er is een rapport beschikbaar met de belangrijkste gegevens van de laatste scan.
- **Kwetsbaarheid.** Om een apparaat te controleren op kwetsbaarheden zoals ontbrekende Windows-updates, verouderde apps of zwakke wachtwoorden klikt u op de knop **SCANNEN** in het tabblad Kwetsbaarheid. Kwetsbaarheden kunnen niet op afstand worden verholpen. Als er een kwetsbaarheid wordt gevonden, moet u een nieuwe scan uitvoeren op het apparaat en vervolgens de aanbevolen acties ondernemen. Klik op **Meer details** voor een gedetailleerd rapport over de gevonden problemen.

2.6.8. Meldingen

Om u op de hoogte te houden van wat er gebeurt op de apparaten die aan uw account gekoppeld zijn, hebt u de -icoon ter beschikking. Zodra u erop klikt, krijgt u een algemeen beeld met informatie over de activiteit van de Bitdefender-producten die op uw apparaten geïnstalleerd zijn.

2.7. Veelgestelde vragen

Hoe kan ik Bitdefender Antivirus for Mac uitproberen voordat ik een abonnement aanvraag?

Als nieuwe klant van Bitdefender kunt u ons product uitproberen voordat u tot aanschaf overgaat. De proefperiode duurt 30 dagen. Na die tijd kunt u het geïnstalleerde product alleen blijven gebruiken als u een Bitdefender-abonnement neemt. Om Bitdefender Antivirus for Mac vrijblijvend uit te proberen, doet u het volgende:

1. Volg de onderstaande stappen om een Bitdefender-account aan te maken:
   a. Ga naar: https://central.bitdefender.com.
   b. Typ de vereiste informatie in de overeenkomende velden. De gegevens die u hier opgeeft, worden vertrouwelijk behandeld.
   c. Voordat u verdergaat, moet u de Gebruiksvoorwaarden aanvaarden. De Gebruiksvoorwaarden bevatten de voorwaarden waaronder u Bitdefender mag gebruiken; lees ze dus grondig door. U kunt eveneens het Privacybeleid lezen.
   d. Klik op **MAAK ACCOUNT AAN**.
2. Download Bitdefender Antivirus for Mac als volgt:
   a. Selecteer de **Mijn apparaten** paneel en klik vervolgens op **INSTALLEER BESCHERMING**.
   b. Kies een van de twee beschikbare opties:
      - **Bescherm dit apparaat**
        i. Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.

ii. Sla het installatiebestand op.

- **Bescherm andere apparaten**
  i. Selecteer deze optie en selecteer vervolgens de eigenaar van het apparaat. Als het apparaat van iemand anders is, klikt u op de bijbehorende knop.
  ii. Klik **STUUR DOWNLOADLINK**.
  iii. Typ een e-mailadres in het overeenkomstige veld en klik **STUUR E-MAIL**.
  Houd er rekening mee dat de gegenereerde downloadlink alleen de komende 24 uur geldig is. Als de link verloopt, moet u een nieuwe genereren door dezelfde stappen te volgen.
  iv. Controleer op het apparaat waarop u uw Bitdefender-product wilt installeren het e-mailaccount dat u hebt ingevoerd en klik vervolgens op de overeenkomstige downloadknop.

c. Voer het Bitdefender-product uit dat u hebt gedownload.

Ik heb een activeringscode. Hoe kan ik deze aan mijn abonnement toevoegen?

Als u een activeringscode hebt gekocht bij een van onze wederverkopers of als cadeau hebt gekregen, kunt u de beschikbaarheid ervan toevoegen aan uw Bitdefender-abonnement.

Volg deze stappen om een abonnement te activeren met een activeringscode:

1. Toegang Bitdefender Centraal.
2. Selecteer de **mijn abonnementen** paneel.
3. Klik op de **ACTIVATIE CODE** en typ vervolgens de code in het overeenkomstige veld.
4. Klik **ACTIVEREN** doorgaan.

De nieuwe geldigheidsduur is nu zichtbaar in uw Bitdefender-account en rechtsonder in het scherm van Bitdefender Antivirus for Mac.

Volgens het scanlog zijn er nog niet-opgeloste problemen. Hoe kan ik deze problemen oplossen?

De niet-opgeloste problemen kunnen betrekking hebben op:

- Archieven met beperkte toegang (bijvoorbeeld xar of rar)
  Oplossing: gebruik de functie **Tonen in Finder** om naar het bestand te gaan en dit handmatig te verwijderen. Vergeet niet ook de Prullenmand leeg te maken.
- Postbussen met beperkte toegang (bijvoorbeeld Thunderbird)
  Oplossing: gebruik het desbetreffende mailprogramma om het item met het geïnfecteerde bestand te verwijderen.
- Inhoud in backups
  Oplossing: selecteer de optie **Inhoud in back-ups niet scannen** bij Beschermingsvoorkeuren of kies **Toevoegen aan uitzonderingen** om de gedetecteerde bestanden uit te sluiten van de scans.
  Als de geïnfecteerd bestanden later worden teruggezet, wordt dit automatisch door Bitdefender Antivirus for Mac gedetecteerd en zal de juiste actie worden ondernomen.

> **Opmerking**
> Bestanden "met beperkte toegang": dit betekent dat Bitdefender Antivirus for Mac de bestanden wel kan openen, maar niet mag wijzigen.

Waar kan ik informatie opvragen over de activiteiten van het product?

Bitdefender houdt een logboek bij van alle belangrijke acties, statuswijzigingen en andere kritieke berichten over de activiteiten van de applicatie. Om toegang te krijgen tot deze informatie, klikt u in het navigatiemenu in de interface van Bitdefender op **Notificaties**.

Kan ik Bitdefender Antivirus for Mac updaten via een Proxyserver?

Bitdefender Antivirus for Mac kan alleen worden bijgewerkt via proxyservers die geen authenticatie vereisen. U hoeft geen programma-instellingen te configureren.

Als u verbinding maakt met internet via een proxyserver die authenticatie vereist, moet u regelmatig overschakelen naar een directe internetverbinding om updates over bedreigingsinformatie te verkrijgen.

Hoe verwijder ik Bitdefender Antivirus for Mac?

Volg deze stappen om Bitdefender Antivirus for Mac te verwijderen:

1. Open een **Finder**-venster en ga naar de map Programma's.
2. Open de Bitdefender-map en dubbelklik op BitdefenderUninstaller.
3. Klik **Verwijderen** en wacht tot het proces is voltooid.
4. Klik **Dichtbij** af te maken.

> **Belangrijk**
> Als er een fout optreedt, kunt u contact opnemen met de Bitdefender Klantenservice zoals beschreven in Hulp vragen (pagina 307).

Hoe kan ik de TrafficLight-extensies uit mijn webbrowser verwijderen?

- Zo verwijdert u de TrafficLight-extensies uit Mozilla Firefox:
  1. Ga naar **Hulpprogramma's** en selecteer **Add-ons**.
  2. Selecteer **Extensies** in de linkerkolom.
  3. Selecteer de extensie en klik op **Verwijderen**.
  4. Start de browser opnieuw om de verwijdering te voltooien.
- Zo verwijdert u de TrafficLight-extensies uit Google Chrome:
  1. Klik rechtsboven op **Meer** ⋮.
  2. Ga naar **Meer hulpprogramma's** en selecteer **Extensies**.
  3. Klik op het symbool **Verwijderen** naast de extensie die u wilt verwijderen.
  4. Klik op **Verwijderen** om de verwijdering te bevestigen.
- Volg deze stappen om Bitdefender TrafficLight uit Safari te verwijderen:
  1. Ga naar **Voorkeuren** of druk op **Command-Comma(,)**.
  2. Selecteer **Extensies**.
     Er verschijnt een lijst van de geïnstalleerde extensies.
  3. Selecteer de Bitdefender TrafficLight extensie, en klik dan op **Deïnstalleren**.
  4. Klik opnieuw op **Deïnstalleren** om het verwijderingsproces te bevestigen.

Wanneer moet ik Bitdefender VPN gebruiken?

U dient voorzichtig te zijn wanneer u inhoud van het internet bekijkt, downloadt of uploadt. Om te verzekeren dat u veilig bent wanneer u surft op het web, raden we aan dat u Bitdefender VPN gebruikt wanneer u:

- wilt verbinden met publieke draadloze netwerken
- inhoud wilt bekijken die normaal afgeschermd wordt in specifieke gebieden, ongeacht of u thuis of in het buitenland bent
- uw persoonlijke gegevens privé wilt houden (gebruikersnamen, wachtwoorden, kredietkaartgegevens enz.)
- uw IP-adres wilt verbergen

Zal Bitdefender VPN een negatief effect hebben op de batterij van mijn apparaat?

Bitdefender VPN is ontworpen om uw persoonlijke gegevens te beschermen, uw IP-adres te verbergen wanneer uw verbonden bent met onbeveiligde draadloze netwerken en om content te bekijken die in bepaalde landen afgeschermd wordt. Om onnodig verbruik van uw batterij te vermijden, raden we u aan VPN enkel te gebruiken indien nodig, en de verbinding te verbreken wanneer u offline bent.

Waarom is het internet soms trager wanneer ik verbonden ben met Bitdefender VPN?

Bitdefender VPN is ontworpen om u een aangename ervaring te bieden tijdens het surfen. Uw internetconnectiviteit of de afstand met de server waarmee u verbonden bent, kan echter zorgen voor vertraging. In dat geval, indien het niet noodzakelijk is om te verbinden met een server die veraf gehost wordt (bijv. van China naar de VS), raden we aan Bitdefender VPN toe te staan om u automatisch te verbinden met de dichtstbijzijnde server, of een server te vinden die dichter bij uw huidige locatie gelegen is.

3. MOBIELE BEVEILIGING VOOR ANDROID

3.1. Wat is Bitdefender Mobile Security

Online activiteiten zoals facturen betalen, vakanties boeken of goederen en diensten kopen zijn eenvoudig en zonder gedoe. Maar naarmate zoveel activiteiten op het internet geëvolueerd zijn, zijn er grote risico's aan verbonden, en als beveiligingsgegevens genegeerd worden, kunnen persoonsgegevens gehackt worden. En wat is er belangrijker dan de bescherming van uw gegevens in online accounts en op uw persoonlijke smartphone?

Met **Bitdefender Mobile Security** kunt u:

- De beste bescherming krijgen voor uw Android smartphone en tablet met minimale impact op de levensduur van de batterij
- Voorkomen dat u het slachtoffer wordt van op links gebaseerde mobiele oplichting
- Toegang krijgen tot uw beveiligde VPN voor een snelle, anonieme en veilige ervaring tijdens het surfen op het web
- Lokaliseer, vergrendel en wis informatie van uw Android-apparaat van op afstand in het geval van verlies of diefstal
- Controleren of uw e-mailaccount betrokken is geweest bij gegevensinbreuken of datalekken

3.2. Aan de slag

3.2.1. Apparaatvereisten

Bitdefender Mobile Security werkt op alle apparaten met Android 6.0 of latere versies van het besturingssysteem. Een actieve internetverbinding is vereist voor in-the-cloud scannen op dreigingen.

3.2.2. Installeer Bitdefender Mobile Security

- **Vanuit Bitdefender Central**
  - Android
    1. Ga naar: https://central.bitdefender.com.

2. Log in op uw Bitdefender-account.
3. Selecteer het paneel **Mijn apparaten**.
4. Tik op **BESCHERMING INSTALLEREN** en tik vervolgens op **Dit apparaat beschermen**.
5. Selecteer de eigenaar van het apparaat. Als het apparaat toebehoort aan iemand anders, druk dan op de overeenstemmende knop.
6. U wordt doorgestuurd naar **Google Play**. In het scherm van Google Play tikt u op de installatie-optie.

- Op Windows, macOS en iOS
  1. Ga naar: https://central.bitdefender.com.
  2. Meld u aan bij uw Bitdefender-account.
  3. Selecteer de **Mijn apparaten** paneel.
  4. Druk op **BESCHERMING INSTALLEREN** en druk vervolgens op **Andere apparaten beschermen**.
  5. Selecteer de eigenaar van het apparaat. Als het apparaat toebehoort aan iemand anders, druk dan op de overeenstemmende knop.
  6. Druk op **DOWNLOADKOPPELING VERZENDEN**.
  7. Voer in het overeenstemmende veld een e-mailadres in en druk op **E-MAIL VERSTUREN**. De gegenereerde downloadlink is slechts 24 uur geldig. Indien de link vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.
  8. Controleer op het apparaat waarop u Bitdefender wilt installeren, het e-mailadres dat u ingevoerd hebt en druk op de overeenstemmende downloadknop.

- **Vanuit Google Play**
  Zoek Bitdefender Mobile Security om de app te vinden en te installeren.
  Als alternatief kunt u de QR-code scannen:

Voordat u de valideringsstappen kunt volgen, dient u in te stemmen met de Abonnementsovereenkomst. Lees de Abonnementsovereenkomst grondig door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Mobile Security.
Tik op **VERDERGAAN** om verder te gaan naar het volgende venster.

3.2.3. Log in op uw Bitdefender-account

Om Bitdefender Mobile Security te gebruiken, moet u uw apparaat aan een Bitdefender-, Facebook-, Google-, Apple- of Microsoft-account koppelen door vanuit de app in te loggen op uw account. De eerste keer dat u de app opent, wordt u gevraagd in the loggen op een account.

Als u Bitdefender Mobile Security hebt geïnstalleerd vanuit uw Bitdefender-account, probeert de app zich automatisch aan te melden bij dat account.

Om uw apparaat te koppelen aan een Bitdefender-account:

1. Geef in de overeenkomstige velden het e-mailadres en wachtwoord in van uw Bitdefender-account. Hebt u geen Bitdefender-account en wenst u er een aan te maken, klik op de daartoe bestemde link.
2. Tik op **AANMELDEN**.

Om in te loggen via een Facebook-, Google- of Microsoft-account, geeft u de dienst die u wilt gebruiken in bij Of log in met. U wordt doorgestuurd naar de inlogpagina van de gewenste dienst. Volg de instructies om uw account te linken met Bitdefender Mobile Security.

> **Opmerking**
> Bitdefender krijgt geen toegang tot vertrouwelijke informatie, zoals het wachtwoord van de account die u gebruikt om aan te melden of de persoonlijke informatie van uw vrienden en contactpersonen.

3.2.4. Bescherming configureren

Eens u ingelogd bent op de toepassing verschijnt het venster Bescherming configureren. Om uw apparaat te beveiligen, raden we aan dat u de volgende stappen doorloopt:

- **Status abonnement**. Om te worden beschermd door Bitdefender Mobile Security, moet u uw product activeren met behulp van een abonnement, dat aangeeft hoelang u het product mag gebruiken.

Wanneer het abonnement verlopen is, zal de toepassing niet meer werken en is uw apparaat niet langer beschermd.
Tik op IK **HEB EEN CODE**, en vervolgens op **ACTIVEREN**, indien u een activeringscode hebt.
Indien u ingelogd bent met een nieuwe Bitdefender-account en geen activeringscode hebt, kunt u het product 14 dagen lang gratis gebruiken.

- **Webbescherming**. Tik op **ACTIVEREN** indien uw apparaat Toegankelijkheid vereist om Webbescherming te activeren. U wordt dan doorgestuurd naar het menu Toegankelijkheid. Tik op Bitdefender Mobile Security, en schakel de overeenkomstige schakelaar in.
- **Malware scanner**. Voer een eenmalige scan uit om te verzekeren dat uw apparaat geen bedreigingen bevat. Tik op **NU SCANNEN** om het scanproces op te starten.
  Het dashboard verschijnt zodra het scanproces begint. Hier ziet u de beveiligingsstatus van uw apparaat.

3.2.5. Dashboard

Tik op het Bitdefender Mobile Security-pictogram in de app drawer van uw apparaat om de app-interface te openen.

Het Dashboard biedt u informatie over de beveiligingsstatus van uw apparaat en helpt u aan de hand van Autopilot de beveiliging van uw apparaat te verbeteren, door u aanbevelingen te doen over de functies.

De statuskaart bovenaan het venster informeert u aan de hand van expliciete berichten en suggestieve kleuren over de beveiligingsstatus van het apparaat. Indien Bitdefender Mobile Security geen waarschuwingen bevat, is de statuskaart groen. Wanneer er een beveiligingsprobleem werd gedetecteerd, verandert de kleur van de statuskaart naar rood.

Bitdefender Autopilot is uw persoonlijke beveiligingsadviseur om u bij al uw activiteiten een effectieve werking en verhoogde bescherming te bieden. Naargelang de activiteiten die u uitvoert, biedt Bitdefender Autopilot contextuele aanbevelingen op basis van het gebruik en de noden van uw apparaat. Hiermee kunt u de voordelen van de functies die in de toepassing van Bitdefender Mobile Security inbegrepen zijn, ontdekken, en ervan genieten.

Als er een procedure actief is of als u actie moet ondernemen, wordt er in het Dashboard een kaart weergegeven met meer informatie en mogelijke acties.

Vanuit de onderste navigatiebalk hebt u toegang tot de Bitdefender Mobile Security-functies en kunt u eenvoudig navigeren:

Malware Scanner

Hiermee kunt u een scan starten en de optie Opslag scannen inschakelen. Zie Malwarescanner (pagina 212) voor meer informatie.

Webbescherming

Garandeert een veilige surfervaring door u te waarschuwen over mogelijke schadelijke websites. Zie Webbescherming (pagina 215) voor meer informatie.

VPN

Versleutelt internetcommunicatie, om uw privacy te verzekeren ongeacht welk netwerk u gebruikt. Zie VPN (pagina 216) voor meer informatie.

Scam Alert

Houdt u veilig door u te waarschuwen voor schadelijke links die binnenkomen via SMS, berichtentoepassingen en elk type melding. Raadpleeg Scam Alert (pagina 220) voor meer informatie.

Anti-Theft

Hiermee kunt u de Anti-Theft-functies in- of uitschakelen en instellingen configureren. Zie Antidiefstalfuncties (pagina 222) voor meer informatie.

Accountprivacy

Controleert of er een gegevenslek was in uw online accounts. Zie Accountprivacy (pagina 226) voor meer informatie.

App Lock

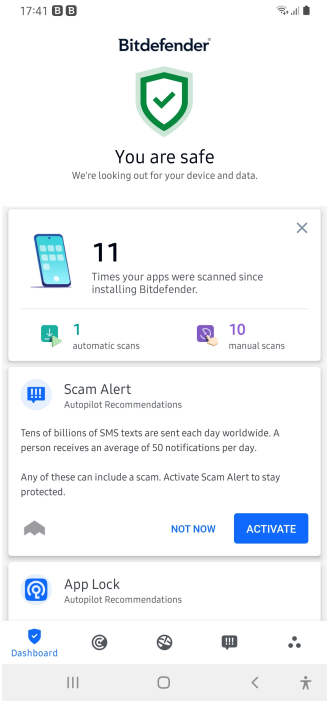
Hiermee kunt u de geïnstalleerde apps beveiligen door een pincode in te stellen. Zie App Lock (pagina 228) voor meer informatie.

Rapporten

Hier wordt een logboek bijgehouden van alle belangrijke acties, statuswijzigingen en andere kritieke berichten over de activiteiten op uw apparaat. Raadpleeg Rapporten (pagina 232) voor meer informatie.

WearON

Deze functie communiceert met uw smartwatch om uw telefoon terug te vinden als deze is zoekgeraakt. Zie WearON (pagina 233) voor meer informatie.



3.3. Malwarescanner

Bitdefender beschermt uw apparaat en uw gegevens tegen schadelijke apps, door scans uit te voeren tijdens de installatie van nieuwe apps. U kunt ook handmatig een scan starten.

De interface van de Malwarescanner biedt een lijst van alle soorten dreigingen waar Bitdefender naar op zoek is, alsook hun definities. Tik op een dreiging om de definitie ervan weer te geven.

Opmerking
Zorg dat uw mobiele apparaat verbonden is met internet. Als uw apparaat geen internetverbinding heeft, kan de scan niet worden gestart.

- **Scannen bij installatie**
  Zodra u een nieuwe app installeert, wordt deze automatisch door Bitdefender Mobile Security gescand met behulp van cloud-technologie. Deze scanprocedure wordt herhaald wanneer u een update van de geïnstalleerde apps uitvoert.
  Als een geïnstalleerde app schadelijk blijkt te zijn, verschijnt er een waarschuwing met het advies de app te verwijderen. Tik dan op **Verwijderen** om naar het verwijderingsscherm voor de app te gaan.
- **Scannen op verzoek**
  Wanneer u wilt controleren of u alle apps op uw apparaat veilig kunt gebruiken, kunt u een scan op aanvraag uitvoeren.
  Om de scan op verzoek te starten:

  1. Tik op **Malware Scanner** in de onderste navigatiebalk.
  2. Tik op **SCAN STARTEN**.

  > **Opmerking**
  > In Android 6 zijn extra machtigingen vereist voor de Malware Scanner-functie. Nadat u de knop **SCAN STARTEN** hebt ingedrukt, selecteert u **Toestaan** voor de volgende items:
  >
  > - **Antivirus** toestaan om telefoongesprekken te starten en te beheren?
  > - **Antivirus** toegang geven tot foto's, media en bestanden op uw apparaat?

  De voortgang van de scan wordt weergegeven. U kunt de scan op elk gewenst moment afbreken.

Bitdefender Mobile Security scant normaal gesproken het interne geheugen van uw apparaat met inbegrip van een eventueel aanwezige SD-kaart (de "opslag"). Hierdoor worden ook schadelijke apps op de geheugenkaart opgespoord voordat ze schade kunnen aanrichten.

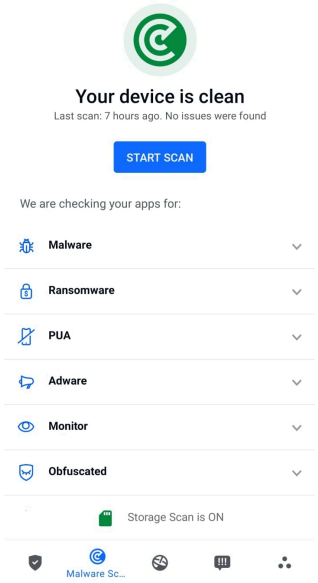
Om de instelling Opslag scannen uit te schakelen:

1. Tik op **Meer** in de onderste navigatiebalk.
2. Tik op **Instellingen**.
3. Schakel de schakelaar **Opslag scannen** in het gebied Malwarescanner uit.

Als er schadelijke apps worden aangetroffen, krijgt u hier bericht over. U kunt deze apps dan verwijderen via de knop **Verwijderen**.

De Malwarescanner-kaart geeft de status van uw apparaat weer. Zolang het apparaat veilig is, is de kaart groen. Wanneer er een scan moet worden uitgevoerd of als u actie moet ondernemen, wordt de kaart rood.

Als uw Android-versie 7.1 of recenter is, kunt u een snelkoppeling gebruiken naar Malware Scanner zodat u scans sneller kunt uitvoeren, zonder de Bitdefender Mobile Security interface te openen. Om dit te doen het Bitdefender icoon op uw startscherm of apps drawer ingedrukt houden, en dan het icoon selecteren.



3.3.1. Detectie van app-afwijkingen

Bitdefender App Anomaly Detection is een nieuwe technologie die is geïntegreerd in de Bitdefender Malware Scanner om een extra beschermingslaag te bieden door voortdurend kwaadaardig gedrag te monitoren en te detecteren en de gebruiker te waarschuwen als er verdachte activiteiten worden geïdentificeerd.

Bitdefender App Anomaly Detection beschermt gebruikers, zelfs als ze onbewust een gevaarlijke app hebben geïnstalleerd die een tijdje inactief is, of een ogenschijnlijk vertrouwde app die de functionaliteit ervan verbreekt en een frauduleuze app wordt.

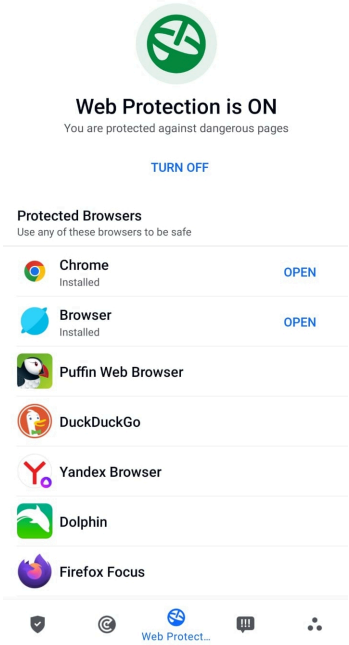
3.4. Webbescherming

Web Protection gebruikt de cloudservices van Bitdefender om de webpagina's te controleren die u bezoekt met de standaard Android-browser, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser en Dolphin.

Opmerking

In Android 6 zijn extra machtigingen vereist voor de functie Webbeveiliging.

Geef de functie toestemming om zich te registreren als een Toegankelijkheid-service en tik op **Aanzetten** wanneer hierom wordt gevraagd. Tik op **Antivirus** en zet de schakelaar aan. Bevestig vervolgens dat u toestemming geeft voor de toegang.



Telkens u een website voor internetbankieren gebruikt, vraagt Bitdefender Web Protection u om Bitdefender VPN te gebruiken. De notificatie verschijnt in de statusbalk. We raden aan dat u Bitdefender VPN gebruikt wanneer u ingelogd bent op uw bankrekening, zodat u beveiligd blijft tegen mogelijke beveiligingsinbreuken.

Om de notificatie Webbescherming uit te schakelen:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Schakel de overeenstemmende schakelaar in het gebied Webbescherming uit.

3.5. VPN

Met Bitdefender VPN houdt u uw data privé telkens u verbindt met onbeveiligde draadloze netwerken in luchthavens, winkelcentra, cafés of hotels. Zo vermijdt u onfortuinlijke situaties, bijvoorbeeld diefstal van

persoonlijke gegevens of pogingen om het IP-adres van uw apparaat toegankelijk te maken voor hackers.

De VPN werkt zoals een tunnel tussen uw apparaat en het netwerk waarmee u verbindt: de VPN beveiligt die verbinding, door aan de hand van versleuteling volgens bankrichtlijnen de gegevens te versleutelen en door uw IP-adres te verbergen, waar u ook bent. Uw dataverkeer wordt omgeleid via een andere server, waardoor het praktisch onmogelijk wordt om uw apparaat te identificeren tussen de talloze andere toestellen die gebruikmaken van onze diensten. Wanneer u via VPN verbonden bent met het internet kunt u bovendien inhoud bekijken die normaal afgeschermd wordt in bepaalde gebieden.

> **Opmerking**
> Sommige landen hanteren internetcensuur. Het gebruik van VPN's is op hun grondgebied dan ook bij wet verboden. Om wettelijke gevolgen te vermijden, is het mogelijk dat er een waarschuwingsbericht verschijnt wanneer u de Bitdefender VPN-app voor het eerst probeert te gebruiken. Door het gebruik van de app verder te zetten, bevestigt u dat u op de hoogte bent van de toepasselijke reguleringen van het land en van de risico's die u mogelijk loopt.

Er zijn twee manieren om Bitdefender VPN in of uit te schakelen:

- Tik in de VPN-kaart op het Dashboard op **VERBINDEN**.
  De status van Bitdefender VPN wordt weergegeven.
- Tik op **VPN** in de onderste navigatiebalk en tik vervolgens op **VERBINDEN**.
  Tik op **VERBINDEN** telkens u bescherming wenst wanneer u verbonden bent met een onbeveiligd draadloos netwerk.
  Tik op **VERBREKEN** wanneer u de verbinding wilt verbreken.

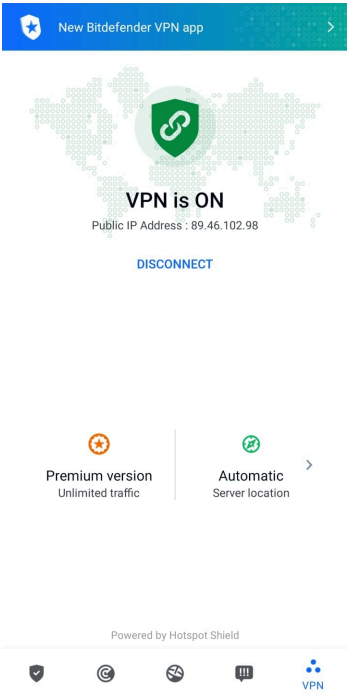
> **Opmerking**
> De eerste keer dat u VPN opstart, zal u worden gevraagd Bitdefender toe te laten een VPN verbinding op te zetten die het netwerkverkeer zal monitoren. Tik op **OK** om verder te gaan.

Als de versie van uw Android 7.1 of hoger is, hebt u toegang tot een snelkoppeling naar Bitdefender VPN, zonder de interface van Bitdefender Mobile Security te openen.

Om dit te doen het Bitdefender icoon op uw startscherm of apps drawer ingedrukt houden, en dan het icoon selecteren.

Om uw batterij te sparen, raden we aan de VPN-functie uit te schakelen wanneer u dit niet gebruikt.

Indien u een premium-abonnement hebt en u de server naar wens wilt veranderen, tik op Serverlocatie in de VPN-functie en selecteer vervolgens de locatie die u wenst. Voor meer info over VPN-abonnementen, raadpleeg



3.5.1. VPN Instellingen

Voor een geavanceerde configuratie van uw VPN:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.

In het VPN-gebied kunt u de volgende opties configureren:

- Snelle toegang VPN - er verschijnt een notificatie in de statusbalk van uw apparaat waarmee u VPN snel kunt inschakelen.
- Waarschuwing Open wifinetwerk - telkens u verbinding maakt met een open wifinetwerk, wordt u via de statusbalk van uw apparaat gevraagd om de VPN te gebruiken.

3.5.2. Abonnementen

Bitdefender VPN biedt dagelijks gratis 200 MB dataverkeer per apparaat om uw verbinding te beveiligen telkens u dit nodig hebt, en verbindt bovendien automatisch met de beste serverlocatie.

Upgrade naar de premium-versie voor onbeperkt dataverkeer en toegang tot afgeschermde inhoud overal ter wereld, doordat u de serverlocatie naar wens kunt selecteren.

U kunt op elk ogenblik upgraden naar de versie Bitdefender Premium VPN door te tikken op **Premium activeren** in het VPN-venster.

Het Bitdefender Premium VPN-abonnement staat los van het Bitdefender Mobile Security-abonnement, wat betekent dat u het kunt gebruiken zolang het beschikbaar is, ongeacht de status van uw beveiligingsabonnement. Als het Bitdefender Premium VPN-abonnement afloopt, maar het abonnement voor Bitdefender Mobile Security nog steeds actief is, wordt u teruggezet naar het gratis plan.

Bitdefender VPN is een cross-platform product en is beschikbaar in de Bitdefender-producten die compatibel zijn met Windows, macOS, Android en iOS. Eens u upgradet naar de premium-versie, kunt u uw abonnement op alle producten gebruiken, op voorwaarde dat u inlogt met dezelfde Bitdefender-account.

> **Opmerking**
> Bitdefender VPN werkt ook als zelfstandige applicatie op alle ondersteunde besturingssystemen, namelijk Windows, macOS, Android en iOS.

3.6. Scam Copilot

Deze functie is in wezen een AI-aangestuurde chatbot die door Bitdefender is getraind om verschillende vormen van oplichting, phishing-pogingen, desinformatiecampagnes en nepwebsites te detecteren.

Om Scam Copilot te activeren:

1. Open de Bitdefender Mobile Security-app. In het dashboard-deelvenster is een kaart met betrekking tot Scam Copilot aanwezig. Tik op **Activeren**.
2. Schakel de toegankelijkheid van Bitdefender Mobile Security in door op de knop **INSCHAKELEN** te tikken.
3. **Sta**Notificatie machtiging toe.

Scam Copilot is nu correct geconfigureerd op uw apparaat.

U kunt toegang krijgen tot het speciale tabblad Scam Copilot. Hier vindt u:

- **Chatbot voor oplichtingsdetectie:** vraag de chatbot om alle berichten die u verdacht vindt, te beoordelen.
- **Preventie-assistent:** helpt u meer te weten te komen over oplichting om vaardig te worden in het herkennen ervan.
- **Automatische scamdetectie** status en configuratiescherm.
- **Sms-filtering**: laat uw gevaarlijke berichten rechtstreeks in uw berichten-app filteren.

3.6.1. Scam Alert

De Scam Alert-functie neemt preventieve maatregelen en pakt potentieel gevaarlijke situaties aan voordat ze een probleem kunnen worden, inclusief malwaredreigingen. Scam Alert controleert alle inkomende SMS-berichten en Android-meldingen in real time.

Wanneer een gevaarlijke link in een bericht op uw telefoon binnenkomt, verschijnt er een waarschuwing op uw scherm. Bitdefender biedt twee opties. De eerste optie is om de informatie te verwerpen. De tweede optie is **DETAILS WEERGEVEN**. Dit geeft u meer informatie over het incident, evenals essentiële adviezen, zoals:

- Open de gedetecteerde koppeling niet en stuur deze niet door.
- Als het om teksten gaat, wis het bericht dan indien mogelijk.
- Blokkeer de afzender als dit geen betrouwbare contactpersoon is.
- Wis de app die gevaarlijke koppelingen verstuurt in notificaties.

Opmerking

Vanwege de beperkingen van het Android-besturingssysteem kan Bitdefender geen tekstberichten verwijderen of directe maatregelen nemen met betrekking tot de SMS-berichten of andere bronnen van schadelijke notificaties. Als u de Scam Alert-waarschuwing negeert en de gevaarlijke koppeling probeert te openen, zal de Web Protection-functie van Bitdefender deze automatisch opvangen en voorkomen dat uw apparaat wordt geïnfecteerd.

Scam Alert activeren

Om Scam Alert in te schakelen, moet u de Bitdefender Mobile Security-app toegang verlenen tot de SMS-berichten en het notificatiesysteem:

1. Open de Bitdefender Mobile Security-app die op uw Android-telefoon of -tablet is geïnstalleerd.
2. Tik in het hoofdscherm van de Bitdefender-app op de optie **Scam Alert** in de onderste navigatiebalk en druk vervolgens op **INSCHAKELEN**.
3. Tik op de knop **TOESTAAN**.
4. Zet Bitdefender Security in de lijst Notificatietoegang op de positie **AAN**.
5. Bevestig de actie door op **TOESTAAN** te drukken.
6. Keer terug naar het Scam Alert-scherm en druk op **TOESTAAN** om Bitdefender de mogelijkheid te geven inkomende SMS-berichten te scannen.

Chatbeveiliging in real time

Chatberichten zijn onze meest comfortabele manier om contact te houden, maar ze zijn ook een gemakkelijke manier voor gevaarlijke koppelingen om u te bereiken.

Als de functie Chatbeveliging actief is, wordt de Scam Alert-module uitgebreid van het beschermen van uw teksten en notificaties tot het beveiligen van uw chats tegen aanvallen op basis van koppelingen, door gevaarlijke koppelingen te detecteren die u tijdens het chatten verzendt of ontvangt.

Om Chatbeveiliging in te schakelen:

1. Open de Bitdefender Mobile Security-app die op uw Android-telefoon of -tablet is geïnstalleerd.
2. Tik in het hoofdscherm van de Bitdefender-app op de optie **Scam Alert** in de onderste navigatiebalk.
3. Bovenaan het tabblad Scam Alert vindt u de functie Chatbeveiliging. Zet de betreffende schakelaar in de stand **AAN**.

> **Opmerking**
> Momenteel is Chatbeveiliging compatibel met de volgende toepassingen:
>
> - WhatsApp
> - Facebook Messenger
> - Telegram
> - Discord

3.7. Antidiefstalfuncties

Bitdefender helpt u bij het terugvinden van uw apparaat en kan verhinderen dat uw gegevens in verkeerde handen vallen.

Hiervoor hoeft u alleen maar Anti-Theft te activeren op het apparaat. Als het nodig blijkt te zijn, kunt u vervolgens vanuit elke webbrowser toegang krijgen tot **Bitdefender Central**.

> **Opmerking**
> In de Antidiefstal-interface vindt u ook een link naar onze Bitdefender Central-app in de Google Play Store. Gebruik deze link om de app te downloaden indien u dat nog niet gedaan hebt.

Bitdefender Mobile Security biedt de volgende Antidiefstalfuncties:

Lokaliseren op afstand

Bekijk de huidige locatie van uw apparaat in Google Maps. De locatie wordt elke 5 seconden vernieuwd, dus u kunt deze volgen indien hij in beweging is.

De nauwkeurigheid van de locatie hangt af van hoe Bitdefender deze kan bepalen:

- Als de GPS is ingeschakeld op het apparaat, kan de locatie worden bepaald tot op enkele meters, zolang deze binnen bereik van GPS-satellieten is (dus niet in een gebouw).
- Indien het apparaat binnenshuis is, kan de locatie worden bepaald tot binnen tientallen meters als Wi-Fi is ingeschakeld en er beschikbare draadloze netwerken in de omtrek zijn.
- Anders wordt de locatie bepaald met gebruikmaking van alleen gegevens van het mobiele netwerk, dat geen betere nauwkeurigheid dan enkele honderden meters kan bieden.

Vergrendelen op afstand

Vergrendel het scherm van uw apparaat en stel een numerieke pincode in, die moet worden ingevoerd om het scherm te ontgrendelen.

Wissen op afstand

U kunt alle persoonlijke gegevens op uw apparaat op afstand wissen als het apparaat niet langer in uw bezit is.

Waarschuwing naar apparaat sturen (Scream-functie)

U kunt op afstand een bericht op het scherm van het apparaat laten weergeven, of een luid geluidssignaal laten afspelen via de luidspreker van het apparaat.

Als het apparaat is zoekgeraakt, kunt u een bericht op het scherm van het apparaat weergeven, zodat de eerlijke vinder weet hoe hij of zij u kan bereiken.

En als u het apparaat niet kunt vinden, terwijl het misschien vlakbij is (bijvoorbeeld ergens in huis of op kantoor), kunt u een luid geluidssignaal laten klinken via de Scream-functie. Dit werkt ook als het apparaat in de stille modus staat.

3.7.1. Antidiefstal activeren

Om de Antidiefstalfuncties te activeren, voltooit u de configuratieprocedure vanaf de Antidiefstalkaart in het Dashboard.

In plaats hiervan kunt u Antidiefstal ook op deze manier activeren:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Tik op **Antidiefstal**.

3. Tik op **INSCHAKELEN**.
4. U kunt deze functie nu als volgt activeren:

   > **Opmerking**
   > In Android 6 zijn extra machtigingen vereist voor de functie Anti-Theft.
   >
   > Volg deze stappen om dit in te schakelen:
   >
   > a. Tik op **Antidiefstal activeren**, tik vervolgens op **INSCHAKELEN**.
   >
   > b. Geef **Antivirus** toestemming om de locatie van uw apparaat te kennen.

   a. **Beheerdersbevoegdheden toekennen**
   Deze bevoegdheden zijn absoluut noodzakelijk om de Anti-Theft-module te kunnen gebruiken. U moet daarom beheerdersbevoegdheden toekennen voordat u verder kunt gaan.

   b. **Pincode van de toepassing instellen**
   Stel een pincode in om ongeoorloofde toegang tot uw apparaat te vermijden. Telkens er een poging wordt gedaan om uw apparaat te gebruiken, moet een pincode worden ingegeven. Voor apparaten die authenticatie via vingerafdruk ondersteunen, kan een bevestiging via vingerafdruk worden ingesteld in plaats van de pincode.
   Dezelfde pincode wordt ook door App Lock gebruikt om uw geïnstalleerde apps te beschermen.

   c. **Snap Photo activeren**
   Telkens iemand het apparaat probeert te ontgrendelen terwijl Snapshot ingeschakeld is, en hier niet in slaagt, neemt Bitdefender een foto van die persoon.
   Meer in detail: telkens wanneer de door u ingestelde pincode, het wachtwoord of de vingerafdruk drie keer na elkaar verkeerd wordt ingevoerd, wordt er een foto gemaakt met de camera aan de voorkant. Deze foto wordt samen met het tijdstempel en de reden opgeslagen. U kunt deze informatie opvragen door Bitdefender Mobile Security te openen en naar het scherm Antidiefstal te gaan.
   Of u kunt de foto bekijken in uw Bitdefender-account.

      i. Ga naar: https://central.bitdefender.com.

ii. Inloggen op uw account.

iii. Selecteer de **Mijn apparaten** paneel.

iv. Selecteer uw Android-apparaat en vervolgens het tabblad **Antidiefstal**.

v. Tik op ⋮ naast **Uw snapshots controleren** om de laatst gemaakte foto's te bekijken.
Alleen de twee recentste foto's worden opgeslagen.

Eens de functie Antidiefstal geactiveerd is, kunt u de Webbeheer-opdrachten vanuit het scherm Antidiefstal individueel in- of uitschakelen door op de bijbehorende opties te tikken.

3.7.2. De Antidiefstalfuncties gebruiken vanuit Bitdefender Central

> **Opmerking**
> Voor alle Anti-Theft-functies is het noodzakelijk dat de optie **Achtergrondgegevens** bij de gegevensgebruik-instellingen van uw apparaat is ingeschakeld.

Zo opent u de Anti-Theft-functies vanuit uw Bitdefender-account:

1. Ga naar **Bitdefender Central**.
2. Selecteer de **Mijn apparaten** paneel.
3. Selecteer in het venster **MIJN APPARATEN** de gewenste apparaatkaart door op de bijbehorende **Details weergeven** knop te tikken.
4. Selecteer het tabblad **Anti-Theft**.
5. Tik op de knop die overeenstemt met de functie die u wilt gebruiken:
   Lokaliseren - geef de locatie van uw apparaat weer in Google Maps.
   IP tonen - geeft het laatste IP-adres voor het geselecteerde apparaat weer.
   Waarschuwing - typ een bericht om op het scherm van uw apparaat te laten weergeven en/of laat het apparaat een geluidssignaal afspelen.
   Vergrendelen - uw toestel vergrendelen en een pincode instellen om het te ontgrendelen.
   Wissen - alle gegevens van uw apparaat verwijderen.

Belangrijk
Nadat u een apparaat hebt gewist, stoppen de functies van Antidiefstal.

3.7.3. Antidiefstalinstellingen.

Als u de opdrachten vanop afstand wilt in- of uitschakelen:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Anti diefstal**.
3. Schakel de gewenste opties in of uit.

3.8. Accountprivacy

Bitdefender Account Privacy gaat na of er gegevensinbreuken hebben plaatsgevonden in de accounts die u gebruikt om online betalingen te verrichten, te winkelen of u aan te melden bij verschillende toepassingen of websites. De gegevens die in een account opgeslagen zijn, kunnen wachtwoorden, kredietkaartinformatie of bankrekeninginformatie betreffen en, indien niet goed beveiligd, kan er sprake zijn van identiteitsdiefstal of inbreuk op uw privacy.

De privacystatus van een account wordt weergegeven na de validering.

Automatische nieuwe controles zijn geprogrammeerd om in de achtergrond uitgevoerd te worden, maar u kunt ook dagelijks manuele scans lanceren.

Telkens wanneer er nieuwe inbreuken worden ontdekt op gevalideerde e-mailaccounts, worden notificaties weergegeven.

Om vanaf nu persoonlijke informatie veilig te houden:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Tik op **Accountprivacy**.
3. Tik op **AAN DE SLAG**.
4. Het e-mailadres dat werd gebruikt om uw Bitdefender-account te maken, verschijnt, en wordt automatisch toegevoegd aan de lijst van gemonitorde accounts.

5. Om een andere account toe te voegen, tikt u in het venster Accountprivacy op **ACCOUNT TOEVOEGEN** en voert u het e-mailadres in.
   Tik op **TOEVOEGEN** om door te gaan.
   Bitdefender moet deze account valideren voordat persoonlijke informatie wordt weergegeven. Daarom werd een e-mailbericht met valideringscode verzonden naar het opgegeven e-mailadres.
   Controleer uw Postvak IN en tik vervolgens de ontvangen code in het vakje **Accountprivacy** van uw app in. Indien u de bevestigingse-mail niet in uw Postvak IN vindt, controleer uw Ongewenste mail.
   De privacystatus van de gevalideerde account wordt weergegeven.

Indien er in een van uw accounts inbreuken worden gevonden, bevelen we u aan het wachtwoord zo snel mogelijk te wijzigen. Om een sterk en veilig wachtwoord te creëren, kunt u deze tips in gedachten houden:

- Zorg ervoor dat het minstens acht karakters lang is.
- Gebruik kleine letters en hoofdletters.
- Voeg ten minste een cijfer of symbool toe, zoals #, @, % of !.

Eens u een account die deel uitmaakte van een privacyschending beveiligd hebt, kunt u de wijzigingen bevestigen door de geïdentificeerde inbreuken aan te duiden als Opgelost. Om dit te doen:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Accountprivacy**.
3. Tik op de account die u net beveiligd hebt.
4. Tik op de inbreuk waarvoor u de account beveiligd hebt.
5. Tik op **OPGELOST** om te bevestigen dat de account beveiligd is.

Wanneer alle gedetecteerde inbreuken aangeduid zijn als **Opgelost**, wordt de account niet langer gemarkeerd als geschonden, tot er een nieuwe inbreuk wordt ontdekt.

Om geen notificaties meer te ontvangen telkens een automatische scan wordt uitgevoerd:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.

3. Schakel de bijbehorende schakelaar in het gebied Accountprivacy uit.

3.9. App Lock

Bepaalde apps, bijvoorbeeld voor e-mail, foto's of berichten, bevatten persoonlijke informatie die u waarschijnlijk graag privé wilt houden. U kunt deze informatie beschermen door de toegang tot deze apps te beperken.

Via App Lock kunt u apps beveiligen met een speciale pincode, zodat onbevoegden deze apps niet meer kunnen gebruiken. U moet hiervoor een pincode van minimaal 4 en maximaal 8 cijfers instellen. Elke keer dat u een van de beveiligde apps wilt gebruiken, moet u deze pincode invoeren.

Biometrische verificatie (zoals vingerafdrukbevestiging of gezichtsherkenning) kan worden gebruikt in plaats van de geconfigureerde pincode.

3.9.1. App Lock activeren

Om de toegang tot bepaalde apps te beperken, configureert u App Lock vanaf de kaart die in het Dashboard wordt weergegeven nadat Antidiefstal is geactiveerd.

In plaats hiervan kunt u App Lock ook op deze manier activeren:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Tik op **App Lock**.
3. Kraan **AANZETTEN**.
4. Toegang tot gebruikersgegevens toestaan voor Bitdefender Security.
5. Sta **Weergeven over andere toepassingen** toe.
6. Ga terug naar de app, configureer de toegangscode en tik op **Pincode instellen**.

   > **Opmerking**
   > Deze stap is alleen beschikbaar als u nog geen pincode voor Antidiefstal hebt ingesteld.

7. Gebruik de optie Snapshot om indringers te betrappen die proberen toegang te krijgen tot uw persoonlijke gegevens.

Opmerking

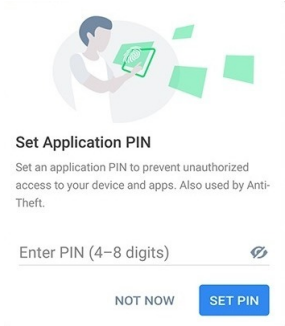
In Android 6 zijn extra machtigingen vereist voor de functie Snapshot. Om deze functie in te schakelen, moet u **Antivirus** toestemming geven om foto's te maken en video's op te nemen.

8. Selecteer welke toepassingen u wilt beschermen.

Als vijf keer achter elkaar een verkeerde pincode of vingerafdruk wordt gebruikt, wordt een time-out van 30 seconden gestart. Hierdoor wordt het vrijwel onmogelijk om in de beveiligde apps in te breken.

Opmerking

Dezelfde pincode wordt ook door Antidiefstal gebruikt.



3.9.2. Vergrendelmodus

De eerste keer dat u een toepassing aan App Lock toevoegt, verschijnt het venster App Lock Mode. Hier kunt u kiezen wanneer de functie App Lock de toepassingen op uw apparaat moet beschermen.

U kunt kiezen uit deze opties:

- **Telkens ontgrendelen** - telkens wanneer de vergrendelde toepassingen worden gebruikt, moet de pincode of vingerafdruk die u hebt ingesteld, worden gebruikt.
- **Ontgrendeld houden tot scherm uit** - de toepassingen zijn toegankelijk totdat het scherm wordt uitgeschakeld.
- **Vergrendelen na 30 seconden** - u kunt uw niet-vergrendelde toepassingen verlaten en binnen 30 seconden terug openen.

Als u de geselecteerde instelling wilt wijzigen:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Tik in het gebied App Lock op **Telkens ontgrendelen**.
4. Kies de gewenste optie.

3.9.3. App Lock-instellingen

Voor een geavanceerde configuratie van App Lock:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.

In het gebied App Lock kunt u de volgende opties configureren:

- **Suggestie gevoelige toepassing** - ontvang een lock-notificatie telkens u een gevoelige toepassing installeert.
- **Telkens ontgrendelen** - kies een van de beschikbare vergrendelings- en ontgrendelingsopties.
- **Smart Unlock** - houdt toepassingen ontgrendeld wanneer u verbonden bent met vertrouwde wifinetwerken.
- V**Willekeurig toetsenbord** - voorkom PIN-aflezing door de posities van de getallen te randomiseren.

3.9.4. Snapshot

Met Bitdefender Snap Photo kunt u uw vrienden of familie op heterdaad betrappen. Zo kunt u hen een lesje leren, zodat ze niet langer nieuwsgierig uw persoonlijke bestanden doorlopen of de apps bekijken die u gebruikt.

Deze functie werkt heel eenvoudig: telkens wanneer de pincode of vingerafdruk drie keer achter elkaar verkeerd wordt ingevoerd, wordt er een foto gemaakt met de camera aan de voorkant. Deze foto wordt samen met het tijdstempel en de reden opgeslagen. U kunt deze informatie opvragen via de App Lock-functie van Bitdefender Mobile Security.

> **Opmerking**
> Deze functie is alleen beschikbaar op apparaten die aan de voorkant beschikken over een camera.

Om de functie Snapshot voor App Lock te configureren:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Schakel de bijbehorende schakelaar in het gebied Snapshot in.

De foto's die tijdens het invoeren van een incorrecte pincode worden gemaakt, worden in het venster App Lock weergegeven en kunnen in het volledige scherm worden bekeken.

U kunt de foto's ook bekijken in uw Bitdefender-account:

1. Ga naar: https://central.bitdefender.com.
2. Meld u aan bij uw account.
3. Selecteer het paneel **Mijn apparaten**.
4. Selecteer uw Android-apparaat en vervolgens het **Anti diefstal** tabblad.
5. Kraan naast **Controleer uw momentopnamen** om de laatste gemaakte foto's te bekijken.

Alleen de twee meest recente foto's worden opgeslagen.

Om de genomen foto's niet langer naar uw Bitdefender-account te uploaden:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Schakel **Foto's uploaden** in het gebied Snapshot uit.

3.9.5. Smart Unlock

Met Smart Unlock kunt u heel eenvoudig voorkomen dat u elke keer een pincode of vingerafdrukscan nodig hebt voor de beveiligde apps.

U kunt bepaalde Wi-Fi-netwerken als 'vertrouwd' aanmerken, zodat de App Lock-blokkeringsinstellingen worden uitgeschakeld zolang u via een van deze netwerken verbonden bent met internet.

Zo configureert u de functie Smart Unlock:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Applicatie vergrendeling**.

3. Tik op de knop.
4. Tik op de schakelaar naast **Smart Unlock** indien de voorziening nog niet ingeschakeld is.
   Valideer aan de hand van uw vingerafdruk of uw pincode.
   Wanneer u de voorziening voor het eerst activeert, moet u de locatiemachtiging inschakelen. Tik op de knop **TOESTAAN** en klik vervolgens opnieuw op **TOESTAAN**.
5. Tik op **TOEVOEGEN** om de wifiverbinding die u momenteel gebruikt, als vertrouwd in te stellen.

Als u later van mening verandert, kunt u de functie weer uitschakelen. De vertrouwde Wi-Fi-netwerken worden dan niet langer vertrouwd.

3.10. Rapporten

De Rapporten-functie houdt een uitgebreid logboek bij van gebeurtenissen met betrekking tot de scanactiviteiten op uw apparaat.

Elke keer dat er iets gebeurt dat van belang is voor de beveiliging van het apparaat, wordt een nieuw bericht toegevoegd aan de rapporten.

Zo opent u de Rapporten:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Tik op **Rapporten**.

Het venster Rapporten bevat de volgende tabbladen:

- **Weekrapporten** - hier kunt u de beveiligingsstatus en de uitgevoerde taken van de huidige en de vorige week bekijken. Elke zondag wordt het rapport van de afgelopen week gegenereerd. U krijgt bericht wanneer het weekrapport beschikbaar is.
  Elke week wordt hier een nieuwe tip weergegeven, dus kom hier regelmatig terug om uw app zo goed mogelijk te leren gebruiken.
  Om geen notificaties meer te ontvangen telkens een rapport werd gegenereerd:

  1. Kraan **Meer** op de onderste navigatiebalk.
  2. Kraan **Instellingen**.
  3. Schakel de schakelaar **Notificatie nieuw rapport** uit in het gebied Rapporten.

- **Activiteitenlogboek** - hier kunt u gedetailleerde informatie bekijken over de activiteiten van uw Bitdefender Mobile Security-app vanaf het moment van installatie op uw Android-apparaat.
  Om het beschikbare activiteitenlogboek te verwijderen:

  1. Kraan **Meer** op de onderste navigatiebalk.
  2. Kraan **Instellingen**.
  3. Tik op **Activiteitenlogboek wissen** en tik vervolgens op **WISSEN**.

3.11. WearON

Met Bitdefender WearON kunt u uw smartphone heel gemakkelijk terugvinden als u deze bent kwijtgeraakt, bijvoorbeeld op kantoor of thuis. Deze functie werkt ook als de stille modus van de telefoon actief is.

Zorg dat deze functie altijd ingeschakeld is, zodat u uw smartphone zo nodig gemakkelijk kunt terugvinden.

> **Opmerking**
> Deze functie werkt met Android 4.3 en Android Wear.

3.11.1. WearON activeren

Om WearON te gebruiken, koppelt u uw smartwatch aan Bitdefender Mobile Security en activeert u de WearON-functie met deze spraakopdracht:

Start:<Waar is mijn telefoon>

Bitdefender WearON heeft twee opdrachten:

1. **Phone Alert**
   De functie Phone Alert waarschuwt u als u te ver van uw smartphone verwijderd bent.
   Indien u uw smartwatch bij zich hebt, detecteert deze automatisch de toepassing op uw telefoon en trilt wanneer u te ver verwijderd bent van uw telefoon, en in het bijzonder wanneer de Bluetooth-verbinding wordt verbroken.
   U kunt deze functie als volgt inschakelen: open Bitdefender Mobile Security, tik in het menu op **Algemene instellingen** en activeer de schakelaar in het gedeelte WearON.

2. **Scream**
   Als uw telefoon toch is zoekgeraakt, kunt u vanaf uw smartwatch een Scream-opdracht naar de telefoon sturen om een luid geluidssignaal op de telefoon te laten klinken.

3.12. Info

Voor meer informatie over de Bitdefender Mobile Security-versie die u geïnstalleerd hebt, raadpleeg de Abonnementsovereenkomst en het Privacybeleid en bekijk de Open source-licenties.

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Tik op de gewenste optie in het gebied Over.

3.13. Veelgestelde vragen

Waarom is er voor Bitdefender Mobile Security een internetverbinding nodig?

De applicatie moet met Bitdefender-servers communiceren om te kunnen bepalen of de geïnstalleerde applicaties en de bezochte webpagina's wel veilig zijn, en ook om opdrachten vanaf uw Bitdefender-account te kunnen ontvangen wanneer u de Anti-Theft-functies gebruikt.

Waar heeft Bitdefender Mobile Security elke toestemming voor nodig?

- Internettoegang -> nodig voor communicatie met de cloud.
- Telefoonstatus en -identiteit lezen -> wordt gebruikt om te bepalen of het apparaat verbonden is met internet en om bepaalde apparaatinformatie op te vragen, waarmee een unieke ID kan worden samengesteld voor de communicatie met de Bitdefender-cloud.
- Browserfavorieten lezen en schrijven -> de module Webbeveiliging verwijdert schadelijke websites uit uw browsergeschiedenis.
- Loggegevens lezen -> Bitdefender Mobile Security detecteert sporen van dreigingsactiviteiten in de Android-logboeken.
- Locatie -> nodig voor lokalisatie op afstand.
- Camera -> nodig voor Snapshot.

- Opslag -> nodig om de Malwarescanner ook de SD-kaart te laten scannen.

Hoe dien ik niet langer informatie in bij Bitdefender over verdachte toepassingen?

Bitdefender Mobile Security stuurt standaard rapporten naar de Bitdefender-servers over verdachte toepassingen die u installeert. Deze informatie is van essentieel belang voor de verbetering van de detectie van dreigingen en kan ons helpen om u in de toekomst een betere ervaring te bieden. Voor het geval u wilt stoppen met het ons toesturen van informatie over verdachte apps:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Schakel **In-de-cloud-detectie** in het gebied Malwarescanner uit.

Waar zie ik de details over de activiteit van de toepassing?

Bitdefender Mobile Security houdt een logboek bij van alle belangrijke acties, statuswijzigingen en andere kritische boodschappen die gelinkt zijn aan de activiteiten. Om de activiteiten van de toepassing te bekijken:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **rapporten**.
   In het venster WEKELIJKSE RAPPORTEN kunt u de rapporten bekijken die wekelijks worden opgesteld en in het venster ACTIVITEITENLOGBOEK ziet u de informatie over de activiteiten van uw Bitdefender-toepassing.

Ik ben de pincode vergeten waarmee ik mijn app heb beveiligd. Wat moet ik doen?

1. Toegang Bitdefender Centraal.
2. Selecteer de **Mijn apparaten** paneel.
3. Tik op de gewenste apparaatkaart en vervolgens op ⋮ in de rechterbovenhoek van het scherm.
4. Selecteer **Instellingen**.
5. De pincode wordt weergegeven in het veld **Applicatiepincode**.

Hoe kan ik de pincode die ik heb ingesteld voor App Lock en Antidiefstal wijzigen?

Als u de pincode die u ingesteld hebt voor App Lock of Antidiefstal wilt wijzigen:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Instellingen**.
3. Tik in het gebied Antidiefstal op Beveiliging **PINCODE**.
4. Voer de huidige pincode in.
5. Voer de nieuwe pincode in die u wilt configureren.

Hoe kan ik App Lock uitzetten?

U kunt de App Lock-functie als zodanig niet uitzetten, maar u kunt de functie wel heel eenvoudig uitschakelen door de selectievakjes naast alle geselecteerde apps leeg te maken. (Hiervoor hebt u uw pincode of vingerafdruk nodig.).

Hoe kan ik een ander draadloos netwerk instellen als vertrouwd netwerk?

Eerst moet u uw apparaat verbinden met het draadloze netwerk dat u als vertrouwd hebt ingesteld. Volg vervolgens deze stappen:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Kraan **Applicatie vergrendeling**.
3. Tik op in de rechterbovenhoek.
4. Tik naast het netwerk dat u als vertrouwd wilt instellen, op **TOEVOEGEN**.

Hoe kan ik de snapshots die op mijn apparaten genomen zijn, niet meer zien?

Om de op uw apparaten gemaakte fotosnaps niet langer zichtbaar te maken:

1. Toegang Bitdefender Centraal.
2. Tik op rechtsboven op het scherm.
3. Tik op **Instellingen** in het schuifmenu.
4. Deactiveer de optie **Snapshots die met uw apparaten zijn gemaakt, tonen/niet tonen**.

Hoe kan ik veilig online blijven winkelen?

Online winkelen gaat gepaard met hoge risico's als u enkele details over het hoofd ziet. Om niet het slachtoffer te worden van fraude, bevelen wij u het volgende aan:

- Houd uw beveiligingsapp up to date.
- Voer enkel online betalingen met kopersbescherming uit.
- Gebruik een VPN wanneer u een verbinding maakt met het internet via openbare en onbeveiligde draadloze netwerken.
- Wees aandachtig voor de wachtwoorden die u hebt toegekend aan uw online accounts. Ze moeten sterk zijn, met hoofdletters en kleine letters, cijfers en symbolen (@, !, %, #, etc.).
- Zorg ervoor dat de informatie die u verzendt, via veilige verbindingen gaat. De online website-extensies moet HTTPS://, zijn, niet HTTP://.

Wanneer moet ik Bitdefender VPN gebruiken?

U dient voorzichtig te zijn wanneer u inhoud van het internet bekijkt, downloadt of uploadt. Om te verzekeren dat u veilig bent wanneer u surft op het web, raden we aan dat u Bitdefender VPN gebruikt wanneer u:

- wilt verbinden met publieke draadloze netwerken
- inhoud wilt bekijken die normaal afgeschermd wordt in specifieke gebieden, ongeacht u thuis of in het buitenland bent
- uw persoonlijke gegevens privé wilt houden (gebruikersnamen, wachtwoorden, kredietkaartgegevens enz.)
- uw IP-adres wilt verbergen

Zal Bitdefender VPN een negatief effect hebben op de batterij van mijn apparaat?

Bitdefender VPN is ontworpen om uw persoonlijke gegevens te beschermen, uw IP-adres te verbergen wanneer uw verbonden bent met onbeveiligde draadloze netwerken en om content te bekijken die in bepaalde landen afgeschermd wordt. Om onnodig verbruik van uw batterij te vermijden, raden we u aan VPN enkel te gebruiken indien nodig, en de verbinding te verbreken wanneer u offline bent.

Waarom is het internet soms trager wanneer ik verbonden ben met Bitdefender VPN?

Bitdefender VPN is ontworpen om u een aangename ervaring te bieden tijdens het surfen. Uw internetconnectiviteit of de afstand met de server

waarmee u verbonden bent, kan echter zorgen voor vertraging. In dat geval, indien het niet noodzakelijk is om te verbinden met een server die veraf gehost wordt (bijv. van China naar de VS), raden we aan Bitdefender VPN toe te staan om u automatisch te verbinden met de dichtstbijzijnde server, of een server te vinden die dichter bij uw huidige locatie gelegen is.

Kan ik het Bitdefender-account dat aan mijn apparaat is gekoppeld wijzigen?

Ja, u kunt als volgt wijzigen welke Bitdefender-account aan uw apparaat is gekoppeld:

1. Kraan **Meer** op de onderste navigatiebalk.
2. Tik op uw e-mailadres.
3. Tik op **Uitloggen van account**. Is er een pincode geconfigureerd, wordt u gevraagd deze in te voeren.
4. Bevestig uw keuze.
5. Voer het e-mailadres en wachtwoord van uw account in de overeenkomende velden in en tik dan op **AANMELDEN**.

Hoe beïnvloedt Bitdefender Mobile Security de prestaties van mijn apparaat en de autonomie van de batterij?

We hebben dit effect tot een minimum beperkt. De toepassing wordt enkel uitgevoerd wanneer dit van essentieel belang is - nadat u een toepassing installeert, wanneer u de interface van de toepassing gebruikt of wanneer u een beveiligingscontrole wenst. Bitdefender Mobile Security is niet op de achtergrond actief wanneer u telefoongesprekken voert, een sms-bericht invoert of een spel speelt.

Wat is apparaatbeheerder?

Apparaatbeheerder is een Android-functie die Bitdefender Mobile Security de benodigde bevoegdheden geeft om bepaalde taken op afstand te kunnen uitvoeren. Zonder deze bevoegdheden zou vergrendeling op afstand niet werken en zouden niet alle gegevens op afstand kunnen worden gewist. Als u de app wilt verwijderen, moet u eerst deze machtigingen intrekken via **Instellingen > Beveiliging > Apparaatbeheerders kiezen**.

Hoe de fout "Geen Google-token" oplossen die verschijnt bij het aanmelden bij Bitdefender Mobile Security.

Deze fout treedt op als het apparaat niet aan een Google-account is gekoppeld of als het apparaat wel aan een account is gekoppeld, maar er vanwege een tijdelijk probleem geen verbinding met Google gemaakt kan worden. Probeer een van de volgende oplossingen:

- Ga naar Android Instellingen > Applicaties > Applicatiebeheer > Bitdefender Mobile Security en tik op **Gegevens wissen**. Probeer vervolgens opnieuw in te loggen.
- Controleer of uw apparaat is gekoppeld aan een Google-account.
  Dit kunt u als volgt controleren: ga naar Instellingen > Accounts & synchronisatie en kijk of er een Google-account wordt weergegeven onder **Accounts beheren**. Voeg uw account toe als er geen account wordt weergegeven, start het apparaat opnieuw op en probeer opnieuw in te loggen op Bitdefender Mobile Security.
- Start het apparaat opnieuw op en probeer opnieuw in te loggen.

In welke talen is Bitdefender Mobile Security beschikbaar?

Bitdefender Mobile Security is momenteel beschikbaar in de volgende talen:

- Braziliaans
- Tsjechisch
- Nederlands
- Engels
- Frans
- Duits
- Grieks
- Hongaars
- Italiaans
- Japans
- Koreaans
- Pools
- Portugees
- Roemeens

- Russisch
- Spaans
- Zweeds
- Thais
- Turks
- Vietnamees

In de toekomst komen nog meer talen beschikbaar. Om de taal voor de interface van Bitdefender Mobile Security te wijzigen, gaat u naar de instellingen voor **Taal en toetsenbord** van uw apparaat en kiest u de gewenste taal.

4. MOBIELE BEVEILIGING VOOR IOS

4.1. Wat is Bitdefender Mobile Security voor iOS

Online activiteiten zoals facturen betalen, vakanties boeken of goederen en diensten kopen zijn eenvoudig en zonder gedoe. Maar naarmate zoveel activiteiten op het internet geëvolueerd zijn, zijn er grote risico's aan verbonden en als beveiligingsgegevens genegeerd worden, kunnen persoonsgegevens gehackt worden. En wat is er belangrijker dan de bescherming van uw gegevens in online rekeningen en op uw persoonlijke smartphone?

Bitdefender Mobile Security for iOS kunt u:

- Biedt de krachtigste bescherming tegen bedreigingen met de minste impact op de batterij
- Bescherm je persoonlijke gegevens: wachtwoorden, adres, sociale en financiële informatie
- Controleer gemakkelijk de beveiliging van uw telefoon om misconfiguraties die deze zouden kunnen blootstellen, op te sporen en op te lossen
- Voorkom accidentele blootstelling en misbruik van gegevens voor alle geïnstalleerde apps
- Scant uw apparaat om optimale beveiligings- en privacy-instellingen te bereiken
- Krijg inzicht in het gebruik van je online activiteiten en de geschiedenis van voorkomen incidenten
- Controleer uw online accounts op gegevensinbreuken of datalekken
- Versleutel het internetverkeer met de bijgeleverde VPN

Bitdefender Mobile Security voor iOS wordt gratis geleverd en vereist de activering met een Bitdefender-account. Sommige belangrijke functies van Bitdefender, zoals onze module 'Webbescherming', vereisen echter een betaald abonnement om toegankelijk te zijn voor onze gebruikers.

4.2. Aan de slag

4.2.1. Apparaatvereisten

Bitdefender Mobile Security voor iOS werkt op elk apparaat met iOS 12 of latere versies van het besturingssysteem, en heeft een actieve internetverbinding nodig om te worden geactiveerd en om te detecteren of er gegevens zijn gelekt in uw online accounts.

4.2.2. Installeren van Bitdefender Mobile Security voor iOS

- **Vanuit Bitdefender Central**
  - Op iOS
    1. Ga naar **Bitdefender Central**.
    2. Selecteer het paneel **Mijn apparaten**.
    3. Tik op **BESCHERMING INSTALLEREN** en tik vervolgens op **Dit apparaat beschermen**.
    4. Selecteer de eigenaar van het apparaat. Als het apparaat toebehoort aan iemand anders, druk dan op de overeenstemmende knop.
    5. U wordt doorgestuurd naar de **App Store**. Tik in dat scherm op de installatie-optie.
  - Op Windows, macOS, Android
    1. Toegang Bitdefender Centraal.
    2. Selecteer de **Mijn apparaten** paneel.
    3. Druk op **BESCHERMING INSTALLEREN** en druk vervolgens op **Andere apparaten beschermen**.
    4. Selecteer de eigenaar van het apparaat. Als het apparaat toebehoort aan iemand anders, druk dan op de overeenstemmende knop.
    5. Druk op **DOWNLOADKOPPELING VERZENDEN**.
    6. Voer in het overeenstemmende veld een e-mailadres in en druk op **E-MAIL VERSTUREN**. De gegenereerde downloadlink

is slechts 24 uur geldig. Indien de link vervalt, dient u aan de hand van dezelfde stappen een nieuwe te genereren.

7. Controleer op het apparaat waarop u Bitdefender wilt installeren, het e-mailadres dat u ingevoerd hebt en druk op de overeenstemmende downloadknop.

- **Vanuit de App Store**
  Zoek Bitdefender Mobile Security voor iOS om de toepassing te vinden en te installeren.

De eerste keer dat u de toepassing opent, wordt een introductievenster over de producteigenschappen geopend. Tik op Starten om verder te gaan naar het volgende venster.

Voordat u de valideringsstappen volgt, moet u de Abonnementsovereenkomst aanvaarden. Lees de Abonnementsovereenkomst grondig door: deze bevat de algemene voorwaarden voor uw gebruik van Bitdefender Mobile Security voor iOS.

Tik op **Verdergaan** om verder te gaan naar het volgende venster.

4.2.3. Log in op uw Bitdefender-account

Om Bitdefender Mobile Security for iOS te gebruiken, moet u uw apparaat aan een Bitdefender-, Facebook-, Google-, Apple-account koppelen door vanuit de app in te loggen op uw account. De eerste keer dat u de app opent, wordt u gevraagd in the loggen op een account.

Om uw apparaat te koppelen aan een Bitdefender-account:

1. Voer het e-mailadres voor uw Bitdefender-account in het bijhorende veld in en tik op **VOLGENDE**. Als u nog geen Bitdefender-account hebt en u er eentje wilt aanmaken, selecteert u de bijhorende link en volgt u de instructies op het scherm tot de account is geactiveerd.
   Om in te loggen via een Facebook-, Google-, Apple- of Microsoft-account, geeft u de dienst die u wilt gebruiken in bij **Of log in met**. U wordt doorgestuurd naar de inlogpagina van de gewenste dienst. Volg de instructies om uw account te linken met Bitdefender Mobile Security for iOS.

Opmerking
Bitdefender krijgt geen toegang tot vertrouwelijke informatie, zoals het wachtwoord van de account die u gebruikt om aan te melden of de persoonlijke informatie van uw vrienden en contactpersonen.

2. Voer uw wachtwoord in en tik op **AANMELDEN**.

Van hieruit hebt u ook toegang tot het privacybeleid van Bitdefender.

4.2.4. Dashboard

Tik op het Bitdefender Mobile Security for iOS-pictogram in de app drawer van uw apparaat om de app-interface te openen.

De eerste keer dat u de app opent, wordt u gevraagd om Bitdefender toe te staan u notificaties te sturen. Tik op **Toestaan** om op de hoogte te blijven telkens Bitdefender iets over uw app moet communiceren. Om de Bitdefender-notificaties te beheren, gaat u naar Instellingen > Notificaties > Mobiele Beveiliging.

Om toegang te krijgen tot de sectie die u nodig hebt, tikt u op de bijhorende pictogram onder in het scherm.

Webbescherming

Blijf veilig tijdens het surfen en wanneer minder beveiligde toepassingen toegang proberen te verkrijgen tot niet-vertrouwde domeinen. Raadpleeg Webbescherming (pagina 249) voor meer informatie.

VPN

Bescherm uw privacy op alle netwerken door uw internetcommunicatie te versleutelen. Raadpleeg VPN (pagina 251) voor meer informatie.

Accountprivacy

Ga na of er lekken zijn in uw e-mailaccounts. Zie Account Privacy (pagina 254) voor meer informatie.

Om andere opties te bekijken, tik op de ···-icoon van uw apparaat terwijl de toepassing op het startscherm staat. U ziet de volgende opties verschijnen:

- **Aankopen herstellen** - van hieruit kunt u teruggaan naar de vorige abonnementen die u via uw iTunes-account hebt aangekocht.
- **Instellingen** - van hieruit hebt u toegang tot:

- **VPN-instellingen**
  - **Overeenkomst**> - u kunt de voorwaarden lezen waaronder u de Bitdefender VPN-dienst gebruikt. Tikt u op **Niet meer akkoord**, dan kunt u Bitdefender VPN niet meer gebruiken, totdat u tikt op **Akkoord**.
  - **Waarschuwing open wifi** - u kunt de productnotificatie die verschijnt telkens u een verbinding maakt met een onbeveiligd wifinetwerk in- of uitschakelen.
    Deze notificatie is bedoeld om u te helpen uw gegevens privé en beveiligd te houden door Bitdefender VPN te gebruiken.
- **Webbeschermingsinstellingen**
  - **Overeenkomst**> - u kunt de voorwaarden lezen waaronder u de Bitdefender VPN-dienst gebruikt. Tikt u op **Niet meer akkoord**, dan kunt u Bitdefender VPN niet meer gebruiken, totdat u tikt op **Akkoord**.
  - **Notificatie voor Webbescherming inschakelen** - Laat u weten dat Webbescherming kan worden ingeschakeld na het beëindigen van een VPN-sessie.
- **Productrapporten**

- **Feedback** - hier lanceert u het standaard e-mailprogramma om ons feedback te sturen over de toepassing.
- **Info toepassing** - hier hebt u toegang tot informatie over de geïnstalleerde versie alsook de Abonnementsovereenkomst, het Privacybeleid en de naleving van de Open source-licenties.

4.3. Scan

Met Bitdefender Mobile Security voor iOS kunt u uw apparaat scannen op kwetsbaarheden in de beveiliging en mogelijke dreigingen op uw apparaat. Het uitvoeren van de scan controleert op:

- **OS-versie:** Controleren van uw iOS-versie op de laatste updates.
- **Wachtwoordcode/Biometrie:** Controle van het beveiligingsniveau met betrekking tot de toegang tot uw apparaat.

- **Webbescherming:** Controleren van de status van de webbeschermingsmodule
- **Accountprivacy:** Controle op de aanwezigheid van bewaakte accounts in de accountprivacy-module.
- **Scan wifi:** Controleert de beveiligingsstatus van het huidige verbonden netwerk.

De beschermingsstatus wordt bepaald nadat u een handmatige scan hebt uitgevoerd.

Na het uitvoeren van de eerste scan krijgt u de Autopilot-aanbevelingen van Bitdefender te zien. Dit is uw persoonlijke beveiligingsadviseur die contextuele aanbevelingen doet op basis van uw apparaatgebruik en behoeften. Zo profiteert u van alles wat uw app te bieden heeft.

> **Opmerking**
> Wanneer u de app voor het eerst opent, wordt u gevraagd een scan uit te voeren.

4.4. Scam Copilot

Deze functie is in wezen een AI-aangestuurde chatbot die door Bitdefender is getraind om verschillende vormen van oplichting, phishing-pogingen, desinformatiecampagnes en nepwebsites te detecteren.

Om Scam Copilot te activeren:

1. Open de Bitdefender Mobile Security-app. In het dashboard-deelvenster is een kaart met betrekking tot Scam Copilot aanwezig. Tik op **Activeren**.
2. U moet sms-filtering inschakelen volgens de onderstaande instructies:
   a. Open **Instellingen** op uw apparaat.
   b. Selecteer **Berichten** in de lijst.
   c. Selecteer **Onbekend en Spam**.
   d. Schakel **Onbekende afzenders filteren**IN.
   e. Selecteer **Mobiele beveiliging** in sms-filtering.
3. Als u klaar bent, drukt u op **Doorgaan**.

4. Schakel agenda-scan in. Kort nadat u op de knop **Inschakelen** hebt gedrukt, verschijnt er een pop-up op uw scherm. Tik op **Volledige toegang toestaan**.

Scam Copilot is nu correct geconfigureerd op uw apparaat.

U kunt toegang krijgen tot het speciale tabblad Scam Copilot. Hier vindt u:

- **Chatbot voor oplichtingsdetectie:** vraag de chatbot om alle berichten die u verdacht vindt, te beoordelen.
- **Preventie-assistent:** helpt u meer te weten te komen over oplichting om vaardig te worden in het herkennen ervan.
- **Automatische scamdetectie** status en configuratiescherm.
- **Sms-filtering**: laat uw gevaarlijke berichten rechtstreeks in uw berichten-app filteren.

4.4.1. Oplichtingswaarschuwing

De Scam Alert-functie die beschikbaar is in Bitdefender Mobile Security voor iOS beschermt Apple-gebruikers proactief tegen phishing-aanvallen. Scam Alert voor iOS bevat twee beschermingslagen die oplichting via sms/mms-berichten en agenda-uitnodigingen monitoren:

- **Tekstberichtenfilter (SMS, MMS)**
  Deze functie identificeert en filtert ongewenste sms- en mms-berichten.
  Een kwaadaardige SMS/MMS (Short Message Service/Multimedia Messaging Service) verwijst naar een type bericht dat met schadelijke bedoelingen naar mobiele apparaten wordt verzonden. Deze berichten zijn bedoeld om kwetsbaarheden te misbruiken, ontvangers te misleiden of schade toe te brengen aan het apparaat, de persoonlijke informatie of de beveiliging van het doelwit.
- **Linkscanner voor agenda-uitnodigingen**
  Deze functie detecteert spamagenda's en evenementen die gevaarlijke links bevatten. Het kalendervirus is een vorm van spam die de Agenda-app van uw iPhone aantast en die vervelend en potentieel gevaarlijk kan zijn:
  - U ontvangt ongewenste agenda-uitnodigingen of gebeurtenismeldingen wanneer u per ongeluk een valse agenda-

uitnodiging accepteert die door hackers of spammers naar uw e-mailadres is verzonden.

- Wanneer u op de link in de uitnodiging klikt, abonneert u zich onbewust op de agenda van de afzender, waardoor deze u meer spamevenementen kan sturen.
- De spamgebeurtenissen kunnen links of bijlagen bevatten die u naar phishingpagina's of andere cyberbedreigingen kunnen leiden als u deze opent.

Hoe Scam Alert in te stellen

Om Scam Alert in te schakelen, moet u de Bitdefender Mobile Security-app toegang verlenen tot agendameldingen en sms-berichten:

SMS-filtering inschakelen:

Om Bitdefender te laten beginnen met het filteren van berichten, moet u handmatig de optie Onbekende afzenders filteren in de Berichten-app-instellingen activeren:

1. Open de **Instellingen** app op uw iPhone of iPad.
2. Scroll naar beneden en selecteer **Berichten** in de lijst.
3. Druk op **Onbekend en spam** sectie.
4. Schakelaar **Filter onbekende afzenders** naar de aan-positie.
5. Selecteer **Mobiele beveiliging** in het gedeelte SMS-filtering en kies vervolgens **Inschakelen**.

Bitdefender kan nu ongewenste berichten op uw iPhone/iPad filteren.

> **Opmerking**
> Vanwege iOS-beperkingen kan de sms-filtering van Bitdefender alleen worden gebruikt voor sms- en mms-berichten die afkomstig zijn van mensen die u niet in uw contacten hebt opgeslagen. Dit betekent dat het geen berichten filtert van mensen die al in uw contactenlijst staan, of iMessage-berichten van wie dan ook.

Agendascan inschakelen:

1. Open de **Bitdefender mobiele beveiliging** app geïnstalleerd op uw iPhone of iPad.

2. Ga naar de **Oplichtingswaarschuwing** optie in de onderste navigatiebalk en druk op **Nu instellen**.
3. Kraan **Doorgaan** en tik vervolgens op **Inschakelen**.
4. Kiezen **OK** om Bitdefender toegang te verlenen tot uw agenda. Er wordt onmiddellijk een kalenderscan gestart.

4.5. Webbescherming

Bitdefender Web Protection verzekert een veilige surfervaring door u op de hoogte te brengen van mogelijke schadelijke webpagina's en wanneer minder beveiligde toepassingen toegang proberen te verkrijgen tot niet-vertrouwde domeinen.

Wanneer een URL naar een gekende phishing-website of frauduleuze website leidt, of naar schadelijke inhoud zoals spyware of virussen, wordt de webpagina geblokkeerd en wordt er een waarschuwing getoond. Hetzelfde gebeurt wanneer geïnstalleerde toepassingen toegang proberen te verkrijgen tot schadelijke domeinen.

> **Belangrijk**
> Als u zich in een gebied bevindt waar het gebruik van een VPN-service wettelijk beperkt is, zal de functionaliteit van de Webbeveiliging niet beschikbaar zijn.

Om Webbescherming te activeren:

1. Tik op het pictogram onderaan het scherm.
2. Tik op **Ik ga akkoord**.
3. Schakel de schakelaar voor Webbescherming in.

> **Opmerking**
> De eerste keer dat u Webbescherming inschakelt, wordt u mogelijk gevraagd Bitdefender toe te staan VPN-configuraties in te stellen die het netwerkverkeer zullen monitoren. Tik op **Toestaan** om verder te gaan. Indien er een authenticatiemethode (vingerafdruk of pincode) werd ingesteld om uw smartphone te beschermen, dient u deze te gebruiken. Om toegang tot niet-vertrouwde domeinen te detecteren, werkt Webbescherming samen met de VPN-diensten.

Belangrijk

De voorziening Webbescherming en de VPN-dienst kunnen niet tegelijkertijd functioneren. Wanneer een van de twee is ingeschakeld, wordt de andere (indien deze op dat moment actief is) uitgeschakeld.

4.5.1. Bitdefender-waarschuwingen

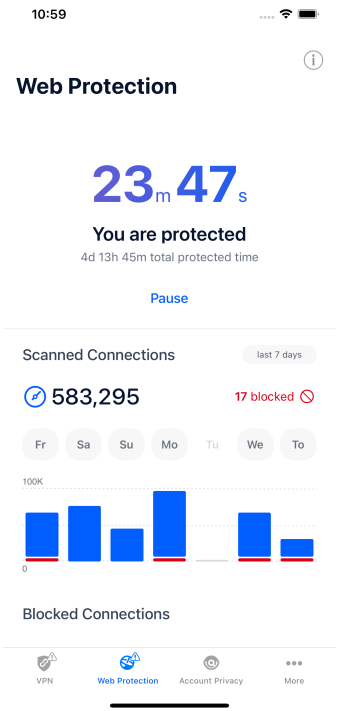
Wanneer u een website die als onveilig wordt beschouwd, probeert te openen, wordt de website geblokkeerd. Om dit aan u kenbaar te maken, wordt u door Bitdefender op de hoogte gebracht in het Notificatiecentrum en in uw browser. De waarschuwingspagina bevat informatie zoals de URL van de website en de gedetecteerde bedreiging. U moet beslissen wat er vervolgens dient te gebeuren.

U krijgt ook een melding in het Notificatiecentrum wanneer een minder beveiligde toepassing toegang probeert te verkrijgen tot niet-vertrouwde domeinen. Tik op de weergegeven notificatie om doorgestuurd te worden naar het venster waar u kunt beslissen wat er vervolgens dient te gebeuren.

De volgende opties zijn beschikbaar voor beide gevallen:

- Verlaat de website door te tikken op **BRENG ME TERUG NAAR EEN VEILIGE LOCATIE**.
- Ga ondanks de waarschuwing verder naar de website, door te tikken op de weergegeven notificatie en vervolgens op **Ik wil de pagina openen**.

Bevestig uw keuze.



4.6. VPN

Met Bitdefender VPN houdt u uw data privé telkens u verbindt met onbeveiligde draadloze netwerken in luchthavens, winkelcentra, cafés of hotels. Zo vermijdt u onfortuinlijke situaties, bijvoorbeeld diefstal van persoonlijke gegevens of pogingen om het IP-adres van uw apparaat toegankelijk te maken voor hackers.

De VPN werkt als een tunnel tussen uw apparaat en het netwerk waarmee u verbinding maakt: de VPN beveiligt die verbinding, door aan de hand van versleuteling volgens militaire richtlijnen de gegevens te versleutelen en door uw IP-adres te verbergen, waar u ook bent. Uw dataverkeer wordt omgeleid via een andere server, waardoor het onmogelijk wordt om uw apparaat te laten identificeren door uw internetprovider, tussen de talloze andere toestellen die gebruikmaken van onze diensten. Wanneer u via Bitdefender VPN verbonden bent met het internet kunt u bovendien inhoud bekijken die normaal afgeschermd wordt in bepaalde gebieden.

> **Opmerking**
> Sommige landen hanteren internetcensuur. Het gebruik van VPN's is op hun grondgebied dan ook bij wet verboden. Om wettelijke gevolgen te vermijden, is het mogelijk dat er een waarschuwingsbericht verschijnt wanneer u de Bitdefender VPN-app voor het eerst probeert te gebruiken. Door het gebruik van de app verder te zetten, bevestigt u dat u op de hoogte bent van de toepasselijke reguleringen van het land en van de risico's die u mogelijk loopt.

Om Bitdefender VPN in the schakelen:

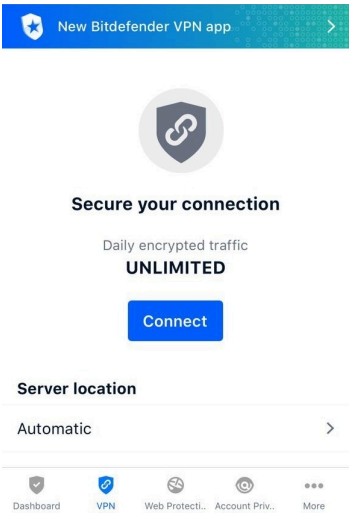
1. Druk op pictogram onderaan het scherm.
2. Klik op **Verbinden** telkens u bescherming wenst wanneer u verbonden bent met een onbeveiligd draadloos netwerk.
   Tik op **Verbreken** wanneer u de verbinding wilt verbreken.

> **Opmerking**
> De eerste keer dat u VPN inschakelt, wordt u gevraagd Bitdefender toe te staan VPN-configuraties in te stellen die het netwerkverkeer zullen monitoren. Tik op **Toestaan** om verder te gaan. Indien er een authenticatiemethode (vingerafdruk of pincode) werd ingesteld om uw smartphone te beschermen, dient u deze te gebruiken.

Het pictogram VPN verschijnt in de statusbalk wanneer VPN actief is.

Om uw batterij te sparen, raden we aan VPN uit te schakelen wanneer u dit niet gebruikt.

Indien u een premium-abonnement heeft en u de server naar wens wilt veranderen, tik op Automatisch in de VPN-interface en selecteer vervolgens de locatie die u wenst. Voor meer info over VPN-abonnementen, raadpleeg Abonnementen (pagina 253).



4.6.1. Abonnementen

Bitdefender VPN biedt dagelijks gratis 200 MB dataverkeer per apparaat om uw verbinding te beveiligen telkens u dit nodig hebt, en verbindt bovendien automatisch met de beste serverlocatie.

Upgrade naar de premium-versie voor onbeperkt dataverkeer en toegang tot afgeschermde inhoud overal ter wereld, doordat u de serverlocatie naar wens kunt selecteren.

U kunt op elk moment upgraden naar de versie Bitdefender Premium VPN door in het VPN-venster te tikken op de knop **Premium VPN activeren**. U kunt kiezen uit twee soorten abonnementen: jaarlijks en maandelijks.

Het Bitdefender Premium VPN-abonnement is onafhankelijk van het gratis abonnement voor Bitdefender Mobile Security for iOS: u kunt het dus gedurende de hele geldigheid ervan gebruiken. Indien het Bitdefender Premium VPN-abonnement vervalt, gaat u automatisch terug naar de gratis versie.

Bitdefender VPN is een cross-platform product en is beschikbaar in de Bitdefender-producten die compatibel zijn met Windows, macOS, Android en iOS. Eens u upgradet naar de premium-versie, kunt u uw abonnement op alle producten gebruiken, op voorwaarde dat u inlogt met dezelfde Bitdefender-account.

Opmerking
Bitdefender VPN werkt ook als zelfstandige applicatie op alle ondersteunde besturingssystemen, namelijk Windows, macOS, Android en iOS.

4.7. Account Privacy

Bitdefender Account Privacy gaat na of er data werd gelekt in de accounts die u gebruikt om online betalingen te verrichten, te winkelen of u aan te melden bij verschillende apps of websites. De data die in een account opgeslagen is, kan gaan om wachtwoorden, kredietkaartinformatie of bankrekeninginformatie en, indien niet goed beveiligd, kan er sprake zijn van identiteitsdiefstal of inbreuk op privacy.

De privacystatus van een account wordt weergegeven na de validering.

Om na te gaan of er lekken zijn op een van uw rekeningen, tik op **Scannen op lekken**.

Om vanaf nu persoonlijke informatie veilig te houden:

1. Druk op pictogram onderaan het scherm.
2. Tik op **Account toevoegen**.
3. Typ uw e-mailadres in het daarvoor bestemde veld en tik daarna op **Volgende**.
   Bitdefender moet deze account valideren voordat persoonlijke informatie wordt weergegeven. Daarom werd een e-mailbericht met valideringscode verzonden naar het opgegeven e-mailadres.
4. Controleer uw Postvak IN en tik vervolgens de ontvangen code in het vakje **Accountprivacy** van uw app in. Indien u de bevestigingse-mail niet in uw Postvak IN vindt, controleer ook uw Ongewenste mail.
   De privacystatus van de gevalideerde account wordt weergegeven.

Indien er in een van uw accounts worden gevonden, bevelen we u aan het wachtwoord zo snel mogelijk te wijzigen. Om een sterk en veilig wachtwoord te creëren, kunt u deze tips in gedachten houden:

- Zorg ervoor dat het minstens acht karakters lang is.
- Gebruik kleine letters en hoofdletters.
- Voeg ten minste een cijfer of symbool toe, zoals #, @, % of !.

Eens u een account die deel uitmaakte van een privacy-schending beveiligd hebt, kunt u de wijzigingen bevestigen door de geïdentificeerde lekken aan te duiden als **Opgelost**. Om dit te doen:

1. Tik op ··· naast de inbreuk die u hebt opgelost.
2. Tik op **Aanduiden als opgelost**.

Wanneer alle gedetecteerde lekken aangeduid zijn als Opgelost, wordt de account niet langer gemarkeerd als gelekt, tot er een nieuw lek wordt ontdekt.

4.8. Veelgestelde vragen

Hoe beschermt Bitdefender Mobile Security for iOS mij tegen virussen en cyberdreigingen?

Bitdefender Mobile Security for iOS biedt absolute bescherming tegen alle cyberdreigingen en werd speciaal ontwikkeld om uw gevoelige gegevens te beveiligen tegen nieuwsgierige blikken.

U geniet van een hele reeks beveiligings- en privacyvoorzieningen voor uw iPhone en iPad - plus talrijke bonusvoorzieningen, waaronder VPN en Webbescherming.

Bitdefender Mobile Security voor iOS reageert onmiddellijk op virus en malware, zonder impact op uw systeemprestaties.

Welk soort apparaten en welke besturingssystemen dekt Bitdefender Mobile Security for iOS?

Bitdefender Mobile Security for iOS beschermt uw smartphones en tablets met iOS tegen alle cyberdreigingen.

Waarom heb ik Bitdefender Mobile Security for iOS nodig voor Apple OS?

Op uw iPhone of iPad staan bepaalde zeer persoonlijke gegevens - u moet dus weten dat die gegevens ten alle tijde veilig zijn. Bitdefender Mobile Security for iOS biedt absolute bescherming tegen cyberdreigingen en zorgt voor uw online privacy en privé-informatie, zonder tussen te komen in uw dagelijkse activiteiten.

Krijg ik een VPN met mijn abonnement voor Bitdefender Mobile Security for iOS?

Bitdefender Mobile Security for iOS wordt geleverd met een basisversie van Bitdefender VPN waarbij gratis een ruime hoeveelheid verkeer (200 MB/dag, een totaal van 6GB/maand) wordt aangeboden.

5. VPN

5.1. Wat is Bitdefender VPN

De VPN fungeert als een tunnel tussen uw apparaat en het netwerk waarmee u verbinding maakt om uw verbinding te beveiligen, de gegevens te coderen met behulp van codering op militair niveau en uw IP-adres te verbergen waar u ook bent. Uw verkeer wordt omgeleid via een aparte server; waardoor uw apparaat onmogelijk kan worden geïdentificeerd door uw ISP, via de talloze andere apparaten die onze services gebruiken. Bovendien hebt u, terwijl u via Bitdefender VPN verbonden bent met internet, toegang tot inhoud die normaal gesproken beperkt is in specifieke gebieden.

Opmerking

Bepaalde landen doen aan internetcensuur, waardoor het gebruik van VPN's op hun grondgebied bij wet verboden is. Om wettelijke gevolgen te vermijden, is het mogelijk dat er een waarschuwingsboodschap verschijnt wanneer u de functie van Bitdefender VPN voor het eerst probeert te gebruiken. Door deze functie te blijven gebruiken, bevestigt u dat u op de hoogte bent van de toepasselijke regels van dat land en van de risico's die u zou kunnen lopen.

5.1.1. Versleutelingsprotocollen

De standaard ciphersuite-sets ingeschakeld in Hydra-client en-server worden hieronder vermeld. Alle andere ciphersuites zijn uitgeschakeld.

Ciphersuites in Hydra-client:

- 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

Opmerking

Set aan server zijde is veel restrictiever, en zowel Hydra-client als -server zullen een modus andere dan GCM met AES weigeren. Hydra-server dwingt prioriteit aan server zijde af voor sterkere ciphersuites en zal TLS handshake weigeren als een zwakkere suite door een client wordt verzocht. Deze lijst kan ook worden geconfigureerd in runtime aan server zijde.

5.2. VPN-abonnementen

Met Bitdefender VPN kunt u kiezen tussen twee soorten abonnementen:

- Het Basis-abonnement
- Het Premium-abonnement

5.2.1. Basis-abonnement

Bitdefender VPN biedt dagelijks 200 MB gratis verkeer per apparaat, om uw verbinding te beveiligen telkens u dat nodig hebt, en laat u verbinding maken met één locatie, die u niet kunt wijzigen.

Het Basis-abonnement is beschikbaar voor alle gebruikers die Bitdefender VPN dowloaden.

5.2.2. Premium-abonnement

Om onbeperkte toegang te krijgen tot alle voorzieningen inbegrepen in Bitdefender VPN, upgradet u naar de Premium-versie. Gebruikers met een actief Premium VPN-abonnement krijgen onbeperkt verkeer en kunnen verbinding maken met al onze servers, overal ter wereld.

Er zijn twee opties beschikbaar voor het Premium-abonnement: het Maandelijkse plan en het Jaarlijkse plan.

- Het Maandelijkse plan: met dit plan wordt u elke maand aangerekend voor de Premium VPN-diensten. U kunt zich altijd afmelden.
- Het Jaarlijkse plan: vereist een eenmalige betaling, en verleent u een gans jaar toegang tot onze Premium VPN-diensten.

5.2.3. Hoe upgraden naar Premium VPN

De meest eenvoudige manier om te upgraden naar de Premium-versie van Bitdefender VPN, is te klikken op de knop **Upgraden** in het onderste

gedeelte van de hoofdinterface. Kies het gewenste abonnement en volg de instructies op het scherm.

Hebt u al een activeringscode, dan volgt u de onderstaande instructies:

- **Voor Windows-gebruikers**
  1. Klik op het pictogram Mijn account aan de linkerkant van de VPN-interface.
  2. Klik op **Hier toevoegen**.
  3. Voer de code in die u via e-mail hebt ontvangen, en klik op de knop **Code activeren**.

- **Voor macOS-gebruikers**
  1. Klik op het tandwiel in de rechterbovenhoek van de VPN-interface en selecteer **Mijn account**.
  2. Klik **Voeg het hier toe**.
  3. Voer de code in die u via e-mail hebt ontvangen en klik vervolgens op de **activerings code** knop.

- **Voor Android-gebruikers**
  1. Tik op het tandwiel in de rechterbovenhoek van de VPN-interface en selecteer **Mijn account**.
  2. Tik op **Code toevoegen**.
  3. Voer de code in die u via e-mail hebt ontvangen en klik vervolgens op de **activerings code** knop.

- **Voor iOS-gebruikers**
  1. Tik op het tandwiel in de rechterbovenhoek van de VPN-interface en selecteer **Mijn rekening**.
  2. Kraan **Code toevoegen**.
  3. Voer de code in die u via e-mail hebt ontvangen en klik vervolgens op de **activerings code** knop.

5.3. Installatie

5.3.1. Voorbereiden voor installatie

Voordat u Bitdefender VPN installeert, moet u deze voorbereidingen voltooien om ervoor te zorgen dat de installatie vlot verloopt:

- Controleer of de apparaat waarop u Bitdefenderwilt installeren, voldoet aan de minimale systeemvereisten. Als de apparaat niet aan alle systeemvereisten voldoet, wordt het Bitdefender niet geïnstalleerd, of als het toch geïnstalleerd wordt, zal het niet goed werken en zal het systeem vertragen en instabiel worden.
  Raadpleeg Systeemvereisten (pagina 260) voor de complete lijst van alle systeemvereisten.
- Meld u aan bij de apparaat met een beheerdersaccount.
- Het wordt aanbevolen uw apparaat verbonden te laten met Internet tijdens de installatie, zelfs wanneer u vanaf een cd/dvd installeert. Indien er nieuwere versies van de toepassingsbestanden in het installatiepakket beschikbaar zijn, kan Bitdefender deze downloaden en installeren.

5.3.2. Systeemvereisten

- **Voor Windows-gebruikers**
  - **Besturingssysteem:** Windows 7 met Service Pack 1, Windows 8, Windows 8.1 Windows 10 en Windows 11
  - **Geheugen (RAM):** 1 GB
  - **Beschikbare vrije schijfruimte:** 500 MB vrije ruimte
  - **Net Framework:** min versie 4.5.2

    Belangrijk
    Systeemprestaties kunnen worden beïnvloed voor apparaten die CPU's van een oudere generatie hebben.
- **Voor macOS-gebruikers**
  - **Besturingssysteem:** macOS Sierra (10.12) of later
  - **Beschikbare vrije schijfruimte:** 100 MB vrije ruimte

- **Voor Android-gebruikers**
  - **Besturingssysteem:** Android 6.0 of later
  - **Opslag:** 100MB
  - Een werkende internetverbinding
- **Voor iOS-gebruikers**
  - **Besturingssysteem:** iOS 12 of later
  - **Opslag op iPhone:** 50MB
  - **Opslag op iPad:** 100MB
  - Een actieve internetverbinding

5.3.3. Bitdefender VPN installeren

Om de installatie te starten, volgt u de instructies voor het besturingssysteem dat u gebruikt:

- **Voor Windows-gebruikers**
  1. Om de installatie van Bitdefender VPN op een Windows pc te starten, downloadt u eerst de installatiekit van https://www.bitdefender.com/solutions/vpn/download of uit de e-mail die u na een aankoop ontvangt.
  2. Dubbelklik op het gedownloade installatiebestand om het uit te voeren.
  3. Kies Ja als u de dialoog Gebruikersaccountbeheer ziet.
  4. Wacht totdat de download is voltooid.
  5. Selecteer de taal voor het product, aan de hand van het vervolgkeuzemenu in het installatiebestand.
  6. Vink “Ik bevestig dat ik de Abonnementsvoorwaarden en het Privacybeleid heb gelezen en aanvaard” aan en klik vervolgens op **INSTALLATIE STARTEN**.
  7. Wacht tot de installatie is voltooid.
  8. **LOG IN** met uw Bitdefender Central-account. Als u geen Central-account hebt, maakt u er een aan via de knop **ACCOUNT MAKEN**.
  9. Kies **Ik heb een activeringscode** als u een Premium VPN-abonnement hebt aangekocht.

Anders kunt u **PROEFPERIODE STARTEN** kiezen, om het product 7 dagen lang gratis te testen, voordat u beslist om ervoor te betalen.

10. Voer de code in die u via e-mail hebt ontvangen, en klik op de knop **PREMIUM ACTIVEREN**.

11. Na een korte wachttijd is Bitdefender VPN geïnstalleerd en klaar voor gebruik op uw computer.

❍ **Voor macOS-gebruikers**

1. Om de installatie van Bitdefender VPN op macOS te starten, downloadt u eerst de installatiekit van https://www.bitdefender.com/solutions/vpn/download of uit de e-mail die u na een aankoop ontvangt.
2. Het installatiebestand wordt opgeslagen op uw Mac. In de map Downloads dubbelklikt u op het -pakketbestand.
3. Volg de instructies op het scherm en kies **Verdergaan**.
4. U wordt door de stappen geleid die nodig zijn om Bitdefender VPN op uw Mac te installeren. Klik tweemaal op de **Continue** knop.
5. Klik op **Akkoord** nadat u de voorwaarden van de softwarelicentie-overeenkomst hebt gelezen en deze aanvaardt.
6. Klik op **Installeren**.
7. Voer een beheerdersgebruikersnaam en -wachtwoord in en klik vervolgens op **Software installeren**.
8. U wordt op de hoogte gebracht dat een systeemextensie, getekend door Bitdefender, werd geblokkeerd. Dit is geen fout, enkel een beveiligingscontrole. Klik op **Beveiligingsvoorkeuren openen**.
9. Klik op het slotpictogram om te ontgrendelen.
   Voer een beheerdersnaam en -wachtwoord in en druk op **Ontgrendelen**.
10. Klik op **Toestaan** om de systeemextensie van BitdefenderBitdefender te laden. Daarna sluit u het venster Beveiliging en Privacy en het Bitdefender-installatiebestand.
11. Ga naar het schildpictogram in de menubalk en **Log in** met uw Bitdefender Central-account. Als u geen Central-account hebt, maakt u er een aan.

12. Kies Ik heb een **Activeringscode** als u een Premium VPN-abonnement hebt aangekocht.
    Anders kun je kiezen **START PROEF** om het product 7 dagen gratis uit te proberen voordat u ervoor gaat betalen.
13. Voer de code in die u via e-mail hebt ontvangen en klik vervolgens op de **activerings code** knop.
14. Na een korte wachttijd is Bitdefender VPN geïnstalleerd en klaar voor gebruik op uw Mac.

- **Voor Android-gebruikers**

1. Om Bitdefender VPN te installeren op Android, opent u eerst de app **Google Play Store** op uw smartphone of tablet.
2. Zoek Bitdefender VPN naar en selecteer deze app.
3. Tik op de knop **Installeren** en wacht totdat de download is voltooid.
4. Tik op **Openen** om de app uit te voeren.
5. Vink het vakje “Ik ga akkoord met de Abonnementsovereenkomst en het Privacybeleid" aan en tik op **Verdergaan**.
6. **Log in** met uw Bitdefender Central-account. Als u geen Central-account hebt, maakt u er een aan door te tikken op **Account maken**.
7. Kies **Ik heb een activeringscode** als u een Premium VPN-abonnement hebt aangekocht.
   Anders kunt u Proefperiode 7 dagen starten kiezen, om het product 7 dagen lang gratis te testen, voordat u beslist om ervoor te betalen.
8. Voer de code in die u via e-mail hebt ontvangen, en tik op **Code activeren**.

- **Voor iOS-gebruikers**

1. Om Bitdefender VPN op iOS te installeren, opent u eerst **App Store** op uw iPhone of iPad.
2. Zoeken Bitdefender VPN en selecteer deze app.
3. Tik op het pictogram **Get** en wacht totdat de download is voltooid.

4. Kraan **Open** om de app uit te voeren.
5. Vink het vakje **Ik ga akkoord met de Abonnementsovereenkomst en het Privacybeleid** aan, en tik op **Verdergaan**.
6. **Log in** met uw Bitdefender Central-account. Als u geen account hebt, maakt u er een aan door te tikken op **Account maken**.
7. Tik op **Toestaan** als u Bitdefender VPN meldingen wilt ontvangen.
8. Kiezen **Ik heb een activeringscode** als je een Premium VPN-abonnement hebt gekocht.
   Anders kunt u Start 7 days Trial kiezen om het product 7 dagen gratis uit te proberen voordat u ervoor gaat betalen.
9. Voer de via e-mail ontvangen code in en tik vervolgens op **Activerings code**.

5.4. Bitdefender VPN gebruiken

5.4.1. Bitdefender VPN openen

- **Voor Windows**
  Om naar de **hoofdinterface van Bitdefender VPN** te gaan, volgt u een van de volgende methoden:
  - **Vanuit het systeemvak**
    Klik met de rechtermuisknop op het rode schildpictogram in het systeemvak, en selecteer dan **Weergeven** in het menu.
  - **Vanuit deBitdefender-interface**
    Als er al een Bitdefender-beveiligingsproduct zoals Bitdefender Total Security of Bitdefender Antivirus Plus, enz. op uw Windows-computer is geïnstalleerd, kunt u Bitdefender VPN van daaruit openen:
    1. Klik **Privacy** in de linkerzijbalk van de Bitdefender-interface.
    2. Klik op **VPN openen** in het VPN-deelvenster.
  - **Vanaf uw bureaublad**
    Dubbelklik op de Bitdefender VPN-snelkoppeling op uw bureaublad.

- **Voor macOS**

  U kunt de Bitdefender VPN-app openen door op het pictogram in de menubalk rechtsboven op het scherm te klikken.
  Als het Bitdefender-schild niet in de menubalk te vinden is, gebruik dan uw Mac Launchpad of Finder om het terug te halen:

  - **Vanuit Launchpad**

    1. Druk op **F4** op uw toetsenbord om naar de Launchpad op uw Mac te gaan.
    2. Blader door de pagina's met geïnstalleerde apps totdat u de Bitdefender VPN-app vindt. U kunt ook **Bitdefender VPN** in Launchpad typen om te beginnen met het filteren van uw resultaten.
    3. Zodra u de Bitdefender VPN-app ziet, klikt u op het pictogram ervan om deze vast te zetten in de menubalk.

  - **Vanuit Finder**

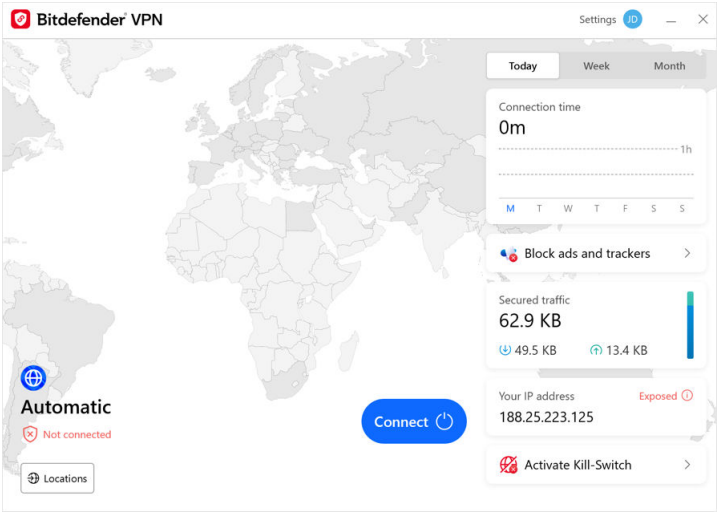
    1. Klik op **Finder** linksonder in het Dock (Finder is het pictogram dat lijkt op een blauw vierkant met een smiley).
    2. Klik vervolgens op **Ga** linksboven in het scherm, op de menubalk.
    3. Kies **Programma's** uit het menu om de map Programma's op uw Mac te openen.
    4. Ga naar de map Programma's, open de map **Bitdefender** en dubbelklik op de **Bitdefender** VPN-app.

  Opmerking
  Om toegang te krijgen tot Bitdefender VPN op uw mobiele Android- of iOS-apparaten, opent u gewoon de Bitdefender VPN-toepassing nadat u deze hebt geïnstalleerd.

5.4.2. Hoe verbinding maken met Bitdefender VPN

De VPN-interface geeft de status van de app weer: verbonden of niet verbonden. Voor gebruikers met de gratis versie stelt Bitdefender de serverlocatie automatisch in op de meest geschikte server. Premium-gebruikers hebben de mogelijkheid om de serverlocatie waarmee ze

wensen te verbinden, te wijzigen, door de locatie te selecteren in de lijst Virtuele locaties. Om verbinding te maken of de verbinding te verbreken, klikt u gewoon op de aan/uit-knop van de VPN-interface.



- **Voor Windows:** Het systeemvakpictogram toont een groen vinkje wanneer het VPN is verbonden, en een zwart vinkje wanneer het VPN is verbroken. Tijdens de verbinding met een handmatig geselecteerde locatie wordt het IP-adres weergegeven op de hoofdinterface.
- **Voor macOS:** Het menubalkpictogram is zwart als het VPN is verbonden, en wit als het VPN is verbroken. Klik op de ronde knop in het midden van de interface en wacht tot de verbinding tot stand is gebracht.
- **Voor Android & iOS:** Om verbinding te maken met Bitdefender VPN voor Android, iOS en iPadOS:
  - **In de Bitdefender VPN-app:** Om verbinding te maken of de verbinding te verbreken, klikt u gewoon op de aan/uit-knop van de VPN-interface. De status van Bitdefender VPN wordt weergegeven.
  - **In de toepassing Bitdefender Mobiele Beveiliging:**
    1. Ga naar het VPN-pictogram op de onderste navigatiebalk van Bitdefender Mobiele Beveiliging.

2. Tik op **VERBINDEN** wanneer u beschermd wilt blijven terwijl u verbonden bent met onbeveiligde draadloze netwerken. Tik op **VERBINDING VERBREKEN** telkens als u de VPN-verbinding wilt uitschakelen.

5.4.3. Hoe verbinding maken met een andere server

Met een Premium abonnement kunt u MET Bitdefender VPN op elk moment verbinding maken met AL onze servers over de hele wereld. Hiervoor moet u:

1. De Bitdefender VPN app openen.
2. Tik op de knop **Virtuele Locatie** in het onderste gedeelte van de interface.
3. Selecteer een land.
4. Klik op de knop **Verbinden met [land]** in het onderste gedeelte van de interface.

- Het systeemvakpictogram geeft een groen vinkje weer wanneer de VPN is verbonden.
- Het IP-adres van de virtuele server wordt weergegeven op het startscherm terwijl u verbonden bent met Bitdefender VPN.
- Een samenvatting van uw verbindingstijd, de hoeveelheid beveiligd verkeer en de laatste 5 locaties waarmee u verbinding hebt gemaakt, worden ook weergegeven op het hoofddashboard.

5.5. Bitdefender VPN Instellingen & Functies

5.5.1. Naar Instellingen gaan

Om naar de instellingen van Bitdefender VPN te gaan, volgt u de onderstaande stappen:

- **In Windows**

  1. Open de app voor Bitdefender VPN op uw apparaat door in het systeemvak te dubbelklikken op het pictogram ervan of door er met de rechtermuisknop op te klikken en Tonen te selecteren.

2. Klik op de knop **Instellingen** (voorgesteld door een tandwiel) aan de linkerkant van de interface.

- **In macOS**

  1. Open de app voor Bitdefender VPN op uw macOS-apparaat, door in de menubalk te klikken op het pictogram ervan.
  2. Klik in de rechterbovenhoek van de Bitdefender VPN-interface op het tandwiel en selecteer Instellingen.

- **Op Android**

  1. Open de Bitdefender VPN app op uw apparaat.
  2. Klik in de rechterbovenhoek van de Bitdefender VPN-interface op het tandwiel.

- **Op iOS**

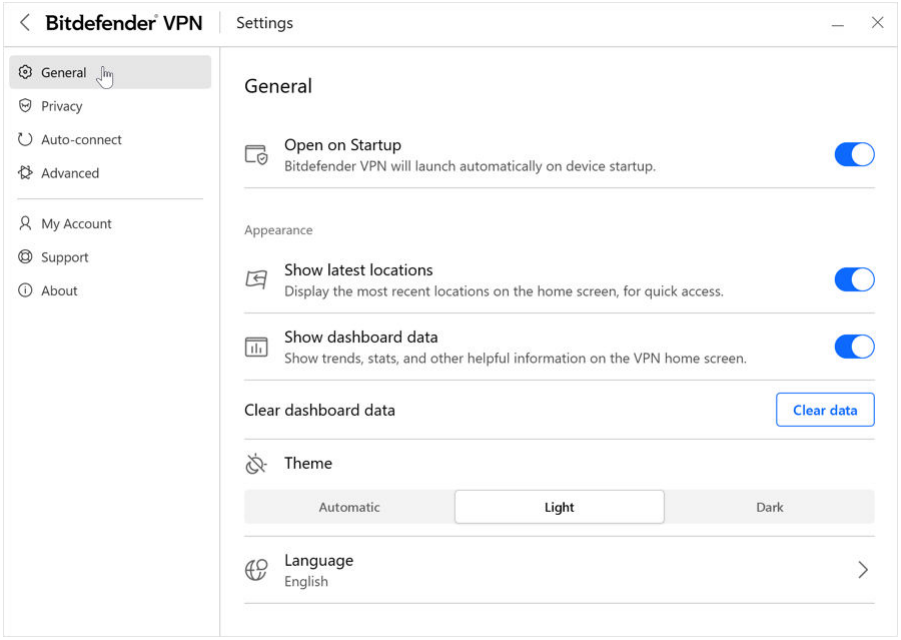
  1. Open de Bitdefender VPN app op uw apparaat.
  2. Klik op de tandwielknop in de rechterbovenhoek van de Bitdefender VPN koppel.

5.5.2. Algemeen

Hier kunt u het volgende wijzigen:

- **Openen bij opstarten**– Bitdefender VPN wordt automatisch gestart bij het opstarten van het apparaat.
- **Toon nieuwste locaties**– Geef de meest recente locaties op het startscherm weer, voor snelle toegang.
- **Dashboardgegevens weergeven** – Toon trends, statistieken en andere nuttige informatie op het VPN-startscherm.
- **Duidelijke dashboardgegevens**– Al uw dashboardgegevens worden gewist en alle tellers worden gereset.
- **Thema**– Licht/donker thema
- **Taal**– Wijzig de taal van Bitdefender VPN.
- **Meldingen**– Beheer uw meldingsvoorkeuren.

- **Help Bitdefender VPN te verbeteren**– Dien anonieme productrapporten in om ons te helpen uw ervaring te verbeteren.
- **Reset alle instellingen**– Reset de VPN naar de oorspronkelijke instellingen zonder deze opnieuw te installeren.



5.5.3. Functies

Privacy

Internet-schakelaar

De Internet-schakelaar is een nieuwe voorziening in Bitdefender VPN. Wanneer ingeschakeld, heft deze voorziening al het internetverkeer tijdelijk op indien de VPN-verbinding wordt verbroken. Zodra u terug online bent, wordt de verbinding opnieuw tot stand gebracht.

Om de Internet-schakelaar te activeren, volgt u de onderstaande stappen:

- **Op Windows**

1. Open de app voor Bitdefender VPN op uw apparaat door in het systeemvak te dubbelklikken op het pictogram ervan of door er met de rechtermuisknop op te klikken en **Weergeven** te selecteren.
2. Klik op de **Instellingen** -knop (weergegeven door een tandwiel) aan de linkerkant van de interface.
3. Selecteer **Geavanceerd**.
4. Schakel de optie **Internet-schakelaar** in.

- **Op Android**
  1. Open de Bitdefender VPN app op uw apparaat.
  2. Klik op de tandwielknop in de rechterbovenhoek van de Bitdefender VPN koppel.
  3. Schakel onder **Instellingen** de optie **Kill-Switch** in.
- **Op iOS**
  1. Open de Bitdefender VPN app op uw apparaat.
  2. Klik op de tandwielknop in de rechterbovenhoek van de Bitdefender VPN koppel.
  3. Onder **Instellingen**, schakel de **Dodemansknop** keuze.

> **Opmerking**
> Deze functie is ook beschikbaar voor macOS-apparaten met besturingssysteem 10.15.4 of latere versies.

Advertentieblokker en anti-tracker

Deze functies zijn ontworpen om u te helpen privé te blijven en van het web te genieten zonder vervelende advertenties of bedrijven die bij u binnengluren. Ze helpen bij het blokkeren van advertenties en het stoppen van online trackers.

Advertentieblokker

De **advertentieblokker** wordt gebruikt om advertenties, popups, luide videoadvertenties of reclamebanners te blokkeren tijdens het surfen. Dit helpt websites sneller te laden, schoner te zijn en ook veiliger om mee te werken.

Om de Advertentieblokker in te schakelen:

1. Zoek de functie **Advertentieblokker en anti-tracker** in **Instellingen**.
2. Zet de schakelaar in de stand **AAN**.

Anti-tracker

De **Anti-tracker** wordt gebruikt om trackers te blokkeren die door adverteerders zijn ingesteld om u online te volgen en te profileren. Sommige websites kunnen storingen vertonen wanneer trackers worden geblokkeerd, maar door de URL aan de whitelist toe te voegen, kan dit worden verholpen.

Om de Anti-tracker in te schakelen:

1. Zoek de **Adblocker en Antitracker** functie in **Instellingen**.
2. Zet de schakelaar op de **OP** positie.

Witte lijst

Sommige websites worden mogelijk niet goed geladen als u hun trackercode en advertenties blokkeert. Door de URL's van deze specifieke domeinen aan de witte lijst toe te voegen, kunt u dit probleem oplossen, maar houd er wel rekening mee dat u tijdens het surfen op deze websites advertenties te zien krijgt en dat hun trackercode actief zal zijn.

Voeg websites toe die u wilt toelaten om advertenties te tonen en trackers te gebruiken door:

1. Zoek de **Adblocker en Antitracker** functie in **Instellingen**.
2. Klik op de koppeling **Beheren**. Ga vervolgens naar de Whitelist-sectie van het venster en klik op de bijbehorende koppeling **Beheren**.
3. Klik op **Website toevoegen** en voeg de gewenste URL in.

Automatisch verbinden

Als u onderweg bent, in een coffee shop gaat werken of in de luchthaven wacht, kan het de snelste oplossing zijn om een verbinding te maken met een openbaar draadloos netwerk om betalingen te doen, e-mails te lezen of sociale netwerkaccounts te raadplegen. Maar er kunnen nieuwsgierige ogen zijn, die uw persoonlijke gegevens proberen te stelen en kijken hoe de informatie door het netwerk heen druppelt.

Om u te beschermen tegen de gevaren van niet-beveiligde of niet-versleutelde openbare draadloze hotspots, omvat Bitdefender VPN de voorziening 'automatisch verbinden'. Dit betekent dat Bitdefender VPN in bepaalde omstandigheden automatisch kan worden geactiveerd, afhankelijk van uw voorkeuren en van het besturingssysteem dat u gebruikt.

- In **Windows en macOS** kan de voorziening automatisch verbinden voor de volgende omstandigheden worden ingeschakeld:
  - **Opstart:** Verbind het VPN bij het opstarten van Windows.
  - **Onbeveiligde wifi:** Gebruik het VPN wanneer u verbinding maakt met openbare of onbeveiligde wifi-netwerken.
  - **Peer-to-peer apps:** Maak verbinding met het VPN wanneer u een peer-to-peer app voor het delen van bestanden start.
  - **Apps en domeinen:** Gebruik het VPN altijd voor bepaalde apps en websites.

    Opmerking

    1. Klik op de koppeling **Beheren**.
    2. Blader naar de locatie van de app waarvoor u VPN wilt gebruiken, selecteer de naam van de app en klik vervolgens op **Toevoegen**.

  - **Websitecategorieën:** Maak verbinding met het VPN wanneer u specifieke websitecategorieën bezoekt. Bitdefender VPN kan automatisch verbinding maken voor de volgende websitecategorieën:
    - Financiën
    - Online betalingen
    - Gezondheid
    - File sharing
    - Online dating
    - Inhoud voor volwassenen

Opmerking
Voor elke categorie kunt u een andere server selecteren waarmee het VPN verbinding moet maken.

- In **macOS** kan de voorziening automatisch verbinden voor de volgende omstandigheden worden ingeschakeld:
  - **Opstart:** Verbind het VPN bij het opstarten van macOS.
  - **Onbeveiligde wifi:** Gebruik de VPN wanneer u verbinding maakt met openbare of onbeveiligde Wi-Fi-netwerken.
  - **Peer-to-peer-apps:** Maak verbinding met de VPN wanneer u een peer-to-peer-app voor het delen van bestanden start.
  - **Toepassingen:** Verbind het VPN altijd voor bepaalde apps.
- In **Android** en **iOS** kan Bitdefender VPN worden ingesteld om enkel automatisch verbinding te maken wanneer u een openbaar of niet-beveiligd wifinetwerk gebruikt.

Geavanceerd

Split-tunneling

Met de split tunneling van het Virtual Private Network (VPN) kunt u een deel van uw applicatie- of apparaatverkeer door een versleuteld VPN leiden, terwijl andere applicaties of apparaten rechtstreeks toegang hebben tot het internet. Dit is vooral nuttig als u wilt profiteren van diensten die het best presteren wanneer uw locatie bekend is, terwijl u ook veilige toegang hebt tot potentieel gevoelige communicatie en gegevens.

Door de functie **Split tunneling** in te schakelen, zullen geselecteerde apps en websites het VPN omzeilen en rechtstreeks toegang krijgen tot het internet.

Om de toepassingen en websites te beheren die het VPN omzeilen:

1. Klik op de koppeling **Beheren** zodra de functie is ingeschakeld.
2. Klik op de knop **Toevoegen**.
3. Blader naar de locatie van de betreffende app of voeg de URL van de gewenste website in en klik vervolgens op **Toevoegen**.

Opmerking
Door het toevoegen van een website wordt het hele domein, inclusief alle subdomeinen, omzeild.

Belangrijk
Op **macOS** apparaten is de functie Split tunneling alleen beschikbaar voor websites.

App Traffic Optimizer

Met de App Traffic Optimizer van Bitdefender VPN kunt u prioriteit geven aan verkeer naar de belangrijkste apps op uw apparaat zonder uw verbinding bloot te stellen aan privacyrisico's. VPN's leiden het internetverkeer om via een veilige tunnel en gebruiken robuuste versleutelingsalgoritmen om het te beschermen.

Deze combinatie van technieken kan echter enkele nadelen hebben, vooral wat de snelheid van de verbinding betreft. Verschillende factoren kunnen leiden tot vertragingen van de verbinding, de meest voorkomende zijn de afstand tot de server waarmee u verbinding maakt, netwerkcongestie en een hoog bandbreedtegebruik. Als u ooit het gevoel hebt gehad dat Bitdefender VPN uw verbinding soms onnodig belast en vertragingen u voortdurend in de weg zitten, is er misschien een beter antwoord dan de verbinding verbreken.

Hoe werkt App Traffic Optimizer?

Bepaalde apps en diensten zoals streamingplatforms, torrent clients en games vereisen meer bandbreedte. Het constante gebruik ervan kan de snelheid van uw internetverbinding beïnvloeden. Routering van uw verkeer door een VPN-tunnel onderwerpt uw verbinding al aan een relatieve vertraging. Uw verbinding extra belasten kan uw online ervaring ernstig verslechteren.

De App Traffic Optimizer-functie van Bitdefender VPN kan u helpen vertragingen van de VPN-verbinding aan te pakken door voorrang te geven aan de app van uw keuze. De functie laat u beslissen welke apps het grootste deel van uw verkeer moeten ontvangen en wijst de middelen dienovereenkomstig toe. Als u bijvoorbeeld in een vergadering zit en merkt dat de kwaliteit van uw gesprek ondermaats is, kunt u met App Traffic Optimizer prioriteit geven aan de videoconferentie-app voor betere resultaten.

Meestal nemen VPN-gebruikers hun toevlucht tot het sluiten van alle storende processen op hun apparaat of schakelen ze zelfs hun VPN-verbinding uit om een snellere internetsnelheid te krijgen. App Traffic Optimizer laat u genieten van ononderbroken privacybescherming zonder afbreuk te doen aan uw verbindingssnelheid.

App Traffic Optimizer gebruiken

Momenteel is de functie alleen beschikbaar op Windows-apparaten en kunt u prioriteit geven aan maximaal 3 toepassingen.

Volg deze stappen om het met minimale inspanning in te schakelen en te configureren:

1. Start de Bitdefender VPN applicatie op uw Windows computer.
2. Klik op de knop in de zijbalk om de instellingen van het VPN te openen.
3. Ga naar het tabblad **Algemeen** en schakel de functie **App Traffic Optimizer** in. De kleur van de schakelaar zal veranderen van grijs naar blauw.

Om de toepassingen te beheren die van deze functie prioriteit krijgen:

1. Klik op de**Beheren**koppeling.
2. Blader naar de locatie van de app waarvoor u het verkeer wilt optimaliseren, selecteer de naam van de app en klik vervolgens op **Toevoegen**. De app verschijnt in de sectie **Met prioriteit**.

> **Opmerking**
> Als u de toepassing waaraan u prioriteit wilt geven onlangs hebt geopend, kunt u ook op de + knop drukken in het venster App Traffic Optimizer.

3. Verbreek de verbinding en maak opnieuw verbinding met Bitdefender VPN na het toevoegen of verwijderen van apps uit de lijst.

Om een app uit App Traffic Optimizer te verwijderen, klikt u gewoon op het pictogram naast de naam van de app.

> **Opmerking**
> De App Traffic Optimizer is niet beschikbaar op macOS.

Protocol

Hier kunt u het type protocol kiezen dat u voor de gegevensoverdracht wilt gebruiken. De volgende opties zijn beschikbaar:

- **Automatisch** - Bitdefender VPN selecteert het optimale protocol voor uw specifieke apparaat en netwerk.
- **Hydra-katapult** - Snel en veilig, ideaal voor streaming en gaming.
- **OpenVPN-UDP** - Geoptimaliseerd voor hoge snelheden. Dit protocol is echter niet zo betrouwbaar in termen van gegevensverlies als andere protocollen in de lijst.
- **OpenVPN-TCP** - Ontworpen voor betrouwbaarheid. Zorgt ervoor dat uw gegevens volledig worden geleverd, maar is niet zo snel als OpenVPN UDP.
- **Draadbeschermer** - Nieuwer protocol, dat krachtige beveiliging en een hoog prestatieniveau biedt.

Dubbele hop

Met deze functie kunt u de servers beheren waarlangs uw internetverkeer moet worden verzonden en dubbel gecodeerd. Uw gegevens gaan via twee VPN-servers in plaats van één, waardoor het moeilijker wordt om uw internetactiviteit te volgen.

Opmerking
Je kunt in totaal slechts 5 double-hop-locaties toevoegen. U kunt echter op elk gewenst moment de aangepaste dubbele hops in uw lijst verwijderen en andere maken.

Belangrijk
Het gebruik van servers op verschillende continenten in dezelfde double-hop kan uw verbindingssnelheid vertragen.

5.6. Bitdefender VPN wordt gede-installeerd

De procedure om Bitdefender VPN te verwijderen, is vergelijkbaar met de procedure om andere programma's van uw computer te verwijderen:

- **Bitdefender VPN wordt gede-installeerd van Windows-apparaten**
  - In **Windows 7**:

1. Klik op **Start**, ga naar **Configuratiescherm** en dubbelklik op **Programma's en onderdelen**.
2. Zoek **Bitdefender VPN** en selecteer De-installeren.
   Wacht tot de de-installatieproces is voltooid.

- In **Windows 8** en **Windows 8.1**:
  1. Zoek vanuit het Windows-startscherm het **Configuratiescherm** (u kunt bijvoorbeeld starten met het typen van "configuratiescherm", rechtstreeks in het startscherm) en klik op het pictogram ervan.
  2. Klik op **Een programma de-installeren** of **Programma's en Functies**.
  3. Vinden **Bitdefender VPN** en selecteer **Verwijderen**.
     Wacht tot het verwijderingsproces is voltooid.

- In **Windows 10** en **Windows 11**:
  1. Klik op **Start**, klik dan op **Instellingen**.
  2. Klik op het pictogram **Systeem** in Instellingen, selecteer dan **Geïnstalleerde apps**.
  3. Vinden **Bitdefender VPN** en selecteer **Verwijderen**.
  4. Klik nogmaals op **De-installeren** om uw keuze te bevestigen.
     Wacht tot het verwijderingsproces is voltooid.

- **Wordt gede-installeerd van macOS-apparaten**
  1. Klik op **Ga** in de menubalk en selecteer **Toepassingen**.
  2. Dubbelklik op de map **Bitdefender**.
  3. **BitdefenderUninstaller** uitvoeren.
  4. In het nieuwe venster vinkt u het vakje naast **Bitdefender VPN** aan en klikt u op **De-installeren**.
  5. Voer een geldige beheerdersaccountnaam en -wachtwoord in en klik op **OK**.
  6. Er wordt uiteindelijk gemeld dat Bitdefender VPN met succes werd gede-installeerd. Klik op **Sluiten**.

- **Wordt gede-installeerd van Android-apparaten**
  1. Open de app **Play Store**.
  2. Zoek naar **Bitdefender VPN**.
  3. Op de Bitdefender VPN app store pagina, selecteer **De-installeren**.
  4. Bevestig door op **OK** te tikken.
- **Wordt gede-installeerd van iOS-apparaten**
  1. Houd uw vinger op de Bitdefender VPN app.
  2. Kies **App verwijderen**.
  3. Tik op **Verwijderen**.

5.7. Veelgestelde vragen

Wanneer moet ik Bitdefender VPN gebruiken?

U dient voorzichtig te zijn wanneer u inhoud van het internet bekijkt, downloadt of uploadt. Om ervoor te zorgen dat u beveiligd bent wanneer u surft op het internet, raden we aan dat u het VPN gebruikt wanneer u:

- wilt verbinden met publieke draadloze netwerken
- inhoud wilt bekijken die normaal afgeschermd wordt in specifieke gebieden, ongeacht of u thuis of in het buitenland bent
- uw persoonlijke gegevens privé wilt houden (gebruikersnamen, wachtwoorden, e-mailadressen, kredietkaartgegevens enz.)
- uw IP-adres wilt verbergen

Kan ik een stad kiezen met Bitdefender VPN?

Ja. Momenteel kunt u met Bitdefender VPN voor Windows, macOS, Android en iOS een specifieke stad selecteren. Hier is de lijst met de steden die op dit ogenblik beschikbaar zijn:

- **VSA:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, New York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Canada:** Montreal, Toronto, Vancouver
- **VK:** Londen, Manchester

Kan Bitdefender VPN geïnstalleerd worden als alleenstaande toepassing?

De VPN-app wordt automatisch geïnstalleerd naast uw Bitdefender-beveiligingsoplossing. Ze kan ook worden geïnstalleerd als een op zichzelf staande app vanaf de productpagina, via Google Play Store & App Store.

Deelt Bitdefender mijn IP-adres en persoonlijke gegevens met derden?

Nee, met Bitdefender VPN is uw privacy 100% veilig. Niemand (reclamebureaus, internetproviders, verzekeringsmaatschappijen enz.) heeft toegang tot uw online logs.

Welk versleutelingsalgoritme gebruikt het?

Bitdefender VPN gebruikt het Hydra-protocol op alle platformen, 256-bit AES-encryptie of de hoogst beschikbare codering die zowel door de client als de server wordt ondersteund, met Perfect Forward Secrecy. Dit betekent dat encryptiesleutels voor elke nieuwe VPN-sessie worden gegenereerd en uit het geheugen worden gewist wanneer de sessie voorbij is.

Heb ik toegang tot inhoud die op basis van geo-IP wordt afgeschermd?

Met Premium VPN hebt u toegang tot een uitgebreid netwerk virtuele locaties, overal ter wereld.

Zal het een negatieve invloed hebben op de levensduur van de batterij van mijn apparaat?

Bitdefender VPN is ontworpen om uw persoonlijke gegevens te beschermen, uw IP-adres te verbergen wanneer uw verbonden bent met onbeveiligde draadloze netwerken en om content te bekijken die in bepaalde landen afgeschermd wordt. Om onnodig verbruik van uw batterij te vermijden, raden we u aan VPN enkel te gebruiken indien nodig, en de verbinding te verbreken wanneer u offline bent.

Waarom vertraagt het VPN mijn internetverbinding?

Bitdefender VPN is ontworpen om een lichte ervaring te bieden tijdens het surfen op het web. Afhankelijk van de afstand tussen uw werkelijke locatie en de serverlocatie die u kiest om verbinding mee te maken, wordt enige snelheidsvermindering verwacht, maar deze is bijna altijd zo klein dat deze onopgemerkt blijft tijdens normale online activiteiten. Bovendien maken wij gebruik van een van de snelste VPN-infrastructuren ter wereld. Als het niet absoluut noodzakelijk is om vanaf uw locatie verbinding te

maken met een ver weg gehoste server (bijv. van de VS naar Frankrijk), raden wij u aan het VPN toe te staan u automatisch te verbinden met de dichtstbijzijnde server of een server te vinden die dichter bij uw huidige locatie ligt.

6. WACHTWOORDBEHEERDER

6.1. Wat is Bitdefender SecurePass

Bitdefender SecurePass is een multi-platform dienst ontworpen om gebruikers te helpen bij het opslaan en organiseren van al hun online wachtwoorden. Het is gebouwd met de sterkste bekende cryptografische algoritmen voor het hoogste niveau van veiligheid en digitale beveiliging. Het werkt als een browserextensie en mobiele app-oplossing voor identiteits- en wachtwoordbeheer, bankieren en alle andere soorten gevoelige informatie op verschillende apparaten.

Bitdefender SecurePass kan uw wachtwoorden automatisch opslaan, invullen, genereren en beheren voor alle websites en online diensten met behulp van een enkel hoofdwachtwoord, waardoor uw digitale identiteit in het algemeen veel gemakkelijker te beheren is.

6.1.1. Proef- en betaalde versies van Password Manager

De proefversie van Bitdefender Password Manager werkt op alle accounts op dezelfde manier als de betaalde versie van het product, maar de beschikbaarheid ervan vervalt 90 dagen na activering.

> **Opmerking**
> Merk op dat de betaalde versie van het product weliswaar kan worden gekocht als een puur standalone product, maar dat onbeperkte toegang tot Password Manager is inbegrepen in de abonnementen Bitdefender Premium Security en Bitdefender Ultimate Security.

6.2. Aan de slag

6.2.1. Systeemvereisten

U kunt de laatste versie van Bitdefender SecurePass alleen gebruiken op apparaten met de volgende besturingssystemen:

- **Voor pc-gebruikers:**
  - Windows 7 met Service Pack 1
  - Windows 8.1

- Windows 10
- Windows 11

- **Voor macOS-gebruikers:**
  - macOS 10.14 (Mojave) en recentere macOS-besturingssystemen

> **Opmerking**
> Merk op dat de systeemprestaties kunnen worden beïnvloed op apparaten met CPU's van een oudere generatie.

- **Voor iOS-gebruikers:**
  - iOS 11.0 of recentere iOS-besturingssystemen

- **Voor Android-gebruikers:**
  - Android 5.1 en recentere Android-besturingssystemen

> **Opmerking**
> - Vingerafdrukontgrendeling wordt ondersteund op **Android 6.0** en hoger.
> - De functie automatisch invullen wordt ondersteund op **Android 8.0** en hoger, en is compatibel met iPhone, iPad en iPod touch.

Softwarevereisten

Om Bitdefender SecurePass en al zijn functies te kunnen gebruiken, moeten uw Windows- of macOS-apparaten aan de volgende softwarevereisten voldoen:

- **Microsoft Edge** (gebaseerd op Chromium 80 en hoger)
- **Mozilla Firefox** (versie 65 of hoger)
- **Google Chrome** (versie 72 of hoger)
- **Safari** (versie 12 of hoger)

> **Opmerking**
> De software-vereisten zijn niet van toepassing voor Android en iOS.

Waarschuwing

Het niet voldoen aan de bovenstaande systeemvereisten heeft tot gevolg dat Bitdefender SecurePass niet kan worden geïnstalleerd of dat het product niet goed functioneert.

6.2.2. Installatie

In dit hoofdstuk wordt uitgelegd hoe u Bitdefender SecurePass installeert op zowel de webbrowsers op uw Windows pc en macOS, als op uw mobiele Android- of iOS-apparaten.

Belangrijk

Zorg er vóór de installatie voor dat u een geldig Password Manager-abonnement hebt in uw **Bitdefender Central**-account, zodat deze browserextensie de geldigheid ervan kan ophalen uit uw account.

Actieve abonnementen worden weergegeven in het onderdeel **Mijn abonnementen** in Bitdefender Central.

6.2.3. Installatieproces

Om Bitdefender SecurePass in te stellen op uw browser/mobiele apparaat:

1. Na het voltooien van het installatieproces opent u de SecurePass-extensie/toepassing en logt u in.
   Gebruik de inloggegevens van het Bitdefender-account dat is gekoppeld aan uw SecurePass-abonnement.
2. U wordt gevraagd om een **Hoofdwachtwoord**.

   Belangrijk

   Houd er rekening mee dat u dit hoofdwachtwoord nodig hebt om alle wachtwoorden, creditcardgegevens en notities te ontgrendelen die zijn opgeslagen in Bitdefender SecurePass. Dit is in wezen de sleutel waarmee de eigenaar dit product kan gebruiken.

   Zorg ervoor dat u een sterk hoofdwachtwoord invoert zonder het risico te lopen dat u het gemakkelijk vergeet.
   Zodra u een sterk en uniek hoofdwachtwoord hebt gekozen, klikt u op **Opslaan en doorgaan**.
3. Vervolgens krijgt u een **Herstelsleutel**.

Waarschuwing

Na het aanmaken van het hoofdwachtwoord ontvangt u een **24-cijferige herstelsleutel**. Noteer uw herstelsleutel op een veilige plaats en raak deze niet kwijt. Deze sleutel is de enige manier om toegang te krijgen tot uw wachtwoorden die zijn opgeslagen in Password Manager voor het geval u **vergeet het hoofdwachtwoord** eerder ingesteld voor je account.

- Sla de herstelsleutel op door deze naar uw klembord te kopiëren of als PDF-bestand te downloaden.
  Je kunt op drukken **Sluiten** als je klaar bent.

4. Als u klaar bent, selecteert u de **Toegang tot je kluis** knop.

Nu het installatieproces is voltooid, kunt u Bitdefender SecurePass gaan gebruiken.

6.3. Uw wachtwoorden importeren en exporteren

Bitdefender Password Manager is zo gebouwd dat communicatie en gegevensoverdracht met externe bronnen, platforms en softwaretools efficiënt verlopen. Dit is de belangrijkste reden waarom met gemak kan worden voldaan aan de zeer vaak voorkomende nood aan het importeren of exporteren van wachtwoorden in of uit Bitdefender Password Manager.

6.3.1. Compatibiliteit

Bitdefender Password Manager kan naadloos gegevens overdragen van de volgende lijst van applicaties:

- Bitdefender wachtwoordbeheerder
- Bitdefender-portemonnee
- Bitdefender SecurePass
- SaferPass
- 1 wachtwoord
- Kaspersky
- Dashlane
- Chrome-browser
- Firefox-browser

- Microsoft Edge
- Bitwarden
- LastPass
- KeePass
- RoboForm

Deze overdracht van gegevens tussen Bitdefender Password Manager en andere software voor accountbeheer kan gebeuren via de volgende gegevensformaten:

CSV, **JSON**, **XML**, **TXT**, **1pif** en **FSK**.

6.3.2. Importeren in Password Manager

Met Bitdefender Password Manager kunt u gemakkelijk wachtwoorden importeren uit andere wachtwoordbeheerders en browsers. Als u momenteel wilt overstappen naar Bitdefender Password Manager vanuit een andere dienst voor wachtwoordbeheer, hebt u waarschijnlijk een aanzienlijke hoeveelheid gegevens opgeslagen, zoals gebruikersnamen, wachtwoorden en andere aanmeldingsgegevens die nodig zijn voor al uw accounts.

Nu u Bitdefender Password Manager hebt gekozen, kunt u de opgeslagen gegevens erin importeren.

Hier leest u hoe u uw opgeslagen informatie van andere apps en webbrowsers kunt importeren in Bitdefender Password Manager, **ongeacht het besturingssysteem** waarop u dit product hebt geïnstalleerd:

1. Open Bitdefender SecurePass en ga naar **Instellingen**.
   - In de browser:
     Klik op **Instellingen** in de rechterbovenhoek van de pagina.
   - In de app:
     Tik op de **Meer** knop in de rechteronderhoek van het scherm en tik bovenaan de lijst die daarna verschijnt op **Instellingen**.
2. In het **Back-up maken en herstellen** sectie, selecteer **Wachtwoorden importeren**. Het importvenster wordt geopend.

3. Selecteer de naam van de wachtwoordbeheerder of webbrowser die u eerder hebt gebruikt in het keuzemenu dat toegankelijk is via de **Selecteer het bestandstype** veld.

   > **Opmerking**
   > Als er een wachtwoord is gebruikt om het bestand te versleutelen, moet u dit invoeren in het **Wachtwoord** veld; anders kunt u het leeg laten.

4. Selecteer de **Selecteer het bestand om te importeren** gearchiveerd. Navigeer naar de locatie waar de geëxporteerde gegevens van uw oude wachtwoordbeheerder zijn opgeslagen. Kies het bestand zodra je het hebt gevonden en klik vervolgens op **Open**.

5. Nadat u het bestand hebt geselecteerd, selecteert u **Importeren** in de linkeronderhoek van het importvenster. Het proces begint binnenkort, vergezeld van een voortgangsbalk.

Na het importeren worden uw wachtwoorden toegankelijk op alle apparaten waarop de toepassing Bitdefender Password Manager of de browserextensie is geïnstalleerd.

> **Opmerking**
> Als u teruggaat naar uw wachtwoordkluis in SecurePass, ziet u een map met de naam **Importeren**, met alle gegevens van uw vorige wachtwoordbeheerder of webbrowser.

6.3.3. Exporteren vanuit Password Manager

Met Bitdefender Password Manager kunt u gemakkelijk uw opgeslagen wachtwoorden (inclusief account-logins, beveiligde notities, enz.) exporteren naar een CSV-bestand (door komma's gescheiden waarden) of een gecodeerd bestand als u ooit wilt overschakelen naar een andere wachtwoordbeheerdienst, zodat uw vertrek van Bitdefender Password Manager geen moeilijk proces zal zijn.

> **Belangrijk**
> Een CSV-bestand is **niet** versleuteld en bevat gebruikersnamen en wachtwoorden in platte tekst, wat betekent dat uw privégegevens kunnen worden gelezen door iedereen die toegang heeft tot uw apparaat. Wij raden u daarom aan de onderstaande instructies te volgen op een vertrouwd apparaat.

Hier leest u hoe u uw gegevens uit Bitdefender Password Manager kunt exporteren:

1. Open Bitdefender SecurePass en ga naar **Instellingen**.
   - In de browser:
     Klik op **Instellingen** in de rechterbovenhoek van de pagina.
   - In de app:
     Tik op de **Meer** knop in de rechteronderhoek van het scherm en tik bovenaan de lijst die daarna verschijnt op **Instellingen**.
2. In het **Back-up maken en herstellen** sectie, selecteer **Wachtwoorden exporteren**. Het exportvenster wordt geopend.
3. Klik op **Selecteer het bestandstype**. Kies in het keuzemenu of u uw gegevens wilt exporteren in een JSON-formaat of een CSV-formaat. U kunt ook een wachtwoord invoeren om het geëxporteerde bestand te beveiligen.
   Vink het bijbehorende vakje aan als je ook gedeelde items wilt toevoegen.
4. Klik **Exporteren** in de linkeronderhoek van het exportvenster en sla het geëxporteerde bestand op uw apparaat op.

6.4. Kenmerken en functionaliteiten

In dit hoofdstuk worden alle kenmerken en functionaliteiten van Bitdefender Password Manager overlopen, met uitleg over hun nut en over hoe u ze zo efficiënt mogelijk kunt gebruiken.

6.4.1. Wachtwoorden handmatig opslaan

U kunt informatie zoals wachtwoorden, inloggegevens en andere gegevens, zoals creditcardgegevens of notities, op de volgende manier veilig handmatig in Bitdefender SecurePass opslaan:

1. Bitdefender SecurePass openen
2. In het **Mijn kluis** tab, druk op de **+Item toevoegen** knop.
3. Selecteer het itemtype dat je wilt toevoegen. (account, creditcard, identiteit of briefje).
4. Vul de verplichte velden in, afhankelijk van het geselecteerde item.

5. Nadat u alle benodigde gegevens hebt ingevuld, slaat u het item op om het aan uw SecurePass-kluis toe te voegen.

6.4.2. Wachtwoordgenerator

Bitdefender SecurePass bevat een functie voor het genereren van wachtwoorden die kan helpen bij het aanmaken van veilige wachtwoorden.

Om toegang te krijgen tot de wachtwoordgenerator en deze te gebruiken:

1. Open Bitdefender SecurePass en krijg toegang tot de **Wachtwoord genereren** tab aan de linkerkant van het scherm. Dit brengt u naar de wachtwoordgenerator die is geïntegreerd in SecurePass
2. Pas het wachtwoord dat u gaat genereren aan uw eigen behoeften en voorkeuren aan.
   - Wachtwoordlengte: versleep de schuifregelaar om een lengte tussen 8 en 32 tekens te bepalen.
   - Hoofdletters en kleine letters: Selecteer welke - of beide - soorten letters je wilt toevoegen voor het complexiteitsniveau van je wachtwoord.
   - Getallen: Als u dit vakje aanvinkt, worden cijfers opgenomen in de tekenreeks die uw wachtwoord bevat.
   - Speciale tekens: Voeg symbolen toe aan je wachtwoord om de complexiteit van het wachtwoord te vergroten.

     Opmerking
     Druk op de **Instellingen opslaan** knop voor SecurePass om ze te onthouden en altijd wachtwoorden te genereren op basis van de instellingen die je hebt opgeslagen.
3. Genereer een nieuw wachtwoord door op het ronde pijlpictogram te klikken dat zich onder het momenteel weergegeven wachtwoord bevindt. Elke klik genereert een nieuwe reeks tekens.
4. Als u tevreden bent met het gegenereerde wachtwoord, kunt u het naar uw klembord kopiëren of op de knop klikken **Account opslaan** knop om het in uw kluis op te slaan (door te koppelen aan andere accountgegevens).

> **Opmerking**
> Je kunt ook snel een wachtwoord genereren **rechtstreeks vanuit aanmeldingsformulieren** door te klikken op het Bitdefender SecurePass-pictogram in het wachtwoordveld van de aanmeldingspagina. Door erop te klikken, kunt u vervolgens kiezen voor de **Wachtwoord genereren** optie.

6.4.3. Controle van de wachtwoordsterkte

Bitdefender SecurePass biedt de mogelijkheid om de sterkte van opgeslagen wachtwoorden en gevoelige gegevens te evalueren. Dit is van essentieel belang bij het evalueren en beoordelen van mogelijke kwetsbaarheden in de privacy en beveiliging van uw gegevens.

Ga als volgt te werk om de sterke punten van opgeslagen wachtwoorden te controleren:

1. Open Bitdefender SecurePass en selecteer in het mailmenu de optie **Beveiligingsrapport** tab.
   Het tabblad Beveiligingsrapport is onderverdeeld in vier secties: geschonden, zwak, oud en dubbel.
2. Het aantal wachtwoorden dat in elk van de vier categorieën valt, wordt op het scherm weergegeven.
   Als u de lijst met opgeslagen wachtwoorden doorloopt, wordt elk wachtwoord bovendien getagd met de categorie waaronder het zich bevindt.

Om de betekenis achter deze beveiligingsniveaus te begrijpen, vindt u hieronder enkele beknopte informatie over elk van deze niveaus:

- Wachtwoorden die zijn geschonden: Als een van uw inloggegevens deel heeft uitgemaakt van een datalek, worden deze vermeld onder de **doorbroken** sectie.

  > **Opmerking**
  > Om te controleren of een van uw wachtwoorden is gehackt en gelekt door datalekken, klikt u op de **Voer een beveiligingsscan uit** knop.

- Zwakke wachtwoorden: SecurePass identificeert en markeert **zwak** wachtwoorden die in uw kluis zijn opgeslagen op basis van een intern, lokaal draaiend algoritme dat onder andere naar verschillende criteria

kijkt, zoals de lengte van het wachtwoord, het aantal tekens en het opnemen van cijfers of hoofdletters.

- Oude wachtwoorden: Wachtwoorden die langer dan zes maanden zijn opgeslagen en ongewijzigd zijn gebleven, worden gemarkeerd als **oud**.
- Dubbele wachtwoorden: Aangezien het gebruik van dezelfde wachtwoorden op meerdere platforms en accounts een groot veiligheidsrisico inhoudt, zal SecurePass wachtwoorden die op meer dan één plaats worden gebruikt, markeren als **duplicaat**.

6.4.4. Organisatie van de gegevens

Binnen Bitdefender SecurePass kunt u al uw opgeslagen items organiseren en dus eenvoudiger beheren.

Je kunt je items in specifieke mappen indelen voor eenvoudige toegang door deze stappen te volgen:

1. Open Bitdefender SecurePass en ga naar **Mijn kluis**. Tik hier op de **Folder toevoegen** knop.
2. Geef je map een naam en tik op **Creëren** knop.
   De nieuwe map verschijnt nu in je kluis.

Om items naar de aangemaakte map te verplaatsen:

1. Klik op een account dat je wilt verplaatsen en druk op **Bewerken** knop.
2. Druk op de locatie die wordt weergegeven naast **Item opslaan in** en selecteer de mapnaam in de keuzelijst.
3. Druk op de **Account opslaan** knop.

Het account wordt nu opgeslagen in de geselecteerde map.

6.4.5. Intelligente automatische aanvulling

Met Bitdefender SecurePass kunt u accountgegevens en -informatie automatisch invullen op alle online aanmeldingsformulieren.

> **Opmerking**
> Als webbrowserextensie zou de functie Automatisch aanvullen op Windows of MacOS naadloos moeten werken.

Automatisch aanvullen op Android

Om SecurePass op Android te configureren om Autofill te gebruiken:

1. Open de Bitdefender SecurePass-app op je Android-apparaat.
2. Tik op de **Meer** menuknop.
3. Tik bovenaan het scherm op **Instellingen**.
4. Tik op **Maak dit uw standaard wachtwoordbeheerder**
5. Schakel Bitdefender SecurePass in de lijst met services voor automatisch aanvullen in.

> **Opmerking**
> Je kunt ook naar de instellingen van je Android-apparaat gaan, in **Wachtwoorden en accounts** > **Service voor automatisch aanvullen** > schakel Bitdefender SecurePass in.
>
> Voor Android 11 of eerdere versies van het besturingssysteem zijn de instellingen: **Systeem** > **Taal en invoer** > **Geavanceerd**.

6. Tik **OK**.

Zodra deze configuratie is voltooid, verschijnt er telkens wanneer u op een aanmeldingsveld tikt een optie genaamd Bitdefender SecurePass op uw scherm. Je kunt erop tikken om de app te openen. Meld u aan bij SecurePass en uw inloggegevens worden automatisch ingevuld

Automatisch aanvullen op iOS

Om SecurePass op uw iOS-apparaat te configureren om Autofill te gebruiken:

1. Open het **Instelling** app op je iPhone of iPad en selecteer **Algemeen**.
2. Tik op **Automatisch aanvullen en wachtwoorden**. Zorg voor de optie **Wachtwoorden en wachtwoordsleutels automatisch invullen** of **Wachtwoorden automatisch invullen** - afhankelijk van de iOS-versie - is ingeschakeld.
3. In het **Formulier automatisch invullen** lijst, schakel de **Bitdefender SecurePass** applicatie.

Zodra deze configuratie is voltooid, verschijnt er telkens wanneer u op een aanmeldingsveld tikt een optie genaamd Bitdefender SecurePass op uw scherm. Je kunt erop tikken om de app te openen. Meld u aan bij SecurePass en uw inloggegevens worden automatisch ingevuld

Kaartgegevens automatisch invullen

SecurePass biedt een gemakkelijk toegankelijk pictogram voor het automatisch invullen van inloggegevens en wachtwoorden, maar de functie voor automatisch aanvullen van creditcardgegevens werkt anders:

1. Navigeer naar de betalings- of betaalpagina van de website waarop u uw opgeslagen creditcardgegevens wilt gebruiken.
2. Klik met de rechtermuisknop op een leeg gedeelte van de betaalpagina. Dit zal ertoe leiden dat het contextmenu op uw scherm verschijnt
3. Selecteer Bitdefender SecurePass in het menu door de muisaanwijzer op de optie te bewegen. Dit opent een submenu met meer opties
4. Kies de **Creditcardgegevens automatisch invullen**. Hiermee wordt een lijst weergegeven van alle creditcards die u in de SecurePass-kluis hebt opgeslagen
5. Selecteer de gewenste kaart.

Op deze manier vult SecurePass de velden van het betalingsformulier automatisch in met de gegevens van de creditcard die u hebt gekozen.

6.5. Gebruik als een 2FA-applicatie

U kunt er altijd voor kiezen om Bitdefender SecurePass te gebruiken als een app voor tweefactorauthenticatie voor elke website of elk gewenst platform, en uw 2FA-codes naast uw wachtwoorden op de volgende manier te beheren:

1. Ga naar de beveiligingsinstellingen van de website of applicatie waar je de 2FA-functie wilt inschakelen. Meestal krijgt u tijdens het proces een QR-code of een verificatiecode te zien.
2. Start Bitdefender SecurePass en open het corresponderende account dat u wilt configureren voor 2FA-gebruik. Klik op de **Bewerken** knop.
3. Blader naar de onderkant van de accountinvoerpagina in SecurePass en druk op de **Twee-factor-authenticatie** optie.
4. Scan de QR-code of voer de code handmatig in.
   Zodra dit is gebeurd, bevestigt SecurePass de succesvolle configuratie van tweefactorauthenticatie.

5. Druk daarna op de nieuwe **Code bekijken** knop nu zichtbaar in de interface. Daar wordt een tijdgevoelige code weergegeven
6. Ga terug naar het account waar u de 2FA-functie hebt ingeschakeld en voer de code van Bitdefender SecurePass in om uw configuratie te verifiëren.

Na het voltooien van dit installatieproces drukt u op de **Account opslaan** knop in SecurePass om het proces te voltooien.

Voortaan wordt u, wanneer u inlogt op het platform waarvoor u de 2FA-functie hebt ingesteld, gevraagd om de 2FA-codes van SecurePass te gebruiken voor het betreffende account, wat een nieuwe beveiligingslaag biedt voor het betreffende account.

6.6. Gegevens delen

Bitdefender SecurePass biedt de mogelijkheid om gevoelige informatie, zoals inloggegevens, wachtwoorden of creditcardgegevens, veilig te delen.

Je kunt de deelfunctie gebruiken via links:

1. Kies een item dat is opgeslagen in je kluis.
   - In de browser:
     Ga naar je kluis en klik op het item dat je wilt delen. Klik aan de rechterkant op het menu met de drie puntjes en selecteer **Link delen**.
   - In de app:
     Ga naar je kluis en tik op het item dat je wilt delen. Tik op het linkpictogram en kies de **Genereer een link om te delen** optie.
2. Maak de link Delen door het volgende op te geven:
   - De vervaldatum van de link.
   - De gebruikslimiet.
   - Of de link wel of niet met een wachtwoord moet worden beveiligd.
3. Eenmaal gegenereerd, kopieert u de gegenereerde link en stuurt u deze naar de beoogde ontvanger.

6.6.1. Delen met groepen

Er worden groepen gemaakt om het delen van gegevens nog eenvoudiger te maken. U kunt binnen Bitdefender SecurePass verschillende groepen aanmaken met andere gebruikers om gevoelige gegevens veilig te delen

1. Een groep aanmaken:
   - Ga naar **Groepen** en druk op de **Een groep aanmaken** knop op het tabblad Groepen.
   - Stel een groepsnaam in en druk vervolgens op **Een groep aanmaken** knop.
2. Items aan groepen toevoegen:
   - In de browser:
     Ga naar je kluis en klik op het item dat je wilt delen. Klik op het menu met de drie puntjes aan de rechterkant van het item en kies **Aan groep toevoegen**.
   - In de app:
     Ga naar je kluis en klik op het item dat je wilt delen. Kies de **Deel met de groep** optie.

   Selecteer de groep waarmee je het item wilt delen.
3. Stel de toegangsrechten (lezen, schrijven, verlenen) in op basis van de mate van controle die je groepsleden wilt geven.
4. Druk op **Opslaan**, dan **Klaar**.

Jij en groepsleden kunnen gedeelde items bekijken in de sectie van de groep.

6.6.2. Groepen beheren

In het **Groepen** in het gedeelte van Bitdefender SecurePass kunt u alle aangemaakte groepen bekijken en beheren op basis van uw behoeften:

- Groepen hernoemen.
- Leden bewerken. (nieuwe leden uitnodigen, rechten toekennen aan specifieke leden, beheer- of deelrechten verlenen en bestaande leden verwijderen)
- Groepen verlaten.

- Groepen verwijderen.

6.7. Account vergrendelen

Bitdefender SecurePass wordt geleverd met een **Account vergrendelen** functie die uw account onmiddellijk vergrendelt en alle actieve sessies beëindigt op alle apparaten die er toegang toe hebben. Deze functie is vooral handig wanneer er vermoedens van ongeoorloofde toegang ontstaan

Om uw SecurePass-account te vergrendelen:

1. Open Bitdefender SecurePass.
2. Eenmaal in SecurePass:
   - In de browser:
     Klik op **Instellingen** in de rechterbovenhoek van de pagina.
   - In de mobiele app:
     Tik op de **Beveilig me** menuknop.
3. Druk op de **Account vergrendelen** knop om direct uit te loggen van alle apparaten en lopende sessies te beëindigen.

6.8. Veelgestelde vragen

Sommige veelgestelde vragen over Bitdefender Password Manager komen vaak terug. Wij hebben de antwoorden! Hier vindt u meer informatie over uw Bitdefender-account, het importeren van wachtwoorden, protocollen voor gegevensbeveiliging en andere onderwerpen die belangrijk zijn voor onze klanten.

Algemene vragen over Bitdefender Password Manager

Wat gebeurt er wanneer Bitdefender Password Manager vervalt?

Wanneer uw abonnement op Bitdefender Password Manager vervalt en niet langer actief is, hebt u maximaal 90 dagen de tijd om uw wachtwoorden te exporteren. De wachtwoorden worden nog 30 dagen in een back-up bewaard. Gedurende deze 90 dagen kunt u alleen uw gegevens exporteren. U kunt Bitdefender Password Manager niet meer gebruiken. De functie voor automatisch invullen werkt niet meer, evenmin als de mogelijkheid om wachtwoorden te genereren.

Aan het einde van de 90 dagen respijtperiode hebt u 30 dagen extra de tijd om contact op te nemen met de ondersteuning van Bitdefender en een verzoek in te dienen om uw wachtwoorden terug te zetten naar de live database. U zult dan uw wachtwoorden kunnen exporteren vanuit Bitdefender Password Manager.

Uw gegevens worden alleen in de live database bewaard tot het einde van de dag dat ze op verzoek werden hersteld. Om middernacht wordt de database gewist - en als u de extra periode van 30 dagen nog niet hebt overschreden, kunnen de wachtwoorden opnieuw worden hersteld vanuit de back-up. Op verzoek van de gebruiker kunnen de ruwe databasegegevens uit de back-up worden verstrekt, maar de database is gecodeerd en de informatie is niet toegankelijk.

Wat is een hoofdwachtwoord en waarom moet ik het onthouden?

Het hoofdwachtwoord is de sleutel die de deur opent naar alle wachtwoorden die in uw Bitdefender Password Manager-account zijn opgeslagen. Het hoofdwachtwoord moet ten minste 8 tekens lang zijn. Maak dus een sterk hoofdwachtwoord, onthoud het en deel het nooit met iemand. Om een sterk hoofdwachtwoord te maken, raden we u aan een combinatie te gebruiken van hoofdletters en kleine letters, cijfers en speciale tekens (zoals #, $, of @).

Waarom slaan jullie mijn hoofdwachtwoord niet op, en wat gebeurt er als ik het vergeet?

De reden waarom we uw hoofdwachtwoord niet opslaan op onze servers is dat alleen u toegang heeft tot uw account. Het is de meest veilige manier. Als Bitdefender Password Manager uw hoofdwachtwoord niet herkent, controleer dan of u het correct typt en of de Caps Lock-toets niet actief is op het toetsenbord.

Als u het hoofdwachtwoord vergeet, kunt u altijd de Herstelsleutel gebruiken om Password Manager te ontgrendelen. Tijdens het aanmeldingsproces biedt Bitdefender Password Manager een **herstelsleutel** die kan worden gebruikt om weer toegang te krijgen tot de account zonder uw gegevens te verliezen.

Wat is de offlinemodus?

offlinemodus wordt automatisch geactiveerd wanneer de internetverbinding wegvalt tijdens het gebruik van Bitdefender SecurePass. Als u al bent aangemeld en uw hoofdwachtwoord hebt

ingevoerd, kunt u in de modus Offline toegang krijgen tot uw wachtwoorden wanneer een internetverbinding buiten bereik is.

Hoe kan ik de installatie van Bitdefender Password Manager ongedaan maken?

Bitdefender Password Manager de-installeren:

- Op Windows en macOS:
  Verwijder de Password Manager-extensie uit uw webbrowser. Klik met de rechtermuisknop op het Bitdefender-pictogram en selecteer "Verwijderen".
- Android:
  Tik en houd de Password Manager-app ingedrukt en sleep deze naar de bovenkant van het scherm waar "Verwijderen" staat.
- Op iOS en iPadOS:
  Tik op de app Password Manager en houd deze ingedrukt totdat alle apps op uw scherm beginnen te wiebelen, tik vervolgens op de "X" linksboven het Bitdefender-pictogram.

Veiligheidsvragen over Bitdefender Password Manager

Kunnen medewerkers van Bitdefender mijn wachtwoorden zien?

Absoluut niet. Uw privacy is onze hoogste prioriteit. Dit is de belangrijkste reden waarom we uw hoofdwachtwoord niet opslaan op onze gegevensservers: zodat niemand toegang heeft tot uw account, zelfs niet de medewerkers van het bedrijf. Elk wachtwoord en account zijn sterk versleuteld met het sterkste algoritme voor gegevensbeveiliging, en de code die we zien ziet er gewoon uit als een willekeurige reeks cijfers en letters die door elkaar zijn gegooid.

Wat zou er gebeuren als de servers van Password Manager worden gehackt?

Elk wachtwoord wordt lokaal op uw apparaat gecodeerd voordat het in de buurt van onze servers komt, dus als hackers in ons systeem zouden inbreken, zouden ze alleen pagina's met willekeurige letters en cijfers krijgen zonder uw sleutel om ze te decoderen. Dit betekent dat u en uw accountgegevens bij ons altijd veilig zijn.

7. DIGITALE IDENTITEITSBESCHERMING

7.1. Wat is Bitdefender VPN

Online privacy en veiligheid zijn tegenwoordig enkele van de belangrijkste aandachtspunten voor internetgebruikers. En daar zijn goede redenen voor. Nu er steeds vaker grote datalekken plaatsvinden, is het absoluut noodzakelijk ervoor te zorgen dat uw persoonlijk identificeerbare informatie (PII) veilig is.

Maar wat kan worden geclassificeerd als persoonlijk identificeerbare informatie? Traditioneel werd gevoelige informatie zoals de volledige naam, het sofi-nummer, het rijbewijs, het postadres of creditcardgegevens als PII beschouwd. Uiteindelijk werd ook minder gevoelige informatie, zoals postcodes, IP-adressen of login-ID's, opgenomen. Na verloop van tijd kan uw digitale voetafdruk, dat wil zeggen de gegevens die u achterlaat als gevolg van uw surfen op het internet, een aantal van deze gegevens gaan omvatten.

Bitdefender VPN vertegenwoordigt de privéweg naar online vrijheid, waardoor u weer controle krijgt over uw digitale leven. En het vereist alleen uw naam, meest gebruikte e-mailadres en uw telefoonnummer. Op basis hiervan wordt zowel op het Surface Web als het Dark Web gezocht naar persoonlijke informatie die openbaar is gemaakt.

Bitdefender VPN biedt het volgende:

- **Monitoring- en detectiediensten:** het monitort meer dan 100 persoonlijk identificeerbare informatie-items zoals sofi-nummers, creditcards of huisadres, en toont alle gevonden gegevens over uw online voetafdruk.

  > **Opmerking**
  > Bitdefender bewaart of verwerkt geen persoonlijk identificeerbare informatie. Alleen verwijzingen naar mogelijke datalekken worden bijgehouden, zonder gevoelige gegevens.

- **Real time waarschuwingen:** U ontvangt meldingen over datalekken en blootgestelde gegevens in Dark Web, persoonlijke informatie in Surface Web en potentiële imitators op sociale media.
- **Oplossingen:** Onze service stelt duidelijke acties voor die nodig zijn om problemen op te lossen en stuurt herinneringen als een probleem

niet volledig is opgelost. Er kunnen ook instructies gegeven worden over hoe u de gepersonaliseerde advertenties kunt verwijderen, uw gegevens kunt exporteren of de tracking kunt uitschakelen.

7.2. Aan de slag

7.2.1. Activeer Digitale Identiteitsbescherming

Activeer het Bitdefender Digital Identity Protection-abonnement nadat uw bestelling is geplaatst en betaald.

1. Open de bevestigingsmail die u kort na het afronden van uw bestelling ontvangt en klik op **AAN DE SLAG**.
2. U wordt doorgestuurd naar https://central.bitdefender.com.
   Meld u aan met uw Bitdefender Central-account. Als u geen account hebt, kunt u er een aanmaken.
3. Na aanmelding wordt het abonnement automatisch gekoppeld aan uw Central-account en start het onboardingproces.

U kunt ook:

- ga naar het **Mijn Abonnementen** paneel vanuit Central, aan de linkerkant van het venster, en klik op **+ Activeren met code**.
- voer de 10-cijferige sleutel in die u in uw bevestigingsmail hebt gevonden en druk op **ACTIVEREN**.
- selecteer, indien gevraagd, hoe u de code wilt gebruiken en klik dan op **ACTIVEREN**.

7.2.2. Configureer Digitale Identiteitsbescherming

1. Ga naar https://central.bitdefender.com/ en log in op uw account.
   Als u nog geen account hebt, klik dan op **CREËER ACCOUNT**, typ uw volledige naam, een e-mailadres en een wachtwoord.
2. Selecteer het Digital Identity Protection-paneel.
   Er verschijnt een welkomstscherm.
3. Klik op **BEGINNEN**.
4. U wordt nu geïnformeerd over welke informatie u moet verstrekken. Uw gegevens worden altijd versleuteld en beveiligd.
   Klik op **VOLGENDE**.

5. Typ uw voornaam, tweede voornaam (indien van toepassing) en achternaam in de overeenkomstige vakken en klik dan op **VOLGENDE**.
6. Voer uw e-mailadres in en klik op **VOLGENDE**.
   Zorg ervoor dat het een geldig e-mailadres is waartoe u toegang hebt.
7. Er wordt een beveiligingscode naar het door u opgegeven adres gestuurd.
   Open uw e-mail, kopieer de code en plak deze in het overeenstemmende veld.
   Klik daarna op **CONTROLEREN**.
8. Selecteer uw land en voer uw telefoonnummer in, en klik vervolgens op **VOLGENDE**.
9. U zou kort daarna een beveiligingscode moeten ontvangen.
   Voer de code in en selecteer **CONTROLEREN**.
10. Nadat de eerste controle is uitgevoerd, klikt u op **VOLTOOIEN**.

.

> **Opmerking**
> U wordt geïnformeerd indien bij deze eerste controle inbreuken, persoonlijk identificeerbare informatie of mogelijke pogingen tot imitatie worden ontdekt.

Bitdefender VPN is nu geconfigureerd.

7.2.3. Bekijk uw digitale voetafdruk, inbreuken op gegevens en mogelijke imitaties

Nadat u de configuratie hebt voltooid, voert Bitdefender VPN een online controle uit om mogelijke imitaties, datalekken en persoonlijk identificeerbare informatie op het Open Web te ontdekken. Wij raden u aan om alle informatie in de tabbladen **DIGITALE VOETAFDRUK**, **DATALEKKEN** en **IMITATIECONTROLE** te bekijken.

- Uw Digitale Voetafdruk evalueren (pagina 302)
- Datalekken evalueren (pagina 303)
- Evalueren van mogelijke imitaties (pagina 304)

7.2.4. Verbeter de controle

We gebruiken de gegevens die u voorziet om het Surface Web en het Dark Web te monitoren en enige activiteiten te detecteren die uw privacy of uw persoonlijke reputatie zouden kunnen aantasten.

Als u een ander e-mailadres of een ander telefoonnummer wilt toevoegen, klik dan op ⊕, klik dan op **E-MAILADRES TOEVOEGEN** of **TELEFOONNUMMER TOEVOEGEN** en volg de instructies.

7.3. Dashboard

Het Dashboard voegt informatie samen uit de secties **DIGITALE VOETAFDRUK**, **DATALEKKEN** en **IMITATIECONTROLE**.

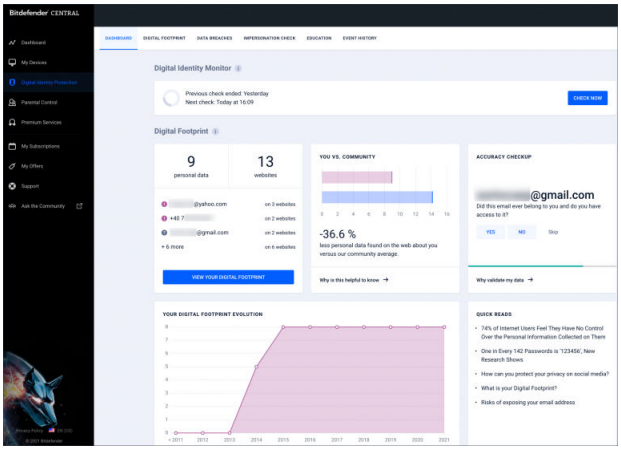
Dit omvat het volgende:

- Uw blootgestelde gegevens en hun webbronnen
- De gemiddelde hoeveelheid blootgestelde gegevens voor de hele gemeenschap
- De evolutie van uw digitale voetafdruk
- Inhoud met betrekking tot privacy
- Gegevensinbreuken
- Het gemiddelde aantal datalekken binnen de gemeenschap

7.3.1. Digital Identity Monitor

Het systeem van Bitdefender zoekt, aan de hand van nauwkeurige informatie, naar persoonsgegevens die zijn blootgesteld op het Open Web en het Dark Web, en scant alle voornaamste sociale mediaplatformen op zoek naar aanwijzingen van pogingen tot imitatie.

Klik op **NU CONTROLEREN** om een online scan uit te voeren.



7.4. Digitale Voetafdruk

Uw persoonlijk identificeerbare informatie en hun bronnen verschijnen hier. Het is aan u om te beoordelen of het openbaar maken van de informatie op het web een bedreiging vormt.

Onze AI-gestuurde monitor is sterk afhankelijk van correcte gegevens om nieuwe dreigingen te detecteren, dus laat ons weten of de informatie juist of onjuist is.

Zodra u bevestigt dat bepaalde informatie van u is, voegen wij deze toe aan ons monitoringsysteem en vergroten wij de kans om in de toekomst andere informatie te ontdekken.

7.4.1. Uw Digitale Voetafdruk evalueren

Om uw digitale voetafdruk te evalueren:

1. Ga naar het tabblad **DIGITALE VOETAFDRUK**.
2. Informatie die nog niet geverifieerd is, verschijnt met de tekst **Verifiëren** aan de rechterkant. Klik op **Verifiëren** en selecteer vervolgens Ja of Nee, afhankelijk van het geval.

> **Opmerking**
> Elk bevestigd informatie-item wordt toegevoegd aan ons monitoringalgoritme, waardoor de door onze diensten getoonde resultaten verbeteren. Informatie die wordt afgewezen, wordt niet langer weergegeven. Ze blijft echter wel beschikbaar op het web.

7.5. Datalekken

Lekken doen zich voor wanneer hackers erin slagen de beveiligingsmaatregelen van een bedrijf te omzeilen en uw persoonlijke informatie te bemachtigen, om die vervolgens te verkopen op het Dark Web. Cybercriminelen richten zich meestal op inloggegevens, persoonlijk identificeerbare informatie (PII), medische gegevens en bankgegevens.

Elke organisatie of dienst kan het slachtoffer worden van een datalek, maar organisaties met een groot klantenbestand zijn een aantrekkelijker doelwit. Inbreuken omvatten gewoonlijk namen, e-mailadressen, gebruikersnamen, wachtwoorden, postadressen, telefoonnummers, sofi-nummers en creditcardgegevens (nummer, vervaldatum, CVV).

7.5.1. Datalekken evalueren

Om uw datalekken te evalueren:

1. Ga naar het tabblad **DATALEKKEN**.
2. Onder sommige items vindt u een lijst met acties die nodig zijn om uw account te beveiligen. Na het uitvoeren van een actie klikt u op het vakje ernaast om te bevestigen.
   Als u niet zeker weet hoe u een taak moet uitvoeren, kunt u altijd op de link in de taakbeschrijving klikken en wordt u doorgestuurd naar een pagina waar u alle nodige stappen vindt.
   Niet alle inbreuken kunnen op deze manier worden aangepakt. Sommige, zoals **Collection #1**, bevatten geen stappen. In plaats daarvan wordt u doorverwezen naar online beschikbare artikels waar u meer hulp kunt vinden.

   Opmerking
   Bitdefender bewaart of verwerkt geen persoonlijk identificeerbare informatie. Alleen verwijzingen naar mogelijke datalekken worden bewaard, zonder gevoelige gegevens op te nemen.

7.6. Controle Imitaties

Criminelen die bekend staan als "pretexters" maken op allerlei manieren gebruik van de kunst van het zich voordoen als een vertrouwd persoon om hun slachtoffers te misleiden en toegang te krijgen tot gevoelige informatie. "Pretexting" wordt gedefinieerd als het zich voordoen als iemand anders om een ontvanger te manipuleren tot het verstrekken van

gevoelige gegevens zoals wachtwoorden, creditcardnummers of andere vertrouwelijke informatie.

Bitdefender VPN bewaakt 25 sociale mediaplatformen en brengt u onmiddellijk op de hoogte als een profiel wordt gevonden dat een poging tot imitatie zou kunnen zijn.

7.6.1. Evalueren van mogelijke imitaties

In het tabblad **IMITATIECONTROLE** worden alle mogelijke pogingen weergegeven. Voor elke detectie kunt u een van drie mogelijkheden kiezen:

- Het is een poging tot imitatie
- Het is uw eigen profiel
- Het is een ander profiel

Afhankelijk van de Bitdefender VPNkeuze zal specifieke stappen aanbevelen om het probleem aan te pakken. Telkens wanneer u een stap hebt voltooid, kunt u deze markeren als **Gereed**.

7.7. Opleiding

Het tabblad Opleiding dient als kennisbank waar gebruikers meer informatie kunnen vinden over hoe zij hun digitale identiteit kunnen beschermen.

De hier vermelde artikels kunnen in verschillende categorieën worden ingedeeld:

- Lekken
- Blootstellingen
- Nabootsing van identiteit

Voor toegang tot de volledige versie van een artikel, klikt u op de overeenstemmende **Meer informatie** link.

7.8. Eventgeschiedenis

De sectie Gebeurtenishistorie is het middel waarmee wij voortdurend met onze gebruikers communiceren. Het is een chronologisch geordende lijst van gebeurtenissen met betrekking tot de bescherming van uw Digitale Identiteit.

Naast nieuw gedetecteerde dreigingen (indien aanwezig), kunt u terugkeren naar deze pagina voor waardevol advies over hoe u zich online correct kunt gedragen, om de kans te vergroten dat u niet te maken krijgt met privacyproblemen.

In de sectie Gebeurtenishistorie vindt u de volgende informatie:

- Uitgevoerde acties
- Service-updates
- Datalekken

7.9. Veelgestelde vragen

Waarom is online privacy tegenwoordig zo belangrijk?

Online privacy betekent het beschermen van uw privé- en financiële gegevens tegen cybercriminelen. Dergelijke persoonlijk identificeerbare informatie heeft grote waarde op het internet en zodra deze gegevens uitlekken, is uw geld niet langer veilig. U hebt een betrouwbare dienst nodig voor continue identiteitsbescherming en -bewaking om ervoor te zorgen dat uw privégegevens altijd privé blijven.

Wat is mijn digitale voetafdruk?

Uw digitale voetafdruk is uw gehele online activiteit. Elke login op uw sociale accounts, elke banktransactie, alles wat u online koopt kan worden blootgesteld aan datalekken. U moet zich te allen tijde bewust zijn van de manier waarop uw persoonlijke en financiële gegevens worden opgeslagen en behandeld - en de nodige stappen ondernemen om ze te beschermen.

Wat zijn datalekken en hoe beïnvloeden ze mijn persoonlijke accounts?

Datalekken zijn beveiligingsincidenten waarbij privégegevens uitlekken naar een onveilige omgeving. Deze kunnen door cybercriminelen overal ter wereld worden misbruikt om toegang te krijgen tot uw online identiteit. Datalekken kunnen gevolgen hebben voor uw kredietscore, ziekteverzekering, studiebeurzen of zelfs uw pensioenrekening.

Hoe kan Bitdefender Digital Identity Protection helpen met mijn online privacy?

Bitdefender Digital Identity Protection bewaakt voortdurend uw persoonlijke gegevens en waarschuwt u in real time in geval van een

datalek. Zo kunt u uw wachtwoorden wijzigen en uw accounts beveiligen om financieel verlies of imitaties op sociale media te voorkomen.

Waar zoekt Bitdefender Digital Identity Protection naar gegevens?

Bitdefender Digital Identity Protection zoekt naar gegevens op het Surface Web (sociale medianetwerken, berichten, blogs, forums, gegevensmakelaars, publicaties, offline databases) maar ook op de Dark Web-marktplaatsen, waar cybercriminelen informatie verhandelen die is verzameld uit datalekken.

Hoe verschilt Bitdefender Digital Identity Protection van andere (gratis) diensten?

Bitdefender Digital Identity Protection heeft ongeëvenaarde mogelijkheden om aanzienlijke volumes en een hogere kwaliteit van gegevens van het Dark Web te bewaken. De informatie van het Dark Web wordt gecureerd en ontdubbeld zodat we het aantal vals-positieve waarschuwingen kunnen verminderen.

Hoe kan ik de dienst gebruiken? Moet ik iets downloaden?

U hoeft niets te downloaden, want Bitdefender Digital Identity Protection is een online dienst. U krijgt toegang tot een web-dashboard waar u al uw persoonlijke accounts in real time kunt controleren.

Hoe kan ik waarschuwingen ontvangen voor toekomstige datalekken?

Om waarschuwingen te ontvangen voor toekomstige datalekken hoeft u zich alleen maar aan te melden voor e-mailwaarschuwingen vanuit uw web-dashboard, en u begint privacywaarschuwingen en beveiligingsrapporten te ontvangen van Bitdefender Digital Identity Protection.

8. HULP VRAGEN

8.1. Hulp vragen

Bitdefender biedt zijn klanten een ongeëvenaard niveau van snelle en nauwkeurige ondersteuning. Als u een probleem ondervindt of een vraag hebt over uw Bitdefender-product, kunt u verschillende online bronnen gebruiken om een oplossing of een antwoord te vinden. Tegelijkertijd kunt u contact opnemen met het klantenserviceteam van Bitdefender. Onze ondersteuningsmedewerkers zullen uw vragen tijdig beantwoorden en u de hulp bieden die u nodig hebt.

8.2. Online bronnen

Er zijn meerdere online informatiebronnen beschikbaar om u te helpen bij het oplossen van problemen en vragen met betrekking tot Bitdefender.

- Bitdefender Support Center:
  https://www.bitdefender.nl/consumer/support/
- De Community van Bitdefender-experts:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

U kunt ook uw favoriete zoekmachine gebruiken om meer informatie te zoeken over computerbeveiliging, de Bitdefender-producten en het bedrijf.

8.2.1. Bitdefender Support Center

Het Bitdefender Support Center is een online opslagplaats van informatie over Bitdefender-producten. Hier worden rapporten bijgehouden in een gemakkelijk toegankelijk formaat over de doorlopende technische ondersteuning en activiteiten voor foutoplossingen van de ondersteunings- en ontwikkelingsteams van Bitdefender. Daarnaast vindt u hier ook meer algemene artikels over dreigingspreventie, het beheer van Bitdefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

De Bitdefender Support Center is toegankelijk voor het publiek en kan vrij worden doorzocht. De uitgebreide informatie die de database bevat is nog

een middel om BitDefender-klanten de technische kennis en het inzicht te bieden die ze nodig hebben. Alle geldige aanvragen voor informatie of foutrapporten die van BitDefender-klanten komen, vinden uiteindelijk hun weg naar de Bitdefender Support Center als rapporten over het oplossen van problemen, tips om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

Het Bitdefender Support Center is te allen tijde beschikbaar op het volgende adres: https://www.bitdefender.nl/consumer/support/.

8.2.2. De Community van Bitdefender-experts

De Community van Experts is een omgeving waar gebruikers, enthousiastelingen en fans van Bitdefender aan kunnen deelnemen, waar ze ideeën kunnen uitwisselen, elkaar kunnen ondersteunen en hun kennis en oplossingen kunnen delen. Het is ook een plaats voor brainstorming en een bron van waardevolle feedback aan onze ontwikkelingsteams. De leden van de gemeenschap zijn ervaren Bitdefender-gebruikers die in hun eigen tijd graag anderen helpen. Met hun enorme bijdrage en oprechte vrijwillige inspanningen hebben we een kennisbank gecreëerd waar gebruikers antwoorden en begeleiding kunnen vinden, maar met dat menselijke tintje.

Hier vindt u zinvolle gesprekken met mensen die Bitdefender gebruiken op hun apparaten. De gemeenschap biedt een echte band met onze leden en laat uw stem horen. Het is een plek waar u wordt aangemoedigd om deel te nemen in de wetenschap dat uw mening en inbreng worden gerespecteerd en gekoesterd. Als gewaardeerde provider streven we ernaar een ongeëvenaard niveau van snelle, accurate ondersteuning te bieden en willen we onze gebruikers dichter bij ons brengen. Wij hebben onze gemeenschap met dit doel voor ogen ontworpen.

U vindt de website van onze Community van experts hier:

https://community.bitdefender.com/en/

8.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia heeft alle informatie die u nodig hebt over de nieuwste cyberdreigingen. Dit is de plaats waar Bitdefender-experts tips en trucs delen over hoe u beschermd kunt blijven tegen hackers, datalekken, identiteitsdiefstal en pogingen tot sociale imitatie.

De webpagina van Bitdefender Cyberpedia vindt u hier:

https://www.bitdefender.com/cyberpedia/.

8.3. Contactinformatie

Efficiënte communicatie is de sleutel tot succes. Sinds 2001 heeft BITDEFENDER een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners telkens te overtreffen. Aarzel daarom niet om rechtstreeks contact met ons op te nemen als u iets wilt vragen, via onze Bitdefender Support Center.

https://www.bitdefender.nl/consumer/support/

8.3.1. Lokale verdelers

De lokale BitDefender-verdelers zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak.

Om een Bitdefender-verdeler te vinden in uw land:

1. Ga naar https://www.bitdefender.com/partners/partner-locator.html.
2. Kies uw land en stad met de overeenkomstige opties.

WOORDENLIJST

Activeringscode

Is een unieke sleutel die u in de handel kunt kopen en die gebruikt wordt om een specifiek product of een dienst te activeren. Met een activeringscode kan een geldig abonnement voor een bepaalde periode en een bepaald aantal toestellen geactiveerd worden en kunt u ook gebruiken om het abonnement te verlengen, op voorwaarde dat het voor hetzelfde product of dezelfde dienst is.

ActiveX

ActiveX is een model voor het schrijven van programma's zodat andere programma's en het besturingssysteem ze kunnen oproepen. De ActiveX-technologie wordt gebruikt bij Microsoft Internet Explorer om interactieve Webpagina's te maken die eruitzien en zich gedragen als computerprogramma's in plaats van statische pagina's. Met ActiveX kunnen gebruikers vragen stellen of beantwoorden, drukknoppen gebruiken en op andere manieren interactief omgaan met de Webpagina. ActiveX-besturingselementen zijn vaak geschreven met de hulp van Visual Basic. ActiveX is berucht door een compleet gebrek aan beveiligingscontroles; computerbeveiligingsexperts raden het gebruik ervan via het internet sterk af.

Advanced persistent threat

Geavanceerde aanhoudende dreiging (Advanced Persistent Threat - APT) maakt misbruik van kwetsbare plekken in systemen om belangrijke informatie te stelen en aan de bron te leveren. Grote groepen, zoals organisaties, bedrijven of overheden zijn doelgroepen voor deze bedreiging. Het doel van een advanced persistent threat is heel lang onopgemerkt te blijven en belangrijke informatie in te kijken en te verzamelen, zonder de toestellen te beschadigen. De methode die gebruikt wordt om de bedreiging in het netwerk te brengen verloopt via een pdf-bestand of een Office-document dat er onschuldig uitziet, zoadat elke gebruiker de bestanden kan openen.

Adware

Adware wordt vaak gecombineerd met een hosttoepassing die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adware-toepassingen doorgaans

worden geïnstalleerd nadat de gebruiker een licentieovereenkomst die het doel van de toepassing vermeldt heeft geaccepteerd, wordt er geen inbreuk gepleegd. Pop-upadvertenties kunnen echter irritant worden en in sommige gevallen de systeemprestaties negatief beïnvloeden. De gegevens die door sommige van deze toepassingen worden verzameld, kunnen bovendien privacy-problemen veroorzaken voor gebruikers die niet volledig op de hoogte waren van de voorwaarden van de licentieovereenkomst.

Archive

Een schijf, tape, of map die bestanden bevat waarvan een back-up werd gemaakt.

Een bestand dat één of meer bestanden bevat in een gecomprimeerd formaat.

Backdoor

Een gat in de beveiliging van een systeem, dat opzettelijk werd achtergelaten door ontwikkelaars of beheerders. De motivatie voor dergelijke gaten is niet altijd boosaardig. Sommige besturingssystemen worden bijvoorbeeld geleverd met bevoegde accounts die bedoeld zijn voor gebruik door technici voor service ter plaatse of onderhoudsprogrammeurs van de leverancier.

Boot sector

Een sector aan het begin van elke schijf die de architectuur van de schijf identificeert (sectorgrootte, clustergrootte, enz.) Bij opstartschijven bevat de opstartsector ook een programma dat het besturingssysteem laadt.

Boot virus

Een bedreiging die de opstartsector van een vaste schijf of een diskette infecteert. Wanneer u probeert op te starten vanaf een diskette die geïnfecteerd is met een opstartsectorvirus, zal de bedreiging actief worden in het geheugen. Wanneer u vanaf dat ogenblik uw systeem opstart, zal de bedreigingen telkens in het geheugen geactiveerd zijn.

Botnet

Het woord "botnet" is samengesteld uit de woorden "robot" en "netwerk". Botnets zijn apparaten die met het internet verbonden zijn en met bedreigingen geïnfecteerd zijn en kunnen gebruikt worden om spammail te verzenden, data te stelen, kwetsbare apparaten van op afstand

te controleren of om spyware, ransomware en andere schadelijke bedreigingen te verspreiden. Het doel ervan is zoveel mogelijk apparaten te infecteren, bijvoorbeeld pc's, servers, mobiele of IoT-apparaten die eigendom zijn van grote bedrijven of sectoren.

Browser

De korte naam voor Webbrowser, een softwaretoepassing die wordt gebruikt op Webpagina's te zoeken en weer te geven. Populaire browsers omvatten Microsoft Internet Explorer, Mozilla Firefox en Google Chrome. Dit zijn grafische browsers. Dit betekent dat ze zowel grafische beelden als tekst kunnen weergeven. Bovendien kunnen de meeste moderne browsers ook multimedia-informatie voorstellen met geluid en video, hoewel voor sommige formaten plug-ins vereist zijn.

Brute Force-aanval

Aanval via raden van wachtwoord, gebruikt om in te breken in een computersysteem door mogelijke wachtwoordcombinaties in te geven, meestal te beginnen met het meest eenvoudig te raden wachtwoord.

Opdrachtregel

In een opdrachtregelinterface typt de gebruiker opdrachten in opdrachttaal rechtstreeks op het scherm in de ruimte die hiervoor wordt geboden.

Cookies

Binnen de Internetindustrie worden cookies beschreven als kleine programma's die informatie bevatten over individuele computers, die door adverteerders wordt geanalyseerd en gebruikt om uw on line interesse en smaak te volgen. De cookietechnologie wordt in dit kader nog steeds verder ontwikkeld met het doel reclameberichten rechtstreeks te richten op de interesses die u hebt meegedeeld. Dit is voor veel mensen een mes dat aan twee kanten snijdt. Aan de ene kant is het efficiënt en relevant aangezien u alleen reclames ontvangt voor zaken waarvoor u interesse hebt. Aan de andere kant betekent het ook dat elke plaats die u bezoekt en alles wat u aanklikt wordt "opgespoord" en "gevolgd". Het is dan ook te begrijpen dat er heel wat wordt gedebatteerd over privacy. Bovendien zijn veel mensen verontwaardigd omdat ze het gevoel hebben dat ze als een "SKU-nummer" worden beschouwd (u weet wel, de barcode op de verpakkingen die bij de kassa van het warenhuis wordt gescand). Hoewel dit standpunt misschien nogal extreem is, is het vaak een bijzonder nauwkeurige omschrijving.

Cyberpesten

Wanneer collega's of onbekenden met opzet onrechtmatige daden stellen tegenover kinderen, met de bedoeling om fysiek te kwetsen. Om emotionele schade te berokkenen, sturen de daders gemene berichten of onflatteuze foto's om hun slachtoffers af te zonderen van anderen of gefrustreerd te doen voelen.

Woordenboekaanval

Aanval via raden van wachtwoord, gebruikt om in te breken in een computersysteem door een combinatie van veel voorkomende woorden in te geven om zo mogelijke wachtwoorden te genereren. Dezelfde methode wordt gebruikt om decryptiesleutels van versleutelde berichten of documenten te raden. Woordenboekaanvallen slagen in hun opzet omdat veel mensen korte wachtwoorden gebruiken die uit slechts één woord bestaan en die makkelijk te raden zijn.

Schijfstation

Dit is een apparaat dat gegevens leest van en schrijft naar een schijf. Een harde-schijfstation leest en schrijft harde schijven. Een diskettestation opent diskettes. Schijfstations kunnen intern (binnen de behuizing van een computer) of extern zijn (in een afzonderlijke behuizing die op de computer wordt aangesloten).

Download

Om gegevens (meestal een volledig bestand) te kopiëren van een hoofdbron naar een randapparaat. De term wordt vaak gebruikt om het proces te beschrijven waarbij een bestand van een on line-service wordt gekopieerd naar de eigen computer. Downloaden kan ook verwijzen naar het kopiëren van een bestand van een netwerkbestandsserver naar een computer in het netwerk.

E-mail

Elektronische post. Een dienst die berichten naar computers verzendt via lokale of globale netwerken.

Gebeurtenissen

Een actie of gebeurtenis die door een programma wordt gedetecteerd. Gebeurtenissen kunnen gebruikersacties zijn, zoals het klikken met de muis of het indrukken van een toets, of systeemgebeurtenissen, zoals een tekort aan geheugen.

Exploits

Een manier om misbruik te maken van verschillende bugs of kwetsbaarheden in een computer (software of hardware). Zo kunnen hackers de controle over computers of over netwerken in handen krijgen.

Vals positief

Doet zich voor wanneer een scanner een bestand ten onrechte beschouwt als geïnfecteerd.

Bestandsextensie

Het gedeelte van een bestandsnaam achter de punt, waarmee het gegevenstype dat in het bestand is opgeslagen wordt aangeduid. Heel wat besturingssystemen, zoals Unix, VMS en MS-DOS, maken gebruik van bestandsextensies. Ze gebruiken doorgaans één tot drie letters (sommige betreurenswaardige oude besturingssystemen ondersteunen niet meer dan drie letters). Voorbeelden hiervan zijn "c" voor C-broncode, "ps" voor PostScript, "txt" voor tekst zonder opmaak.

Heuristisch

Een methode voor het identificeren van nieuwe bedreigingen op basis van regels. Deze scanmethode is niet gebaseerd op een specifieke informatie-database voor bedreigingen. Het voordeel van de heuristische scan is dat hij zich niet laat misleiden door een nieuwe variant van een bestaande bedreiging. Dit type kan echter af en toe een verdachte code rapporteren in normale programma's, zodat de zogenoemde "valse positieve" rapporten worden gegenereerd.

Honeypot

Een afleiding in uw computersysteem dat hackers aantrekt om te onderzoeken hoe ze te werk gaan en de afwijkende methodes die ze gebruiken om systeeminformatie te verzamelen, te identificeren. Bedrijven zijn steeds meer geïnteresseerd om honingpotten te implementeren en te gebruiken om hun algemene beveiligingsstatus te verbeteren.

IP

Internet Protocol - Een routeerbaar protocol in de TCP/OP-protocolreeks die verantwoordelijk is voor de IP-adressering, routing en de fragmentatie en defragmentatie van IP-pakketten.

Java applet

Een Java-programma dat is ontwikkeld om alleen op een webpagina te worden uitgevoerd. Om een applet op een webpagina te gebruiken, zou u de naam van het applet opgeven en de grootte (lengte en breedte in pixels) die het applet kan gebruiken. Wanneer de webpagina wordt geopend, downloadt de browser het applet van een server en voert hij het uit op de computer van de gebruiker (de client). Applets onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

Zelfs wanneer applets op de client worden uitgevoerd kunnen ze, bijvoorbeeld, geen gegevens lezen van of schrijven naar de computer van de client. Bovendien worden applets verder beperkt zodat ze alleen gegevens kunnen lezen van en schrijven naar hetzelfde domein waarvan ze worden bediend.

Keylogger

Een keylogger is een toepassing die alles wat u typt, logt. Keyloggers zijn in wezen niet kwaadaardig. Ze kunnen worden gebruikt voor rechtmatige doeleinden, zoals het bewaken van de activiteiten van werknemers of kinderen. Ze worden echter steeds meer gebruikt door cybercriminele voor boosaardige doeleinden (bijv. voor het verzamelen van persoonlijke gegevens, zoals aanmeldingsgegevens en nummer van de sociale zekerheid).

Macro virus

Een type computerbedreiging die is gecodeerd als een macro die in een document is ingesloten. Talrijke toepassingen, zoals Microsoft Word en Excel, ondersteunen krachtige macrotalen. Met deze toepassingen kan u een macro in een document insluiten, en die macro telkens laten uitvoeren wanneer het document wordt geopend.

Mail client

Een e-mailclient is een toepassing waarmee u e-mail kunt verzenden en ontvangen.

Geheugen

Interne opslaggebieden in de computer. De term geheugen staat voor gegevensopslag die in de vorm van chips wordt geleverd. Het woord opslag wordt gebruikt voor geheugen dat aanwezig is op tapes of schijven. Elke computer wordt geleverd met een bepaalde hoeveelheid fysiek geheugen, dat meestal het hoofdgeheugen of RAM wordt genoemd.

Niet-heuristisch

Deze scanmethode is gebaseerd op een specifieke informatie-database voor bedreigingen. Het voordeel van de niet-heuristische scan is dat deze zich niet laat misleiden door iets dat kan lijken op een bedreiging en geen vals alarm genereert.

Online predatoren

Personen die minderjarigen of adolescenten met opzet willen betrekken in gesprekken, om hen zo te betrekken in illegale seksuele activiteiten. Sociale netwerken zijn de ideale plaats waar kwetsbare kinderen gemakkelijk kunnen worden verleid om seksuele activiteiten uit te voeren, online of tijdens fysieke ontmoetingen.

Ingepakte programma's

Een bestand in een gecomprimeerd formaat. Talrijke besturingssystemen en toepassingen beschikken over opdrachten waarmee u bestanden kunt inpakken, zodat ze minder geheugen in beslag nemen. Veronderstel bijvoorbeeld dat u een tekstbestand hebt dat tien opeenvolgende spatietekens bevat. Normaal zou dit tien bytes opslagruimte vereisen.

Een programma dat bestanden inpakt kan echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval hebben de tien spaties slechts twee bytes nodig. Dit is slechts één inpaktechniek, maar er zijn er veel meer.

Pad

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische bestandssysteem van boven naar beneden.

De route tussen twee willekeurige punten, zoals het communicatiekanaal tussen twee computers.

Phishing

Het onder valse voorwendselen verzenden van een e-mail aan een gebruiker, waarbij de indruk wordt gewekt dat het bericht afkomstig is van een bestaande onderneming, in een poging de gebruiker persoonlijke gegevens te ontfutselen die zullen worden gebruikt voor identiteitsroof. In het e-mailbericht wordt de gebruiker doorverwezen naar een website waar persoonlijke gegevens kunnen worden bijgewerkt,

zoals wachtwoorden en creditcard-, sofi- en bankrekeningnummers, die reeds in het bezit zijn van de rechtmatige organisatie. De website is echter nep en alleen opgezet om de gebruikersgegevens te stelen.

Foton

Photon is een vernieuwende, niet opdringerige Bitdefender technologie, ontworpen om de invloed van uw beveiligingsoplossing op de prestaties te beperken. Door de activiteit van uw pc's op de achtergrond te bewaken, maakt het gebruikspatronen die helpen opstart- en scanprocessen te optimaliseren.

Polymorf virus

Een bedreiging die zijn vorm wijzigt bij elk bestand dat het infecteert. Aangezien ze geen consequent binair patroon hebben, zijn dergelijke bedreigingen moeilijk te identificeren.

Poort

Een interface op een computer waarop u een apparaat kan aansluiten. PC's hebben verschillende types poorten. Intern zijn er verschillende poorten voor het aansluiten van schijfstations, beeldschermen en toetsenborden. Extern beschikken PC's over poorten voor het aansluiten van modems, printers, muizen en andere randapparatuur.

Bij TCP/IP- en UDP-netwerken, zijn ze een eindpunt voor een logische verbinding. Het poortnummer duidt aan over welk type poort het gaat. Poort 80 wordt bijvoorbeeld gebruikt voor HTTP-verkeer.

Ransomware

Ransomware is kwaadaardige software waarmee criminelen proberen geld af te persen van gebruikers, door hun systemen ontoegankelijk te maken totdat er losgeld is betaald. Enkele van de vele varianten van ransomware voor persoonlijke computersystemen zijn CryptoLocker, CryptoWall en TeslaWall.

De infectie kan verspreid worden door spam-e-mail te openen, e-mailbijlagen te openen of toepassingen te installeren zonder dat de gebruiker weet wat er op zijn systeem gaande is. Dagelijkse gebruikers en bedrijven vormen een doelwit voor ransomwarehackers.

Rapportbestand

Een bestand dat de acties weergeeft die zich hebben voorgedaan. BitDefender houdt een rapportbestand bij met het gescande pad,

het aantal gescande mappen, archieven en bestanden, en het aantal gevonden geïnfecteerde en verdachte bestanden.

Rootkit

Een rootkit is een verzameling softwareprogramma's die op beheerdersniveau toegang biedt tot een systeem. Deze term werd voor het eerst gebruikt voor Unix-besturingssystemen en verwees naar opnieuw gecompileerde hulpprogramma's die beheerdersrechten gaven aan indringers, zodat ze hun aanwezigheid konden verbergen en onzichtbaar bleven voor de echte systeembeheerders.

De belangrijkste functie van rootkits is het verbergen van processen, bestanden, logins en logbestanden. Rootkits die de hiervoor benodigde software bevatten, kunnen ook gegevens onderscheppen van terminals, netwerkverbindingen of randapparaten.

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om bedreigingen of de aanwezigheid van een indringer op het systeem te verbergen. In combinatie met bedreigingen, vormen rootkits een ernstige bedreiging voor de integriteit en beveiliging van een systeem. Ze kunnen het verkeer controleren, achterpoortjes in het systeem maken, bestanden en logboeken wijzigen en detectie vermijden.

Script

Script, een andere term voor een macro of batchbestand, is een lijst opdrachten die kunnen worden uitgevoerd zonder tussenkomst van de gebruiker.

Spam

Elektronische junkmail of berichten van junknieuwsgroepen. Algemeen bekend als ongewenste e-mail.

Spyware

Elke software die heimelijk gebruikersgegevens verzamelt via de internetverbinding van de gebruikers zonder dat hij/zij zich hiervan bewust is, doorgaans voor reclamedoeleinden. Spywaretoepassingen worden doorgaans gebundeld als een verborgen onderdeel van freeware- of sharewareprogramma's die kunnen worden gedownload van het internet. We moeten echter wel vermelden dat de meeste shareware- en freewaretoepassingen geen spyware bevatten. Zodra de spyware is

geïnstalleerd, worden de activiteiten van de gebruiker op het internet gevolgd en wordt deze informatie op de achtergrond naar iemand anders doorgestuurd. Spyware kan ook informatie verzamelen over e-mailadressen en zelfs wachtwoorden en creditcardnummers.

Spyware is vergelijkbaar met een Trojaans paard omdat gebruikers ook in dat geval het product onbewust installeren wanneer ze een ander programma installeren. Een veel voorkomende manier waarbij men het slachtoffer wordt van spyware is bepaalde P2P-programma's voor bestandsuitwisseling te downloaden.

Naast het feit dat deze methode onethisch is en een inbreuk op de privacy van de gebruiker betekent, steelt spyware van de gebruiker door de geheugenbronnen van de computer te gebruiken en bandbreedte te verbruiken wanneer de informatie naar de thuisbasis van de spyware wordt verzonden via de internetverbinding van de gebruiker. Aangezien spyware geheugen- en systeemgeheugen gebruikt, kunnen de toepassingen die op de achtergrond worden uitgevoerd leiden tot systeemfouten of een algemene systeeminstabiliteit.

Startup items

Elk bestand in deze map wordt geopend wanneer de computer wordt gestart. Een opstartitem kan bijvoorbeeld een opstartscherm zijn, een geluidsbestand dat moet worden afgespeeld wanneer de computer voor de eerste maal opstart, een herinneringsagenda of apps. In normale omstandigheden wordt een alias van een bestand in deze map geplaatst, en niet het bestand zelf.

Abonnement

Koopovereenkomst die u het recht heeft om een specifiek(e) product of dienst op een specifiek aantal toestellen en voor een bepaalde tijd te gebruiken. Een vervallen abonnement kan automatisch worden verlengd met gebruik van de informatie van de gebruiker tijdens de eerste aankoop.

Systeemvak

Het systeemvak, dat met Windows 95 werd ingevoerd, bevindt zich in de taakbalk van Windows (doorgaans onderaan naast de klok) en bevat miniatuurpictogrammen die systeemfuncties zoals fax, printer, modem, volume en meer, gemakkelijk toegankelijk maken. Dubbelklik of klik met de rechtermuisknop op een pictogram om de details en de besturingselementen te bekijken en te openen.

TCP/IP

Transmission Control Protocol/Internet Protocol - Een reeks netwerkprotocollen, wijdverspreid gebruikt op het internet, die communicatie bieden tussen onderling verbonden computernetwerken met verschillende hardware-architecturen en diverse besturingssystemen. TCP/IP bevat standaarden voor de manier waarop computers communiceren en regels voor het aansluiten van netwerken en het routeren van het verkeer.

Dreiging

Een programma of een deel van een code die op uw computer wordt geladen zonder uw medeweten en tegen uw wil wordt uitgevoerd. De meeste bedreigingen kunnen zichzelf ook dupliceren. Alle computerbedreigingen zijn door de mens gemaakt. Een eenvoudige bedreiging die zichzelf steeds opnieuw kan dupliceren is relatief eenvoudig te maken. Zelfs een dergelijke eenvoudige bedreiging is gevaarlijk aangezien het snel al het beschikbare geheugen zal opgebruiken en het systeem zal blokkeren. Een nog gevaarlijker type is een bedreiging die in staat is zichzelf te verzenden via netwerken en beveiligingssystemen te omzeilen.

informatie-updates van dreigingen

Het binaire patroon van een bedreiging, gebruikt door de beveiligingsoplossing om de bedreiging te detecteren en te verwijderen.

Trojaans paard

Een destructief programma dat zich voordoet als een goedaardige toepassing. In tegenstelling tot kwaadaardige softwareprogramma's en wormen, vermenigvuldigen Trojaanse paarden zich niet, maar ze kunnen even vernietigend zijn. Een van de meest verraderlijke bedreigingstypes van de Trojaanse paarden is een programma dat beweert dat het uw computer kan bevrijden van bedreigingen, maar dat in werkelijkheid bedreigingen op uw computer installeert.

De naam komt uit een verhaal uit de Ilias van Homerus. De Grieken schonken hun vijanden, de Trojanen, een reusachtig houten paard, zogenaamd als vredesgebaar. Maar nadat de Trojanen het paard binnen de stadsmuren hadden gesleept, kwamen de Griekse soldaten uit de holle romp van het paard tevoorschijn en openden ze de poorten van de stad, zodat hun landgenoten Troje konden binnendringen en veroveren.

Update

Een nieuwe versie van een software- of hardwareproduct, dat werd ontwikkeld om een oudere versie van hetzelfde product te vervangen. Daarnaast zullen de installatieroutines voor updates vaak controleren of er reeds een oudere versie van het product op uw computer is geïnstalleerd. Is dat niet het geval, dan kunt u de update niet installeren.

Bitdefender heeft zijn eigen updatefunctie waarmee u handmatig kunt controleren op updates of die het product automatisch kan updaten.

Virtueel privénetwerk (VPN)

Dit is een technologie die een tijdelijke en versleutelde rechtstreekse verbinding met een zeker netwerk over een minder beveiligd netwerk mogelijk maakt. Op die manier is het verzenden en ontvangen van data veilig en versleuteld, zodat ze moeilijk te vangen is door spionnen. Een bewijs van veiligheid is de authentificatie, die enkel mogelijk is via een gebruikersnaam en wachtwoord.

Worm

Een programma dat zich verspreidt via een netwerk en zichzelf ondertussen reproduceert. Dit type kan zich niet vasthechten aan andere programma's.