GUIDA DELL'UTENTE

Bitdefender CONSUMER SOLUTIONS

Ultimate Small Business Security

Bitdefender Ultimate Small Business Security

Guida dell'utente

Publication date 05/31/2024

Avviso legale

Bitdefender

Indice

INFORMAZIONI SU QUESTA GUIDA

Scopo e pubblico previsto

Bitdefender La massima sicurezza per le piccole imprese è un pacchetto di abbonamento multi-abbonamento su misura per soddisfare le esigenze di sicurezza informatica delle piccole imprese. Con un set completo di funzionalità, onboarding dedicato e strumenti di gestione intuitivi, i proprietari di piccole imprese possono proteggere le proprie risorse digitali senza competenze IT o di sicurezza informatica.

Il piano offre una protezione completa appositamente progettata per le piccole imprese, tra cui:

- **Protezione del dispositivo multipiattaforma:** Proteggi tutti i tuoi dispositivi, dai computer ai telefoni cellulari e ai server.
- **Gestione semplice:** Mantieni la sicurezza del tuo team e delle operazioni aziendali senza sforzo.
- **Tutela del patrimonio e della reputazione aziendale:** Garantisci il massimo livello di protezione alla tua azienda prevenendo l'associazione ad attività fraudolente.
- **Configurazione semplificata:** Il processo di onboarding semplifica la configurazione per gli utenti non tecnici, garantendo una configurazione fluida e sicura.

Come usare questa guida

Questa guida è organizzata attorno ai quattro prodotti inclusi in Bitdefender Total Security:

- Sicurezza totale per PC (pagina 9)
  Scopri come utilizzare il prodotto su PC e laptop basati su Windows.
- Antivirus per Mac (pagina 150)
  Scopri come utilizzare il prodotto sui tuoi Mac.
- Sicurezza mobile per Android (pagina 183)
  Scopri come utilizzare il prodotto su smartphone e tablet basati su Android.
- Sicurezza mobile per iOS (pagina 217)

Scopri come utilizzare il prodotto su smartphone e tablet basati su iOS.

- VPN (pagina 232)
  Scopri come nascondere la tua identità online utilizzando Bitdefender VPN su qualsiasi tuo dispositivo.
- Gestore delle password (pagina 254)
  Tieni traccia e archivia in modo sicuro tutte le tue password e credenziali con Password Manager.
- Protezione dell'identità digitale (pagina 279)
  Scopri come gestire correttamente la protezione della tua identità digitale.
- Ottenere aiuto (pagina 287)
  Scopri dove cercare aiuto se si presenta qualcosa di inaspettato.

Convenzioni usate in questo manuale

Convenzioni tipografiche

Nel manuale vengono usati diversi stili di testo per migliorare la leggibilità. L'aspetto e il significato sono illustrati nella tabella sottostante.

Aspetto	Descrizione
sample syntax	Gli esempi di sintassi vengono stampati con monospaced caratteri.
https://www.bitdefender.com	I link URL indirizzano a una qualche ubicazione esterna, su server http o ftp.
documentation@bitdefender.com	Gli indirizzi e-mail vengono inseriti nel testo come informazioni di contatto.
A proposito di questa guida (pagina 1)	Questo è un link interno, verso una qualche ubicazione nel documento.
filename	File e directory vengono stampati utilizzando monospaced font.
opzione	Tutte le opzioni del prodotto vengono stampate utilizzando **grassetto** caratteri.
parola chiave	Le parole chiave o le frasi importanti vengono evidenziate utilizzando **grassetto** caratteri.

Avvertenze

Le avvertenze appaiono sotto forma di note di testo, segnalate graficamente, portando alla tua attenzione ulteriori informazioni relative al paragrafo attuale.

Nota

Le note sono solo piccole osservazioni. Anche se si possono omettere, le note potrebbe fornire informazioni preziose, come una determinata caratteristica o un link verso eventuali temi collegati.

Importante

Richiede la tua attenzione e non è consigliato ignorarla. Solitamente, fornisce informazioni non critiche ma importanti.

Avvertimento

Si tratta di un'informazione critica che dovresti trattare con maggiore cautela. Se segui le istruzioni, non accadrà nulla di male. Dovresti leggerla e comprenderla, perché descrive qualcosa di estremamente rischioso.

Richiesta di commenti

Ti invitiamo ad aiutarci a migliorare il presente manuale. Abbiamo provato e verificato tutte le informazioni con la massima attenzione. Ti preghiamo di scriverci per indicarci eventuali errori che dovessi riscontrare nel manuale o suggerirci come poterlo migliorare, per aiutarci a fornirti la migliore documentazione possibile.

Segnalacelo inviando una mail a documentation@bitdefender.com. Scrivi tutte le tue e-mail relative alla documentazione in inglese in modo che possiamo elaborarle in modo efficiente.

1. CONFIGURARE L'ABBONAMENTO

Il processo di configurazione iniziale dell'abbonamento a **Bitdefender Ultimate Small Business Security** è stato appositamente progettato per essere facile e veloce, senza la necessità di specifiche conoscenze informatiche o di cybersecurity. È necessario:

1. **Attivare Bitdefender Ultimate Small Business Security:**
   È possibile farlo seguendo le istruzioni indicate nell'e-mail di conferma ricevuta al momento dell'acquisto del prodotto.
2. **Configurare il proprio account aziendale:**
   Al momento dell'attivazione, sarà chiesto di inserire il nome della propria azienda. La richiesta è al solo scopo di identificazione e tale nome sarà visualizzato in vari punti dell'interfaccia. Si può comunque usare il proprio nome preferito, poiché non è richiesta alcuna convalida al riguardo.
3. **Scegliere il proprio ruolo nell'organizzazione:**
   - **Titolare dell'azienda:** se si è titolari dell'attività e si gestiscono gli acquisti e la configurazione, scegliere questa opzione.
   - **Amministratore della sicurezza:** se si è responsabili della sicurezza all'interno dell'azienda, scegliere questa opzione.

     Nota
     L'Amministratore della sicurezza ha autorizzazioni simili al titolare dell'azienda, ad eccezione delle capacità di acquisto.
4. **Invitare i membri del team a configurare i propri account:**
   Una volta terminata la scelta del proprio nome e ruolo, comparirà una panoramica del proprio abbonamento a Bitdefender. Da qui, è possibile scegliere di condividere il piano con altri membri del team o continuare la configurazione, seguendo le procedure di installazione appropriate per il dispositivo su cui si sta cercando di installare Bitdefender, ognuna descritta nel capitolo corrispondente all'interno di questo documento.

> **Importante**
> Si consiglia di iniziare invitando i propri dipendenti prima di passare alle procedure di installazione.

5. **Selezionare i ruoli dei membri del team:**
   Occorre selezionare i ruoli dei dipendenti che si stanno invitando a partecipare al proprio piano di sicurezza aziendale. È possibile invitarli come:
   - **Amministratore della sicurezza:** questo ruolo comporta la gestione di membri, dispositivi e operazioni di sicurezza, ed è destinato a coloro che, tra i dipendenti, hanno un determinato livello di competenze informatiche, con il compito di gestire e monitorare gli aspetti della cybersecurity dell'azienda.
   - **Dipendente:** i dipendenti hanno visibilità e capacità di gestione limitate. Gli servirà un account di Bitdefender Central per proteggere i propri dispositivi, mentre chi avrà il ruolo di **Amministratore della sicurezza** potrà supervisionare la loro protezione e gestire i loro dispositivi da remoto.

6. **Mandare gli inviti ai membri del team:**
   Inserire gli indirizzi e-mail dei dipendenti con cui si vuole condividere il piano di Bitdefender. È possibile mandare più inviti alla volta.

   > **Nota**
   > I membri invitati, indipendentemente dal ruolo, riceveranno un invito via e-mail. Devono cliccare sul pulsante **Attiva in Bitdefender Central** e accettare l'invito utilizzando lo stesso indirizzo e-mail con cui sono stati invitati.

7. **Aggiungere informazioni aziendali sensibili da monitorare:**
   Ora si dovrà impostare il monitoraggio delle risorse aziendali come fase finale del processo.

   > **Nota**
   > **Business Assets Exposure** è un servizio disponibile solo per i ruoli di amministratore. (**amministratore della sicurezza** e **titolare dell'azienda**)

   Questa funzionalità controlla l'esposizione dei dati a livello aziendale per proteggere la reputazione dell'azienda e prevenire potenziali attacchi mirati.

- Dal menu a sinistra del proprio account di Bitdefender Central, andare alla sezione **Attività aziendali**.
- Cliccare sul pulsante **Vai alla configurazione** nel pannello **Business Assets Exposure**.
- Aggiungere le informazioni aziendali richieste:
  - Indirizzo e-mail aziendale
  - Carta di credito aziendale
  - Account di social media
- Dopo aver completato tutte le azioni suggerite, cliccare sul pulsante **Segna come fatto** per confermare l'esito e tenere traccia dei propri progressi.

Una volta completati questi passaggi, è possibile iniziare a configurare **Bitdefender Ultimate Small Business Security** per la propria attività:

- Installazione sui dispositivi Windows: Installazione (pagina 9)
- Installazione sui dispositivi macOS: Installazione di Bitdefender Antivirus for Mac (pagina 151)
- Installazione sui dispositivi mobili Android: Installare Bitdefender Mobile Security (pagina 183)
- Installazione sui dispositivi mobili iOS: Installare Bitdefender Mobile Security for iOS (pagina 218)
- Installazione di Bitdefender VPN sui propri dispositivi: Installazione di Bitdefender Password Manager (pagina 234)
- Configurazione di Password Manager: Installazione (pagina 256)
- Configurazione di Digital Identity Protection: Configurare Digital Identity Protection (pagina 280)

Il seguito di questo processo segna l'avvenuta attivazione e configurazione di **Bitdefender Ultimate Small Business Security** per la propria azienda.

2. ESPOSIZIONE DELLE ATTIVITÀ AZIENDALI

Business Assets Exposure è un servizio di Bitdefender Ultimate Small Business Security gestito dagli amministratori (titolare dell'azienda e amministratore della sicurezza) che fornisce visibilità sull'esposizione delle informazioni aziendali chiave nelle violazioni dei dati. Business Assets Exposure monitora 3 componenti per rilevare le violazioni dei dati:

- Indirizzo e-mail aziendale
- Carta di credito aziendale
- Account di social media

Perché Business Assets Exposure è importante:

- **Protezione della reputazione:** previene danni alla reputazione della propria azienda affrontando tempestivamente le violazioni.
- **Sicurezza dei dipendenti:** protegge i dipendenti da phishing e altri attacchi di social engineering monitorando e gestendo i dati esposti.
- **Prevenzione degli attacchi mirati:** limita il potenziale di attacchi mirati garantendo la sicurezza delle informazioni sensibili.

Una volta impostati i dettagli di **Business Assets Exposure** come parte del **Configurare l'abbonamento (pagina 4)**processo, è possibile **esaminare i risultati e agire in base ai suggerimenti:**

Il sistema informerà l'utente di eventuali violazioni che coinvolgono queste risorse monitorate, tra cui i servizi violati e le tipologie di informazioni esposte (ad esempio, indirizzi e-mail, nomi utente, password e posizioni geografiche). Non vengono mostrati dettagli specifici, ma solo le categorie dei dati esposti.

Per ogni componente monitorato (e-mail aziendale, carta di credito aziendale, account dei social media), occorre applicare i suggerimenti di sicurezza forniti. Le azioni consigliate possono includere:

- Chiedere ai dipendenti di monitorare i propri indirizzi e-mail aziendali con Bitdefender Digital Identity Protection.
- Modificare le password in siti web violati e consigliare ai dipendenti di utilizzare Bitdefender Password Manager.

- Assicurarsi che i dipendenti installino le soluzioni di sicurezza Bitdefender su tutti i dispositivi per prevenire eventuali attacchi informatici.
- Consigliare ai dipendenti di usare Scam Copilot per eventuali consigli su potenziali truffe e pratiche di prevenzione delle truffe.
- Monitorare le transazioni e cambiare il numero di carta di credito con l'aiuto dell'istituto bancario che l'ha emessa.
- Attivare l'autenticazione a due fattori sulle piattaforme social media violate per impedire accessi non autorizzati.

> **Nota**
> Dopo aver eseguito le azioni consigliate, è necessario cliccare sul pulsante **Segna come fatto** per confermare il completamento e tenere traccia dei propri progressi.

Seguendo questi passaggi, gli amministratori possono monitorare e proteggere facilmente la propria azienda dai rischi dell'esposizione dei dati utilizzando il servizio **Business Assets Exposure**.

3. SICUREZZA TOTALE PER PC

3.1. Installazione

3.1.1. Prepararsi all'installazione

Prima di Bitdefender Ultimate Small Business Securityinstallare , completa questi passaggi preliminari per assicurarti che l'installazione funzioni senza problemi:

- Assicurati che il dispositivo su cui desideri installare Bitdefender soddisfi i requisiti di sistema. Se il dispositivo non soddisfa tutti i requisiti di sistema, Bitdefender non sarà installato, o, nel caso venisse installato, non funzionerà correttamente e causerà rallentamenti e instabilità. Per un elenco completo dei requisiti di sistema, consultare la sezione Requisiti di sistema (pagina 9).
- Accedi al dispositivo utilizzando un account Amministratore.
- Rimuovi qualsiasi altro programma simile dal dispositivo. Se dovesse rilevarne uno durante l'installazione di Bitdefender, ti sarà chiesto di disinstallarlo. L'esecuzione simultanea di due programmi di sicurezza può influenzarne il funzionamento e causare problemi seri al sistema. Durante l'installazione Windows Defender sarà disattivato.
- Disabilita o rimuovi qualsiasi programma firewall che possa essere in esecuzione sul dispositivo. L'esecuzione simultanea di due programmi firewall può influenzarne il funzionamento e causare problemi seri al sistema. Durante l'installazione il firewall di Windows sarà disattivato.
- Assicurati che il dispositivo sia connesso a Internet durante l'installazione, anche se l'hai avviata da un CD/DVD. Se sono disponibili versioni più recenti dei file dell'applicazione inclusi nel pacchetto d'installazione, Bitdefender può scaricarli e installarli.

3.1.2. Requisiti di sistema

Puoi installare Bitdefender Ultimate Small Business Security solo su dispositivi con i seguenti sistemi operativi:

- Windows 7 con Service Pack 1
- Windows 8.1

- Windows 10
- 2,5 GB di spazio disponibile su disco rigido (almeno 800 MB sull'unità di sistema)
- 2 GB di memoria (RAM)

Puoi anche installare ed eseguire Bitdefender Ultimate Small Business Security su quanto segue:

- Windows Server 2016 (con esperienza desktop):
  - Standard/RTM
  - Elementi essenziali
  - Banca dati
- Windows Server 2019 (con esperienza desktop):
  - Standard/RTM
  - Essenziale
  - Banca dati
- Windows Server 2022 (con esperienza desktop):
  - Standard/RTM
  - Banca dati

Importante
Le prestazioni del sistema potrebbero essere influenzate su dispositivi dotati di CPU di vecchia generazione.

Nota

Per scoprire quale versione di Windows è attiva sul dispositivo e maggiori informazioni sull'hardware:

- In **Windows 7**, clicca con il pulsante destro del mouse su **Computer** nel desktop e seleziona **Proprietà** nel menu.
- In **Windows 8**, dal menu Start di Windows, localizza l'opzione **Computer** (puoi anche digitare direttamente "Computer" nella finestra di ricerca del menu Start), e poi clicca sulla sua icona con il pulsante destro. In **Windows 8.1**, localizza **Questo PC**.
  Seleziona **Proprietà** nel menu inferiore. Individua la sezione **Sistema** per trovare maggiori informazioni sul tuo sistema.
- In **Windows 10**, digita **Sistema** nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona. Nella sezione **Sistema** puoi trovare maggiori informazioni sul tuo tipo di sistema.

3.1.3. Requisiti software

Per poter usare Bitdefender e tutte le sue funzioni, il tuo dispositivo deve soddisfare i seguenti requisiti software:

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

3.1.4. Installare il tuo prodotto Bitdefender

Puoi installare Bitdefender dal disco di installazione, oppure utilizzare il programma d'installazione web scaricato sul tuo dispositivo da Bitdefender Central.

Se il tuo acquisto copre più di un dispositivo, ripeti l'installazione e attiva il prodotto con lo stesso account su ogni dispositivo. L'account che devi utilizzare è quello che include il tuo abbonamento attivo a Bitdefender.

Installare da Bitdefender Central

Da Bitdefender Central puoi scaricare il kit d'installazione corrispondente all'abbonamento acquistato. Una volta completato il processo

d'installazione, Bitdefender Ultimate Small Business Security viene attivato.

Per scaricare Bitdefender Ultimate Small Business Security da Bitdefender Central:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **I miei dispositivi** e clicca su **INSTALLA PROTEZIONE**.
3. Seleziona una delle due opzioni disponibili:
   - **Proteggi questo dispositivo**
     a. Seleziona questa opzione e poi il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, clicca sul pulsante corrispondente.
     b. Salva il file di installazione.
   - **Proteggi altri dispositivi**
     a. Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.
     b. Premi **INVIA LINK DI DOWNLOAD**.
     c. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA EMAIL**.
     Nota che il link di download generato è valido solo per le prossime 24 ore. Se il link dovesse scadere, dovrai generarne uno nuovo seguendo gli stessi passaggi.
     d. Sul dispositivo su cui vuoi installare il tuo prodotto Bitdefender, controlla l'account e-mail che hai digitato e poi clicca sul pulsante di download corrispondente.
4. Attendi il completamento del download ed esegui il programma d'installazione.

Convalidare l'installazione

Per prima cosa, Bitdefender controlla il tuo sistema per convalidare l'installazione.

Se il tuo sistema non soddisfa i requisiti di sistema per installare Bitdefender, ti saranno comunicate le caratteristiche da migliorare prima di poter procedere.

Se viene rilevata una soluzione di sicurezza incompatibile o una versione precedente di Bitdefender, ti sarà chiesto di rimuoverla dal sistema. Segui le istruzioni per rimuovere il programma dal sistema, per evitare eventuali problemi in seguito. Potrebbe essere necessario riavviare il dispositivo per completare la rimozione delle soluzioni di sicurezza rilevate.

Il pacchetto d'installazione di Bitdefender Total Security viene aggiornato costantemente.

> **Nota**
> Scaricare i file d'installazione può richiedere un po' di tempo, soprattutto con le connessioni a Internet più lente.

Una volta confermata l'installazione, compare la procedura guidata di configurazione. Segui i passaggi indicati per installare Bitdefender Ultimate Small Business Security.

Fase 1 - Installazione di Bitdefender

Prima di procedere con l'installazione, devi accettare l'Accordo di abbonamento. Prenditi qualche istante per leggere l'Accordo di abbonamento in quanto contiene i termini e le condizioni con cui è possibile Bitdefender Ultimate Small Business Securityutilizzare .

Se non accetti tali termini, chiudi la finestra. Il processo di installazione sarà abbandonato e uscirai dalla configurazione.

In questa fase possono essere eseguite due attività aggiuntive:

- Mantieni attivata l'opzione **Invia rapporti sul prodotto**. Permettendo questa opzione, i rapporti contenenti informazioni su come il prodotto viene utilizzato sono inviati ai server Bitdefender. Queste informazioni sono essenziali per migliorare il prodotto e possono aiutarci a offrire una migliore esperienza in futuro. I rapporti non conterranno dati confidenziali, come nome o indirizzo IP, e non saranno utilizzati per scopi commerciali.
- Seleziona la lingua con cui desideri installare il prodotto.

Clicca su **INSTALLA** per lanciare la fase di installazione del tuo prodotto Bitdefender.

Fase 2 - Installazione in corso

Attendi il completamento dell'installazione. Nel frattempo vengono mostrate alcune informazioni dettagliate sui progressi.

Fase 3 - Fine dell'installazione

Il tuo prodotto Bitdefender è stato installato con successo.

Viene mostrato un resoconto dell'installazione. Se durante l'installazione viene rilevata e rimossa una minaccia attiva, è necessario riavviare il sistema.

Fase 4 - Analisi del dispositivo

Ora ti sarà chiesto se desideri eseguire un'analisi del tuo dispositivo, per assicurarti che sia sicuro. Durante questa fase, Bitdefender esaminerà le aree critiche del sistema. Clicca su **Avvia analisi dispositivo** per avviarla.

Puoi nascondere l'interfaccia della scansione cliccando su **Esegui scansione in background**. Poi, scegli se desideri ricevere informazioni oppure no sul termine della scansione.

Una volta completata la scansione, clicca su **Apri interfaccia di Bitdefender**.

> **Nota**
> In alternativa, se non vuoi eseguire la scansione, puoi semplicemente cliccare su **Salta**.

Fase 5 - Come iniziare

Nella finestra **Come iniziare**, puoi trovare maggiori informazioni sul tuo abbonamento attivo.

Clicca su **TERMINA** per accedere all'interfaccia di Bitdefender Ultimate Small Business Security.

Installa dal disco di installazione

Per installare Bitdefender dal disco di installazione, inserisci il disco nel lettore.

Dopo alcuni istanti, dovrebbe comparire una schermata d'installazione. Segui le indicazioni per avviare l'installazione.

Se la schermata d'installazione non compare, utilizza Esplora risorse per sfogliare la cartella principale del disco e clicca due volte sul file autorun.exe.

Se la tua connessione a Internet è lenta o il tuo sistema non è proprio connesso a Internet, clicca sul pulsante **Installa da CD/DVD**. In questo caso, sarà installato il prodotto Bitdefender disponibile sul disco e successivamente sarà scaricata una nuova versione dai server di Bitdefender tramite un aggiornamento.

Convalidare l'installazione

Per prima cosa, Bitdefender controlla il tuo sistema per convalidare l'installazione.

Se il tuo sistema non soddisfa i requisiti di sistema per installare Bitdefender, ti saranno comunicate le caratteristiche da migliorare prima di poter procedere.

Se viene rilevata una soluzione di sicurezza incompatibile o una versione precedente di Bitdefender, ti sarà chiesto di rimuoverla dal sistema. Segui le istruzioni per rimuovere il programma dal sistema, per evitare eventuali problemi in seguito. Potrebbe essere necessario riavviare il dispositivo per completare la rimozione delle soluzioni di sicurezza rilevate.

Il pacchetto d'installazione di Bitdefender Total Security viene aggiornato costantemente.

> **Nota**
> Scaricare i file d'installazione può richiedere un po' di tempo, soprattutto con le connessioni a Internet più lente.

Una volta confermata l'installazione, compare la procedura guidata di configurazione. Segui i passaggi indicati per installare Bitdefender Ultimate Small Business Security.

Fase 1 - Installazione di Bitdefender

Prima di procedere con l'installazione, è necessario accettare il contratto di abbonamento. Si prega di dedicare un po' di tempo alla lettura dell'Accordo di abbonamento in quanto contiene i termini e le condizioni in base ai quali è possibile utilizzare Bitdefender Ultimate Small Business Security.

Se non accetti questi termini, chiudi la finestra. Il processo di installazione verrà abbandonato e uscirai dalla configurazione.

In questa fase è possibile eseguire due attività aggiuntive:

- Mantieni il **Invia rapporti sui prodotti** opzione abilitata. Abilitando questa opzione, i rapporti contenenti informazioni su come utilizzi il prodotto vengono inviati ai server di Bitdefender. Queste informazioni sono essenziali per migliorare il prodotto e possono aiutarci a fornire una migliore esperienza in futuro. Tieni presente che questi rapporti non contengono dati riservati, come il tuo nome o indirizzo IP, e che non verranno utilizzati per scopi commerciali.
- Seleziona la lingua in cui desideri installare il prodotto.

Clic **INSTALLARE** per avviare il processo di installazione del tuo prodotto Bitdefender.

Passaggio 2: installazione in corso

Attendere il completamento dell'installazione. Vengono visualizzate informazioni dettagliate sullo stato di avanzamento.

Passaggio 3: installazione completata

Viene visualizzato un riepilogo dell'installazione. Se durante l'installazione è stata rilevata e rimossa una minaccia attiva, potrebbe essere necessario riavviare il sistema.

Passaggio 4: analisi del dispositivo

Ora ti verrà chiesto se desideri eseguire un'analisi del tuo dispositivo, per assicurarti che sia sicuro. Durante questa fase, Bitdefender analizzerà le aree critiche del sistema. Clic **Avvia l'analisi del dispositivo** per avviarlo.

È possibile nascondere l'interfaccia di scansione facendo clic su **Esegui la scansione in background**. Successivamente, scegli se vuoi essere informato o meno al termine della scansione.

Una volta completata la scansione, clicca su **Continua con Crea account**.

> **Nota**
> In alternativa, se non desideri eseguire la scansione, puoi semplicemente fare clic su **Saltare**.

Fase 5 - Account di Bitdefender

Dopo aver completato la configurazione iniziale, comparirà la finestra Bitdefender Account. Per attivare il prodotto e utilizzare le sue funzioni online, è necessario avere un account Bitdefender. Per maggiori informazioni, fai riferimento a .

Procedi in base alla tua situazione.

- **Voglio creare un account Bitdefender**

  1. Digita le informazioni richieste nei campi corrispondenti. I dati forniti resteranno riservati. La password deve essere lunga almeno 8 caratteri, includendo almeno un numero o un simbolo, una lettera minuscola e una maiuscola.
  2. Prima di procedere ulteriormente devi accettare i Termini di utilizzo. Accedi ai Termini di utilizzo e leggili attentamente, in quanto contengono i termini e le condizioni con cui puoi utilizzare Bitdefender.
     Inoltre, potrai accedere e leggere l'Informativa sulla privacy.
  3. Clicca su **CREA ACCOUNT**.

  > **Nota**
  > Una volta creato l'account, puoi usare l'indirizzo email e la password forniti per accedere al tuo account su https://central.bitdefender.com, o nella app Bitdefender Central, fatto salvo che sia stata installata su uno dei tuoi dispositivi Android o iOS. Per installare la app Bitdefender Central su Android, devi accedere a Google Play, cercare Bitdefender Central e poi toccare l'opzione corrispondente di installazione. Per installare la app Bitdefender Central su iOS, devi accedere a App Store, cercare Bitdefender Central e poi toccare l'opzione corrispondente di installazione.

- **Ho già un account Bitdefender**

  1. Clicca su **Accedi**.
  2. Inserisci l'indirizzo e-mail nel campo corrispondente e clicca su **AVANTI**.
  3. Inserisci la tua password e clicca su **ACCEDI**.
     Se hai dimenticato la password per il tuo account o vuoi semplicemente modificare quella già impostata:

a. Clicca su **Hai dimenticato la password?**.

b. Inserisci il tuo indirizzo e-mail e clicca su **AVANTI**.

c. Controlla la tua casella di posta, inserisci il codice di sicurezza che hai ricevuto e clicca su **AVANTI**.
In alternativa, puoi cliccare su **Cambia password** nella e-mail che ti abbiamo inviato.

d. Digita la nuova password che vuoi impostare e inseriscila nuovamente. Clicca su **SALVA**.

> **Nota**
> Se hai già un account di Bitdefender Central, puoi usarlo per accedere al tuo account Bitdefender. Se hai dimenticato la password, devi prima andare su https://central.bitdefender.com per modificarla. Poi, usa le credenziali aggiornate per accedere al tuo account Bitdefender.

- **Voglio accedere usando il mio account Microsoft, Facebook o Google**
  Per accedere con il tuo account Microsoft, Facebook o Google:

  1. Seleziona il servizio che vuoi utilizzare. Sarai reindirizzato alla pagina di accesso del servizio.
  2. Segui le istruzioni fornite dal servizio selezionato per collegare il tuo account a Bitdefender.

> **Nota**
> Bitdefender non accede ad alcuna informazione confidenziale, come la password dell'account con cui accedi o le informazioni personali dei tuoi amici e contatti.

Fase 6 - Attiva il prodotto

> **Nota**
> Questa fase compare se hai selezionato di creare un nuovo account Bitdefender durante il passaggio precedente o se hai eseguito l'accesso utilizzando un account con un abbonamento scaduto.

Per completare l'attivazione del tuo prodotto è necessaria una connessione a Internet attiva.

Procedi secondo la tua situazione:

- Ho un codice di attivazione
  In questo caso, attiva il prodotto seguendo questi passaggi:

  1. Inserisci il codice di attivazione nel campo Ho un codice di attivazione e poi clicca su **CONTINUA**.

     Nota
     Puoi trovare il codice di attivazione:
     - Sull'etichetta del CD/DVD.
     - Sulla scheda di registrazione del prodotto.
     - Nella e-mail di acquisto online.

  2. **Voglio valutare Bitdefender**
     In questo caso, puoi usare il prodotto per un periodo di 30 giorni. Per iniziare il periodo di prova, seleziona **Non ho un abbonamento, voglio provare il prodotto gratuitamente** e clicca su **CONTINUA**.

Fase 7 - Come iniziare

Nella finestra **Come iniziare**, puoi trovare maggiori informazioni sul tuo abbonamento attivo.

Clic **FINE** per accedere al Bitdefender Ultimate Small Business Security interfaccia.

3.2. Gestire la tua sicurezza

3.2.1. Protezione antivirus

Bitdefender protegge il tuo dispositivo da ogni tipo di minaccia malware (malware, trojan, spyware, rootkit e altro). La protezione che BitDefender vi offre è divisa in due categorie:

- **Scansione all'accesso** - Impedisce a nuove minacce di accedere al tuo sistema. Per esempio, Bitdefender esaminerà un documento Word alla ricerca di minacce note quando lo apri, e un messaggio e-mail quando lo ricevi.
  La scansione all'accesso garantisce una protezione in tempo reale dalle minacce, essendo una componente essenziale di ogni programma di sicurezza informatica.

Importante
Per impedire alle minacce di infettare il tuo dispositivo, tieni attivata la **Scansione all'accesso**.

- **Scansione su richiesta** - Permette di rilevare e rimuovere minacce già residenti nel tuo sistema. Si tratta della classica scansione dei virus avviata dall'utente – si sceglie quale drive, cartella o file BitDefender deve esaminare e BitDefender li esamina – a richiesta.

Bitdefender controlla automaticamente ogni supporto rimovibile che è collegato al dispositivo per assicurarti di accedervi in sicurezza. Per maggiori informazioni, fai riferimento a Scansione automatica di supporti rimovibili (pagina 34).

Gli utenti più esperti possono configurare le eccezioni della scansione, se non desiderano controllare determinati file o estensioni. Per maggiori informazioni, fai riferimento a Configurare le eccezioni della scansione (pagina 36).

Quando rileva una minaccia, Bitdefender tenterà automaticamente di rimuovere il codice dannoso dal file infetto, ricostruendo il file originale. Questa operazione è denominata disinfezione. I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione. Per maggiori informazioni, fai riferimento a Gestire i file in quarantena (pagina 38).

Se il tuo dispositivo è stato infettato da una minaccia, fai riferimento a Rimuovere le minacce dal sistema (pagina 143). Per aiutarti a ripulire il tuo dispositivo dalle minacce che non possono essere rimosse dal sistema operativo Windows, Bitdefender ti offre una Ambiente di salvataggio (pagina 144). Si tratta di un ambiente sicuro, realizzato specificatamente per la rimozione delle minacce, che ti consente di avviare il tuo dispositivo in modo indipendente da Windows. Quando il dispositivo è nell'Ambiente di soccorso, le minacce Windows sono inattive, rendendo quindi più semplice la loro rimozione.

Scansione all'accesso (protezione in tempo reale)

Bitdefender fornisce una protezione in tempo reale contro una vasta gamma di minacce, esaminando tutti i file e le e-mail a cui si accede.

Attivare o disattivare la protezione in tempo reale

Per attivare o disattivare la protezione dalle minacce in tempo reale:

1. Clicca su **Protezione** nel menu di navigazione nell'**interfaccia di Bitdefender**.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Avanzate**, attiva o disattiva **Bitdefender Shield**.
4. Se vuoi disattivare la protezione in tempo reale, comparirà una finestra di avviso. Devi confermare la tua scelta selezionando dal menu per quanto tempo desideri disattivare la protezione in tempo reale. Puoi disattivare la protezione in tempo reale per 5, 15 o 30 minuti, un'ora, in modo permanente o fino a un riavvio del sistema. La protezione in tempo reale si attiverà automaticamente allo scadere del tempo indicato.

   Avvertimento
   È una questione di sicurezza piuttosto importante. Si consiglia di disattivare la protezione in tempo reale per il minimo tempo possibile. Se la protezione in tempo reale è disattivata, non si è protetti dalle minacce.

Configurare le impostazioni avanzate della protezione in tempo reale

Gli utenti avanzati possono trarre vantaggio dalle impostazioni di scansione offerte da Bitdefender. Puoi configurare le impostazioni della protezione in tempo reale in ogni dettaglio, creando un livello di protezione personalizzato.

Per configurare le impostazioni avanzate della protezione in tempo reale:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Nella finestra **Avanzate** puoi configurare le impostazioni di scansione in base alle tue esigenze.

Informazioni sulle opzioni di scansione

Questa informazione potrebbe esserti utile:

- **Esamina solo le applicazioni**. Puoi impostare Bitdefender per esaminare solo le app a cui accedi.
- **Esamina le applicazioni potenzialmente indesiderate**. Seleziona questa opzione per esaminare le applicazioni indesiderate.

Un'applicazione potenzialmente indesiderata (PUA) o un programma potenzialmente indesiderato (PUP) è un software in genere abbinato a un altro software freeware che mostra finestre di pop-up o installa una barra degli strumenti nel browser predefinito. Alcuni di questi programmi modificheranno la homepage o il motore di ricerca predefinito, altri eseguiranno diversi processi in background che rallentano il PC oppure mostreranno numerosi annunci pubblicitari. Tali programmi possono essere installati senza il tuo consenso (sono chiamati anche adware) o saranno inclusi in modo predefinito nel kit di installazione rapida (supportato da pubblicità).

- **Esamina script**. La funzionalità Esamina script consente a Bitdefender di esaminare gli script di Powershell e i documenti Office che potrebbero contenere malware basati su script.
- **Scansiona condivisioni di rete**. Per accedere in remoto in modo sicuro a una rete remota dal tuo dispositivo, ti consigliamo di mantenere attivata l'opzione Scansiona condivisioni di rete.
- **Scansiona memoria del processo**. Una scansione per rilevare attività dannose nella memoria dei processi in esecuzione.
- **Scansiona riga di comando**. Esamina la riga di comando di applicazioni appena eseguite per impedire gli attacchi privi di file.
- **Scansiona gli archivi**. Esaminare gli archivi è un processo lento e che richiede molte risorse, che pertanto non è consigliato per una protezione in tempo reale. Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del tuo sistema. La minaccia può interessare il tuo sistema solo se il file infetto viene estratto dall'archivio ed eseguito senza avere una protezione in tempo reale attivata.

  Se decidi di usare questa opzione, attivala, e trascina il cursore lungo la scala per escludere dalla scansione gli archivi superiori a un determinato valore di MB (Megabytes).
- **Scansiona i settori di avvio**. Puoi impostare Bitdefender per esaminare i settori di avvio del tuo disco rigido. Questo settore del disco rigido contiene il codice informatico necessario per iniziare la fase di avvio. Quando una minaccia infetta il settore di avvio, l'unità potrebbe diventare inaccessibile e potresti non poter più avviare il sistema e accedere ai dati.

- **Esamina solo file nuovi e modificati**. Esaminando solo i file nuovi o modificati, puoi migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.
- **Scansiona keylogger**. Seleziona questa opzione per esaminare il tuo sistema alla ricerca di app keylogger. I keylogger registrano tutto ciò che digiti con la tastiera e inviano rapporti su Internet a un eventuale aggressore (hacker). L'hacker può scoprire molte informazioni sensibili dai dati sottratti, come numeri di conti bancari e password, e usarli per il proprio tornaconto personale.
- **Scansione immediata all'avvio**. Seleziona l'opzione **Scansione immediata all'avvio** per esaminare il sistema all'avvio non appena vengono caricati i sistemi critici. L'obiettivo di questa funzionalità è migliorare il rilevamento delle minacce all'avvio del sistema.

Azioni intraprese sulle minacce rilevate

Puoi configurare le azioni intraprese dalla protezione in tempo reale seguendo questi passaggi:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Nella finestra **Avanzate**, scorri verso il basso nella finestra finché non trovi l'opzione **Azioni minaccia**.
4. Configura le impostazioni della scansione come necessario.

In Bitdefender, la protezione in tempo reale può intraprendere le seguenti azioni:

Esegui azioni appropriate

Bitdefender intraprenderà le azioni consigliate in base al tipo di file rilevato:

- **File infetti**. I file rilevati come infetti corrispondono a una parte delle informazioni sulle minacce trovate nel Bitdefender Threat Information Database. Bitdefender tenterà di rimuovere automaticamente il codice dannoso dal file infetto e ricostruire il file originale. Questa operazione viene definita disinfezione.

  I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Per maggiori informazioni, fai riferimento a Gestire i file in quarantena (pagina 38).

Importante

Per alcune particolari tipologie di minacce, non è possibile usare la disinfezione perché il file rilevato è interamente dannoso. In questi casi, il file infetto è eliminato dal disco.

- **File sospetti.** I file vengono rilevati come sospetti dall'analisi euristica. I file sospetti non possono essere disinfettati perché non è disponibile alcuna routine di disinfezione. Saranno messi in quarantena per evitare una potenziale infezione.
- **Archivi contenenti file infetti.**
  - Gli archivi che contengono solo file infetti sono eliminati automaticamente.
  - Se un archivio contiene sia file puliti che infetti, Bitdefender tenterà di eliminare i file infetti a condizione che possa riformare l'archivio con i file puliti. Se la ricostruzione dell'archivio non è possibile, sarai informato del fatto che non può essere intrapresa alcuna azione in modo da evitare la perdita di file puliti.

Sposta in quarantena

Sposta i file infetti nella quarantena. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Per maggiori informazioni, fai riferimento a Gestire i file in quarantena (pagina 38).

Nega l'accesso

Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.

Ripristinare le impostazioni predefinite

Le impostazioni predefinite della protezione in tempo reale assicurano una buona protezione dalle minacce, con un impatto minimo sulle prestazioni del sistema.

Per ripristinare le impostazioni predefinite della protezione in tempo reale:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.

3. Nella finestra **Avanzate**, scorri in basso fino a visualizzare l'opzione **Reimposta impostazioni avanzate**. Selezionala per riportare le impostazioni dell'antivirus ai valori predefiniti.

Scansione a richiesta

L'obiettivo principale di Bitdefender è di mantenere il proprio dispositivo privo di minacce. Ciò avviene tenendo lontani le nuove minacce dal dispositivo ed esaminando i messaggi e-mail e qualsiasi nuovo file scaricato o copiato sul sistema.

Esiste il rischio che una minaccia sia già contenuta nel tuo sistema, addirittura prima dell'installazione di Bitdefender. Questo è il motivo per cui suggeriamo di effettuare una scansione sul tuo dispositivo alla ricerca di minacce residenti dopo aver installato Bitdefender. Inoltre, è una buona idea effettuare frequentemente una scansione del dispositivo, alla ricerca di minacce.

La scansione su richiesta si basa sulle impostazioni della scansione. Le impostazioni della scansione specificano le opzioni della scansione e gli elementi da esaminare. Puoi eseguire la scansione del dispositivo ogni volta che vuoi, avviando le attività predefinite o una tua scansione (attività definite dall'utente). Se desideri controllare ubicazioni particolari sul tuo dispositivo o impostare le opzioni di scansione, configura ed esegui una scansione personale.

Controllare un file o una cartella alla ricerca di minacce

Dovresti esaminare cartelle e file ogni volta che sospetti possano essere stati infettati. Clicca con il pulsante destro del mouse sul file o sulla cartella che vuoi esaminare, porta il cursore su **Bitdefender** e seleziona **Esamina con Bitdefender**. Comparirà la **procedura guidata della Scansione antivirus**, che ti guiderà nella fase di scansione. Al termine della scansione, ti sarà chiesto di scegliere le azioni da intraprendere sui file rilevati, nel caso sia necessario.

Eseguire una Scansione veloce

La Scansione veloce utilizza una scansione in-the-cloud per rilevare eventuali minacce in esecuzione sul tuo sistema. In genere, eseguire una Scansione veloce richiede meno di un minuto e usa una frazione delle risorse di sistema necessarie per una scansione antivirus standard.

Per eseguire una scansione veloce:

1. Clicca su Protection nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Nella finestra **Scansioni**, clicca sul pulsante **Esegui scansione** accanto a **Scansione veloce**.
4. Segui la **procedura guidata della scansione antivirus** per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati. Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

Eseguire una scansione del sistema

La Scansione del sistema esamina l'intero dispositivo per rilevare tutti i tipi di minacce che mettono in pericolo la sua sicurezza, come malware, spyware, adware, rootkit e altri.

> **Nota**
> Poiché la **Scansione del sistema** esegue una scansione accurata dell'intero sistema, potrebbe richiedere un po' di tempo. Pertanto, si consiglia di eseguire questa operazione quando non si utilizza il dispositivo.

Prima di eseguire una Scansione del sistema, si consiglia di:

- Assicurati che Bitdefender sia aggiornato con il suo database delle informazioni delle minacce. Eseguire la scansione con un database delle informazioni delle minacce obsoleto può impedire a Bitdefender di rilevare nuove minacce, trovate dopo l'ultimo aggiornamento. Per maggiori informazioni, fai riferimento a Mantenere Bitdefender aggiornato.
- Chiudere tutti i programmi aperti.

Se desideri controllare ubicazioni particolari sul tuo dispositivo o impostare le opzioni di scansione, configura ed esegui una scansione personale. Per maggiori informazioni, fai riferimento a Configurare una scansione personale (pagina 27).

Per eseguire una scansione del sistema:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.

3. Nella finestra **Scansioni**, clicca sul pulsante **Esegui scansione** accanto a **Scansione sistema**.
4. La prima volta che esegui una Scansione di sistema, ti sarà presentata questa funzionalità. Clicca su **OK, ho capito** per continuare.
5. Segui il Procedura guidata di scansione antivirus per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati. Se rimangono minacce irrisolte, ti verrà chiesto di scegliere le azioni da intraprendere su di esse.

Configurare una scansione personale

Nella finestra **Gestisci scansioni**, puoi impostare Bitdefender per eseguire le scansioni ogni volta che ritieni che il tuo dispositivo abbia bisogno di un controllo per potenziali minacce. Puoi scegliere di programmare una **Scansione del sistema** o una **Scansione veloce**, o puoi creare una scansione personalizzata a tuo piacimento.

Per configurare una nuova scansione personalizzata nei dettagli:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Nella finestra **Scansioni**, clicca su **+Crea scansione**.
4. Nel campo **Nome dell'attività**, inserisci un nome per la scansione, seleziona i percorsi che vorresti esaminare e clicca su **Avanti**.
5. Configura queste opzioni generali:
   - **Scansiona solo le applicazioni.** Puoi impostare Bitdefender in modo che controlli solo le app a cui si accede.
   - **Priorità dell'attività di scansione.** Puoi scegliere l'impatto che un processo di scansione dovrebbe avere sulle prestazioni del tuo sistema.
     - Automatico - La priorità del processo di scansione dipenderà dalle attività del sistema. Per assicurarsi che la fase di scansione non influenzi le attività del sistema, Bitdefender deciderà se eseguire la scansione con una maggiore o minore priorità.
     - Alta - La priorità della fase di scansione sarà elevata. Scegliendo questa opzione, consentirai ad altri programmi di funzionare più

lentamente, diminuendo il tempo necessario per completare la scansione.

- Bassa - La priorità della fase di scansione sarà bassa. Scegliendo questa opzione, consentirai ad altri programmi di funzionare più velocemente, aumentando il tempo necessario per completare la scansione.

- **Pubblica azioni di scansione.** Scegli quale azione Bitdefender dovrebbe intraprendere nel caso non venisse trovata alcuna minaccia:
  - Mostra la finestra del sommario
  - Spegni il dispositivo
  - Chiudi la finestra di scansione

6. Se vuoi configurare le opzioni di scansione nel dettaglio, clicca su **Mostra impostazioni avanzate**. Puoi trovare informazioni sulle scansioni elencate al termine di questa sezione.
   Clicca su **Avanti**.
7. Se lo desideri, puoi attivare **Programma attività di scansione** e poi scegli quando dovrebbe iniziare la scansione personalizzata che hai creato.
   - All'avvio del sistema
   - Giornalmente
   - Mensilmente
   - Settimanalmente

   Se scegli Giornalmente, Mensilmente o Settimanalmente, trascina il cursore lungo la scala per impostare il periodo di tempo desiderato in cui dovrebbe iniziare la scansione programmata.
8. Clicca su **Salva** per salvare le impostazioni e chiudere la finestra di configurazione.
   In base ai percorsi da controllare, la scansione potrebbe richiedere un po' di tempo. Se durante la scansione venissero rilevate delle minacce, ti sarà chiesto di scegliere le azioni da intraprendere sui file rilevati.

Informazioni sulle opzioni di scansione

Potresti trovare utili queste informazioni:

- Se non conosci alcuni termini, verificali nel {1}glossario{2}. Puoi anche trovare informazioni utili cercando su Internet.
- **Scansiona le applicazioni potenzialmente indesiderate.** Seleziona questa opzione per cercare applicazioni indesiderate. Un'applicazione potenzialmente indesiderata (PUA) o un programma potenzialmente indesiderato (PUP) è un software che di solito viene fornito in bundle con software freeware e visualizzerà popup o installerà una barra degli strumenti nel browser predefinito. Alcuni cambieranno la home page o il motore di ricerca, altri eseguiranno diversi processi in background rallentando il PC o visualizzeranno numerosi annunci. Questi programmi possono essere installati senza il tuo consenso (chiamati anche adware) o saranno inclusi per impostazione predefinita nel kit di installazione rapida (supportato da pubblicità).
- **Esamina gli archivi.** Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del tuo sistema. La minaccia può interessare il tuo sistema solo se il file infetto viene estratto dall'archivio ed eseguito senza avere la protezione in tempo reale attivata. Tuttavia, si consiglia di usare questa opzione per rilevare e rimuovere qualsiasi minaccia potenziale, persino se non è una minaccia immediata.
  Trascina il cursore lungo la scala per escludere dalla scansione gli archivi superiori a un determinato valore di MB (Megabytes).

  > **Nota**
  > La scansione dei file archiviati incrementa la durata totale della scansione e richiede più risorse di sistema.

- **Scansiona solo i file nuovi e modificati.** Analizzando solo i file nuovi e modificati, è possibile migliorare notevolmente la reattività complessiva del sistema con un compromesso minimo in termini di sicurezza.
- **Scansiona i settori di avvio.** Puoi impostare Bitdefender in modo che esegua la scansione dei settori di avvio del tuo disco rigido. Questo settore del disco rigido contiene il codice del computer necessario per avviare il processo di avvio. Quando una minaccia infetta il settore di

avvio, l'unità potrebbe diventare inaccessibile e potresti non essere in grado di avviare il sistema e accedere ai tuoi dati.

- **Scansiona memoria.** Seleziona questa opzione per esaminare i programmi in esecuzione nella memoria di sistema.
- **Scansiona registro.** Seleziona questa opzione per esaminare le chiavi del registro. Il registro di Windows è un database che memorizza le impostazioni e le opzioni di configurazione per i componenti del sistema operativo Windows, nonché per le app installate.
- **Scansiona i cookie.** Seleziona questa opzione per esaminare i cookie memorizzati dai browser sul tuo dispositivo.
- **Scansiona i keylogger.** Seleziona questa opzione per scansionare il tuo sistema alla ricerca di app keylogger. I keylogger registrano ciò che digiti sulla tastiera e inviano rapporti su Internet a una persona malintenzionata (hacker). L'hacker può scoprire informazioni sensibili dai dati rubati, come numeri di conto bancario e password, e utilizzarle per ottenere vantaggi personali.

Procedura guidata scansione antivirus

Ogni volta che inizi una scansione a richiesta (per esempio, cliccando con il pulsante destro del mouse su una cartella), seleziona Bitdefender e poi **Esamina con Bitdefender**. Comparirà la procedura guidata di Bitdefender Antivirus Scan. Seguila per completare il processo di scansione.

> **Nota**
> Se la procedura guidata della scansione non compare, la scansione potrebbe essere configurata per operare silenziosamente in background. Cerca l'icona dei progressi della scansione nella **barra delle applicazioni**. Puoi cliccare su questa icona per aprire la finestra di scansione e visualizzarne i progressi.

Fase 1 - Eseguire la scansione

BitDefender inizierà la scansione degli oggetti selezionati. Puoi vedere in tempo reale informazioni sulle statistiche e sullo stato della scansione (incluso il tempo trascorso, una stima del tempo rimasto e il numero di minacce rilevate).

Attendere che BitDefender finisca la scansione. La durata del processo dipende dalla complessità della scansione.

Fermare o sospendere la scansione. Puoi fermare la scansione in qualsiasi momento cliccando su **FERMA**. Andrai direttamente all'ultimo passaggio della procedura guidata. Per arrestare temporaneamente il processo di scansione, clicca su **SOSPENDI**. Dovrai cliccare su **RIPRENDI** per riprendere la scansione.

Archivi protetti da password. Quando viene rilevato un archivio protetto da password, in base alle impostazioni della scansione, potrebbe esserti chiesto di fornire la password. Gli archivi protetti da password non possono essere esaminati a meno di fornire la password. Sono disponibili le seguenti opzioni:

- **Password.** Se vuoi che Bitdefender esamini l'archivio, seleziona questa opzione e inserisci la password. Se non conosci la password, scegli una delle altre opzioni.
- **Non chiedere una password e ignora questo elemento per la scansione.** Seleziona questa opzione per salvare la scansione di questo archivio.
- **Ignora tutti gli elementi protetti da password senza controllarli.** Seleziona questa opzione se non vuoi ricevere avvisi inerenti gli archivi protetti da password. Bitdefender non potrà esaminarli, ma sarà conservata una nota nel registro della scansione.

Seleziona l'opzione desiderata e clicca su **OK** per continuare la scansione.

Fase 2 - Scegliere le azioni

Al termine della scansione, ti sarà chiesto di scegliere quali azioni intraprendere sui file rilevati, se presenti.

> **Nota**
> Eseguendo una scansione veloce o una scansione completa del sistema, Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati durante la scansione. Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

Gli elementi infetti vengono mostrati in gruppi in base alle minacce con le quali sono stati infettati. Clicca sul collegamento corrispondente alla minaccia per trovare più informazioni sugli oggetti infetti.

Puoi scegliere di intraprendere un'azione globale per tutti i problemi oppure selezionare azioni separate per ogni gruppo di problemi. Una o più delle seguenti opzioni possono comparire nel menu:

Esegui azioni appropriate

Bitdefender intraprenderà le azioni consigliate a seconda del tipo di file rilevato:

- **File infetti.** I file rilevati come infetti corrispondono a informazioni sulle minacce trovate nel database delle informazioni sulle minacce di Bitdefender. Bitdefender tenterà automaticamente di rimuovere il codice dannoso dal file infetto e di ricostruire il file originale. Questa operazione viene definita disinfezione.

  I file che non possono essere disinfettati vengono spostati in quarantena per contenere l'infezione. I file in quarantena non possono essere eseguiti o aperti; quindi, il rischio di contrarre l'infezione scompare. Per ulteriori informazioni, fare riferimento a Gestire i file in quarantena (pagina 38).

  > **Importante**
  > Per particolari tipi di minacce, la disinfezione non è possibile perché il file rilevato è interamente dannoso. In tali casi, il file infetto viene eliminato dal disco.

- **Documenti sospetti.** I file vengono rilevati come sospetti dall'analisi euristica. I file sospetti non possono essere disinfettati perché non è disponibile alcuna routine di disinfezione. Saranno spostati in quarantena per prevenire una potenziale infezione.
- **Archivi contenenti file infetti.**
  - Gli archivi che contengono solo file infetti vengono eliminati automaticamente.
  - Se un archivio contiene sia file infetti che file puliti, Bitdefender tenterà di eliminare i file infetti a condizione che possa ricostruire l'archivio con i file puliti. Se la ricostruzione dell'archivio non è possibile, verrai informato che non è possibile intraprendere alcuna azione per evitare di perdere file puliti.

Elimina

Rimuove i file rilevati dal disco.

Se i file infetti sono memorizzati in un archivio con altri file puliti, Bitdefender tenterà di eliminarli e di riformare l'archivio con i file puliti. Se la ricostruzione dell'archivio non è possibile, sarai informato del fatto

che non può essere intrapresa alcuna azione in modo da evitare la perdita di file puliti.

Non fare nulla

Sui file rilevati non sarà eseguita alcuna azione. Dopo che la scansione è stata completata, potrai aprire il registro della scansione per visualizzare le informazioni su questi file.

Clicca su **Continua** per applicare le azioni specificate.

Fase 3 - Sommario

Quando BitDefender completa la risoluzione dei problemi, i risultati della scansione appariranno in una nuova finestra. Se desideri ricevere informazioni esaurienti sul processo di scansione, clicca su **REGISTRO** per visualizzare il registro della scansione.

> **Importante**
> Nella maggior parte dei casi BitDefender disinfetta con successo i file infetti che rileva o isola l'infezione. Tuttavia, ci sono problemi che non possono essere risolti automaticamente. Se richiesto, riavvia il sistema per completare il processo di pulizia. Per maggiori informazioni e istruzioni su come rimuovere una minaccia manualmente, fai riferimento a Rimuovere le minacce dal sistema (pagina 143).

Controllare i registri di scansione

Ogni volta che viene eseguita una scansione, viene creato un registro di scansione e Bitdefender memorizza i problemi rilevati nella finestra Antivirus. Il registro di scansione contiene informazioni dettagliate sul processo di scansione registrato, sull'obiettivo della scansione, le minacce individuate e le azioni intraprese su queste minacce.

Puoi aprire il registro della scansione direttamente dalla procedura guidata di scansione, una volta completata, cliccando su **REGISTRO**.

Per controllare in un secondo tempo un registro di una scansione o eventuali infezioni rilevate:

1. Clic **Notifiche** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nella scheda **Tutto**, seleziona la notifica relativa all'ultima scansione.

Qui puoi trovare tutti gli eventi della scansione anti-minacce, incluso le minacce rilevate dalla scansione all'accesso, le scansioni avviate dall'utente e le variazioni di stato per le scansioni automatiche.

3. Nell'elenco delle notifiche, puoi verificare quali scansioni sono state eseguite di recente. Clicca su una notifica per visualizzare maggiori dettagli al riguardo.
4. Per aprire il registro della scansione, clicca su **Guarda registro**.

Scansione automatica di supporti rimovibili

Bitdefender rileva automaticamente quando si collega un dispositivo di archiviazione rimovibile al dispositivo e ne esegue una scansione in background, quando la scansione automatica è attivata. Questa operazione è consigliata per impedire che virus e altre minacce infettino il dispositivo.

I dispositivi rilevati rientrano in una di queste categorie:

- CD/DVD
- Unità USB, ad esempio chiavette e dischi rigidi esterni
- Unità di rete (remote) mappate

Puoi configurare la scansione automatica separatamente per ciascuna categoria di dispositivi di memorizzazione. Di norma la scansione automatica delle unità di rete mappate è disattivata.

Come funziona?

Quando rileva un dispositivo rimovibile di archiviazione, Bitdefender inizia la scansione delle minacce (a condizione che la scansione automatica sia attivata per quel tipo di dispositivo). Sarai avvisato attraverso una finestra pop-up che un nuovo dispositivo è stato rilevato ed è in fase di scansione.

Comparirà un'icona della scansione di Bitdefender nella **barra delle applicazioni**. Puoi cliccare su questa icona per aprire la finestra di scansione e visualizzare i progressi della scansione.

Al termine della scansione, la finestra dei risultati della scansione ti informa se puoi accedere tranquillamente ai file sui supporti rimovibili.

Nella maggior parte dei casi, Bitdefender rimuove automaticamente le minacce rilevate o isola i file infetti mettendoli in quarantena. Se dopo

la scansione ci sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

> **Nota**
> Tieni presente che nessuna azione può essere intrapresa su file sospetti rilevati su CD/DVD. Allo stesso modo, non può essere intrapresa alcuna azione su file sospetti rilevati su unità di rete mappate, se non si hanno privilegi appropriati.

Queste informazioni potrebbero esserti utili:

- Fai attenzione a usare un CD/DVD infettato da una minaccia, perché le minacce non possono essere rimosse dal disco (è un supporto di sola lettura). Assicurati che la protezione in tempo reale sia attivata per impedire la diffusione di minacce nel tuo sistema. Si consiglia di copiare tutti i dati importanti dal disco al proprio sistema e poi eliminare il disco.
- In alcuni casi, Bitdefender può non essere in grado di rimuovere le minacce da file specifici a causa di vincoli legali o tecnici. Un esempio sono i file archiviati con una tecnologia proprietaria (questo perché l'archivio non può essere ricreato correttamente).

  Per scoprire come comportarsi con le minacce, fai riferimento a Rimuovere le minacce dal sistema (pagina 143).

Gestire la scansione di supporti rimovibili

Per gestire la scansione automatica di supporti rimovibili:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Seleziona la finestra **Impostazioni**.

Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono rilevati file infetti, Bitdefender proverà a disinfettarli (rimuovere il codice dannoso) o a spostarli in quarantena. Se entrambe le azioni falliscono, la procedura guidata della scansione antivirus ti permetterà di specificare altre azioni da intraprendere sui file infetti. Le opzioni di scansione sono standard e non puoi modificarle.

Per la migliore protezione, si consiglia di lasciare selezionata la **Scansione automatica** per tutte le tipologie di dispositivi rimovibili di archiviazione.

Esamina file hosts

Il file hosts viene fornito di norma con l'installazione del sistema operativo ed è utilizzato per mappare gli hostname in indirizzi IP ogni volta che accedi a una nuova pagina web, ti connetti a un FTP o a un altro server Internet. Si tratta di un semplice file di testo e i programmi potenzialmente dannosi possono modificarlo. Gli utenti avanzati sanno come utilizzarlo per bloccare pubblicità, banner, cookie di terze parti o hijacker fastidiosi.

Per configurare la scansione del file hosts:

1. Clic **Impostazioni** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Seleziona il **Avanzate** scheda.
3. Attiva o disattiva **Esamina file hosts**.

Configurare le eccezioni della scansione

Bitdefender consente di escludere determinati file, cartelle o estensioni di file dalla scansione. Questa funzione ha lo scopo di evitare interferenze con il tuo lavoro e può anche contribuire a migliorare le prestazioni del sistema. Le eccezioni devono essere utilizzate da utenti con conoscenze informatiche avanzate, o altrimenti, si consiglia di seguire le raccomandazioni degli operatori di Bitdefender.

Puoi configurare le eccezioni da applicare solo alla scansione all'accesso o su richiesta, oppure a entrambe. Gli oggetti esclusi dalla scansione all'accesso non saranno esaminati, non importa se sono stati visitati da te o da un'applicazione.

> **Nota**
> Le eccezioni NON saranno applicate per la scansione contestuale. La scansione contestuale è un tipo di scansione su richiesta: clicca con il pulsante destro sul file o sulla cartella che si vuole esaminare e selezionare **Scansiona con BitDefender**.

Escludere file e cartelle dalla scansione

Per escludere determinati file e cartelle dalla scansione:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.

2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Nella finestra **Impostazioni**, clicca su **Gestisci le eccezioni**.
4. Clicca su **+Aggiungi un'eccezione**.
5. Inserisci il percorso della cartella che vuoi escludere dalla scansione nel campo corrispondente.
   In alternativa, puoi raggiungere la cartella cliccando sul pulsante Sfoglia nel lato destro dell'interfaccia, selezionala e clicca su **OK**.
6. Disattiva l'interruttore accanto alla funzionalità di protezione così da non esaminare la cartella. Ci sono tre opzioni:
   - Antivirus
   - Prevenzione minacce online
   - Advanced Threat Defense
7. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

Escludere estensioni dei file dalla scansione

Se escludi un'estensione di un file dalla scansione, Bitdefender non controllerà più i file con tale estensione, indipendentemente dalla loro posizione nel dispositivo. L'eccezione si applica anche ai file su supporti rimovibili, come CD, DVD, unità USB o di rete.

> **Importante**
> Usa la massima cautela nell'escludere le estensioni dalla scansione, perché tali estensioni possono rendere il dispositivo vulnerabile alle minacce.

Per escludere estensioni di file dalla scansione:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Nel **Impostazioni** finestra, fare clic **Gestisci eccezioni**.
4. Clic **+ Aggiungi un'eccezione**.
5. Inserisci le estensioni che vuoi escludere dalla scansione con un punto prima di loro e separate da punto e virgola (;).
   txt;avi;jpg

6. Attiva l'interruttore accanto alla funzione di protezione che non deve esaminare l'estensione.
7. Clicca su **Salva**.

Gestire le eccezioni della scansione

Se le eccezioni della scansione configurata non sono più necessarie, si consiglia di eliminarle o disattivare le eccezioni della scansione.

Per gestire le eccezioni della scansione:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Nella finestra **Impostazioni**, clicca su **Gestisci le eccezioni**. Sarà visualizzato un elenco con tutte le tue eccezioni.
4. Per rimuovere o modificare le eccezioni della scansione, clicca su uno dei pulsanti disponibili. Procedi come segue:
   - Per rimuovere una voce dall'elenco, clicca sul pulsante accanto ad essa.
   - Per modificare una voce dalla tabella, clicca sul pulsante **Modifica** accanto ad essa. Apparirà una nuova finestra, dove potrai modificare l'estensione o il percorso da escludere e la funzionalità di sicurezza dal quale escluderlo, a seconda delle necessità. Esegui i cambiamenti necessari, poi clicca su **MODIFICA**.

Gestire i file in quarantena

Bitdefender isola i file infettati da minacce che non può disinfettare e i file sospetti in un'area sicura chiamata quarantena. Quando una minaccia è in quarantena, non può più arrecare alcun danno, in quanto non può essere eseguita o letta.

Inoltre Bitdefender controlla i file in quarantena ogni volta che il database delle informazioni sulle minacce viene aggiornato. I file puliti vengono spostati automaticamente alla loro ubicazione originale.

Per controllare e gestire i file in quarantena:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.

3. Vai alla finestra **Impostazioni**.
   Qui puoi visualizzare il nome dei file in quarantena, la loro posizione originale e il nome delle minacce rilevate.

4. I file in quarantena sono gestiti automaticamente da Bitdefender in base alle impostazioni di quarantena predefinite.
   Anche se non consigliato, puoi modificare le impostazioni della quarantena in base alle tue preferenze, cliccando su **Vedi impostazioni**.
   Clicca sugli interruttori per attivare o disattivare:
   Esamina nuovamente la quarantena dopo l'aggiornamento delle informazioni delle minacce
   Mantieni questa opzione attivata per eseguire automaticamente la scansione dei file in quarantena dopo ogni aggiornamento del database delle informazioni sulle minacce. I file puliti vengono spostati automaticamente alla loro ubicazione originale.
   Elimina i contenuti più vecchi di 30 giorni
   I file in quarantena più vecchi di 30 giorni sono eliminati automaticamente.
   Crea eccezioni per i file ripristinati
   I file ripristinati dalla quarantena vengono riportati alla loro posizione originale senza essere riparati e vengono esclusi automaticamente dalle scansioni future.

5. Per eliminare un file in quarantena, selezionalo e clicca sul pulsante **Elimina**. Se desideri ripristinare un file in quarantena alla sua ubicazione originale, selezionalo e clicca su **Ripristina**.

3.2.2. Difesa avanzata dalle minacce

Bitdefender Advanced Threat Defense è una tecnologia di rilevamento innovativa e proattiva che utilizza metodi euristici avanzati per rilevare ransomware e altre nuove potenziali minacce in tempo reale.

Advanced Threat Defense monitora continuamente le applicazioni in esecuzione sul dispositivo, cercando eventuali minacce. A ognuna viene assegnato un punteggio e per ogni processo viene poi assegnato un punteggio totale.

Come misura di sicurezza sarai informato ogni volta che vengono rilevate e bloccate possibili minacce e processi potenzialmente dannosi.

Attivare o disattivare Advanced Threat Defense

Per attivare o disattivare Advanced Threat Defense:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel pannello **ADVANCED THREAT DEFENSE**, clicca su **Apri**.
3. Vai alla finestra **Impostazioni** e clicca sull'interruttore accanto a **Bitdefender Advanced Threat Defense**.

> **Nota**
> Per mantenere il sistema protetto dai ransomware o altre minacce, ti consigliamo di disattivare Advanced Threat Defense per il minor tempo possibile.

Verificare gli attacchi dannosi rilevati

Ogni volta che vengono rilevate minacce o processi potenzialmente dannosi, Bitdefender li bloccherà per impedire l'infezione del tuo dispositivo di ransomware o altri malware. Puoi controllare in qualsiasi momento l'elenco degli attacchi dannosi rilevati, seguendo questi passaggi:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **DIFESA AVANZATA DALLE MINACCE** riquadro, fare clic **Aprire**.
3. Vai alla finestra **Threat Defense**.
   Vengono mostrati gli attacchi rilevati negli ultimi 90 giorni. Per scoprire dettagli sul tipo di ransomware rilevato, il percorso del processo dannoso o se la disinfezione ha avuto successo, basta cliccarci sopra.

Aggiungere processi alle eccezioni

Puoi configurare le regole delle eccezioni per le applicazioni affidabili in modo che Advanced Threat Defense non le blocchi, se eseguono azioni simili a minacce.

Per iniziare ad aggiungere processi all'elenco delle eccezioni di Advanced Threat Defense:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **DIFESA AVANZATA DALLE MINACCE** riquadro, fare clic **Aprire**.
3. Nel **Impostazioni** finestra, fare clic **Gestisci eccezioni**.

4. Clic **+ Aggiungi un'eccezione**.
5. Immettere il percorso della cartella che si desidera escludere dalla scansione nel campo corrispondente.
   In alternativa, puoi raggiungere il file eseguibile cliccando sul pulsante Sfoglia nel lato destro dell'interfaccia, selezionalo e clicca su **OK**.
6. Attiva l'interruttore accanto a **Advanced Threat Defense**.
7. Clic **Salva**.

Rilevazioni exploit

Un modo sfruttato dagli hacker per violare i sistemi è trarre vantaggio di particolari bug o vulnerabilità presenti nei software (app o plugin) e nei prodotti hardware. Per assicurarti che il tuo dispositivo resti alla larga da tali attacchi, che normalmente si diffondono molto velocemente, Bitdefender usa le più moderne tecnologie anti-exploit.

Attivare o disattivare la rilevazione degli exploit

Per attivare o disattivare la rilevazione degli exploit:

- Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
- Nel **DIFESA AVANZATA DALLE MINACCE** riquadro, fare clic **Aprire**.
- Vai alla finestra **Impostazioni** e clicca sull'interruttore accanto a **Rilevamento exploit** per attivare o disattivare la funzionalità.

> **Nota**
> Di norma, l'opzione Rilevazione exploit è attivata.

3.2.3. Prevenzione delle minacce online

Bitdefender Online Threat Prevention assicura una navigazione sicura, avvisandoti in caso di eventuali pagine web potenzialmente dannose.

Bitdefender fornisce una prevenzione dalle minacce online in tempo reale per:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox

- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Per configurare le impostazioni della Prevenzione minacce online:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel pannello **ONLINE THREAT PREVENTION**, clicca su **Impostazioni**.

Nelle sezioni **Protezione web**, clicca sugli interruttori per attivare o disattivare:

- La Prevenzione attacchi web blocca le minacce che provengono da Internet, tra cui download di tipo drive-by.
- Ricerca sicura, una componente che valuta i risultati delle tue ricerche e i link pubblicati sui social network, posizionando un'icona accanto a ogni risultato:

  Non dovresti visitare questa pagina web.

  Questa pagina web può contenere contenuti pericolosi. Presta la massima cautela se decidi di visitarla.

  Questa è pagina sicura da visitare.

  Ricerca sicura valuta i risultati delle ricerche dei seguenti motori di ricerca via web:

  - Google
  - Yahoo!
  - Bing
  - Baidu

  Ricerca sicura valuta i link pubblicati sui seguenti servizi di social network:

  - Facebook
  - 121

- Scansione web cifrata.

Gli attacchi più sofisticati possono usare il traffico web sicuro per ingannare le loro vittime. Quindi ti consigliamo di mantenere attivata l'opzione Scansione web cifrata.

- Protezione frodi.
- Protezione da phishing.

Scorri in basso e raggiungerai la sezione **Prevenzione minacce di rete**. Qui avrai l'opzione **Prevenzione minacce di rete**. Per mantenere il tuo dispositivo libero da attacchi compiuti da malware complessi (come i ransomware) tramite lo sfruttamento di vulnerabilità, mantieni attiva questa opzione.

Puoi creare un elenco di siti web, domini e indirizzi IP che non saranno esaminati dai motori anti-minacce, antiphishing e antifrode di Bitdefender. L'elenco dovrebbe includere solo siti web, domini e indirizzi IP di assoluta fiducia.

Per configurare e gestire siti web, domini e indirizzi IP usando la funzionalità Protezione minacce online fornita da Bitdefender:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **PREVENZIONE DELLE MINACCE ONLINE** riquadro, fare clic **Impostazioni**.
3. Clicca su **Gestisci eccezioni**.
4. Clic **+ Aggiungi un'eccezione**.
5. Inserisci nel campo corrispondente il nome del sito web, il nome del dominio o l'indirizzo IP che vuoi aggiungere alle eccezioni.
6. Clicca sull'interruttore accanto a **Prevenzione minacce di rete**.
7. Per rimuovere una voce dall'elenco, fare clic su pulsante accanto ad esso.
   Clic **Salva** per salvare le modifiche e chiudere la finestra.

Bitdefender ti avvisa nel browser

Ogni volta che provi a visitare un sito web classificato come poco sicuro, il sito web viene bloccato e nel tuo browser compare una pagina di avvertimento.

La pagina contiene informazioni quali l'URL del sito web e la minaccia rilevata.

Devi decidere la tua prossima azione. Sono disponibili le seguenti opzioni:

- Allontanati dal sito web cliccando su **RIPORTAMI ALLA PROTEZIONE**.
- Accedi al sito web, malgrado l'avvertimento, cliccando su **Sono a conoscenza dei rischi, quindi procedi**.
- Se hai la certezza che il sito web rilevato sia sicuro, clicca su **INVIA** per aggiungerlo alle eccezioni. Ti consigliamo di aggiungere solo siti web di cui ti fidi completamente.

3.2.4. Protezione e-mail

La tua posta elettronica è una parte importante della tua vita digitale e, date le sue molteplici applicazioni nella vita reale, è diventata un vettore di attacco preferito dai malintenzionati e una delle principali preoccupazioni di sicurezza informatica dell'utente quotidiano.

Protezione e-mail è una funzionalità di sicurezza che ti consente di scansionare e identificare contenuti potenzialmente pericolosi nelle email ricevute nella tua casella di posta. Questa funzionalità è un pacchetto di diverse tecnologie riunite sotto lo stesso modulo di protezione, come software antiphishing, antimalware, antispam, antifrode e antitruffa.

Creando una connessione diretta tra Bitdefender e il tuo fornitore di servizi di posta elettronica, consenti all'antivirus di scansionare direttamente le tue e-mail ed eliminare le limitazioni derivanti dall'utilizzo di dispositivi o client di posta diversi.

> **Nota**
> Puoi proteggere fino a 5 diversi account di posta elettronica.

Configurazione del tuo account

Questa funzionalità è perfettamente integrata nell'interfaccia utente. Per iniziare a utilizzare Protezione e-mail:

1. Sotto **Protezione**, fare clic **Aprire** nel **Protezione e-mail** carta.
2. Scegli il tuo provider di posta elettronica per l'account di posta elettronica che desideri proteggere.

> **Nota**
> Protezione e-mail è attualmente disponibile per gli account Google, gli account Outlook e presto sarà disponibile anche per Yahoo Mail.

3. Clicca sul **Registrazione** pulsante.
   L'operazione continuerà quindi nel tuo browser.
4. Inserisci il tuo indirizzo email e clicca su **Prossimo** pulsante
5. Per continuare, inserisci la tua password e clicca su **Prossimo** pulsante.
6. Controlla le autorizzazioni richieste sullo schermo e consenti a Bitdefender di proteggere il tuo account e-mail.

Il tuo account e-mail è ora protetto e tutte le e-mail in arrivo verranno scansionate contro le minacce.

> **Nota**
> Ogni email scansionata verrà contrassegnata con un'etichetta per indicarne i livelli di sicurezza.

Pannello di controllo

La dashboard visualizzerà le tue email protette sotto le quali troverai:

- data di configurazione (la data in cui l'account è stato configurato per Protezione e-mail)
- stato (attivo o inattivo)
- numero di email filtrate negli ultimi 30 giorni.
  Qui vedrai un grafico che mostra il numero di email sicure ed email pericolose ricevute.

Per aggiungere più account di posta elettronica clicca sul **Aggiungi un altro account** e segui il processo di configurazione sopra descritto per ciascuno di essi.

Per mettere in pausa la scansione o rimuovere un account da questa funzionalità clicca sui tre puntini accanto all'account in questione e clicca su **Gestisci profilo**.

3.2.5. Antispam

Spam è un termine usato per descrivere ogni e-mail non richiesta. Lo spam rappresenta un problema in continua crescita, sia per i privati

che per le aziende. Non è piacevole, si vuole evitare che i propri figli lo ricevano, potrebbe penalizzarti (per aver sprecato troppo tempo o per aver ricevuto e-mail pornografiche in ufficio) e non puoi impedire ad alcuni di inviarlo. La miglior cosa da fare, ovviamente, è impedirne la ricezione. Purtroppo di norma lo spam abbonda, oltre a presentarsi sotto molte forme e dimensioni.

Bitdefender Antispam impiega notevoli innovazioni tecnologiche e filtri antispam divenuti uno standard del settore per eliminare lo spam prima che raggiunga la posta in arrivo dell'utente. Per maggiori informazioni, fai riferimento a Approfondimenti antispam (pagina 46).

La protezione di Bitdefender Antispam è disponibile solo per i client e-mail configurati per ricevere messaggi e-mail tramite il protocollo POP3. POP3 è uno dei protocolli più usati per scaricare messaggi e-mail da un server di posta.

> **Nota**
> Bitdefender non fornisce protezione antispam agli account e-mail cui accedi direttamente tramite Internet.

I messaggi spam rilevati da Bitdefender sono marcati con il prefisso **spam** nella linea dell'oggetto. Bitdefender sposta automaticamente i messaggi di spam in una cartella specifica, come segue:

- In Microsoft Outlook, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Posta eliminata**. La cartella **Spam** viene creata quando un'e-mail viene indicata come spam.
- In Mozilla Thunderbird, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Posta eliminata**. La cartella **Spam** viene creata quando un'e-mail viene indicata come spam.

Se usi altri client di posta, devi creare una regola per spostare i messaggi e-mail marcati come [spam] da Bitdefender in una cartella di quarantena personale. Se le cartelle Posta eliminata o Cestino vengono eliminate, sarà eliminata anche la cartella Spam. Tuttavia, sarà creata una nuova cartella Spam non appena un'e-mail viene etichettata come spam.

Approfondimenti antispam

La funzione Antispam ha le seguenti caratteristiche e impostazioni:

Filtri Antispam

Il motore antispam di Bitdefender include una protezione cloud e altri filtri, che proteggono la tua casella Posta in arrivo da ogni SPAM, come **Elenco amici**, **Elenco spammer** e **Filtro caratteri**.

Elenco amici / Elenco spammer

La maggior parte delle persone comunica regolarmente con un gruppo di persone o riceve messaggi da organizzazioni o società nello stesso dominio. Utilizzando l'**elenco Amici o Spammer**, potrai facilmente classificare da quali persone vuoi ricevere e-mail (amici) indipendentemente dal contenuto del messaggio, o da quali persone non vuoi più ricevere nulla (spammer).

> **Nota**
> Ti consigliamo di aggiungere i nomi e gli indirizzi e-mail dei tuoi amici all'**Elenco amici**. Bitdefender non blocca i messaggi dai mittenti inclusi nell'elenco; perciò, aggiungendo degli amici ti assicurerai di ricevere sempre i loro messaggi.

Filtro caratteri

La maggior parte dei messaggi Spam sono scritti in caratteri cirillici e/o asiatici. Il filtro Carattere rileva questo tipo di messaggi e li etichetta come SPAM.

Operazione antispam

Il motore antispam di Bitdefender usa tutti i filtri antispam combinati per determinare se un certo messaggio e-mail dovrebbe essere consegnato alla **Posta in arrivo** o no.

Ogni e-mail che arriva da Internet viene prima controllata con il filtro **Elenco amici**/**Elenco spammer**. Se l'indirizzo del mittente viene trovato nell'**Elenco amici**, l'e-mail viene spostata direttamente nella tua **Posta in arrivo**.

Diversamente, il filtro **Elenco Spammer** prenderà in carico l'e-mail per verificare se l'indirizzo del mittente è contenuto nel suo elenco. L'e-mail verrà contrassegnata come spam e spostata nella cartella **Spam**, qualora il confronto con l'elenco abbia dato esito positivo.

Ancora, il **filtro caratteri** controllerà se l'e-mail è scritta con caratteri cirillici o asiatici. In questo caso l'e-mail verrà marcata come SPAM e spostata nella cartella **Spam**.

> **Nota**
> Se l'e-mail è marcata come SEXUALLY-EXPLICIT nella riga dell'oggetto, Bitdefender la considererà SPAM.

Programmi e protocolli di posta elettronica supportati

È fornita una protezione antispam per tutti i client di posta POP3/SMTP. La barra degli strumenti di BitDefender Antispam è integrata solo in:

- Microsoft Outlook 2007 / 2010 / 2013 / 2016 / 2019
- Mozilla Thunderbird 14 e versioni superiori

Attivare o disattivare la protezione antispam

Di norma la protezione antispam è attivata.

Per attivare o disattivare la funzionalità Antispam:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel pannello **ANTISPAM**, attiva o disattiva l'interruttore.

Usare la barra degli strumenti antispam nella finestra del tuo client e-mail

Nella parte superiore della finestra del client di posta puoi vedere la barra degli strumenti antispam. La barra degli strumenti Antispam aiuta a gestire la protezione antispam direttamente dal client di posta. È possibile correggere facilmente BitDefender se segnala un messaggio legittimo come SPAM.

> **Importante**
> BitDefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo. Per un elenco completo delle applicazioni di posta supportate, fai riferimento a Programmi e protocolli di posta elettronica supportati (pagina 48).

Qui di seguito la spiegazione di ogni pulsante:

Impostazioni - Apre una finestra in cui puoi configurare i filtri antispam e le impostazioni della barra degli strumenti.

È spam - Indica che l'e-mail selezionata è spam. Il messaggio sarà subito spostato nella cartella **Spam**. Se i servizi antispam cloud sono attivati, il messaggio viene inviato a Bitdefender Cloud per ulteriori analisi.

Non spam - Indica che l'e-mail selezionata non è spam e Bitdefender non avrebbe dovuto segnarla come tale. L'e-mail sarà spostata dalla cartella **Spam** alla cartella **Posta in arrivo**. Se i servizi cloud antispam sono attivati, il messaggio viene inviato a Bitdefender Cloud per ulteriori analisi.

> **Importante**
> Il pulsante **Non spam** diventa attivo quando selezioni un messaggio segnato come SPAM da Bitdefender (normalmente questi messaggi sono situati nella cartella **Spam**).

Aggiungi spammer - Aggiunge il mittente dell'e-mail selezionata all'elenco degli spammer. Potresti dover cliccare su **OK** per confermare. I messaggi e-mail ricevuti dagli indirizzi nell'elenco degli spammer vengono segnati automaticamente come [spam].

Aggiungi amico - Aggiunge il mittente dell'e-mail selezionata all'elenco degli amici. Potresti dover cliccare su **OK** per confermare. Riceverai sempre i messaggi e-mail da questo indirizzo, indipendentemente dal loro contenuto.

Spammer - Apre l'**Elenco spammer** che contiene tutti gli indirizzi e-mail da cui non vuoi ricevere messaggi, indipendentemente dal loro contenuto. Per maggiori informazioni, fai riferimento a Configurazione dell'elenco Spammer (pagina 52).

Amici - Apri l'**Elenco amici** che contiene tutti gli indirizzi e-mail da cui vuoi sempre ricevere i messaggi e-mail, indipendentemente dai loro contenuti. Per maggiori informazioni, fai riferimento a Configurazione dell'elenco Amici (pagina 51).

Indicare gli errori di rilevazione

Se stai utilizzando un client di posta supportato, puoi correggere facilmente il filtro antispam (indicando quali messaggi e-mail non devono essere contrassegnati come spam). Così facendo si migliorerà considerevolmente l'efficienza del filtro antispam. Segui questi passaggi:

1. Apri il tuo client e-mail.

2. Vai alla cartella posta indesiderata, dove vengono spostati i messaggi spam.
3. Seleziona il messaggio legittimo segnato erroneamente come **spam** da Bitdefender.
4. Clicca sul pulsante **Aggiungi amico** nella barra degli strumenti dell'antispam di Bitdefender per aggiungere il mittente all'elenco degli amici. Potresti dover cliccare su **OK** per confermare. Riceverai sempre i messaggi e-mail da questo indirizzo, indipendentemente dal loro contenuto.
5. Clicca sul pulsante **Non è Spam** sulla barra degli strumenti antispam di Bitdefender (in genere localizzata nella parte superiore della finestra del client di posta). L'e-mail sarà spostata nella cartella Posta in arrivo.

Indicare messaggi spam non rilevati

Se si utilizza un'applicazione di posta supportata si può facilmente indicare quali messaggi e-mail avrebbero dovuto essere rilevati come spam. Così facendo si migliorerà considerevolmente l'efficienza del filtro antispam. Segui questi passaggi:

1. Apri il tuo client di posta.
2. Vai alla cartella Posta in arrivo.
3. Seleziona i messaggi di spam non rilevati.
4. Clicca sul pulsante **È spam** nella barra degli strumenti dell'antispam di Bitdefender (normalmente posizionata nella parte superiore della finestra del client di posta). Vengono subito segnati come [{9}spam{10}] e spostati nella cartella Cestino.

Configurare le impostazioni della barra degli strumenti

Per configurare le impostazioni della barra degli strumenti antispam per il client e-mail, clicca sul pulsante **Impostazioni** nella barra degli strumenti e poi sulla scheda **Impost. Barra strumenti**.

Hai le seguenti opzioni:

- **Etichetta i messaggi di spam come "letti"** - Etichetta i messaggi di spam come letti in modo automatico, in modo tale da non disturbare quando questi vengono ricevuti.
- Puoi scegliere se visualizzare o meno le finestre di conferma quando clicchi sui pulsanti **Aggiungi spammer** e **Aggiungi amico** nella barra degli strumenti dell'antispam.
  Le finestre di conferma possono impedire di aggiungere accidentalmente i mittenti all'elenco Amici / Spammer.

Configurazione dell'elenco Amici

L'**elenco Amici** è un elenco di tutti gli indirizzi e-mail dai quali desideri sempre ricevere messaggi, indipendentemente dal loro contenuto. I messaggi provenienti dagli amici non verranno etichettati come spam, anche se il loro contenuto potrebbe assomigliare allo spam.

> **Nota**
> Qualsiasi e-mail in arrivo da un indirizzo contenuto nell'**elenco Amici**, sarà automaticamente consegnata nella Posta in arrivo, senza alcuna ulteriore elaborazione.

Per configurare e gestire l'elenco Amici:

- Se stai usando Microsoft Outlook o Thunderbird, clicca sul pulsante Amici nella **barra degli strumenti dell'antispam di Bitdefender**.
- In alternativa:
  1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
  2. Nel pannello **ANTISPAM**, clicca su **Impostazioni**.
  3. Accedi alla finestra **Gestisci amici**.

Per aggiungere un indirizzo e-mail, seleziona l'opzione **Indirizzo e-mail**, inserisci l'indirizzo e clicca su **AGGIUNGI**. Sintassi: name@domain.com.

Per aggiungere tutti gli indirizzi e-mail da un dominio specifico, seleziona l'opzione **Nome dominio**, inserisci il nome del dominio e clicca su **AGGIUNGI**. Sintassi:

- @domain.com e domain.com - Tutte le e-mail provenienti da domain.com raggiungeranno la **Posta in arrivo** indipendentemente dal loro contenuto;
- domain - Tutte le e-mail provenienti da domain (indipendentemente dai suffissi del dominio) saranno marcate come Spam;
- com - Tutte le e-mail con il suffisso di dominio com saranno marcate come Spam;

Si consiglia di evitare di aggiungere interi domini, ma potrebbe essere utile in alcune situazioni. Per esempio, puoi aggiungere il dominio e-mail della società per cui lavori o quello dei tuoi contatti di fiducia.

Per eliminare una voce dall'elenco, clicca sul pulsante corrispondente accanto ad essa. Per eliminare tutte le voci dall'elenco, clicca su **Cancella lista**.

Puoi salvare l'elenco Amici in un file in modo da poterlo riutilizzare su un altro dispositivo o dopo aver reinstallato il prodotto. Per salvare l'elenco Amici, clicca sul pulsante Salva e salvalo nella posizione desiderata. Il file avrà estensione .bwl.

Per caricare un elenco Amici salvato in precedenza, clicca su **Carica** e apri il corrispondente file .bwl. Per reimpostare il contenuto dell'elenco esistente quando si carica un elenco salvato in precedenza, seleziona la casella accanto a **Sovrascrivi elenco attuale**.

Configurazione dell'elenco Spammer

L'**elenco Spammer** è l'elenco di tutti gli indirizzi e-mail dai quali non desideri ricevere messaggi, indipendentemente dal loro contenuto. Qualsiasi e-mail in arrivo da un indirizzo contenuto nell'**elenco Spammer** sarà automaticamente marcata come spam, senza alcun ulteriore processo.

Per configurare e gestire l'elenco Spammer:

- Se stai usando Microsoft Outlook o Thunderbird, clicca sul pulsante **Spammer** nella **barra degli strumenti dell'antispam di Bitdefender** integrata nel tuo client di posta.
- In alternativa:

  1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.

2. Nel **ANTI-SPAM** riquadro, fare clic **Impostazioni**.
3. Accedi alla finestra **Gestisci spammer**.

Per aggiungere un indirizzo e-mail, seleziona il **Indirizzo e-mail** opzione, immettere l'indirizzo, quindi fare clic su **AGGIUNGERE**. Sintassi: nome@dominio.com.

Per aggiungere tutti gli indirizzi email di un dominio specifico, seleziona il **Nome del dominio** opzione, immettere il nome del dominio, quindi fare clic su **AGGIUNGERE**. Sintassi:

- @domain.comand domain.com - Tutti i messaggi e-mail ricevuti da domain.com raggiungeranno la tua **Posta in arrivo** indipendentemente dal loro contenuto;
- dominio - tutti i messaggi e-mail ricevuti da dominio (indipendentemente dai suffissi del dominio) verranno contrassegnati come SPAM;
- com - Tutte le e-mail con il suffisso di dominio com saranno marcate come Spam.

Si consiglia di evitare di aggiungere interi domini, ma potrebbe essere utile in alcune situazioni.

> **Avvertimento**
> Non aggiungere domini di servizi di posta web-based legittimi (come Yahoo, Gmail, Hotmail o altro) all'Elenco spammer. Altrimenti, i messaggi e-mail ricevuti da qualsiasi utente registrato a uno di questi servizi saranno rilevati come spam. Se, per esempio, hai aggiunto **yahoo.com** all'Elenco spammer, tutti i messaggi di e-mail che arrivano dagli indirizzi **yahoo.com** saranno segnati come [spam].

Per eliminare un elemento dall'elenco, fare clic sul corrispondente pulsante accanto ad esso. Per eliminare tutte le voci dall'elenco, fare clic su **Elenco chiaro**.

Puoi salvare l'elenco spammer in un file in modo da poterlo riutilizzare su un altro dispositivo o dopo aver reinstallato il prodotto. Per salvare l'elenco Spammer, clicca sul pulsante **Salva** e salvalo nella posizione desiderata. Il file avrà estensione .bwl.

Per caricare un elenco Spammer salvato in precedenza, clicca sul pulsante **CARICA** e apri il corrispondente file .bwl. Per ripristinare il contenuto

dell'elenco esistente quando si carica un elenco salvato in precedenza, seleziona Sovrascrivi elenco attuale.

Configurare i filtri locali antispam

Come descritto in Approfondimenti antispam (pagina 46), Bitdefender usa una combinazione di diversi filtri antispam per identificare lo spam. I filtri antispam sono pre-configurati per una protezione ottimale.

> **Importante**
> A seconda che tu riceva o no e-mail legittime, scritte in caratteri asiatici o cirillici, disattiva o attiva l'impostazione che blocca automaticamente tali e-mail. L'impostazione corrispondente è disattivata nelle versioni localizzate del programma che usano tali set di caratteri (per esempio, nella versione russa e cinese).

Per configurare i filtri locali antispam:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTI-SPAM** riquadro, fare clic **Impostazioni**.
3. Vai alla finestra **Impostazioni** e clicca sull'interruttore attiva/inattiva corrispondente.

Se stai usando Microsoft Outlook o Thunderbird, puoi configurare i filtri antispam locali direttamente dal tuo client di posta. Clicca sul pulsante **Impostazioni** nella barra degli strumenti dell'antispam di Bitdefender (normalmente localizzata nella parte superiore della finestra del client di posta) e poi sulla scheda **Filtri antispam**.

Configurare le impostazioni cloud

La rilevazione cloud sfrutta i servizi di Bitdefender Cloud per fornirti una protezione antispam efficace e sempre aggiornata.

La protezione cloud funziona finché si tiene attivo Bitdefender Antispam.

Campioni di e-mail legittime o spam possono essere inviate a Bitdefender Cloud indicando errori di rilevazioni o messaggi spam non rilevati. Ciò contribuisce a migliorare la rilevazione antispam di Bitdefender.

Configura l'invio di un'e-mail campione a Bitdefender Cloud selezionando le opzioni desiderate seguendo questi passaggi:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.

2. Nel **ANTI-SPAM** riquadro, fare clic **Impostazioni**.
3. Vai al **Impostazioni** finestra e fare clic sugli interruttori di attivazione o disattivazione corrispondenti.

Se stai usando Microsoft Outlook o Thunderbird, puoi configurare il rilevamento cloud direttamente dal tuo client di posta. Clicca sul pulsante **Impostazioni** nella barra degli strumenti dell'antispam di Bitdefender (normalmente posizionata nella parte superiore della finestra del client di posta) e poi sulla scheda **Impostazioni cloud**.

3.2.6. Firewall

> **Nota**
> Il modulo Firewall all'interno di Bitdefender Ultimate Small Business Security sarà disattivato per impostazione predefinita. È necessario riattivarlo manualmente.
>
> Se **Windows Defender Firewall** è attivato durante questa procedura, prima sarà richiesto di disattivarlo.

Il Firewall protegge il proprio dispositivo da tentativi di connessione non autorizzati in entrata e in uscita, sia sulle reti locali che su Internet. È come avere una guardia al proprio cancello: tiene traccia dei tentativi di connessione e decide quali consentire e quali bloccare.

Il firewall di Bitdefender usa un set di regole per filtrare i dati trasmessi da e verso il proprio sistema.

In condizioni normali, Bitdefender crea automaticamente una regola ogni volta che una app tenta di accedere a Internet. È anche possibile aggiungere o modificare manualmente le regole per le app.

Come misura di sicurezza, si riceverà una notifica ogni volta che a una app potenzialmente dannosa viene impedito di accedere a Internet.

Bitdefender assegna automaticamente un tipo di rete a ogni connessione di rete che rileva. In base al tipo di rete, la protezione del firewall viene impostata sul livello appropriato per ogni connessione.

Per maggiori informazioni sulle impostazioni del firewall per ogni tipo di rete e su come modificare le impostazioni di rete, fare riferimento a Gestire le impostazioni di connessione (pagina 59).

Attivare o disattivare la protezione del firewall

Per attivare o disattivare la protezione del firewall:

1. Cliccare su **Protezione** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nel pannello **FIREWALL**, attivare o disattivare l'interruttore.

> **Attenzione**
> Dato che potrebbe esporre il dispositivo a connessioni non autorizzate, la disattivazione del firewall dovrebbe essere solo una misura temporanea. Riattivare il firewall il prima possibile.

Gestire le regole delle app

Per visualizzare e gestire le regole del firewall che controllano l'accesso delle applicazioni alle risorse di rete e a internet:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel pannello **FIREWALL**, clicca su **Impostazioni**.
3. Vai alla finestra **Accesso applicazione**.

Puoi visualizzare i programmi più recenti (processi) che sono passati da Bitdefender Firewall e la rete Internet a cui hai scelto di connetterti. Per vedere le regole create per una determinata app, cliccaci semplicemente sopra e poi clicca sul link **Vedi regole applicazione**. Si aprirà la finestra **Regole**.

Per ogni regola sono visualizzate le seguenti informazioni:

- **RETE** - I processi e i tipi di adattatori di rete (Casa / Ufficio, Pubblici o Tutti) a cui applicare la regola. Le regole sono create automaticamente per filtrare l'accesso alla rete o a Internet attraverso tutti gli adattatori. Di norma, le regole si applicano a ogni rete. Puoi creare nuove regole manualmente o modificare regole esistenti per filtrare l'accesso alla rete o a Internet di un'applicazione attraverso un adattatore specifico (ad esempio, un adattatore di rete wireless).
- **PROTOCOLLO** - il protocollo IP al quale si applica la regola. Di norma, le regole si applicano a ogni protocollo.
- **TRAFFICO** - La regola si applica in entrambe le direzioni, in entrata e in uscita.
- **PORTE** - Il protocollo della PORTA a cui si applica la regola. Di norma, le regole si applicano a tutte le porte.

- **IP** - Il protocollo Internet (IP) a cui si applica la regola. Di norma, le regole si applicano a qualsiasi indirizzo IP.
- **ACCESSO** - Se all'applicazione è permesso o vietato l'accesso alla rete o a Internet in base alle circostanze specificate.

Per modificare o eliminare le regole per la app selezionata, clicca sull'icona ⋯ .

- **Modifica regola** - Apre una finestra dove poter modificare la regola attuale.
- **Elimina regola** - Puoi scegliere di rimuovere il set attuale di regole della app selezionata.

Aggiungere regole per le app

Per aggiungere una regola per una app:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **FUOCO** riquadro, fare clic **Impostazioni**.
3. Nella finestra **Regole**, clicca su **Aggiungi regola**.

Qui puoi applicare le seguenti modifiche:

- **Applica questa regola a tutte le applicazioni.** Attiva questo interruttore per applicare la regola creata a tutte le app.
- **Percorso del programma.** Clicca su **SFOGLIA** e seleziona la app a cui si applica la regola.
- **Autorizzazione.** Seleziona una delle autorizzazioni disponibili:

Autorizzazione	Descrizione
Consenti	L'accesso alla rete / Internet dell'applicazione sarà autorizzato quando si verifichino le circostanze specificate.
Nega	L'accesso alla rete / Internet dell'applicazione sarà negato nelle circostanze specificate.

- **Tipo di rete.** Seleziona il tipo di rete a cui si applica la regola. Puoi modificare il tipo aprendo il menu a discesa **Tipo di rete** e selezionando uno dei tipi disponibili dall'elenco.

Tipo di rete	Descrizione
Qualsiasi rete	Consenti tutto il traffico tra il tuo dispositivo e gli altri dispositivi, indipendentemente dal tipo di rete.
Casa/Ufficio	Consenti tutto il traffico tra il tuo dispositivo e altri dispositivi nella rete locale.
Pubblico	Tutto il traffico viene filtrato.

- **Protocollo.** Seleziona dal menu il protocollo IP a cui sarà applicata la regola.
  - Se desideri che la regola venga applicata a tutti i protocolli, seleziona **Qualsiasi**.
  - Se desideri che la regola venga applicata a TCP, seleziona **TCP**.
  - Se desideri che la regola venga applicata a UDP, seleziona **UDP**.
  - Se vuoi che la regola venga applicata all'ICMP, seleziona **ICMP**.
  - Se vuoi che la regola venga applicata all'IGMP, seleziona **IGMP**.
  - Se vuoi che la regola venga applicata a GRE, seleziona **GRE**.
  - Se desideri applicare la regola a un protocollo specifico, digita il numero assegnato al protocollo che desideri filtrare nel campo vuoto da compilare.

    Nota
    I numeri del protocollo IP sono assegnati dall'Internet Assigned Numbers Authority (IANA). Puoi trovare l'elenco completo dei numeri di protocollo IP su http://www.iana.org/assignments/protocol-numbers.

- **Direzione**. Seleziona dal menu la direzione del traffico alla quale sarà applicata la regola.

Direzione	Descrizione
In uscita	La regola sarà applicata solo per il traffico in uscita.
In entrata	La regola sarà applicata solo per il traffico in entrata.
Entrambi	La regola sarà applicata in entrambe le direzioni.

Clicca sul pulsante **Impostazioni avanzate** nella parte inferiore della finestra per personalizzare le seguenti impostazioni:

- **Indirizzo locale personale.** Specifica l'indirizzo IP locale e la porta a cui sarà applicata la regola.
- **Indirizzo remoto personale.** Specifica l'indirizzo IP remoto e la porta a cui sarà applicata la regola.

Per rimuovere il set di regole attuali e ripristinare quelle predefinite, clicca su **Annulla regole** nella finestra **Regole**.

Gestire le impostazioni di connessione

Che tu voglia connetterti a Internet usando una rete Wi-Fi o un adattatore Ethernet, puoi configurare le opzioni da applicare per una navigazione sicura. Le opzioni tra cui puoi scegliere sono:

- **Dinamico** - Il tipo di rete sarà impostato automaticamente in base al profilo della rete a cui si è connessi, Casa/Ufficio o Pubblico. Quando ciò accade, saranno applicate solo le regole del Firewall per il tipo di rete specifico o quelle definite per tutti i tipi di rete.
- **Casa / Ufficio** - Il tipo di rete sarà sempre Casa / ufficio, ignorando il profilo della rete a cui si è connessi. Quando ciò accade, saranno applicate solo le regole del Firewall per la rete Casa/Ufficio o quelle definite per tutti i tipi di rete.
- **Pubblico** - Il tipo di rete sarà sempre Pubblico, ignorando il profilo della rete a cui si è connessi. Quando ciò accade, saranno applicate solo le regole del Firewall per la rete di tipo Pubblico o quelle definite per tutti i tipi di rete.

Per configurare i tuoi adattatori di rete:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **FUOCO** riquadro, fare clic **Impostazioni**.
3. Seleziona la finestra **Adattatori di rete**.
4. Seleziona le impostazioni che desideri applicare quando ti connetti ai seguenti adattatori:
   - Wi-Fi
   - Ethernet

Configurare le impostazioni avanzate

Per configurare le impostazioni avanzate del firewall:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **FUOCO** riquadro, fare clic **Impostazioni**.
3. Seleziona il **Impostazioni** finestra.

Possono essere configurate le seguenti funzionalità:

- **Protezione da port scan** - rileva e blocca i tentativi di scoprire quali porte sono aperte.
  Le scansioni delle porte vengono comunemente usate dagli hacker per scoprire quali porte sono aperte sul tuo dispositivo. Potrebbero quindi introdursi nel dispositivo, se trovassero una porta meno sicura o vulnerabile.
- **Modalità allerta** - Le allerte vengono mostrate ogni volta che una app prova a connettersi a Internet. Seleziona **Consenti** o **Blocca**. Quando la modalità Allerta è attivata, la funzione **Profili** viene disattivata automaticamente. La modalità Allerta può essere usata contemporaneamente con la **modalità Batteria**.
- **Consenti accesso al dominio di rete** - Consente o nega l'accesso a risorse e condivisioni definite dai controller di dominio.
- **Modalità invisibile** - Possibilità di essere rilevati da altri dispositivi. Clicca su **Modifica impostazioni modalità invisibile** per scegliere quando il dispositivo deve o non deve essere visibile agli altri dispositivi.
- **Comportamento applicazione predefinito** - Consente a Bitdefender di applicare impostazioni automatiche alle applicazioni senza regole definite. Clicca su **Modifica regole predefinite** per scegliere se applicare o no le impostazioni automatiche.
  - Automatico - L'accesso alle applicazioni sarà autorizzato o negato in base al Firewall automatico e alle regole utente.
  - Consenti - Le applicazioni che non hanno una regola del Firewall definita saranno autorizzate automaticamente.
  - Blocca - Le applicazioni che non hanno una regola del Firewall definita saranno bloccate automaticamente.

3.2.7. Vulnerabilità

Un passaggio importante nella protezione del dispositivo contro azioni e applicazioni dannose è mantenere aggiornato il sistema operativo e le

applicazioni che usi regolarmente. Inoltre, per prevenire l'accesso fisico non autorizzato al tuo dispositivo, è necessario configurare password sicure (ovvero non facilmente indovinabili) per ogni account utente di Windows e per le reti Wi-Fi a cui ti connetti.

Bitdefender offre due semplici modi per risolvere le vulnerabilità del tuo sistema:

- Puoi verificare le vulnerabilità del sistema e risolverle passaggio dopo passaggio, utilizzando l'opzione **Scansione vulnerabilità**.
- Usando il monitoraggio automatico delle vulnerabilità, puoi controllare e risolvere le vulnerabilità rilevate nella finestra **Notifiche**.

Ogni una o due settimane dovresti controllare e sistemare le vulnerabilità del sistema.

Controllare il sistema per rilevare vulnerabilità

Per rilevare le vulnerabilità del sistema, Bitdefender richiede una connessione a Internet attiva.

Per esaminare il sistema alla ricerca di vulnerabilità:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel pannello **VULNERABILITÀ**, clicca su **Apri**.
3. Nella scheda **Scansione vulnerabilità**, clicca su **Avvia scansione**, poi attendi che Bitdefender controlli l'eventuale presenza di vulnerabilità nel tuo sistema. Le vulnerabilità rilevate sono raggruppate in tre categorie:
   - **SISTEMA OPERATIVO**
     - **Sicurezza del sistema operativo**
       Impostazioni di sistema modificate che possono compromettere il dispositivo e i dati, come la mancata visualizzazione di avvisi quando i file eseguiti effettuano modifiche sul sistema senza la tua autorizzazione o quando dispositivi MTP, come telefoni o fotocamere, si connettono ed eseguono operazioni diverse a tua insaputa.
     - **Aggiornamenti critici di Windows**
       Viene mostrato un elenco degli aggiornamenti critici di Windows che non sono stati installati sul computer. Per consentire a Bitdefender di completare l'installazione potrebbe essere

necessario riavviare il sistema. Ricordati che potrebbe volerci un po' per installare gli aggiornamenti.

- **Account Windows poco sicuri**
  Puoi visualizzare l'elenco degli account utente di Windows configurati sul tuo dispositivo e il livello di protezione che le loro password forniscono. Puoi scegliere tra chiedere di cambiare la password al prossimo accesso o cambiare subito la password direttamente. Per impostare una nuova password per il sistema, seleziona **Cambia la password ora**.
  Per creare una password sicura, ti consigliamo di usare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

- **APPLICAZIONI**
  - **Sicurezza browser**
    Modifica delle impostazioni del dispositivo che consente l'esecuzione di file e programmi scaricati tramite Internet Explorer senza una convalida dell'integrità, che potrebbe comportare la compromissione del dispositivo.
  - **Aggiornamenti applicazioni**
    Per visualizzare maggiori informazioni sulla app che necessita di essere aggiornata, clicca sul nome nell'elenco.
    Se un'applicazione non è aggiornata, clicca su **Scarica nuova versione** per scaricare la versione più recente.

- **RETE**
  - **Rete e credenziali**
    Impostazioni di sistema modificate come l'eventuale connessione automatica a reti di hotspot aperte a tua insaputa o la mancata applicazione della cifratura sul traffico di un canale sicuro in uscita.
  - **Reti Wi-Fi e router**
    Per avere maggiori informazioni sul router e la rete wireless a cui hai effettuato la connessione, clicca sul suo nome nell'elenco. Se ti venisse consigliato di impostare una password più sicura per la rete domestica, assicurati di seguire le nostre istruzioni, in modo da poterti connettere senza preoccuparti della privacy.

Quando sono disponibili altri suggerimenti, segui le istruzioni fornite per assicurarti che la tua rete di casa sia sempre protetta dagli occhi indiscreti dei pirati informatici.

Usare il controllo automatico delle vulnerabilità

Bitdefender controlla regolarmente e in background il sistema alla ricerca di vulnerabilità, tenendo traccia dei problemi rilevati nella finestra {1}Notifiche{2}.

Per controllare e correggere i problemi rilevati:

1. Clic **Notifiche** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nella scheda **Tutto**, seleziona la notifica relativa alla scansione vulnerabilità.
3. Puoi visualizzare informazioni dettagliate sulle vulnerabilità del sistema rilevate. In base al problema, per risolvere una vulnerabilità specifica procedi come segue:
   - Se sono disponibili aggiornamenti di Windows, clicca su **Installa**.
   - Se gli aggiornamenti automatici di Windows sono disattivati, clicca su **Attiva**.
   - Se un'applicazione non è aggiornata, clicca su **Aggiorna ora** per trovare un link alla pagina web del distributore, da cui poter installare la versione più recente dell'applicazione.
   - Se un account utente Windows ha una password poco sicura, clicca su **Cambia password** per costringere l'utente a modificare la password al prossimo accesso, oppure cambiala direttamente. Per avere una password sicura, utilizza una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).
   - Se la funzione di esecuzione automatica di Windows è attivata, clicca su **Risolvi** per disattivarla.
   - Se il router che hai configurato ha una password poco sicura, clicca su **Cambia password** per accedere alla sua interfaccia da dove potrai impostarne una migliore.
   - Se la rete a cui ti connetti ha alcune vulnerabilità che potrebbero esporre il tuo sistema a eventuali rischi, clicca su **Cambia impostazioni Wi-Fi**.

Per configurare le impostazioni del monitoraggio vulnerabilità:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **VULNERABILITÀ** riquadro, fare clic **Aprire**.

   > **Importante**
   > Per essere avvertito automaticamente sulle vulnerabilità del sistema o delle applicazioni, mantieni l'opzione **Vulnerabilità** attivata.

3. Vai alla scheda **Impostazioni**.
4. Seleziona le vulnerabilità del sistema che desideri siano controllate regolarmente usando gli interruttori corrispondenti.

   Aggiornamenti di Windows

   Verifica se il sistema operativo Windows ha gli ultimi aggiornamenti di sicurezza di Microsoft.

   Aggiornamenti dell'applicazione

   Verifica se le applicazioni installate sul sistema sono aggiornate. Applicazioni datate possono essere sfruttate da software dannosi, rendendo il tuo PC vulnerabile agli attacchi esterni.

   Password dell'utente

   Verifica se le password degli account Windows e dei router configurati sul sistema sono più o meno facili da indovinare. Impostare password difficili da indovinare (password sicure) ostacola l'accesso al tuo sistema da parte degli hacker. Una password sicura include una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

   Esecuzione automatica

   Verifica lo stato della funzione di esecuzione automatica di Windows. Questa caratteristica consente alle applicazioni di essere avviate automaticamente da unità CD, DVD, USB o altri dispositivi esterni.

   Alcuni tipi di minacce usano l'esecuzione automatica per diffondersi automaticamente da supporti rimovibili al PC. Ecco perché si consiglia di disattivare questa funzione di Windows.

   Wi-Fi Security Advisor

   Verifica se la rete wireless di casa a cui sei connesso è sicura oppure no, e se ha eventuali vulnerabilità. Inoltre, verifica se la password del router domestico sia abbastanza sicura e ti consiglia come potenziarla.

La maggior parte delle reti wireless non cifrate sono poco sicure, cosa che consente agli occhi indiscreti dei pirati informatici di accedere alle tue attività personali.

Nota
Disattivando il monitoraggio di una determinata vulnerabilità, i relativi problemi non saranno più registrati nella finestra Notifiche.

Wi-Fi Security Advisor

Mentre sei in viaggio, lavorando in un bar o aspettando all'aeroporto, connettersi a una rete wireless pubblica per effettuare pagamenti, controllare le e-mail o gli account dei social network può essere la soluzione più rapida. Ma potrebbero esserci alcuni occhi indiscreti che cercheranno di ottenere i tuoi dati personali, sfruttando ogni falla nella rete per sottrarre informazioni.

E i dati personali sono password e nomi utenti che utilizzi per accedere ai tuoi account online, come e-mail, conti bancari, social network, ma anche i messaggi che invii.

In genere, le reti wireless pubbliche possono essere più pericolose in quando non richiedono una password per accedervi, e se lo fanno, la password potrebbe essere comunque disponibile per chiunque voglia connettersi. Inoltre, potrebbero esserci reti pericolose o honeypot, che rappresentano un bersaglio per i pirati informatici.

Bitdefender Wi-Fi Security Advisor ti fornisce informazioni su:

- **Reti Wi-Fi di casa**
- **Reti Wi-Fi ufficio**
- **Reti Wi-Fi pubbliche**

Attivare o disattivare le notifiche di Wi-Fi Security Advisor

Per attivare o disattivare le notifiche di Wi-Fi Security Advisor:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **VULNERABILITÀ** riquadro, fare clic **Aprire**.
3. Vai alla finestra **Impostazioni** e attiva o disattiva l'opzione **Wi-Fi Security Advisor**.

Configurare la rete Wi-Fi di casa

Per iniziare a configurare la tua rete di casa:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **VULNERABILITÀ** riquadro, fare clic **Aprire**.
3. Vai alla finestra **Wi-Fi Security Advisor** e clicca su **Wi-Fi di casa**.
4. Nella scheda **Wi-Fi di casa**, clicca su **SELEZIONA WI-FI DI CASA**.
   Viene mostrato un elenco con tutte le reti wireless a cui ti sei connesso finora.
5. Individua la tua rete di casa e clicca su **SELEZIONA**.

Se una rete di casa viene considerata poco sicura o non protetta, vengono mostrati alcuni suggerimenti per migliorarne la sicurezza.

Per rimuovere la rete wireless che hai impostato come rete di casa, clicca sul pulsante **RIMUOVI**.

Per aggiungere una nuova rete wireless come casa, clicca su **Seleziona nuovo Wi-Fi di casa**.

Configurare la rete Wi-Fi dell'ufficio

Per iniziare a configurare la tua rete dell'ufficio:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **VULNERABILITÀ** riquadro, fare clic **Aprire**.
3. Vai alla finestra **Wi-Fi Security Advisor**, clicca su **Wi-Fi ufficio**.
4. Nella scheda **Wi-Fi ufficio**, clicca su **SELEZIONA WI-FI UFFICIO**.
   Viene visualizzato un elenco con le reti wireless a cui sei connesso fino ad ora.
5. Individua la tua rete dell'ufficio e clicca su **SELEZIONA**.

Se una rete di ufficio viene considerata poco sicura o non protetta, vengono mostrati alcuni suggerimenti per migliorarne la sicurezza.

Per rimuovere la rete wireless che hai impostato come rete di ufficio, clicca su **RIMUOVI**.

Per aggiungere una nuova rete wireless come ufficio, clicca **Seleziona nuovo Wi-Fi dell'ufficio**.

Wi-Fi pubblica

Mentre sei connesso a una rete wireless non sicura o poco protetta, viene attivato il profilo Wi-Fi pubblica. Mentre esegui questo profilo, Bitdefender Ultimate Small Business Security viene configurato per eseguire automaticamente le seguenti impostazioni del programma:

- Advanced Threat Defense è attivato
- Il Firewall di Bitdefender è stato attivato e al tuo adattatore wireless verranno applicate le seguenti impostazioni:
  - Modalità invisibile - ATTIVATA
  - Tipo di rete - Pubblica
- Vengono attivate le seguenti impostazioni della Prevenzione minacce online:
  - Scansione web cifrata
  - Protezione dalle frodi
  - Protezione da phishing
- È disponibile un pulsante che apre Bitdefender Safepay™. In questo caso, la protezione degli Hotspot per le reti non sicure viene attivata in maniera predefinita.

Controllare le informazioni sulle reti Wi-Fi

Per controllare le informazioni sulle reti wireless in genere ti connetti a:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **VULNERABILITÀ** riquadro, fare clic **Aprire**.
3. Vai alla finestra **Wi-Fi Security Advisor**.
4. In base alle informazioni che ti servono, seleziona una delle tre schede, **Wi-Fi di casa**, **Wi-Fi ufficio** o **Wi-Fi pubblica**.
5. Clicca su **Mostra dettagli** accanto alla tua rete per trovare maggiori informazioni al riguardo.

Ci sono tre tipi di reti wireless filtrate per la loro importanza, ognuna indicata da un'icona specifica:

La rete Wi-Fi non è sicura - Indica che il livello di sicurezza della rete è bassa. Ciò significa che usarla è molto rischioso e non si

consiglia di effettuare pagamenti o controllare gli account bancari senza una protezione extra. In tali situazioni, ti consigliamo di usare Bitdefender Safepay™ con la protezione degli Hotspot attivata per le reti non sicure.

La rete Wi-Fi non è sicura - Indica che il livello di sicurezza della rete è moderato. Ciò significa che potrebbe avere delle vulnerabilità e non si consiglia di effettuare pagamenti o controllare gli account bancari senza una protezione extra. In tali situazioni, ti consigliamo di usare Bitdefender Safepay™ con la protezione degli Hotspot attivata per le reti non sicure.

La rete Wi-Fi è sicura - Indica che la rete che stai usando è sicura. In questo caso, puoi utilizzare dati sensibili per effettuare operazioni online.

Cliccando sul link **Mostra dettagli** nell'area di ciascuna rete, vengono mostrati i seguenti dettagli:

- **Protetto** - Qui puoi visualizzare se la rete selezionata è protetta oppure no. Reti non cifrate possono lasciare esposti i dati che utilizzi.
- **Tipo di cifratura** - Qui puoi visualizzare il tipo di cifratura utilizzato dalla rete selezionata. Alcuni tipi di cifratura potrebbero non essere sicuri. Inoltre, consigliamo vivamente di controllare le informazioni sul tipo di cifratura indicato, per assicurarsi di essere protetti durante la navigazione.
- **Canale/Frequenza** - Qui puoi visualizzare la frequenza del canale utilizzata dalla rete selezionata.
- **Complessità password** - Qui puoi visualizzare il livello di sicurezza della password. Ricordati che le reti dotate di password poco sicure rappresentano un facile bersaglio per i pirati informatici.
- **Tipo di accesso** - Qui puoi visualizzare se la rete selezionata è protetta da una password oppure no. Si consiglia vivamente di connettersi solo a reti dotate di password sicure.
- **Tipo di autenticazione** - Qui puoi visualizzare il tipo di autenticazione utilizzato dalla rete selezionata.

3.2.8. Protezione audio e video

Sempre più minacce sono sviluppate per accedere alle webcam e ai microfoni integrati. Per prevenire un accesso non autorizzato alla tua webcam e informarti su quali app non affidabili accedano al microfono del tuo dispositivo e quando, Bitdefender Video & Audio ha incluso:

- **Protezione webcam**
- **Controllo microfono**

Protezione webcam

Che gli hacker possano impossessarsi della tua webcam per spiarti non è più una novità e le soluzioni per proteggerla, come revocare i privilegi della app, disattivare la videocamera integrata o coprirla, non sono comunque molto pratiche. Per prevenire ulteriori tentativi di ottenere accesso alla tua privacy, Protezione webcam di Bitdefender monitora permanentemente le app che provano ad accedere alla tua videocamera e blocca quelle non indicate come affidabili.

Come misura di sicurezza sarai avvisato ogni volta che una app non affidabile tenterà di accedere alla tua telecamera.

Attivare o disattivare la Protezione webcam

1. Clicca su **Privacy** nel menu di navigazione nell'**interfaccia di Bitdefender**.
2. Nel pannello **PROTEZIONE AUDIO E VIDEO**, clicca su **Impostazioni**.
3. Ora vai alla finestra **Impostazioni** e attiva o disattiva l'interruttore corrispondente.

Configurare la Protezione webcam

Puoi configurare le regole da applicare quando una app cercherà di accedere alla tua videocamera, seguendo questi passaggi:

1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **PROTEZIONE VIDEO E AUDIO** riquadro, fare clic **Impostazioni**.
3. Vai al **Impostazioni** scheda.

Sono disponibili le seguenti opzioni:

Regole di blocco delle applicazioni

- **Blocca ogni accesso alla webcam** - Nessuna applicazione potrà accedere alla tua webcam.
- **Blocca l'accesso dei browser alla webcam** - A nessun browser web tranne Internet Explorer e Microsoft Edge sarà permesso accedere alla

tua webcam. A causa della procedura delle app di Windows Store di operare in un solo processo, Internet Explorer e Microsoft Edge non possono essere rilevati da Bitdefender come browser web e quindi sono esclusi da questa impostazione.

- **Imposta i permessi dell'applicazione in base alla scelta della community** - Se la maggior parte degli utenti di Bitdefender considera una app popolare come affidabile, allora il suo accesso alla webcam sarà impostato automaticamente su Consenti. Se una app popolare viene considerata pericolosa da molti utenti, allora l'accesso sarà impostato automaticamente su Bloccato.

Notifiche

- **Notifica quando applicazioni consentite si connettono alla webcam** - Sarai avvisato ogni volta che una app autorizzata accederà alla webcam.

Aggiungere app all'elenco della Protezione webcam

Le app che cercano di connettersi alla tua webcam vengono rilevate automaticamente e in base al loro comportamento e alle scelte della community, il loro accesso può essere consentito o negato. Tuttavia, puoi iniziare a configurare manualmente quale azione intraprendere, seguendo questi passaggi:

1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **PROTEZIONE VIDEO E AUDIO** riquadro, fare clic **Impostazioni**.
3. Vai alla finestra **Protezione webcam**.
4. Clicca sulla finestra **Aggiungi applicazione**.
5. Clicca sul link desiderato:
   - **Da Windows Store** - viene mostrato un elenco con tutte le app di Windows Store rilevate. Attiva gli interruttori accanto alle app che vuoi aggiungere all'elenco.
   - **Dalle tue app** - trova il file .exe che vuoi aggiungere all'elenco e clicca su **OK**.

Per visualizzare ciò che gli utenti di Bitdefender hanno scelto di fare con la app selezionata, clicca sull'icona .

In questa finestra compariranno le app che richiederanno l'accesso alla tua videocamera con l'indicazione dell'ultima attività avvenuta.

Sarai informato ogni volta che una delle app autorizzate viene bloccata dagli utenti di Bitdefender.

Per impedire l'accesso di una app aggiunta alla tua webcam, clicca sull'icona .

L'icona diventa , indicando che la app selezionata non avrà alcun accesso alla tua webcam.

Controllo microfono

Le app fraudolente possono accedere al tuo microfono integrato in modo silenzioso o in background senza il tuo consenso. Per renderti consapevole dei potenziali exploit dannosi, Controllo microfono di Bitdefender ti informerà di tali eventi. In questo modo, nessuna app sarà in grado di ottenere l'accesso al tuo microfono in tua assenza.

Attivare o disattivare Controllo microfono

1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **PROTEZIONE VIDEO E AUDIO** riquadro, fare clic **Impostazioni**.
3. Seleziona il **Impostazioni** finestra.
4. Nella finestra **Impostazioni**, attiva o disattiva l'interruttore **Controllo microfono**.

Configurare le notifiche per Controllo microfono

Per configurare quali notifiche debbano comparire quando le app proveranno a ottenere l'accesso al tuo microfono, segui questi passaggi:

1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **PROTEZIONE VIDEO E AUDIO** riquadro, fare clic **Impostazioni**.
3. Vai al **Impostazioni** finestra.

Notifiche

- **Informa quando un'applicazione prova ad accedere al microfono**

- **Ti informa quando i browser accedono al microfono**
- **Ti informa quando app non affidabili accedono al microfono**
- **Mostra una notifica in base alle scelte degli utenti di Bitdefender**

Aggiungere app all'elenco di Controllo microfono

Le app che proveranno a connettersi al tuo microfono saranno rilevate automaticamente e aggiunte all'elenco delle notifiche. Tuttavia, puoi configurare manualmente se mostrare o no una notifica, seguendo questi passaggi:

1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **PROTEZIONE VIDEO E AUDIO** riquadro, fare clic **Impostazioni**.
3. Vai alla finestra **Protezione audio**.
4. Clic **Aggiungi applicazione** finestra.
5. Fare clic sul collegamento desiderato:
   - **Da Windows Store** - viene visualizzato un elenco con le app di Windows Store rilevate. Attiva gli interruttori accanto alle app che desideri aggiungere all'elenco.
   - **Dalle tue app** - vai al file .exe che desideri aggiungere all'elenco, quindi fai clic su **OK**.

Per visualizzare ciò che gli utenti di Bitdefender hanno scelto di fare con l'app selezionata, fai clic su icona.

In questa finestra compariranno le app che richiederanno l'accesso al tuo microfono con l'indicazione dell'ultima attività avvenuta.

Per interrompere la ricezione di notifiche relative all'attività di un'app aggiunta, clicca sull'icona .

L'icona diventa , indicando che nessuna notifica di Bitdefender sarà mostrata quando la app selezionata cercherà di accedere al tuo microfono.

3.2.9. Risanamento da ransomware

Bitdefender Ransomware Remediation esegue un backup dei tuoi file, come documenti, immagini, video o musica per assicurarsi che siano

protetti dall'essere danneggiati o persi in caso di cifratura di ransomware. Ogni volta che viene rilevato un attacco ransomware, Bitdefender bloccherà tutti i processi coinvolti nell'attacco e avvierà il processo di risanamento. In questo modo, potrai recuperare i contenuti dei tuoi interi file senza pagare alcun riscatto.

Attivare o disattivare il Risanamento da ransomware

Per attivare o disattivare il Risanamento da ransomware:

1. 1. Clicca su **Protezione** nel menu di navigazione nell'**interfaccia di Bitdefender**.
2. Nel pannello **RISANAMENTO DA RANSOMWARE**, attiva o disattiva l'interruttore.

> **Nota**
> Per assicurarsi che i tuoi file siano protetti dai ransomware, ti consigliamo di tenere attivata la funzionalità Risanamento da ransomware.

Attivare o disattivare il ripristino automatico

Il ripristino automatico si assicura che i tuoi file vengano ripristinati automaticamente nel caso di una cifratura da ransomware.

Per attivare o disattivare il ripristino automatico:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel pannello **RISANAMENTO DA RANSOMWARE**, clicca su **Gestisci**.
3. Nella finestra Impostazioni, attiva o disattiva l'interruttore **Ripristino automatico**.

Visualizzare i file che sono stati ripristinati automaticamente

Quando l'opzione **Ripristino automatico** è attiva, Bitdefender ripristinerà automaticamente i file che sono stati cifrati da un ransomware. Quindi potrai avere un'esperienza senza preoccupazioni, sapendo che i tuoi file sono al sicuro.

Per visualizzare i file che sono stati ripristinati automaticamente:

1. Clic **Notifiche** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nella scheda **Tutti**, seleziona la notifica sul più recente comportamento ransomware risanato, e clicca su **File ripristinati**.

Viene mostrato l'elenco con i file ripristinati. Qui puoi anche visualizzare il percorso in cui i tuoi file sono stati memorizzati.

Ripristinare file cifrati manualmente

Nel caso dovessi ripristinare manualmente i file che sono stati cifrati da un ransomware, segui questi passaggi:

1. Clic **Notifiche** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nella scheda **Tutti**, seleziona la notifica sul più recente comportamento ransomware rilevato, e clicca su **File cifrati**.
3. Viene mostrato l'elenco con i file cifrati.
   Clicca su **Ripristina file** per continuare.
4. Nel caso l'intero processo di ripristino o una parte fallisse, dovrai scegliere il percorso in cui salvare i file decifrati. Clicca su **Ripristina l'ubicazione** e scegli un percorso sul tuo PC.
5. Apparirà una finestra di conferma.
   Clicca su **Fine** per terminare il processo di ripristino.

I file con le seguenti estensioni possono essere ripristinati nel caso fossero stati cifrati:

.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;

Aggiungere applicazioni alle eccezioni

Puoi configurare le regole delle eccezioni per le app affidabili, in modo che la funzionalità Risanamento da ransomware non le blocchi, nel caso avessero comportamenti simili a un ransomware.

Per aggiungere app all'elenco delle eccezioni di Risanamento da ransomware:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **RISOLUZIONE DEL RANSOMWARE** riquadro, fare clic **Maneggio**.

3. Vai alla finestra **Eccezioni** e clicca su **+Aggiungi un'eccezione**.

3.2.10. Cryptomining Protection

Cos'è la protezione dal cryptomining?

Con l'uso del cryptomining gli aggressori possono trarre vantaggi finanziari senza sostenere i costi associati e le conseguenze legali.

La funzionalità Cryptomining Protection di Bitdefender difende i computer Windows dalla crescente minaccia di attività di cryptomining non autorizzate, una pratica dannosa che sfrutta le risorse e l'elettricità di un utente per generare entrate per gli aggressori.

> **Nota**
> La protezione dal cryptomining si basa su:
>
> - Scudo di Bitdefender
> - Prevenzione degli attacchi web
>
> Per poter eseguire la protezione Cryptomining, è necessario che entrambe queste due funzionalità siano abilitate.

Abilitazione della protezione dal cryptomining

La funzionalità Protezione dal cryptomining si trova nella scheda Protezione.

Per abilitarlo, è sufficiente attivare l'interruttore corrispondente.

> **Nota**
> La protezione dal cryptomining è disabilitata per impostazione predefinita, garantendo che gli utenti abbiano il controllo sulla sua attivazione.

Modalità di funzionamento

Una volta abilitata, la funzionalità Cryptomining Protection opera in 2 stati distinti, ciascuno adattato alle preferenze dell'utente:

1. **Blocca tutte le attività di Cryptomining.** (blocca automaticamente qualsiasi attività di crypto mining e intraprende le azioni necessarie per prevenire ulteriori tentativi non autorizzati)
   Questa modalità è ideale per gli utenti che non hanno intenzione di impegnarsi in attività di crypto-mining.

2. **Rileva attività di Cryptomining.** (emette avvisi ogni volta che viene rilevata un'attività di crypto mining e richiede l'input dell'utente per determinare l'azione appropriata)
   Questa modalità è adatta agli utenti attivamente coinvolti nelle proprie attività di crypto-mining ma che desiderano monitorare e controllare eventuali tentativi non autorizzati.

Gestisci le eccezioni

È possibile specificare eccezioni per le applicazioni, con la possibilità aggiuntiva di definire righe di comando specifiche. Tuttavia, è possibile stabilire eccezioni anche senza la necessità di fornire parametri così dettagliati, offrendo un equilibrio tra personalizzazione e semplicità.

Per aggiungere un'eccezione:

1. Clic**Protezione**nel menu a sinistra nell'interfaccia di Bitdefender.
2. Nel**Protezione dal cryptomining**riquadro, fare clic su**Impostazioni**.
3. Clicca il**Gestisci le eccezioni**opzione.
4. Quindi, fare clic su**Aggiungi un'eccezione**pulsante.
5. Verrà aperta una nuova finestra. Puoi escludere manualmente applicazioni, URL e indirizzi IP.
6. Infine, fai clic**Salva**. La nuova regola viene aggiunta all'elenco delle eccezioni di Cryptomining Protection.

> **Nota**
> Per rimuovere un'eccezione, fai semplicemente clic sull'icona del cestino accanto ad essa.

3.2.11. Anti-tracker

Molti siti web che visiti utilizzano tracker per ottenere informazioni sul tuo comportamento, per condividerle con aziende di terze parti o mostrarti pubblicità più rilevanti per te. Quindi, i possessori dei siti web guadagnano per essere in grado di fornirti contenuti gratuitamente o continuare a operare. Oltre a raccogliere informazioni, i tracker possono rallentare la tua esperienza di navigazione oppure occupare la tua banda.

Con l'estensione anti-tracker di Bitdefender Anti-tracker attivata nel tuo browser web, puoi evitare la tracciatura così che i tuoi dati restino privati

mentre navighi online, velocizzando il tempo necessario per caricare i siti web.

L'estensione di Bitdefender è compatibile con i seguenti browser web:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

I tracker che rileviamo vengono raggruppati nelle seguenti categorie:

- **Pubblicità** - Usati per analizzare il traffico del sito web, il comportamento dell'utente o gli schemi di traffico dei visitatori.
- **Interazione del cliente** - Usati per misurare l'interazione dell'utente con diverse forme di input, come chat o supporto.
- **Essenziali** - Usati per monitorare funzionalità critiche della pagina web.
- **Analisi dei siti** - Usati per raccogliere dati relativi all'uso della pagina web.
- **Social media** - Usati per monitorare il pubblico dei social, attività e coinvolgimento degli utenti con diverse piattaforme di social media.

Interfaccia anti-tracker

Quando l'estensione Bitdefender Anti-tracker viene attivata, compare l'icona accanto alla barra di ricerca nel tuo browser web. Ogni volta che visiti un sito web, sull'icona si può notare un contatore, che indica i tracker rilevati e bloccati. Per maggiori dettagli sui tracker bloccati, clicca sull'icona per aprire l'interfaccia. Accanto al numero dei tracker bloccati, puoi visualizzare il tempo richiesto per il caricamento della pagina e le categorie di appartenenza dei tracker rilevati. Per vedere l'elenco dei siti web che stanno usando la tracciatura, clicca sulla categoria desiderata.

Per impedire a Bitdefender di bloccare i tracker sul sito web che stai attualmente visitando, clicca su **Sospendi la protezione su questo sito web**. Questa applicazione si applica solo finché il sito web sarà aperto e sarà riportata allo stato iniziale quando lo chiuderai.

Per consentire ai tracker di una determinata categoria di monitorare le tue attività, clicca sull'attività desiderata e poi sul pulsante corrispondente. Se cambiassi idea, clicca sullo stesso pulsante un'altra volta.

Disattivare Bitdefender Anti-tracker off

Per disattivare Bitdefender Anti-tracker:

- Dal tuo browser web:
  1. Apri il tuo browser web.
  2. Clicca sull'icona accanto alla barra dell'indirizzo nel tuo browser web.
  3. Clicca sull'icona nell'angolo in alto a destra.
  4. Usa l'interruttore corrispondente per disattivarlo.
     L'icona Bitdefender diventa grigia.
- Dall'interfaccia di Bitdefender:
  1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
  2. Nel pannello **ANTI-TRACKER**, clicca su **Impostazioni**.
  3. Accanto al browser web per cui vuoi disattivare l'estensione, disattiva l'interruttore corrispondente.

Consentire a un sito web di essere monitorato

Se vorresti essere monitorato mentre visiti un determinato sito web, puoi aggiungere questo indirizzo alle eccezioni nel seguente modo:

1. Apri il browser web.
2. Clicca sull'icona accanto alla barra di ricerca.
3. Clicca il icona nell'angolo in alto a destra.
4. Se sei sul sito web che vuoi aggiungere alle eccezioni, clicca su **Aggiungi questo sito web all'elenco**.
   Se vuoi aggiungere un altro sito web, inserisci il suo indirizzo nel campo corrispondente, e clicca su .

3.2.12. Safepay: sicurezza per le transazioni online

Il computer sta diventando rapidamente lo strumento principale per fare acquisti ed eseguire transazioni bancarie online. Pagare bollette, trasferire denaro, acquistare praticamente tutto ciò che puoi immaginare non è mai stato così semplice e veloce.

Tutto ciò richiede l'invio su Internet di dati personali, come numero di conto e carta di credito, password e altre tipologie di informazioni private, in altre parole esattamente quel tipo di informazioni a cui gli hacker sono particolarmente interessati. Infatti, non conoscono soste nei loro sforzi per sottrarre tali informazioni, perciò non si è mai troppo prudenti sulla necessità di proteggere le proprie transazioni online.

Bitdefender Safepay™ è prima di tutto un browser protetto, un ambiente isolato che è stato progettato per mantenere le tue operazioni bancarie, i tuoi acquisti e altri tipi di transazioni online assolutamente sicuri e privati.

Bitdefender Safepay™ offre le seguenti funzioni:

- Blocca l'accesso al proprio desktop, impedendo qualsiasi tentativo di catturare delle immagini del proprio schermo.
- È dotato di una tastiera virtuale che, quando viene utilizzata, rende impossibile agli hacker rilevare la combinazione di tasti premuta.
- È completamente indipendente dagli altri browser.
- È dotato di una protezione integrata degli hotspot da utilizzare quando il dispositivo è connesso a reti Wi-Fi non protette.
- Supporta i segnalibri e consente di navigare nei propri siti bancari/commerciali preferiti.
- Non è limitato alle operazioni bancarie e lo shopping online. Infatti, è possibile aprire qualsiasi sito web in Bitdefender Safepay™.

Utilizzare Bitdefender Safepay™

Di norma, Bitdefender rileva quando navighi in un sito bancario o di acquisti online su qualsiasi browser nel tuo dispositivo e ti chiederà di aprirlo in Bitdefender Safepay™.

Per accedere all'interfaccia principale di Bitdefender Safepay™, usa uno dei seguenti metodi:

- Dall'**interfaccia di Bitdefender**:
  1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
  2. Nel pannello **SAFEPAY**, clicca su **Impostazioni**.
  3. Nella finestra **Safepay**, clicca su **Lancia Safepay**.

- Da Windows:
  - In **Windows 7**:
    1. Clicca su **Avvia** e vai su **Tutti i programmi**.
    2. Clicca su **Bitdefender**.
    3. Clicca su **Bitdefender Safepay™**.
  - In **Windows 8** e **Windows 8.1**:
    Localizza Bitdefender Safepay™ nella schermata di Windows Start (per esempio, puoi iniziare digitando “Bitdefender Safepay™” direttamente nella schermata di Start) e poi clicca sulla relativa icona.
  - In **Windows 10** e **Windows 11**:
    Digita "Bitdefender Safepay™" nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona.

Se sei abituato a utilizzare i browser per Internet, non avrai alcun problema con Bitdefender Safepay™, poiché appare e si comporta proprio come un normale browser:

- Inserisci gli URL che desideri utilizzare nella barra degli indirizzi.
- aggiungi schede per visitare più siti web nella finestra di Bitdefender Safepay™ cliccando su ⊞.
- naviga avanti e indietro e aggiorna le pagine usando ← → ↻ rispettivamente.
- accedi alle **Impostazioni** di Bitdefender Safepay™ cliccando e scegliendo **Impostazioni**.
- gestisci i tuoi **preferiti** cliccando ☆ accanto alla barra dell'indirizzo.
- apri la tastiera virtuale cliccando su .
- aumenta o riduci la dimensione del browser, premendo contemporaneamente **Ctrl** e i tasti **+/-** nel tastierino numerico.
- visualizza informazioni sul tuo prodotto Bitdefender, cliccando su ⋯ e selezionando **Informazioni**.
- stampa informazioni importanti cliccando su ⋯ e scegliendo **Stampa**.

> **Nota**
> Per alternarti tra Bitdefender Safepay™ e il desktop di Windows, premi i tasti **Alt+Tab** o clicca sull'opzione **Passa al desktop** nel lato superiore sinistro della finestra.

Configurare le impostazioni

Clicca su ⋯ e seleziona **Impostazioni** per configurare Bitdefender Safepay™:

Applica le regole di Bitdefender Safepay per i domini a cui si accede

I siti web che hai aggiunto ai **Preferiti** con l'opzione **Apri automaticamente in Safepay** attivata compariranno qui. Se vuoi bloccare automaticamente l'apertura con Bitdefender Safepay™ di un sito web nell'elenco, clicca × accanto alla voce desiderata nella colonna **Rimuovi**.

Blocca pop-up

Puoi scegliere di bloccare le finestre pop-up, cliccando sull'interruttore corrispondente.

Puoi anche creare un elenco di siti web in cui consentire le finestre pop-up. L'elenco dovrebbe contenere solo siti web di cui ti fidi completamente.

Per aggiungere un sito all'elenco, inserisci il suo indirizzo nel campo corrispondente e clicca su **Aggiungi dominio**.

Per rimuovere un sito web dall'elenco, seleziona la X corrispondente alla voce desiderata.

Gestisci plugin

Puoi scegliere se desideri attivare o disattivare determinati plugin in Bitdefender Safepay™.

Gestisci certificati

Puoi importare i certificati dal sistema a un archivio di certificati.

Clicca su **IMPORTA** e segui la procedura guidata per utilizzare i certificati in Bitdefender Safepay™.

Usa tastiera virtuale

La tastiera virtuale comparirà automaticamente quando viene selezionato un campo dove inserire la password.

Usa l'interruttore corrispondente per attivare o disattivare la funzione.

Conferma di stampa

Attiva questa opzione se desideri dare la tua conferma prima che il processo di stampa inizi.

Gestire i segnalibri

Se hai disattivato la rilevazione automatica di alcuni o di tutti i siti web, o semplicemente Bitdefender non rileva determinati siti, puoi aggiungere dei segnalibri a Bitdefender Safepay™ in modo da poter lanciare rapidamente i tuoi siti web preferiti in futuro.

Segui questi semplici passaggi per aggiungere un URL ai segnalibri di Bitdefender Safepay™:

1. Clicca su ⋯ e seleziona **Preferiti** per aprire la pagina dei Preferiti.

   > **Nota**
   > Di norma, la pagina dei Segnalibri viene aperta all'avvio di Bitdefender Safepay™.

2. Clicca sul pulsante **+** per aggiungere un nuovo segnalibro.
3. Inserisci l'URL e il nome del segnalibro, poi clicca su **CREA**. Seleziona l'opzione **Apri automaticamente in Safepay**, se desideri che la pagina salvata nei segnalibri si apra in Bitdefender Safepay™ ogni volta che vi accedi. L'URL viene aggiunto anche nell'elenco dei domini alla pagina delle impostazioni.

Disattivare le notifiche di Safepay

Quando viene rilevato un sito bancario, il prodotto Bitdefender è impostato per avvisarti tramite una finestra pop-up.

Per disattivare le notifiche di Safepay:

1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **SAFEPAY** riquadro, fare clic **Impostazioni**.
3. Nella finestra **Impostazioni**, disattiva l'interruttore accanto a **Notifiche di Safepay**.

3.2.13. Dispositivo antifurto

Il furto di laptop è un problema importante che colpisce allo stesso modo individui e organizzazioni. Ancor più che perdere l'hardware stesso, i dati persi con esso possono causare danni significativi, sia finanziari che emotivi.

Tuttavia, poche persone adottano le misure adeguate per proteggere i propri importanti dati personali, aziendali e finanziari in caso di furto o smarrimento.

Bitdefender Anti-Theft ti aiuta a essere meglio preparato per un tale evento consentendoti di localizzare o bloccare in remoto il tuo laptop e persino di cancellare tutti i dati da esso, nel caso dovessi separarti dal tuo laptop contro la tua volontà.

Per utilizzare le funzionalità di Antifurto, devono essere soddisfatti i seguenti prerequisiti:

- I comandi possono essere inviati solo dall'account Bitdefender.
- Il laptop deve essere connesso a Internet per ricevere i comandi.

Le funzionalità Antifurto funzionano nel modo seguente:

Individuare

Visualizza la posizione del tuo dispositivo su Google Maps.

La precisione della posizione dipende da come Bitdefender è in grado di determinarla. La posizione è determinata entro decine di metri se il Wi-Fi è abilitato sul tuo laptop e ci sono reti wireless nel suo raggio d'azione.

Se il laptop è connesso a una LAN cablata senza una posizione Wi-Fi disponibile, la posizione verrà determinata in base all'indirizzo IP, che è notevolmente meno preciso.

Mettere in guardia

Invia un avviso remoto sul dispositivo.

La funzione è disponibile solo su dispositivi mobili.

Serratura

Blocca il tuo laptop e imposta un PIN di 4 cifre per sbloccarlo. Quando invii il **Serratura** comando, il sistema si riavvia e l'accesso a Windows è possibile solo dopo aver inserito il PIN impostato.

Se vuoi che Bitdefender scatti delle foto a chi tenta di accedere al tuo laptop, seleziona la casella di controllo corrispondente. Le foto scattate vengono scattate utilizzando la fotocamera frontale e visualizzate insieme al timestamp nella dashboard di Antifurto. Verranno salvate solo le due foto più recenti.

Questa azione è disponibile solo per i laptop dotati di fotocamera frontale.

Pulire

Rimuovi tutti i dati dal tuo sistema. Quando invii il **Pulire** comando, il laptop si riavvia e i dati su tutte le partizioni del disco rigido vengono cancellati.

Mostra IP

Visualizza l'ultimo indirizzo IP per il dispositivo selezionato. Clic **MOSTRA IP** per renderlo visibile.

Anti-Theft viene attivato dopo l'installazione ed è possibile accedervi esclusivamente tramite il tuo account Bitdefender da qualsiasi dispositivo connesso a Internet, ovunque.

Utilizzo delle funzionalità Antifurto

Per accedere alle funzionalità Antifurto, utilizzare una delle seguenti possibilità:

- Dall'interfaccia principale di Bitdefender:
  1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
  2. Clic **VAI AL CENTRALE**.
     Verrai reindirizzato alla pagina di Bitdefender Central. Assicurati di aver effettuato l'accesso con le tue credenziali.
  3. Nella finestra di Bitdefender Central che si apre, clicca sulla scheda del dispositivo desiderato, quindi seleziona **Antifurto**.

- Su qualsiasi dispositivo con accesso a Internet:
  1. Apri un browser Web e vai a: https://central.bitdefender.com.
  2. Accedi al tuo account Bitdefender utilizzando il tuo indirizzo e-mail e la password.
  3. Seleziona il **I miei dispositivi** pannello.

4. Fare clic sulla scheda del dispositivo desiderato, quindi selezionare **Antifurto**.
5. Seleziona la funzione che desideri utilizzare:
   Individuare - visualizzare la posizione del tuo dispositivo su Google Maps.
   Mostra IP - visualizzare l'ultimo indirizzo IP del tuo dispositivo.
   Mettere in guardia - inviare un avviso sul dispositivo.
   Serratura - blocca il tuo laptop e imposta un codice PIN per sbloccarlo.
   Pulire - cancella tutti i dati dal tuo laptop.

   Importante
   Dopo aver cancellato i dati da un dispositivo, tutte le funzionalità di Antifurto smettono di funzionare.

3.3. Utilità

3.3.1. Profili

Le attività quotidiane, guardare un film o usare un videogioco, possono causare rallentamenti al sistema, in particolare se sono eseguite contemporaneamente ai processi di aggiornamento di Windows o alle attività di manutenzione. Con Bitdefender, ora puoi scegliere e applicare il tuo profilo preferito, che adatta le impostazioni del sistema in modo da incrementare le prestazioni di determinate applicazioni installate.

Bitdefender offre i seguenti profili:

- Profilo di lavoro
- Profilo del film
- Profilo di gioco
- **Profilo Wi-Fi pubblico**
- Profilo modalità batteria

Se decidi di non utilizzare i **Profili**, viene attivato un profilo predefinito chiamato **Standard**, che non offre particolari ottimizzazioni al tuo sistema.

In base alle tue attività, vengono applicate le seguenti impostazioni del prodotto quando si attivano i profili Lavoro, Film o Gioco:

- Tutti gli allarmi e pop-up BitDefender sono disabilitati.
- L'Aggiornamento automatico è stato ritardato.
- Le scansioni programmate sono rinviate.
- Il modulo Antispam è attivato.
- **Ricerca sicura** è disattivata.
- Le notifiche sulle offerte speciali sono disattivate.

In base alle tue attività, vengono applicate le seguenti impostazioni di sistema quando si attivano i profili Lavoro, Film o Gioco:

- Gli Aggiornamenti automatici di Windows sono stati ritardati.
- Gli avvisi e le finestre pop-up di Windows sono state disattivate.
- I programmi in background non necessari sono stati sospesi.
- Gli effetti visivi sono stati regolati per ottenere le migliori prestazioni.
- Le attività di manutenzione sono state ritardate.
- Le impostazioni di alimentazione sono state regolate.

Mentre è in esecuzione nel profilo Rete Wi-Fi pubblica, Bitdefender Ultimate Small Business Security viene impostato automaticamente per applicare le seguenti impostazioni del programma:

- La protezione avanzata dalle minacce è attivata
- Bitdefender Firewall è attivo e le seguenti impostazioni vengono applicate al tuo adattatore wireless:
  - Modalità invisibile - ATTIVA
  - Tipo di rete - Pubblico
- Le seguenti impostazioni di Prevenzione delle minacce online sono attivate:
  - Scansione Web crittografata
  - Protezione contro le frodi
  - Protezione contro il phishing

Profilo Lavoro

Eseguire più attività, come inviare e-mail, tenere una comunicazione video con alcuni colleghi in remoto o lavorare con applicazioni grafiche può

influenzare notevolmente le prestazioni del sistema. Il profilo Lavoro è stato progettato per aiutarti a migliorare la tua efficienza lavorativa, disattivando alcuni servizi e attività di manutenzione in background.

Configurare il profilo Lavoro

Per configurare le azioni da intraprendere quando sei nel profilo Lavoro:

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Profili** scheda, fare clic **Impostazioni**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Lavoro.
4. Seleziona le regolazioni del sistema da applicare, spuntando le seguenti opzioni:
   - Aumenta le prestazioni delle applicazioni
   - Ottimizza le impostazioni del prodotto per il profilo Lavoro
   - Rimanda i programmi in background e le attività di manutenzione
   - Posticipa gli aggiornamenti automatici di Windows
5. Clicca su **SALVA** per salvare le modifiche e chiudere la finestra.

Aggiungere manualmente le applicazioni all'elenco del profilo Lavoro

Se Bitdefender non attiva automaticamente il Profilo Lavoro quando lanci una determinata app lavorativa, puoi aggiungere manualmente la app nell'**Elenco applicazioni Lavoro**.

Per aggiungere manualmente le app all'Elenco applicazioni lavoro:

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Profili** scheda, fare clic **Impostazioni**.
3. Clicca il **CONFIGURA** pulsante dall'area Profilo di lavoro.
4. Nella finestra **Impostazioni Profilo Lavoro**, clicca su **Elenco applicazioni**.
5. Clicca su **AGGIUNGI**.
   Comparirà una nuova finestra. Cerca il file eseguibile della app, selezionalo e clicca su **OK** per aggiungerlo all'elenco.

Profilo Film

Visualizzare contenuti video di alta qualità, come film in alta definizione, richiede molte risorse di sistema. Il profilo Film regola le impostazioni del sistema e del prodotto, per consentirti di visualizzare il film senza interruzioni e rallentamenti.

Configurare il profilo Film

Per configurare le azioni da intraprendere quando sei nel profilo Film:

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Profili** scheda, fare clic **Impostazioni**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Film.
4. Scegli le regolazioni del sistema che desideri vengano applicate selezionando le seguenti opzioni:
   - Aumenta le prestazioni dei lettori multimediali
   - Ottimizza le impostazioni del prodotto per il profilo Film
   - Rinvia i programmi in background e le attività di manutenzione
   - Rinvia gli aggiornamenti automatici di Windows
   - Modifica le impostazioni dei consumi energetici per i film
5. Clic **SALVA** per salvare le modifiche e chiudere la finestra.

Aggiungere manualmente i lettori multimediali all'elenco del profilo Film

Se lanciando una determinata app per la riproduzione di video, Bitdefender non attiva automaticamente il profilo Film, puoi aggiungere manualmente l'applicazione nell'**Elenco applicazioni film**.

Per aggiungere manualmente lettori video all'elenco applicazioni film nel profilo Film:

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Profili** scheda, fare clic **Impostazioni**.
3. Clicca il **CONFIGURA** pulsante dall'area Profilo film.
4. Nella finestra **Impostazioni Profilo Film**, clicca su **Elenco lettori**.

5. Clic **AGGIUNGERE**.
   Viene visualizzata una nuova finestra. Passare al file eseguibile dell'app, selezionarlo e fare clic **OK** per aggiungerlo all'elenco.

Profilo Gioco

Per usufruire di un'esperienza di gioco senza interruzioni, bisogna ridurre i caricamenti del sistema e diminuire i rallentamenti. Utilizzando euristiche comportamentali con un elenco di giochi conosciuti, Bitdefender è in grado di rilevare automaticamente i giochi in esecuzione e ottimizzare le risorse del sistema, in modo da usufruire di una perfetta esperienza di gioco.

Configurare il profilo Gioco

Per configurare le azioni da intraprendere quando sei nel profilo Gioco:

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Profili** scheda, fare clic **Impostazioni**.
3. Clicca sul pulsante **Configura** nella sezione del Profilo gioco.
4. Scegli le regolazioni del sistema che desideri vengano applicate selezionando le seguenti opzioni:
   - Aumenta le prestazioni con i giochi
   - Ottimizza le impostazioni del prodotto per il profilo Gioco
   - Rinvia i programmi in background e le attività di manutenzione
   - Rinvia gli aggiornamenti automatici di Windows
   - Modifica le impostazioni dei consumi energetici per i giochi
5. Clic **SALVA** per salvare le modifiche e chiudere la finestra.

Aggiungere manualmente giochi all'Elenco dei giochi

Se lanciando una determinata applicazione o un videogioco, Bitdefender non attiva automaticamente il profilo Gioco, puoi aggiungere manualmente l'applicazione nell'**Elenco applicazioni giochi**.

Per aggiungere manualmente i giochi all'Elenco applicazioni giochi nel profilo Gioco:

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.

2. Nel **Profili** scheda, fare clic **Impostazioni**.
3. Clicca il **Configura** pulsante dall'area Profilo di gioco.
4. Nella finestra **Impostazioni Profilo Gioco**, clicca su **Elenco giochi**.
5. Clic **AGGIUNGERE**.
   Comparirà una nuova finestra. Cerca il file eseguibile del gioco, selezionalo e clicca su **OK** per aggiungerlo all'elenco.

Profilo rete Wi-Fi pubblica

Inviare e-mail, inserire credenziali riservate o fare shopping online mentre si è connessi a reti wireless non sicure potrebbe mettere a rischio i tuoi dati personali. Il profilo Rete Wi-Fi pubblica regola le impostazioni del prodotto per darti la possibilità di effettuare i pagamenti online e utilizzare ogni informazione riservata in un ambiente protetto.

Configurare il profilo Rete Wi-Fi pubblica

Per configurare Bitdefender per applicare le impostazioni del prodotto mentre si è connessi a una rete wireless non sicura:

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Profili** scheda, fare clic **Impostazioni**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Rete Wi-Fi pubblica.
4. Mantieni attivata l'opzione **Modifica le impostazioni del prodotto per incrementare la protezione quando ci si connette a una rete Wi-Fi pubblica poco sicura**.
5. Clic **Salva**.

Profilo Modalità Batteria

Il profilo Modalità Batteria è stato progettato appositamente per gli utenti di computer portatili e tablet. Il suo scopo è ridurre al minimo l'impatto del sistema e di Bitdefender sul consumo energetico, quando il livello di carica della batteria è inferiore a quello predefinito o selezionato.

Configurare il profilo Modalità Batteria

Per configurare il profilo Modalità Batteria:

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Profili** scheda, fare clic **Impostazioni**.
3. Clicca sul pulsante **Configura** nella sezione del Profilo Modalità Batteria.
4. Seleziona le regolazioni del sistema da applicare, spuntando le seguenti opzioni:
   - Ottimizza le impostazioni del prodotto per la modalità Batteria.
   - Rimanda i programmi in background e le attività di manutenzione.
   - Posticipa aggiornamenti automatici di Windows.
   - Modifica le impostazioni dei consumi energetici per la modalità Batteria.
   - Disattiva i dispositivi esterni e le porte di rete.
5. Clic **SALVA** per salvare le modifiche e chiudere la finestra.

Digita un valore valido nella casella numerica o selezionane uno usando le frecce su e giù per specificare quando il sistema deve iniziare a operare in modalità Batteria. Di norma, la modalità si attiva quando il livello di carica della batteria è inferiore al 30%.

Quando Bitdefender funziona con il profilo Modalità Batteria, vengono applicate le seguenti impostazioni del prodotto:

- L'aggiornamento automatico di Bitdefender è stato rinviato.
- Le scansioni pianificate vengono posticipate.

Bitdefender rileva quando il portatile sta funzionando con la batteria e in base al livello di carica della batteria, passa automaticamente in Modalità Batteria. Nello stesso modo, Bitdefender uscirà automaticamente dalla Modalità Batteria quando rileverà che il portatile non sta più utilizzando.

Ottimizzazione in tempo reale

L'ottimizzazione in tempo reale di Bitdefender è un plug-in che migliora le prestazioni del tuo sistema in modo silenzioso, in background, assicurandosi di non subire interruzioni mentre sei in una modalità profilo. In base al carico della CPU, il plug-in monitora tutti i processi, concentrandosi su quelli che hanno un carico maggiore, per regolarli in base alle tue esigenze.

Per attivare o disattivare l'Ottimizzazione in tempo reale:

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Profili** scheda, fare clic **Impostazioni**.
3. Scorri verso il basso finché non trovi l'opzione dell'ottimizzazione in tempo reale e usa l'interruttore corrispondente per attivarla o disattivarla.

3.3.2. Ottimizzatore con un clic

Problemi come errori del disco rigido, file di registro rimanenti e cronologia del browser possono rallentare il tuo lavoro, il che potrebbe diventare fastidioso per te. Tutti questi possono ora essere risolti con un solo clic di un pulsante.

OneClick Optimizer ti consente di identificare e rimuovere i file inutili eseguendo più attività di pulizia contemporaneamente.

Per avviare il processo di OneClick Optimizer:

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Clicca il **Ottimizzare** pulsante.
   a. **Analizzando**
      Attendi che Bitdefender finisca di cercare problemi di sistema.
      - Pulizia disco: identifica i file e le cartelle non necessari.
      - Pulizia del registro: identifica riferimenti non validi o obsoleti nel registro di Windows.
      - Pulizia della privacy: identifica i file e i cookie Internet temporanei, la cache del browser e la cronologia.

      Viene visualizzato il numero di problemi rilevati. Fare clic sul collegamento Visualizza dettagli per rivederli prima di procedere con il processo di pulizia. Fai clic su Ottimizza per continuare.
   b. **Ottimizzazione**
      Attendi che Bitdefender finisca di ottimizzare il tuo sistema.
   c. **Problemi**
      Qui è possibile visualizzare il risultato dell'operazione.
      Se desideri informazioni complete sul processo di ottimizzazione, fai clic su **Visualizza rapporto dettagliato** pulsante.

3.3.3. Protezione dati

Eliminare i file in modo permanente

Quando elimini un file, non puoi più accedervi con i normali strumenti. Comunque, il file continua a essere archiviato sul disco rigido finché non verrà sovrascritto copiando nuovi file.

Bitdefender File Shredder ti aiuta a eliminare definitivamente i dati rimuovendoli fisicamente dal tuo disco rigido.

Puoi distruggere file o cartelle rapidamente dal dispositivo usando il menu contestuale di Windows seguendo questi passaggi:

1. Clicca con il pulsante destro sul file o la cartella che vuoi eliminare in modo permanente.
2. Seleziona **Bitdefender > Distruttore di file** nel menu contestuale che apparirà.
3. Clicca su **Elimina definitivamente** e poi conferma di voler continuare con l'eliminazione.
   Attendi che Bitdefender termini la distruzione dei file.
4. I risultati sono mostrati. Clicca su **Fine** per uscire dalla procedura guidata.

In alternativa, puoi distruggere i file dall'interfaccia di Bitdefender, nel seguente modo:

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel pannello **Protezione dati**, clicca su **Distruttore di file**.
3. Segui la procedura guidata del Distruttore di file:
   a. Clicca sul pulsante **Aggiungi cartelle** per aggiungere i file o le cartelle che vuoi rimuovere definitivamente.
      In alternativa, trascina i file o le cartelle in questa finestra.
   b. Clicca su **Elimina definitivamente** e conferma la tua volontà di continuare.
      Attendi che Bitdefender finisca di distruggere i file.
   c. **Sommario dei risultati**
      I risultati vengono visualizzati. Clic **Fine** per uscire dalla procedura guidata.

3.4. Come fare

3.4.1. Installazione

Come posso installare Bitdefender su un secondo dispositivo?

Se l'abbonamento che hai acquistato copre più di un computer, puoi utilizzare il tuo account Bitdefender per attivare un secondo dispositivo.

Per installare Bitdefender su un secondo dispositivo:

1. Clicca su **Installa su un altro dispositivo** nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
   Sullo schermo viene visualizzata una nuova finestra.
2. Clic **CONDIVIDI IL LINK PER IL DOWNLOAD**.
3. Segui le istruzioni sullo schermo per installare Bitdefender.

Il nuovo dispositivo su cui hai installato il prodotto Bitdefender comparirà nell'interfaccia di Bitdefender Central.

Come posso reinstallare Bitdefender?

Alcune tipiche situazioni in cui dovresti reinstallare Bitdefender sono:

- hai reinstallato il sistema operativo.
- vuoi risolvere problemi che potrebbero causare rallentamenti e blocchi.
- il tuo prodotto Bitdefender non si è avviato o funziona correttamente.

Se una delle situazioni indicate è il tuo caso, segui questi passaggi:

- In **Windows 7**:
  1. Clic **Inizio** e vai a **Tutti i programmi**.
  2. Trova *Bitdefender Ultimate Small Business Security* e seleziona **Disinstalla**.
  3. Clicca su **REINSTALLA** nella finestra che comparirà.
  4. Devi riavviare il dispositivo per completare il processo.
- In **Windows 8** E **Windows 8.1**:
  1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di

controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.

2. Clicca su **Disinstalla** un programma o **Programmi e funzionalità**.
3. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
4. Clic **REINSTALLARE** nella finestra che appare.
5. È necessario riavviare il dispositivo per completare il processo.

- In **Windows 10** E **Finestre 11**:

1. Clicca su **Inizia** e poi su **Impostazioni**.
2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **App e funzionalità**.
3. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
5. Clicca su **REINSTALLA**.
6. È necessario riavviare il dispositivo per completare il processo.

> **Nota**
> Seguendo questa procedura di reinstallazione, le impostazioni personalizzate vengono salvate e sono disponibili nel nuovo prodotto. Altre impostazioni potrebbero essere riportate alla loro configurazione predefinita.

Dove posso scaricare il mio prodotto Bitdefender?

Puoi installare Bitdefender dal disco di installazione oppure utilizzare il programma d'installazione che puoi scaricare sul tuo dispositivo dalla piattaforma Bitdefender Central.

> **Nota**
> Prima di iniziare l'installazione, si consiglia di rimuovere qualsiasi altra soluzione di sicurezza installata sul tuo sistema. Usando più di una soluzione di sicurezza sullo stesso dispositivo, il sistema diventa instabile.

Per installare Bitdefender da Bitdefender Central:

1. Accesso Bitdefender centrale.
2. Seleziona il **I miei dispositivi** pannello, quindi fare clic su **INSTALLA LA PROTEZIONE**.
3. Scegli una delle due opzioni disponibili:
   - **Proteggi questo dispositivo**
     Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.
   - **Proteggi altri dispositivi**
     Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.
     Clic **INVIA IL LINK PER IL DOWNLOAD**. Digita un indirizzo email nel campo corrispondente e fai clic **INVIA UNA EMAIL**. Si noti che il collegamento per il download generato è valido solo per le prossime 24 ore. Se il link scade, dovrai generarne uno nuovo seguendo gli stessi passaggi.
     Sul dispositivo su cui desideri installare il tuo prodotto Bitdefender, controlla l'account e-mail che hai digitato, quindi fai clic sul pulsante di download corrispondente.
4. Esegui il prodotto Bitdefender che hai scaricato.

Come posso utilizzare il mio abbonamento a Bitdefender dopo aver aggiornato Windows?

Questa situazione si verifica quando, dopo aver aggiornato il sistema operativo, vuoi continuare a utilizzare il tuo abbonamento a Bitdefender.

Se stai usando una versione precedente di Bitdefender, puoi effettuare l'upgrade, gratuitamente, alla versione più recente di Bitdefender, come segue:

- Da una versione precedente di Bitdefender Antivirus al più recente Bitdefender Antivirus disponibile.
- Da una versione precedente di Bitdefender Internet Security alla versione più recente di Bitdefender Internet Security disponibile.

- Da una versione precedente di Bitdefender Total Security alla versione più recente di Bitdefender Total Security disponibile.

Potrebbero verificarsi due casi:

- Dopo aver aggiornato il sistema operativo con Windows Update, scopri che Bitdefender non funziona più.
  In questo caso, devi reinstallare il prodotto seguendo questi passaggi:
  - In **Windows 7**:
    1. Clicca su **Inizia**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
    2. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
    3. Clic **REINSTALLARE** nella finestra che appare.
    4. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
       Apri l'interfaccia del tuo nuovo prodotto installato di Bitdefender per accedere alle sue funzionalità.
  - In **Windows 8** E **Windows 8.1**:
    1. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.
    2. Clicca su **Disinstalla un programma** o **Programmi e funzionalità**.
    3. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
    4. Clic **REINSTALLARE** nella finestra che appare.
    5. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.
       Apri l'interfaccia del tuo nuovo prodotto Bitdefender installato per avere accesso alle sue funzionalità.
  - In **Windows 10** E **Finestre 11**:
    1. Clic **Inizio**, quindi fare clic su **Impostazioni**.

2. Clicca sull'icona **Sistema** nelle Impostazioni e seleziona **App**.
3. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
4. Clic **Disinstalla** di nuovo per confermare la tua scelta.
5. Clic **REINSTALLARE** nella finestra che appare.
6. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.
   Apri l'interfaccia del tuo nuovo prodotto Bitdefender installato per avere accesso alle sue funzionalità.

> **Nota**
> Seguendo questa procedura di reinstallazione, le impostazioni personalizzate vengono salvate e rese disponibili nel nuovo prodotto installato. Altre impostazioni possono essere ripristinate alla loro configurazione predefinita.

- Hai cambiato sistema e vuoi continuare a utilizzare la protezione di Bitdefender. In questo caso, devi installare nuovamente il prodotto utilizzando la versione più recente.
  Per risolvere questa situazione:

  1. Scarica il file di installazione:
     a. Accesso Bitdefender centrale.
     b. Seleziona il **I miei dispositivi** pannello, quindi fare clic su **INSTALLA LA PROTEZIONE**.
     c. Scegli una delle due opzioni disponibili:
        - **Proteggi questo dispositivo**
          Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.
        - **Proteggi un altro dispositivo**
          Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.
          Clic **INVIA IL LINK PER IL DOWNLOAD**. Digita un indirizzo email nel campo corrispondente e fai clic **INVIA UNA**

EMAIL. Si noti che il collegamento per il download generato è valido solo per le prossime 24 ore. Se il link scade, dovrai generarne uno nuovo seguendo gli stessi passaggi.
Sul dispositivo su cui desideri installare il tuo prodotto Bitdefender, controlla l'account e-mail che hai digitato, quindi fai clic sul pulsante di download corrispondente.

2. Esegui il prodotto Bitdefender che hai scaricato.

Per maggiori informazioni sull'installazione di Bitdefender, fai riferimento a Installare il tuo prodotto Bitdefender (pagina 11).

Come posso fare l'upgrade alla versione più recente di Bitdefender?

D'ora in poi, l'upgrade alla versione più recente è possibile senza dover eseguire la disinstallazione manuale e la procedura di reinstallazione. Più precisamente, il nuovo prodotto, che include nuove funzionalità e importanti miglioramenti, viene fornito tramite l'aggiornamento del prodotto stesso e nel caso avessi già un abbonamento attivo di Bitdefender, viene attivato automaticamente.

Se stai giù usando la versione 2020, puoi fare l'upgrade alla versione più recente seguendo questi passaggi:

1. Clicca su **RIAVVIA ORA** nella notifica che ricevi con le informazioni dell'upgrade. Se non l'hai vista, accedi alla finestra **Notifiche**, cerca l'aggiornamento più recente e clicca sul pulsante **RIAVVIA ORA**. Attendi il riavvio del dispositivo.
   Comparirà la finestra **Novità** con maggiori informazioni sulle nuove funzionalità e quelle migliorate.
2. Clicca sui link **Leggi altro** per essere reindirizzato alla nostra pagina dedicata con maggiori dettagli e articoli utili.
3. Chiudi la finestra **Novità** per accedere all'interfaccia della nuova versione installata.

Gli utenti che vogliono fare l'upgrade gratuitamente da Bitdefender 2016 o precedente alla versione di Bitdefender più recente, devono rimuovere la loro versione attuale dal Pannello di Controllo e scaricare il file di installazione più recente dal sito web di Bitdefender al seguente indirizzo: https://www.bitdefender.com/Downloads/. L'attivazione è possibile solo con un abbonamento valido.

3.4.2. Bitdefender centrale

Come posso accedere all'account Bitdefender con un altro account?

Hai creato un nuovo account Bitdefender e ora vuoi utilizzarlo.

Per accedere con un altro account di Bitdefender:

1. Clicca sul nome del tuo account nella parte superiore dell'**interfaccia di Bitdefender**.
2. Clicca su **Cambia account** nell'angolo in alto a destra dello schermo per cambiare l'account collegato al dispositivo.
3. Digitare l'indirizzo e-mail nel campo corrispondente, quindi fare clic su **PROSSIMO**.
4. Digitare la password, quindi fare clic su **REGISTRAZIONE**.

> **Nota**
> Il prodotto Bitdefender del tuo dispositivo cambia automaticamente in base all'abbonamento associato al nuovo account Bitdefender. Se non vi è alcun abbonamento associato disponibile al nuovo account Bitdefender o desideri trasferirlo dall'account precedente, puoi contattare Bitdefender per ottenere assistenza come descritto nella sezione Richiesta d'aiuto (pagina 287).

Come disattivo i messaggi di aiuto di Bitdefender Central?

Per aiutarti a comprendere l'utilità di ogni opzione in Bitdefender Central, nell'interfaccia principale vengono mostrati alcuni messaggi di aiuto.

Se desideri disattivare questo tipo di messaggi:

1. Accesso Bitdefender centrale.
2. Clicca il icona nella parte in alto a destra dello schermo.
3. Clicca su **Il mio account** nel menu scorrevole.
4. Clicca su **Impostazioni** nel menu scorrevole.
5. Disattiva l'opzione **Attiva/disattiva i messaggi di aiuto**.

Ho dimenticato la password del mio account Bitdefender. Come posso cambiarla?

Ci sono due possibilità per impostare una nuova password per il tuo account di Bitdefender:

- Dal Interfaccia di Bitdefender:
  1. Clic **Il mio conto** nel menu di navigazione sul Interfaccia di Bitdefender.
  2. Clicca su **Cambia account** nell'angolo in alto a destra dello schermo.
     Comparirà una nuova finestra.
  3. Inserisci il tuo indirizzo e-mail e clicca su **AVANTI**.
     Viene visualizzata una nuova finestra.
  4. Clic **Ha dimenticato la password?**.
  5. Clicca su **AVANTI**.
  6. Controlla il tuo account e-mail, digita il codice di sicurezza che hai ricevuto, quindi fai clic **PROSSIMO**.
     In alternativa, puoi fare clic **Cambiare la password** nell'e-mail che ti abbiamo inviato.
  7. Digitare la nuova password che si desidera impostare, quindi digitarla nuovamente. Clic **SALVA**.

- Dal tuo browser web:
  1. Vai a: https://central.bitdefender.com.
  2. Clicca su **ACCEDI**.
  3. Digita il tuo indirizzo e-mail, quindi fai clic su **PROSSIMO**.
  4. Clic **Ha dimenticato la password?**.
  5. Clic **PROSSIMO**.
  6. Verifica il tuo account e-mail e segui le istruzioni fornite per impostare una nuova password per il tuo account Bitdefender.

D'ora in poi, per accedere al tuo account Bitdefender, digita il tuo indirizzo e-mail e la nuova password che hai appena impostato.

Come posso gestire le sessioni di accesso associate al mio account di Bitdefender?

Nel tuo account di Bitdefender, hai la possibilità di visualizzare le ultime sessioni di accesso inattive e attive in esecuzione sui dispositivi associati al tuo account. Inoltre, puoi uscire in remoto seguendo questi passaggi:

1. Accesso Bitdefender centrale.
2. Clicca il icona nella parte in alto a destra dello schermo.
3. Clicca su **Sessioni** nel menu scorrevole.
4. Nell'area **Sessioni attive**, seleziona l'opzione **ESCI** accanto al dispositivo in cui vuoi terminare la sessione.

3.4.3. Scansione con BitDefender

Come posso controllare un file o una cartella?

Il modo più semplice di controllare un file o una cartella è cliccare con il pulsante destro sull'elemento che desideri controllare, puntare Bitdefender e poi **Esamina con Bitdefender** dal menu.

Per completare la scansione, segui la procedura guidata della Scansione antivirus. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati.

Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

Tipiche situazioni in cui si userebbe questo metodo includono:

- Si sospetta che un file o una cartella specifica sia infetta.
- Ogni volta che scarichi file da Internet che ritieni potrebbero essere pericolosi.
- Controlla una rete condivisa prima di copiare i file sul dispositivo.

Come posso eseguire una scansione del mio sistema

Per eseguire una scansione completa del sistema:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.

3. Clicca sul pulsante **Esegui scansione** accanto a **Scansione sistema**.
4. Segui la procedura guidata della Scansione di sistema per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati.
   Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo. Per maggiori informazioni, fai riferimento a Richiesta d'aiuto (pagina 287).

Come posso programmare una scansione?

Puoi impostare il tuo prodotto Bitdefender affinché esegua la scansione di alcune importanti sezioni del sistema quando non sei di fronte al dispositivo.

Per programmare una scansione:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Clicca su ··· accanto al tipo di scansione che vuoi programmare, Scansione sistema o Scansione veloce, nella parte inferiore dell'interfaccia, poi seleziona **Modifica**.
   In alternativa, puoi creare un tipo di scansione che si adatti alle tue esigenze, cliccando su **+Crea scansione** accanto a **Gestisci scansioni**.
4. Personalizza la scansione in base alle tue esigenze, poi clicca su **Avanti**.
5. Seleziona la casella accanto a **Scegli quando programmare questa attività**.
   Seleziona una delle opzioni corrispondenti per impostare un elenco:
   - ❍ All'avvio del sistema
   - ❍ Quotidiano
   - ❍ settimanalmente
   - ❍ Mensile

   Se scegli Giornaliero, Mensile o Settimanale, trascina il dispositivo di scorrimento lungo la scala per impostare il periodo di tempo desiderato in cui deve iniziare la scansione pianificata.

Se scegli di creare una nuova scansione personalizzata, comparirà la finestra **Attività di scansione**. Qui puoi selezionare i percorsi che desideri esaminare con la scansione.

Come posso creare un'attività di scansione personale?

Se desideri controllare percorsi particolari sul tuo dispositivo o impostare le opzioni di scansione, configura ed esegui una scansione personalizzata.

Per creare un'attività di scansione personale, procedi così:

1. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
2. Clicca su **+Crea scansione** accanto a **Gestisci scansioni**.
3. Nel campo del nome dell'attività, inserisci un nome per la scansione, seleziona i percorsi che vorresti esaminare e poi clicca su **AVANTI**.
4. Configura queste opzioni generali:
   - **Esamina solo le applicazioni**. Puoi impostare Bitdefender affinché esamini solo le app a cui accedi.
   - **Priorità dell'attività di scansione**. Puoi scegliere l'impatto che un processo di scansione dovrebbe avere sulle prestazioni del sistema.
     - Auto: la priorità del processo di scansione dipenderà dall'attività del sistema. Per assicurarsi che il processo di scansione non influisca sull'attività del sistema, Bitdefender deciderà se eseguire il processo di scansione con priorità alta o bassa.
     - Alta: la priorità del processo di scansione sarà alta. Scegliendo questa opzione, consentirai ad altri programmi di funzionare più lentamente e ridurrai il tempo necessario per il completamento del processo di scansione.
     - Bassa: la priorità del processo di scansione sarà bassa. Scegliendo questa opzione, consentirai ad altri programmi di funzionare più velocemente e aumenterai il tempo necessario per il completamento del processo di scansione.
   - **Pubblica azioni di scansione**. Scegli quale azione Bitdefender dovrebbe intraprendere nel caso non venisse trovata alcuna minaccia:

- Mostra finestra Riepilogo
- Dispositivo di spegnimento
- Chiudi la finestra di scansione

5. Se vuoi configurare le opzioni di scansione nel dettaglio, clicca su **Mostra impostazioni avanzate**.
   Clic **Prossimo**.
6. Se lo desideri, puoi attivare l'opzione **Programma attività di scansione** e poi scegli quando dovrebbe iniziare la scansione personalizzata che hai creato.
   - All'avvio del sistema
   - Quotidiano
   - Mensile
   - settimanalmente

   Se scegli Giornaliera, Mensile o Settimanale, trascina il dispositivo di scorrimento lungo la scala per impostare il periodo di tempo desiderato in cui deve iniziare la scansione pianificata.
7. Clic **Salva** per salvare le impostazioni e chiudere la finestra di configurazione.
   A seconda delle posizioni da scansionare, la scansione potrebbe richiedere del tempo. Se durante il processo di scansione vengono rilevate minacce, verrà richiesto di scegliere le azioni da intraprendere sui file rilevati.

Se lo desideri, puoi eseguire nuovamente una scansione personale precedente cliccando sulla rispettiva voce nell'elenco disponibile.

Come posso escludere una cartella dalla scansione?

Bitdefender consente di escludere determinati file, cartelle o estensioni di file dalla scansione.

Le eccezioni devono essere utilizzate da utenti con una conoscenza avanzata del computer e solo nelle seguenti situazioni:

- Hai una cartella di grandi dimensioni sul tuo sistema, dove tieni film e musica.

- Hai una cartella di grandi dimensioni sul tuo sistema, dove tieni diversi dati.
- Tieni una cartella dove installare diversi tipi di programmi e applicazioni a scopo di prova. La scansione della cartella può causare la perdita di alcuni dati.

Per aggiungere una cartella alla lista delle eccezioni:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Clicca sulla scheda **Impostazioni**.
4. Clicca su **Gestisci eccezioni**.
5. Clic **+ Aggiungi un'eccezione**.
6. Immettere il percorso della cartella che si desidera escludere dalla scansione nel campo corrispondente.
   In alternativa, puoi accedere alla cartella facendo clic sul pulsante Sfoglia nella parte destra dell'interfaccia, selezionarla e fare clic su **OK**.
7. Attiva l'interruttore accanto alla funzione di protezione che non dovrebbe eseguire la scansione della cartella. Ci sono tre opzioni:
   - antivirus
   - Prevenzione delle minacce online
   - Difesa avanzata dalle minacce
8. Clic **Salva** per salvare le modifiche e chiudere la finestra.

Cosa fare quando Bitdefender rileva un file pulito come infetto?

In alcuni casi, Bitdefender potrebbe segnare erroneamente un file legittimo come una minaccia (un falso positivo). Per correggere tale errore, aggiungi il file all'area Eccezioni di Bitdefender:

1. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
   b. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.

c. Nella finestra **Avanzate**, disattiva **Bitdefender Shield**.
Comparirà una finestra di avviso. Devi confermare la tua scelta selezionando dal menu per quanto tempo desideri disattivare la protezione in tempo reale. Puoi disattivare la protezione in tempo reale per 5, 15 o 30 minuti, un'ora, in modo permanente o fino a un riavvio del sistema.

2. Mostra gli oggetti nascosti in Windows. Per scoprire come fare, fai riferimento a Come posso visualizzare gli elementi nascosti in Windows? (pagina 118).
3. Ripristina il file dalla quarantena:
   a. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
   b. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
   c. Vai alla finestra **Impostazioni** e clicca su **Gestisci quarantena**.
   d. Seleziona il file e poi clicca su **Ripristina**.
4. Aggiungi il file all'elenco delle eccezioni. Per scoprire come fare, fai riferimento a Come posso escludere una cartella dalla scansione? (pagina 105).
5. Attiva la protezione antivirus in tempo reale di Bitdefender.
6. Contatta gli operatori del nostro supporto in modo da poter rimuovere la rilevazione dell'aggiornamento delle informazioni sulle minacce. Per scoprire come fare, fai riferimento a Richiesta d'aiuto (pagina 287).

Come posso verificare quali minacce sono state rilevate da Bitdefender?

Ogni volta che viene eseguita una scansione, viene creato un registro di scansione dove Bitdefender registra i problemi rilevati.

Il registro di scansione contiene informazioni dettagliate sul processo di scansione registrato, sull'obiettivo della scansione, le minacce individuate e le azioni intraprese su queste minacce.

È possibile aprire il registro della scansione direttamente dalla scansione guidata, una volta completata la scansione, facendo clic su **MOSTRA REGISTRO**.

Per controllare un registro di scansione o qualsiasi infezione rilevata in un secondo momento:

1. Clic **Notifiche** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Tutto** scheda, selezionare la notifica relativa all'ultima scansione. Qui è possibile trovare tutti gli eventi di scansione delle minacce, incluse le minacce rilevate dalla scansione in accesso, le scansioni avviate dall'utente e le modifiche di stato per le scansioni automatiche.
3. Nell'elenco delle notifiche, puoi controllare quali scansioni sono state eseguite di recente. Fare clic su una notifica per visualizzarne i dettagli.
4. Per aprire un registro di scansione, clicca su **Guarda registro**.

3.4.4. Controllo privacy

Come posso essere certo che le mie transazioni online sono sicure?

Per assicurarti che le tue operazioni online restino private, puoi utilizzare il browser fornito da Bitdefender per proteggere le transazioni e le applicazioni di home banking.

Bitdefender Safepay™ è un browser sicuro e progettato per proteggere i dati della tua carta di credito, il numero del tuo conto bancario e altre informazioni personali che potresti inserire nei più diversi siti web.

Per mantenere le tue attività online sempre sicure e private:

1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **SAFEPAY** riquadro, fare clic **Impostazioni**.
3. Nel **Pagamento Sicuro** finestra, fare clic **Avvia SafePay**.
4. Clicca sul pulsante per accedere alla **tastiera virtuale**. Usa la **tastiera virtuale** ogni volta che devi digitare informazioni personali, come le password.

Cosa posso fare in caso di furto del mio dispositivo?

Il furto del proprio dispositivo mobile, sia esso uno smartphone, un tablet o un portatile, è uno dei problemi principali, che oggi colpiscono molte persone e società in tutto il mondo.

Bitdefender Anti-Theft ti consente non solo di localizzare e bloccare il dispositivo rubato, ma anche di eliminare tutti i dati personali, assicurandoti che non vengano utilizzati dal ladro.

Per accedere alle funzionalità di Anti-Theft dal tuo account:

1. Accesso Bitdefender centrale.
2. Seleziona il **I miei dispositivi** pannello.
3. Clicca sulla scheda del dispositivo desiderato e seleziona **Anti-Theft**.
4. Seleziona la funzione che vuoi utilizzare:
   - **LOCALIZZA** - Mostra la posizione del dispositivo su Google Maps. **Mostra IP** - Mostra l'ultimo indirizzo IP per il dispositivo selezionato.
   - **Allerta** - Invia un'allerta al dispositivo.
   - **Blocco** - Blocca il tuo dispositivo e imposta un codice PIN numerico per sbloccarlo. In alternativa, attiva l'opzione corrispondente per consentire a Bitdefender di scattare delle immagini della persona che sta cercando di accedere al tuo dispositivo.
   - **Elimina** - Elimina tutti i dati dal tuo dispositivo.

     Importante
     Dopo aver cancellato il contenuto di un dispositivo, tutte le funzioni Antifurto cessano di funzionare.

Come posso eliminare un file in modo permanente con Bitdefender?

Se desideri eliminare un file in modo permanente dal sistema, devi cancellare i dati fisicamente dal tuo disco rigido.

Il Distruttore di file di Bitdefender ti aiuterà a distruggere rapidamente file o cartelle dal tuo dispositivo usando il menu contestuale di Windows seguendo questi passaggi:

1. Clicca con il pulsante destro del mouse sul file o la cartella che vuoi eliminare in maniera definitiva, seleziona Bitdefender e poi **Distruttore di file**.

2. Clic **Elimina definitivamente**, quindi confermare che si desidera continuare con il processo.
   Attendi che Bitdefender finisca di distruggere i file.
3. I risultati sono mostrati. Clicca su **FINE** per uscire dalla procedura guidata.

Come posso proteggere la mia webcam da accessi non autorizzati?

Puoi impostare il tuo prodotto Bitdefender per consentire o negare l'accesso delle app installate alla tua webcam seguendo questi passaggi:

1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **PROTEZIONE VIDEO E AUDIO** riquadro, fare clic **Impostazioni**.
3. Vai alla finestra **Protezione webcam** e vedrai l'elenco delle applicazioni che hanno richiesto l'accesso alla tua videocamera.
4. Evidenzia la app a cui vuoi consentire o impedire l'accesso e poi clicca sull'interruttore rappresentato da una videocamera, accanto ad essa.
   Per visualizzare ciò che gli altri utenti di Bitdefender hanno scelto di fare con la app selezionata, clicca sull'icona . Riceverai un avviso ogni volta che una delle app elencate viene bloccata dagli utenti di Bitdefender.

Per aggiungere manualmente app a questo elenco, clicca sul pulsante **Aggiungi applicazione** e seleziona una delle due opzioni.

- Da Windows Store
- Dalle tue app

Come posso ripristinare manualmente i file cifrati quando il processo di ripristino fallisce?

Nel caso i file cifrati non possano essere ripristinati automaticamente, puoi ripristinarli manualmente seguendo questi passaggi:

1. Clic **Notifiche** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Tutto** scheda, selezionare la notifica relativa all'ultimo comportamento ransomware rilevato, quindi fare clic su **File crittografati**.

3. Viene visualizzato l'elenco con i file crittografati.
   Clicca su **Ripristina file** per continuare.
4. Nel caso in cui l'intero o parte del processo di ripristino fallisca, è necessario scegliere la posizione in cui salvare i file decrittografati. Clic **Ripristina posizione**, quindi scegli una posizione sul tuo PC.
5. Viene visualizzata una finestra di conferma.
   Clic **Fine** per terminare il processo di ripristino.

I file con le seguenti estensioni possono essere ripristinati nel caso in cui vengano crittografati:

.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; .ph p; .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; .wa v; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

3.4.5. Strumenti di ottimizzazione

Come posso migliorare le prestazioni del mio sistema?

Le prestazioni del sistema dipendono non solo dalla configurazione hardware, come il carico della CPU, l'utilizzo della memoria e lo spazio su disco rigido. È inoltre direttamente collegato alla configurazione del software e alla gestione dei dati.

Queste sono le azioni principali che puoi intraprendere con Bitdefender per migliorare la velocità e le prestazioni del tuo sistema:

❍ Ottimizza le prestazioni del tuo sistema con un solo clic (pagina 111)
❍ Scansiona periodicamente il tuo sistema (pagina 112)

Ottimizza le prestazioni del tuo sistema con un solo clic

L'opzione OneClick Optimizer consente di risparmiare tempo prezioso quando si desidera un modo rapido per migliorare le prestazioni del sistema mediante la scansione rapida, il rilevamento e la pulizia dei file inutili.

Per avviare il processo di OneClick Optimizer:

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Clicca il **Ottimizzare** pulsante.
3. Lascia che Bitdefender cerchi i file che possono essere eliminati, quindi fai clic su **Ottimizzare** pulsante per terminare il processo.

Scansiona periodicamente il tuo sistema

Anche la velocità del tuo sistema e il suo comportamento generale possono essere influenzati dalle minacce.

Assicurati di eseguire periodicamente la scansione del sistema, almeno una volta alla settimana.

Si consiglia di utilizzare la scansione del sistema perché esegue la scansione di tutti i tipi di minacce che mettono in pericolo la sicurezza del sistema ed esegue anche la scansione all'interno degli archivi.

Per avviare la scansione del sistema:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Clic **Esegui scansione** accanto a **Scansione del sistema**.
4. Segui i passaggi della procedura guidata.

3.4.6. Informazioni utili

Come posso testare la mia soluzione di sicurezza?

Per assicurarti che il tuo prodotto Bitdefender stia funzionando correttamente, ti consigliamo di utilizzare il test Eicar.

Il test Eicar ti consente di verificare l'efficacia della tua soluzione di sicurezza, utilizzando un file sicuro appositamente sviluppato a tale scopo.

Per testare la tua soluzione di sicurezza:

1. Scarica il test dalla pagina web ufficiale dell'organizzazione EICAR http://www.eicar.org/.
2. Clicca sull'opzione **Anti-Malware Testfile**.
3. Clicca su **Download** nel menu a sinistra.

4. Dalla voce **Download area using the standard protocol http**, clicca sul file di test **eicar.com**.
5. Sarai avvisato che la pagina a cui stai cercando di accedere contiene il file sospetto EICAR-Test-File (in realtà NON è una minaccia).
   Cliccando sull'opzione **Conosco i rischi, quindi prosegui**, il test sarà scaricato e comparirà una finestra di Bitdefender per informarti che ha rilevato una minaccia.
   Clicca su **Maggiori dettagli** per scoprire altre informazioni su questa azione.

Se non ricevi alcun avviso da parte di Bitdefender, ti consigliamo di contattare il supporto tecnico di Bitdefender come descritto nella sezione Richiesta d'aiuto (pagina 287).

Come posso rimuovere Bitdefender?

Se vuoi rimuovere Bitdefender Ultimate Small Business Security:

- In **Windows 7**:
  1. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.
  2. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
  3. Clicca su **RIMUOVI** nella finestra che comparirà.
  4. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

- In **Windows 8** E **Windows 8.1**:
  1. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.
  2. Clic **Disinstallare un programma** O **Programmi e caratteristiche**.
  3. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
  4. Clic **RIMUOVERE** nella finestra che appare.

5. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

- In **Windows 10** E **Finestre 11**:
  1. Clicca su **Start** e poi su Impostazioni.
  2. Clicca il **Sistema** nell'area Impostazioni, quindi selezionare **App**.
  3. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
  4. Clic **Disinstalla** di nuovo per confermare la tua scelta.
  5. Clic **RIMUOVERE** nella finestra che appare.
  6. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

> **Nota**
> Questa procedura di reinstallazione eliminerà in modo permanente le impostazioni personalizzate.

Come posso rimuovere Bitdefender VPN?

La procedura di rimozione di Bitdefender VPN è simile a quella che useresti per rimuovere qualsiasi altro programma dal dispositivo:

- In **Windows 7**:
  1. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.
  2. Trova **Bitdefender VPN** e seleziona **Disinstalla**.
     Attendere che il processo di disinstallazione sia terminato.

- In **Windows 8** E **Windows 8.1**:
  1. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.
  2. Clic **Disinstalla** un programma o **Programmi e caratteristiche**.
  3. Trovare **VPN di Bitdefender** e seleziona **Disinstalla**.
     Attendere il completamento del processo di disinstallazione.

- In **Windows 10** E **Finestre 11**:
  1. Clic **Inizio**, quindi fai clic su Impostazioni.
  2. Clicca sull'icona **Sistema** e seleziona **App installate**.
  3. Trovare **VPN di Bitdefender** e seleziona **Disinstalla**.
  4. Clic **Disinstalla** di nuovo per confermare la tua scelta.
     Attendere il completamento del processo di disinstallazione.

Come posso rimuovere l'estensione Bitdefender Anti-tracker?

In base al browser web utilizzato, segui questi passaggi per disinstallare l'estensione Bitdefender Anti-tracker:

- Internet Explorer
  1. Clicca su accanto alla barra di ricerca e seleziona Gestisci add-on. Comparirà un elenco delle estensioni installate.
  2. Clicca su Bitdefender Anti-tracker.
  3. Clicca su **Disattiva** nel lato inferiore destro.
- Google Chrome
  1. Clicca su accanto alla barra di ricerca.
  2. Seleziona **Altri strumenti** e poi **Estensioni**.
     Comparirà un elenco con le estensioni installate.
  3. Clicca su **Rimuovi** nella scheda Bitdefender Anti-tracker.
  4. Clicca su **Rimuovi** nella finestra che comparirà.
- Mozilla Firefox
  1. Clic accanto alla barra di ricerca.
  2. Seleziona **Add-on** e poi **Estensioni**.
     Viene visualizzato un elenco con le estensioni installate.
  3. Clicca su ··· e seleziona **Rimuovi**.

Come posso spegnere automaticamente il dispositivo al termine della scansione?

Bitdefender offre diverse attività di scansione che puoi utilizzare per assicurarti che il tuo sistema sia privo di minacce. Eseguire una scansione

dell'intero dispositivo potrebbe richiedere molto tempo in base alla propria configurazione hardware e software.

Per questo motivo, Bitdefender ti consente di configurare il tuo prodotto per spegnere il sistema al termine della scansione.

Considera questo esempio: hai terminato il tuo lavoro e vuoi andare a riposare. Ti piacerebbe che Bitdefender eseguisse una scansione per rilevare eventuali minacce sull'intero sistema.

Per spegnere il dispositivo quando la Scansione veloce o la Scansione del sistema è terminata:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Nella finestra **Scansioni**, clicca su ⋯ accanto a Scansione veloce o Scansione sistema, e seleziona {9}Modifica{10}.
4. Personalizza la scansione in base alle tue esigenze e clicca su **Avanti**.
5. Seleziona la casella accanto a **Scegli quando programmare questa attività** e poi seleziona quando l'attività dovrà iniziare.
   Se scegli Giornaliera, Mensile o Settimanale, trascina il dispositivo di scorrimento lungo la scala per impostare il periodo di tempo desiderato in cui deve iniziare la scansione pianificata.
6. Clic **Salva**.

Per spegnere il dispositivo al termine di una scansione personalizzata:

1. Clicca su ⋯ accanto alla scansione personale che hai creato.
2. Clicca su **Avanti** e poi ancora su **Avanti**.
3. Seleziona la casella **Scegli quando programmare questa attività** e poi seleziona quando l'attività dovrà iniziare.
4. Clic **Salva**.

Se non vengono rilevate minacce, il dispositivo si spegnerà.

Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo. Per maggiori informazioni, fai riferimento a Procedura guidata scansione antivirus (pagina 30).

Come posso configurare Bitdefender per usare una connessione a Internet tramite proxy?

Se il tuo dispositivo si collega a Internet tramite un server proxy, devi configurare Bitdefender con le impostazioni del proxy. Normalmente Bitdefender rileva automaticamente e importa le impostazioni proxy dal sistema.

> **Importante**
> Le connessioni Internet domestiche normalmente non usano un server proxy. Come regola empirica, quando gli aggiornamenti non funzionano, controlla e configura le impostazioni di connessione proxy del tuo programma di Bitdefender. Se Bitdefender può essere aggiornato, allora è configurato correttamente per connettersi a Internet.

Per gestire le impostazioni del proxy:

1. Clic **Impostazioni** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Seleziona il **Avanzate** scheda.
3. Attiva **Server proxy**.
4. Clicca su **Modifica proxy**.
5. Ci sono due opzioni per determinare le impostazioni proxy:
   - **Importa le impostazioni del proxy dal browser predefinito** - le impostazioni del proxy dell'utente attuale, estratte dal browser predefinito. Se il server proxy richiede un nome utente e una password, devi specificarle nei campi corrispondenti.

     > **Nota**
     > Bitdefender può importare le impostazioni del proxy dai browser più diffusi, incluso le ultime versioni di Microsoft Edge, Internet Explorer, Mozilla Firefox e Google Chrome.

   - **Impostazioni proxy personalizzate** - Le impostazioni proxy che puoi configurare direttamente.
     Le seguenti impostazioni devono essere specificate:
     - **Indirizzo** - Inserisci l'indirizzo IP del server proxy.
     - **Porta** - Inserisci la porta che Bitdefender utilizza per connettersi al server proxy.

- **Nome utente** - Inserisci un nome utente riconosciuto dal proxy.
- **Password** - Inserisci la password valida dell'utente già specificato in precedenza.

6. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

Bitdefender userà le impostazioni del proxy disponibili finché non riesce a connettersi a Internet.

Sto usando una versione di Windows a 32 o 64 bit?

Per scoprire se hai un sistema operativo a 32 o 64 bit:

- In **Windows 7**:
  1. Clicca su **Start**.
  2. Localizza **Computer** nel menu **Start**.
  3. Clicca con il pulsante destro su **Computer** e seleziona **Proprietà**.
  4. Vai in **Sistema** per verificare le informazioni sul tuo sistema.
- In **Windows 8**:
  1. Dal menu Start di Windows, localizza l'opzione **Computer** (puoi anche digitare direttamente "Computer" nella finestra di ricerca del menu Start) e poi clicca sulla sua icona con il pulsante destro.
  2. Seleziona **Proprietà** nel menu inferiore.
  3. Controlla in Sistema per verificare il tipo di sistema.
- In **Windows 10** E **Finestre 11**:
  1. Digita "Sistema" nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona.
  2. Individua la sezione Sistema per trovare maggiori informazioni sul tuo sistema.

Come posso visualizzare gli elementi nascosti in Windows?

Questi passaggi sono utili nel caso in cui tu debba occuparti di un minaccia per trovare e rimuovere i file infetti, che potrebbero essere nascosti.

Segui questi passaggi per mostrare gli elementi nascosti in Windows:

1. Clicca su **Start** e vai in **Pannello di Controllo**.
   In **Windows 8** e **Windows 8.1**: dalla schermata Start di Windows, localizza **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella schermata Start) e poi clicca sulla sua icona.
2. Seleziona **Opzioni cartella**.
3. Vai alla scheda **Visualizza**.
4. Seleziona **Mostra file e cartelle nascoste**.
5. Deseleziona **Nascondi estensioni per i file conosciuti**.
6. Deseleziona **Nascondi file protetti del sistema operativo**.
7. Clicca su **Applica** e clicca su **OK**.

In **Windows 10** E **Finestre 11**:

1. Digita "Visualizza cartelle e file nascosti" nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona.
2. Seleziona **Visualizza cartelle, file e unità nascosti**.
3. Chiaro **Nascondi le estensioni per i tipi di file conosciuti**.
4. Chiaro **Nascondi i file protetti del sistema operativo**.
5. Clic **Fare domanda a**, quindi fare clic su **OK**.

Come posso rimuovere le altre soluzioni di sicurezza?

La ragione principale per usare una soluzione di sicurezza è garantire la protezione e la sicurezza dei tuoi dati. Ma cosa succede quando si ha più di un prodotto di sicurezza sullo stesso sistema?

Usando più di una soluzione di sicurezza sullo stesso dispositivo, il sistema diventa instabile. Il programma d'installazione di Bitdefender Ultimate Small Business Security rileva automaticamente altri programmi di sicurezza e ti offre la possibilità di disinstallarli.

Se non hai rimosso le altre soluzioni di sicurezza durante l'installazione iniziale:

- In **Windows 7**:
  1. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.

2. Attendi per qualche istante, finché non compare l'elenco del software installato.
3. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
4. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

- In **Windows 8** E **Windows 8.1**:
  1. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.
  2. Clic **Disinstallare un programma** O **Programmi e caratteristiche**.
  3. Attendere qualche istante finché non viene visualizzato l'elenco dei software installati.
  4. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
  5. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

- In **Windows 10** E **Finestre 11**:
  1. Clic **Inizio**, quindi fai clic su Impostazioni.
  2. Clicca il **Sistema** nell'area Impostazioni, quindi selezionare **App**.
  3. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
  4. Clic **Disinstalla** di nuovo per confermare la tua scelta.
  5. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

Se non dovessi riuscire a rimuovere le altre soluzioni di sicurezza dal tuo sistema, cerca uno strumento di disinstallazione nel sito web del venditore o contattalo direttamente per ricevere le istruzioni di disinstallazione.

Come posso riavviare in modalità provvisoria?

La modalità provvisoria è una modalità operativa diagnostica, usata principalmente per risolvere problemi che affliggono il normale uso di Windows. Problemi quali conflitti di driver o minacce, impediscono a Windows di avviarsi regolarmente. In modalità provvisoria solo poche applicazioni funzionano e Windows carica soltanto i driver e le componenti di base del sistema operativo. Ecco perché la maggior parte delle minacce sono inattive usando Windows in modalità provvisoria e possono essere rimosse facilmente.

Per avviare Windows in modalità provvisoria:

- In **Windows 7**:
  1. Riavvia il dispositivo.
  2. Premi più volte il tasto **F8** prima del lancio di Windows per accedere al menu di avvio.
  3. Seleziona **Modalità provvisoria** nel menu di avvio o **Modalità provvisoria con supporto di rete** se desideri avere l'accesso a Internet.
  4. Premi **Invio** e attendi il caricamento di Windows in modalità provvisoria.
  5. Questo processo termina con un messaggio di conferma. Clicca su **OK** per confermare.
  6. Per avviare Windows normalmente, riavvia semplicemente il sistema.

- In **Windows 8**, **Windows 8.1**, **Windows 10** e **Windows 11**:
  1. Lancia **Configurazione di sistema** in Windows, premendo contemporaneamente i tasti **Windows + R** sulla tastiera.
  2. Scrivi **msconfig** nella finestra di dialogo **Apri** e clicca su **OK**.
  3. Seleziona la scheda **Avvio**.
  4. Nella sezione **Opzioni di avvio**, seleziona la casella **Avvio in modalità provvisoria**.
  5. Clicca su **Rete** e poi su **OK**.

6. Clicca su **OK** nella finestra **Configurazione di sistema**, che ti informa della necessità di riavviare il sistema per effettuare le modifiche selezionate.
   Il sistema sarà riavviato in modalità provvisoria con supporto di rete.

Per riavviare la modalità normale, torna alle impostazioni lanciando di nuovo **Operazione di sistema** e deselezionando la casella **Avvio in modalità sicura**. Clicca su **OK** e poi **Riavvia**. Attendi che vengano applicate le nuove impostazioni.

3.5. Risoluzione dei problemi

3.5.1. Risolvere i problemi più comuni

In questo capitolo vengono spiegati alcuni problemi che si possono incontrare utilizzando BitDefender e vengono inoltre fornite possibili soluzioni per questi problemi. La maggior parte di questi problemi possono essere risolti tramite una configurazione appropriata delle impostazioni del prodotto.

- ❍ Il mio sistema sembra lento (pagina 123)
- ❍ La scansione non parte (pagina 124)
- ❍ Non posso più usare una app (pagina 127)
- ❍ Cosa fare quando Bitdefender blocca un sito web, un dominio, un indirizzo IP o una app online che sono sicuri (pagina 128)
- ❍ Come aggiornare Bitdefender con una connessione a Internet lenta (pagina 132)
- ❍ I servizi di Bitdefender non rispondono (pagina 133)
- ❍ Il filtro antispam non funziona correttamente (pagina 134)
- ❍ Rimozione di Bitdefender non riuscita (pagina 138)
- ❍ Il sistema non si riavvia dopo aver installato Bitdefender (pagina 140)

Se non è possibile trovare il problema qui, o se la soluzione fornita non lo risolve, è possibile contattare un rappresentante del supporto tecnico di BitDefender come delineato nel capitolo {1}{2}.

Il mio sistema sembra lento

In genere, dopo aver installato un software di sicurezza, potrebbe verificarsi un certo rallentamento del sistema, che fino a un certo grado è normale.

Se noti un rallentamento significativo, questo problema si può verificare per le seguenti ragioni:

- **Bitdefender non è l'unico programma di sicurezza installato sul sistema**.
  Sebbene Bitdefender cerchi e rimuova i programmi di sicurezza trovati durante l'installazione, si consiglia di rimuovere ogni altra soluzione di sicurezza in uso prima dell'installazione di Bitdefender. Per maggiori informazioni, fai riferimento a Come posso rimuovere le altre soluzioni di sicurezza? (pagina 119).
- **Non ci sono i requisiti di sistema per l'esecuzione di Bitdefender.**
  Se il tuo dispositivo non soddisfa i requisiti di sistema, il dispositivo diventerà lento, specialmente quando si eseguono più applicazioni contemporaneamente. Per maggiori informazioni, fai riferimento a Requisiti di sistema (pagina 9).
- **Hai installato app che non utilizzi.**
  Ogni dispositivo ha programmi o app che non utilizzi. E molti programmi indesiderati sono eseguiti in background, occupando spazio su disco e memoria. Se non utilizzi un programma, disinstallalo. Ciò vale anche per qualsiasi altro programma pre-installato o di prova che ci si è dimenticati di rimuovere.

  > **Importante**
  > Se sospetti che un programma o una app sia essenziale per il sistema operativo, non rimuoverla e contatta l'assistenza clienti di Bitdefender.

- **Il tuo sistema potrebbe essere infetto.**
  Anche la velocità del sistema e il suo funzionamento generale possono essere influenzati dalle minacce. Spyware, malware, trojan e adware hanno tutti un impatto sulle prestazioni del tuo dispositivo. Assicurati di esaminare il tuo sistema periodicamente, almeno una volta a settimana. Si consiglia di usare la Scansione di sistema di Bitdefender perché esegua una scansione per tutti i tipi di minaccia che mettono in pericolo la sicurezza del tuo sistema.

Per avviare la scansione del sistema:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Nella finestra **Scansioni**, clicca su **Esegui scansione** accanto a **Scansione sistema**.
4. Segui i passaggi della procedura guidata.

La scansione non parte

Questo tipo di problema può avere due cause principali:

- **Un'installazione precedente di Bitdefender che non è stata rimossa completamente o un'installazione difettosa di Bitdefender.**
  In questo caso, reinstalla Bitdefender:
  - In **Windows 7**:
    1. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.
    2. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
    3. Clic **REINSTALLARE** nella finestra che appare.
    4. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.
  - In **Windows 8** E **Windows 8.1**:
    1. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.
    2. Clic **Disinstalla** un programma o **Programmi e caratteristiche**.
    3. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
    4. Clic **REINSTALLARE** nella finestra che appare.

5. Attendere il completamento del processo di reinstallazione, quindi riavviare il sistema.

- In **Windows 10** E **Finestre 11**:
  1. Clic **Inizio**, quindi fare clic su **Impostazioni**.
  2. Clicca il **Sistema** icona nell'area Impostazioni, quindi selezionare **App installate**.
  3. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
  4. Clic **Disinstalla** di nuovo per confermare la tua scelta.
  5. Clic **REINSTALLARE** nella finestra che appare.
  6. Attendere il completamento del processo di reinstallazione, quindi riavviare il sistema.

> **Nota**
> Seguendo questa procedura di reinstallazione, le impostazioni personalizzate vengono salvate e rese disponibili nel nuovo prodotto installato. Altre impostazioni possono essere ripristinate alla loro configurazione predefinita.

- **Bitdefender non è l'unica soluzione di sicurezza installata sul tuo sistema.**
  In questo caso:
  1. Rimuovi l'altra soluzione di sicurezza. Per maggiori informazioni, fai riferimento a Come posso rimuovere le altre soluzioni di sicurezza? (pagina 119).
  2. Reinstallare Bitdefender:
     - In **Windows 7**:
       a. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.
       b. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
       c. Clic **REINSTALLARE** nella finestra che appare.

d. Attendere il completamento del processo di reinstallazione, quindi riavviare il sistema.

- In **Windows 8** E **Windows 8.1**:

  a. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.

  b. Clic **Disinstalla** un programma o **Programmi e caratteristiche**.

  c. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.

  d. Clic **REINSTALLARE** nella finestra che appare.

  e. Attendere il completamento del processo di reinstallazione, quindi riavviare il sistema.

- In **Windows 10** E **Finestre 11**:

  a. Clic **Inizio**, quindi fare clic su **Impostazioni**.

  b. Clicca il **Sistema** nell'area Impostazioni, quindi selezionare **App installate**.

  c. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.

  d. Clic **Disinstalla** di nuovo per confermare la tua scelta.

  e. Clicca su **REINSTALLA** nella finestra che comparirà

  f. Attendere il completamento del processo di reinstallazione, quindi riavviare il sistema.

> **Nota**
> Seguendo questa procedura di reinstallazione, le impostazioni personalizzate vengono salvate e rese disponibili nel nuovo prodotto installato. Altre impostazioni possono essere ripristinate alla loro configurazione predefinita.

Se questa informazione non è stata utile, è possibile contattare BitDefender per avere assistenza, come descritto alla sezione Richiesta d'aiuto (pagina 287).

Non posso più usare una app

Questo problema si verifica quando stai cercando di usare un programma che prima dell'installazione di Bitdefender funzionava normalmente.

Dopo aver installato Bitdefender potrebbe verificarsi una di queste situazioni:

- Potresti ricevere un messaggio da Bitdefender che il programma sta cercando di eseguire una modifica al sistema.
- Potresti ricevere un messaggio d'errore dal programma che stai cercando di usare.

Questo tipo di situazione si verifica quando Advanced Threat Defense rileva alcune applicazioni come dannose per errore.

Advanced Threat Defense è una funzionalità di Bitdefender, che monitora costantemente le applicazioni in esecuzione sul tuo sistema, segnalando quelle con un comportamento potenzialmente dannoso. Poiché questa opzione è basata su un sistema euristico, potrebbero verificarsi dei casi in cui applicazioni legittime siano segnalate da Advanced Threat Defense.

Quando si verifica questa situazione, puoi escludere la rispettiva applicazione dal controllo di Advanced Threat Defense.

Per aggiungere il programma all'elenco delle eccezioni:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **DIFESA AVANZATA DALLE MINACCE** riquadro, fare clic **Aprire**.
3. Nel **Impostazioni** finestra, fare clic **Gestisci eccezioni**.
4. Clic **+ Aggiungi un'eccezione**.
5. Inserisci il percorso dell'eseguibile che vuoi escludere dalla scansione nel campo corrispondente.
   In alternativa, puoi accedere all'eseguibile facendo clic sul pulsante Sfoglia nella parte destra dell'interfaccia, selezionarlo e fare clic su **OK**.
6. Attiva l'interruttore accanto a **Difesa avanzata dalle minacce**.
7. Clic **Salva**.

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 287).

Cosa fare quando Bitdefender blocca un sito web, un dominio, un indirizzo IP o una app online che sono sicuri

Bitdefender offre un'esperienza di navigazione web sicura filtrando tutto il traffico web e bloccando qualsiasi contenuto dannoso. Tuttavia, è possibile che Bitdefender consideri un sito web, un dominio, un indirizzo IP o una app online sicuri come non sicuri, cosa che li farà bloccare in maniera errata dalla scansione del traffico HTTP di Bitdefender.

Qualora la stessa pagina, dominio, indirizzo IP o applicazione venisse bloccata più volte, è possibile aggiungerla alle eccezioni per evitare che venga controllata dai motori di Bitdefender, assicurando così un'esperienza di navigazione web più regolare.

Per aggiungere un sito web alle **Eccezioni**:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **PREVENZIONE DELLE MINACCE ONLINE** riquadro, fare clic **Impostazioni**.
3. Clic **Gestisci le eccezioni**.
4. Clic **+ Aggiungi un'eccezione**.
5. Digita nel campo corrispondente il nome del sito Web, il nome del dominio o l'indirizzo IP che desideri aggiungere alle eccezioni.
6. Fai clic sull'interruttore accanto a **Prevenzione delle minacce online**.
7. Clic **Salva** per salvare le modifiche e chiudere la finestra.

Dovresti aggiungere all'elenco solo siti web, domini, indirizzi IP e applicazioni di cui ti fidi assolutamente. Saranno esclusi dalle scansioni eseguite dai seguenti motori: minacce, phishing e frodi.

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 287).

Non riesco a connettermi a Internet

Dopo aver installato Bitdefender, potresti rilevare che un programma o un browser non è più in grado di connettersi a Internet o accedere ai servizi di rete.

In questo caso, la miglior soluzione è configurare Bitdefender per consentire automaticamente le connessioni da e per la rispettiva applicazione:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **FUOCO** riquadro, fare clic **Impostazioni**.
3. Nel **Regole** finestra, fare clic **Aggiungi regola**.
4. Comparirà una nuova finestra in cui potrai aggiungere i dettagli. Assicurati di selezionare tutti i tipi di rete disponibili e seleziona **Consenti** nella sezione **Autorizzazione**.

Chiudi Bitdefender, apri l'applicazione e riprova a connetterti a Internet.

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 287).

Non riesco ad accedere a un dispositivo nella mia rete

In base alla rete a cui sei connesso, il firewall di Bitdefender potrebbe bloccare la connessione tra il sistema e un altro dispositivo (come un altro computer o stampante). Di conseguenza, non potresti più condividere o stampare file.

In questo caso, la migliore soluzione è configurare Bitdefender per consentire automaticamente le connessioni da e per il rispettivo dispositivo, come segue:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **FUOCO** riquadro, fare clic **Impostazioni**.
3. Nel **Regole** finestra, fare clic **Aggiungi regola**.
4. Attiva l'opzione **Applica questa regola a tutte le applicazioni**.
5. Clicca sul pulsante **Impostazioni Avanzate**.
6. Nella casella **Indirizzo remoto personale**, digita l'indirizzo IP del computer o della stampante a cui vuoi accedere senza restrizioni.

Se non riesci ancora a collegarti al dispositivo, il problema potrebbe non essere causato da Bitdefender.

Controllare altre potenziali cause, ad esempio le seguenti:

- Il firewall nell'altro dispositivo potrebbe bloccare la condivisione di file e stampanti con il tuo PC.
  - Se viene utilizzato il firewall di Windows, è possibile configurarlo per permettere la condivisione di file e stampanti nel modo seguente:
    - In **Windows 7**:
      1. Clicca su **Start**, vai nel **Pannello di controllo** e seleziona **Sistema e sicurezza**.
      2. Vai in **Windows Firewall** e clicca su **Consenti un programma con Windows Firewall**.
      3. Seleziona la casella **Condivisione file e stampanti**.
    - In **Windows 8** E **Windows 8.1**:
      1. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.
      2. Clicca su **Sistema e sicurezza**, vai in **Windows Firewall** e seleziona **Consenti una app con Windows Firewall**.
      3. Seleziona la casella **Condivisione file e stampanti** e clicca su **OK**.
    - In **Windows 10** E **Finestre 11**:
      1. Digita "Consenti app attraverso Windows Firewall" nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona.
      2. Clicca su **Cambia impostazioni**.
      3. Nell'elenco **App e funzionalità consentite**, seleziona la casella **Condivisione file e stampanti** e clicca su **OK**.
  - Se viene utilizzato un altro programma firewall, fai riferimento alla sua documentazione o al file della guida.
- Condizioni generiche che possono impedire l'utilizzo o la connessione a una stampante condivisa:

- Potrebbe essere necessario accedere a un account di amministratore di Windows per poter accedere alla stampante condivisa.
- Potrebbero essere state impostate delle autorizzazioni per la stampante condivisa che permettono l'accesso solo a specifici dispositivo e utenti. Se stai condividendo la tua stampante, controlla le autorizzazioni impostate per la stampante per verificare che l'utente dell'altro dispositivo sia autorizzato ad accedervi. Se stai provando a collegarti a una stampante condivisa, controlla insieme all'utente dell'altro dispositivo di disporre delle autorizzazioni al collegamento alla stampante.
- La stampante associata al tuo dispositivo o all'altro non è condivisa.
- La stampante condivisa non è stata aggiunta al dispositivo.

> **Nota**
> Per apprendere come gestire la condivisione di stampanti (condividere una stampante, impostare o rimuovere autorizzazioni per una stampante, collegarsi a una stampante di rete o a una stampante condivisa) vai alla Guida in Linea e Supporto Tecnico di Windows (nel menu Start, clicca su {1}Guida in Linea e Supporto Tecnico{2}).

- L'accesso a una stampante di rete potrebbe essere ristretto a specifici dispositivi o utenti. Controlla con l'amministratore della rete, se disponi delle autorizzazioni al collegamento con tale stampante.

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 287).

Internet è lento

Questa situazione potrebbe verificarsi dopo aver installato Bitdefender. Il problema potrebbe essere causato da errori nella configurazione del firewall di Bitdefender.

Per risolvere questa situazione:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel pannello **FIREWALL**, disattiva l'interruttore per disattivare la funzionalità.

3. Verifica se la tua connessione a Internet è migliorata con il firewall di Bitdefender disattivato.
   - ❍ Se hai ancora una connessione a Internet lenta, il problema potrebbe non essere causato da Bitdefender. Contatta il tuo fornitore di servizi Internet per verificare se la connessione è attiva. Se ricevi conferma dal tuo fornitore di servizi Internet che la connessione è operativa e il problema persiste, contatta Bitdefender come descritto nella sezione Richiesta d'aiuto (pagina 287).
   - ❍ Se la connessione a Internet è migliorata dopo aver disattivato il firewall di Bitdefender:
     a. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
     b. Nel **FUOCO** riquadro, fare clic **Impostazioni**.
     c. Vai alla scheda **Adattatori di rete** e imposta la tua connessione a Internet come **Casa/Ufficio**.
     d. Nella scheda **Impostazioni**, disattiva **Protezione da port scan**. Nella sezione **Modalità invisibile**, clicca su **Modifica impostazioni mod. invisibile**. Attiva la modalità invisibile per l'adattatore di rete a cui ti connetti.
     e. Chiudi Bitdefender, riavvia il sistema e verifica la velocità della connessione a Internet.

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 287).

Come aggiornare Bitdefender con una connessione a Internet lenta

Se hai una connessione a Internet lenta (ad esempio modem tramite linea telefonica), potrebbero verificarsi degli errori durante l'aggiornamento.

Per mantenere il tuo sistema aggiornato con il più recente database delle informazioni sulle minacce di Bitdefender:

1. Clic **Impostazioni** nel menu di navigazione sul Interfaccia di Bitdefender.

2. Seleziona il **Aggiornamento** scheda.
3. Disattiva l'interruttore **Aggiornamento silenzioso**.
4. La prossima volta che sarà disponibile un aggiornamento, ti sarà chiesto di selezionare quale aggiornamento vuoi scaricare. Seleziona solo **Aggiornamento delle firme**.
5. Bitdefender scaricherà e installerà solo il database delle informazioni sulle minacce.

I servizi di Bitdefender non rispondono

Questo articolo aiuta a risolvere i problemi nel caso in cui **I servizi BitDefender non funzionano**. Si potrebbe trovare questo errore:

- L'icona Bitdefender nella **barra delle applicazioni** è grigia e ti sarà comunicato che i servizi di Bitdefender non rispondono.
- La finestra BitDefender mostra che i servizi BitDefender non stanno rispondendo.

L'errore potrebbe essere causato da una delle seguenti condizioni:

- errori temporanei di comunicazione tra i servizi di BitDefender.
- alcuni servizi di BitDefender sono arrestati.
- altri programmi di sicurezza sono in esecuzione sul dispositivo contemporaneamente a Bitdefender.

Per risolvere questo errore, provare queste soluzioni:

1. Aspettare alcuni momenti e vedere se qualcosa cambia. L'errore potrebbe essere temporaneo.
2. Riavviare il dispositivo e aspettare alcuni attimi fino a quando Bitdefender è caricato. Aprire BitDefender per vedere se l'errore persiste. Riavviare il dispositivo di solito risolve il problema.
3. Controllare che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di BitDefender. Se è così si raccomanda di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente BitDefender.
   Per maggiori informazioni, fai riferimento a Come posso rimuovere le altre soluzioni di sicurezza? (pagina 119).

Se l'errore persiste, contatta i nostri operatori del supporto tecnico per ricevere assistenza, come indicato nella sezione Richiesta d'aiuto (pagina 287).

Il filtro antispam non funziona correttamente

Questo articolo permette di risolvere i seguenti problemi delle operazioni di filtro Antispam di BitDefender:

- **Un numero di messaggi e-mail legittimi sono contrassegnati come [spam].**
- **Molti messaggi spam non sono contrassegnati come tali dal filtro antispam.**
- **Il filtro antispam non rileva nessun messaggio spam.**

I messaggi legittimi sono contrassegnati come [spam]

I messaggi legittimi sono segnati come [spam] semplicemente perché sembrano spam per il filtro antispam di Bitdefender. Normalmente puoi risolvere il problema configurando correttamente il filtro antispam.

Bitdefender aggiunge automaticamente i destinatari dei tuoi messaggi e-mail alla Lista amici. I messaggi e-mail ricevuti dai contatti nella lista amici vengono considerati legittimi. Non vengono verificati dal filtro antispam e, perciò, non verranno mai segnati come [spam].

La configurazione automatica dell'elenco Amici non impedisce gli errori di rilevamento che possono accadere in queste situazioni:

- Si ricevono molte e-mail commerciali richieste come risultato della sottoscrizione a vari siti web. In questo caso la soluzione è di aggiungere gli indirizzi e-mail da cui ricevi tali messaggi all'elenco amici.
- Una parte significativa delle tue e-mail legittime proviene da individui a cui non hai mai inviato e-mail in precedenza, ad esempio clienti, potenziali partner d'affari o altri. In questo caso sono richieste altre soluzioni.

Se stai utilizzando uno dei client e-mail con cui Bitdefender si integra, **indica gli errori di rilevazione**.

> **Nota**
> Bitdefender si integra nei client di posta più comunemente utilizzati tramite una barra degli strumenti antispam di facile utilizzo. Per un elenco completo dei client di posta supportati, fare riferimento a Programmi e protocolli di posta elettronica supportati (pagina 48).

Aggiungi contatti all'elenco Amici

Se stai utilizzando un'applicazione di posta supportata, puoi facilmente aggiungere i mittenti dei messaggi legittimi all'elenco amici. Segui questi passaggi:

1. Nell'applicazione di posta seleziona un messaggio e-mail inviato dal mittente che desideri aggiungere all'elenco Amici.
2. Clicca sul pulsante **Aggiungi amico** nella barra degli strumenti antispam di Bitdefender.
3. Può essere richiesto di accettare gli indirizzi aggiunti all'elenco Amici. Seleziona **Non mostrare di nuovo questo messaggio** e clicca su **OK**.

Riceverai sempre e-mail provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

Se si utilizza un'applicazione di posta differente, è possibile aggiungere i contatti all'elenco degli Amici dall'interfaccia di BitDefender. Segui questi passaggi:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel pannello **ANTISPAM**, clicca su **Gestisci amici**.
   Apparirà una finestra di configurazione.
3. Digita l'indirizzo e-mail da cui vuoi sempre ricevere i messaggi e clicca su **AGGIUNGI**. Puoi aggiungere quanti indirizzi e-mail desideri.
4. Clic **OK** per salvare le modifiche e chiudere la finestra.

Indica gli errori di rilevazione

Se stai utilizzando un client di posta supportato, puoi correggere facilmente il filtro antispam (indicando quali messaggi e-mail non devono essere contrassegnati come [spam]). Così facendo si migliorerà considerevolmente l'efficienza del filtro antispam. Segui questi passaggi:

1. Apri il tuo client di posta.

2. Vai alla cartella della posta indesiderata in cui vengono spostati i messaggi di spam.
3. Seleziona il messaggio legittimo scorrettamente contrassegnato come [spam] da Bitdefender.
4. Clicca sul pulsante **Aggiungi amico** nella barra degli strumenti dell'antispam di Bitdefender per aggiungere un mittente all'elenco amici. Potrebbe essere necessario cliccare su **OK** per confermare. Riceverai sempre i messaggi e-mail da questo indirizzo indipendentemente dal loro contenuto.
5. Clicca il **Non spam** pulsante sulla barra degli strumenti antispam di Bitdefender (normalmente situata nella parte superiore della finestra del client di posta). Il messaggio e-mail verrà spostato nella cartella Posta in arrivo.

Molti messaggi spam non vengono rilevati

Se si ricevono molti messaggi spam che non vengono contrassegnati come [spam], è necessario configurare il filtro antispam di Bitdefender in modo da migliorarne l'efficienza.

Prova le seguenti soluzioni:

1. Se stai utilizzando uno dei client di posta in cui Bitdefender è integrato, dovresti **indicare i messaggi spam non rilevati**.

> **Nota**
> Bitdefender si integra nei client di posta più comunemente utilizzati tramite una barra degli strumenti antispam di facile utilizzo. Per un elenco completo dei client di posta supportati, fare riferimento a Programmi e protocolli di posta elettronica supportati (pagina 48).

2. **Aggiungi gli spammer all'elenco Spammer**. I messaggi e-mail ricevuti dagli indirizzi nell'elenco Spammer vengono segnati automaticamente come [spam].

Indica i messaggi spam non rilevati

Se utilizzi un client di posta supportato, puoi facilmente indicare quali messaggi di posta elettronica avrebbero dovuto essere rilevati come spam. In questo modo si migliora l'efficienza del filtro antispam. Segui questi passi:

1. Apri il tuo client di posta.
2. Vai alla cartella Posta in arrivo.
3. Seleziona i messaggi di spam non rilevati.
4. Clicca sul pulsante **È spam** sulla barra degli strumenti antispam di Bitdefender (normalmente localizzata nella parte superiore della finestra del client di posta). Sono subito marcati come [spam] e spostati nella cartella Cestino.

Aggiungi spammer a elenco Spammer

Se stai utilizzando un'applicazione di posta supportata, puoi facilmente aggiungere i mittenti dei messaggi di spam all'elenco Spammer. Segui questi passaggi:

1. Apri il tuo client di posta.
2. Vai alla cartella della posta indesiderata in cui vengono spostati i messaggi di spam.
3. Selezionare i messaggi contrassegnati come [spam] da Bitdefender.
4. Clicca sul pulsante **Aggiungi spammer** nella barra degli strumenti antispam di Bitdefender.
5. Può essere richiesto di accettare gli indirizzi aggiunti all'elenco degli Spammer. Seleziona **Non mostrare di nuovo questo messaggio** e clicca su **OK**.

Se utilizzi un client di posta diverso, puoi aggiungere manualmente nuovi contatti all'elenco Spammer dall'interfaccia di Bitdefender. Si tratta di un metodo conveniente solo quando si ricevono diversi messaggi spam dallo stesso indirizzo e-mail. Segui questi passaggi:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTI-SPAM** riquadro, fare clic **Impostazioni**.
3. Vai alla finestra **Gestisci spammer**.
4. Digita l'indirizzo e-mail dello spammer e poi clicca su **Aggiungi**. Puoi aggiungere quanti indirizzi e-mail desideri.
5. Clic **OK** per salvare le modifiche e chiudere la finestra.

Il Filtro antispam non rileva alcun messaggio spam

Se nessun messaggio spam viene contrassegnato come [spam], potrebbe esserci un problema relativo al filtro Antispam BitDefender. Prima di

risolvere questo problema, assicurati che non sia causato da una delle seguenti condizioni:

- La protezione antispam potrebbe essere disattivata. Per verificare lo stato della protezione antispam, clicca su **Protezione** nel menu di navigazione nell'**interfaccia di Bitdefender**. Guarda nel pannello **Antispam** per controllare se la funzionalità è attivata.
  Se l'antispam è disattivato, questa è la causa dei problemi. Clicca sull'interruttore corrispondente per attivare la protezione antispam.
- La protezione antispam di Bitdefender è disponibile solo per i client e-mail configurati per ricevere messaggi e-mail tramite il protocollo POP3. Ciò può significare:
  - I messaggi e-mail ricevuti tramite servizi e-mail web (ad esempio Yahoo, Gmail, Hotmail o altri) non sono filtrati per spam da Bitdefender.
  - Se il tuo client di e-mail è configurato per ricevere messaggi e-mail usando un protocollo diverso da POP3 (per esempio, IMAP4), il filtro Antispam di Bitdefender non li controllerà per cercare eventuali spam.

  > **Nota**
  > POP3 è uno dei protocolli più usati per scaricare messaggi e-mail da un server di posta. Se non si conosce il protocollo usato dal proprio client e-mail per scaricare messaggi e-mail, chiedere alla persona che ha configurato il proprio client e-mail.
- Bitdefender Ultimate Small Business Security non esegue la scansione del traffico POP3 di Lotus Notes.

Una possibile soluzione consiste nel riparare o reinstallare il prodotto. Tuttavia si consiglia di contattare BitDefender per supporto, come descritto nella sezione Richiesta d'aiuto (pagina 287).

Rimozione di Bitdefender non riuscita

Se desideri rimuovere il tuo prodotto Bitdefender ma il processo o il sistema si blocca, clicca su **Annulla** per interrompere l'operazione. Se questo non dovesse funzionare, riavviare il sistema.

Se la rimozione non riesce, alcuni file e alcune chiavi di registro di Bitdefender potrebbero rimanere sul sistema. Tali rimanenze potrebbero

impedire una nuova installazione di Bitdefender. Potrebbero inoltre influenzare le prestazioni e la stabilità del sistema.

Per rimuovere completamente Bitdefender dal sistema:

- In **Windows 7**:
  1. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.
  2. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
  3. Clic **RIMUOVERE** nella finestra che appare.
  4. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

- In **Windows 8** E **Windows 8.1**:
  1. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.
  2. Clic **Disinstallare un programma** O **Programmi e caratteristiche**.
  3. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
  4. Clic **RIMUOVERE** nella finestra che appare.
  5. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

- In **Windows 10** E **Finestre 11**:
  1. Clic **Inizio**, quindi fai clic su Impostazioni.
  2. Clicca il **Sistema** nell'area Impostazioni, quindi selezionare **App installate**.
  3. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
  4. Clic **Disinstalla** di nuovo per confermare la tua scelta.
  5. Clic **RIMUOVERE** nella finestra che appare.

6. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

Il sistema non si riavvia dopo aver installato Bitdefender

Se hai appena installato Bitdefender e non riesci più a riavviare il sistema in modalità normale potrebbero esserci varie cause per questo problema.

Molto probabilmente la causa è un'installazione precedente di Bitdefender che non è stata rimossa correttamente o un'altra soluzione di sicurezza ancora presente sul sistema.

Ecco come affrontare ogni situazione:

- **In precedenza hai avuto Bitdefender e non l'hai rimosso correttamente.**
  Per risolvere:

  1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a Come posso riavviare in modalità provvisoria? (pagina 121).
  2. Rimuovere Bitdefender dal tuo sistema:
     - In **Windows 7**:
       a. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.
       b. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.
       c. Clic **RIMUOVERE** nella finestra che appare.
       d. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.
       e. Riavvia il sistema in modalità normale.
     - In **Windows 8** E **Windows 8.1**:
       a. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.

b. Clic **Disinstallare un programma** O **Programmi e caratteristiche**.

c. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.

d. Clic **RIMUOVERE** nella finestra che appare.

e. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

f. Riavvia il sistema in modalità normale.

- In **Windows 10** E **Finestre 11**:

  a. Clic **Inizio**, quindi fai clic su Impostazioni.

  b. Clicca il **Sistema** icona nell'area Impostazioni, quindi selezionare **App installate**.

  c. Trovare **Bitdefender Ultimate Small Business Security** e seleziona **Disinstalla**.

  d. Clic **Disinstalla** di nuovo per confermare la tua scelta.

  e. Clic **RIMUOVERE** nella finestra che appare.

  f. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

  g. Riavvia il sistema in modalità normale.

3. Reinstalla il tuo prodotto Bitdefender.

- **In precedenza avevi un'altra soluzione di sicurezza e non l'hai rimossa correttamente.**
  Per risolvere questo:

  1. Riavvia il sistema ed entra in modalità provvisoria. Per sapere come fare, fare riferimento a Come posso riavviare in modalità provvisoria? (pagina 121).
  2. Rimuovi l'altra soluzione di sicurezza dal sistema:
     - In **Windows 7**:

       a. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.

b. Trova il nome del programma che desideri rimuovere e seleziona {1}Rimuovi{2}.

c. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

- In **Windows 8** E **Windows 8.1**:

  a. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.

  b. Clic **Disinstallare un programma** O **Programmi e caratteristiche**.

  c. Trova il nome del programma che desideri rimuovere e seleziona **Rimuovere**.

  d. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

- In **Windows 10** E **Finestre 11**:

  a. Clic **Inizio**, quindi fai clic su Impostazioni.

  b. Clicca il **Sistema** nell'area Impostazioni, quindi selezionare **App installate**.

  c. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.

  d. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

Per disinstallare correttamente l'altro software, vai nel sito web del produttore ed esegui lo strumento di disinstallazione o contattalo direttamente per ricevere le istruzioni di disinstallazione.

3. Riavvia il sistema in modalità normale e reinstalla Bitdefender.

Hai già seguito i passaggi sopra indicati e la situazione non è cambiata.

Per risolvere questo:

1. Riavvia il sistema ed entra in modalità provvisoria. Per sapere come fare, fare riferimento a Come posso riavviare in modalità provvisoria? (pagina 121).
2. Usa l'opzione Ripristino configurazione di sistema di Windows per ripristinare il dispositivo a uno stato precedente all'installazione del prodotto Bitdefender.
3. Riavvia il sistema in modalità normale e contatta i nostri operatori del supporto per assistenza, come indicato nella sezione Richiesta d'aiuto (pagina 287).

3.5.2. Rimuovere le minacce dal sistema

Le minacce possono influenzare il sistema in molti modi diversi e l'approccio di Bitdefender dipende dal tipo di attacco della minaccia. Poiché le minacce modificano spesso il loro comportamento, è difficile stabilire uno schema per il loro comportamento e le loro azioni.

Ci sono alcune circostanze in cui Bitdefender non può rimuovere automaticamente l'infezione della minaccia dal tuo sistema. In tali casi, è richiesto il tuo intervento.

- Ambiente di salvataggio (pagina 144)
- Cosa fare quando Bitdefender trova delle minacce sul tuo dispositivo? (pagina 144)
- Come posso rimuovere una minaccia in un archivio? (pagina 146)
- Come posso rimuovere una minaccia in un archivio di e-mail? (pagina 147)
- Cosa fare se sospetti che un file possa essere pericoloso? (pagina 148)
- Quali sono i file protetti da password nel registro della scansione? (pagina 148)
- Quali sono gli elementi ignorati nel registro della scansione? (pagina 149)
- Quali sono i file supercompressi nel registro della scansione? (pagina 149)
- Perché Bitdefender ha eliminato automaticamente un file infetto? (pagina 149)

Se non riesci a trovare il tuo problema qui, o se le soluzioni presentate non lo risolvono, puoi contattare i rappresentanti dell'assistenza tecnica di Bitdefender come presentato nel capitolo Richiesta d'aiuto (pagina 287).

Ambiente di salvataggio

L'**Ambiente di soccorso** è una funzionalità di Bitdefender che ti consente di controllare e disinfettare tutte le partizioni del disco rigido esistenti, interne ed esterne al tuo sistema operativo.

L'ambiente di soccorso di Bitdefender è integrato con Windows RE.

Avviare il tuo sistema nell'Ambiente di soccorso

Puoi accedere all'ambiente di soccorso solo dal tuo prodotto Bitdefender, come segue:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Clicca su **Apri** accanto ad **Ambiente di soccorso**.
4. Clicca su **RIAVVIA** nella finestra che comparirà.
   L'ambiente di soccorso di Bitdefender sarà pronto tra pochi istanti.

Controllare il sistema nell'Ambiente di soccorso

Per esaminare il tuo sistema nell'Ambiente di soccorso:

1. Accedi all'ambiente di soccorso, come descritto in .
2. Il processo di scansione di Bitdefender parte automaticamente non appena il sistema viene caricato nell'ambiente di soccorso.
3. Attendi il completamento della scansione. Se viene rilevata una minaccia, segui le istruzioni per rimuoverla.
4. Per uscire dall'Ambiente di soccorso, clicca sul pulsante Chiudi nella finestra dei risultati della scansione.

Cosa fare quando Bitdefender trova delle minacce sul tuo dispositivo?

Potresti scoprire che esiste una minaccia sul tuo dispositivo in uno dei seguenti modi:

- Hai controllato il tuo dispositivo e Bitdefender ha trovato alcuni elementi infetti.
- Un avviso di minaccia ti informa che Bitdefender ha bloccato una o più minacce sul tuo dispositivo.

In tali situazioni, aggiorna Bitdefender per assicurarti di avere il più recente database delle informazioni sulle minacce e avvia una Scansione del sistema per analizzarlo.

Al termine della scansione del sistema, seleziona l'azione desiderata per gli elementi infetti (Disinfetta, Elimina, Sposta in quarantena).

> **Avvertimento**
> Se sospetti che il file sia parte del sistema operativo Windows o che non sia un file infetto, non seguire questi passaggi e contatta l'assistenza clienti di Bitdefender il prima possibile.

Se l'azione selezionata non può essere eseguita e il registro della scansione rivela un'infezione non eliminabile, devi rimuovere manualmente i file:

Il primo metodo può essere usato in modalità normale:

1. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
   b. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
   c. Nel **Avanzate** finestra, spegnere **Scudo di Bitdefender**.
2. Visualizza gli oggetti nascosti in Windows. Per sapere come fare, fare riferimento a Come posso visualizzare gli elementi nascosti in Windows? (pagina 118).
3. Trova l'ubicazione del file infetto (controlla il registro della scansione) ed eliminalo.
4. Attiva la protezione antivirus in tempo reale di Bitdefender.

Se il primo metodo non riuscisse a rimuovere l'infezione:

1. Riavvia il sistema ed entra in modalità provvisoria. Per sapere come fare, fare riferimento a Come posso riavviare in modalità provvisoria? (pagina 121).

2. Visualizza gli oggetti nascosti in Windows. Per sapere come fare, fare riferimento a Come posso visualizzare gli elementi nascosti in Windows? (pagina 118).
3. Individuare la posizione del file infetto (controllare il registro della scansione) ed eliminarlo.
4. Riavvia il sistema ed entra in modalità normale.

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 287).

Come posso rimuovere una minaccia in un archivio?

Un archivio è un file o una raccolta di file compressi in un formato speciale per ridurre lo spazio su disco necessario alla loro archiviazione.

Alcuni di questi formati sono aperti, offrendo così a Bitdefender l'opportunità per controllarli all'interno e intraprendere le azioni adeguate per rimuoverli.

Altri formati dell'archivio sono chiusi parzialmente o interamente, e Bitdefender può solo rilevare la presenza di minacce al loro interno, senza poter intraprendere alcuna azione.

Se Bitdefender ti avvisa di aver rilevato una minaccia in un archivio e di non poter attuare alcuna azione, significa che non puoi rimuovere la minaccia a causa delle restrizioni sulle impostazioni di permesso dell'archivio.

Ecco come rimuovere una minaccia in un archivio:

1. Identifica l'archivio che include la minaccia, eseguendo una scansione del sistema.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
   b. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
   c. Nel **Avanzate** finestra, spegnere **Scudo di Bitdefender**.
3. Vai all'ubicazione dell'archivio e decomprimilo usando un programma di compressione, come WinZip.

4. Identifica il file infetto e lo elimina.
5. Elimina l'archivio originale per assicurarti che l'infezione sia stata rimossa completamente.
6. Ricomprimi i file in un nuovo archivio usando un'applicazione di archiviazione, come WinZip.
7. Attiva la protezione antivirus in tempo reale di Bitdefender ed esegui una scansione del sistema per assicurarti che non ci siano altre infezioni.

   Nota
   È importante notare che una minaccia in un archivio non è una minaccia immediata al sistema, poiché deve essere decompressa ed eseguita per infettarlo.

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 287).

Come posso rimuovere una minaccia in un archivio di e-mail?

Bitdefender può anche identificare le minacce nei database e-mail e negli archivi e-mail presenti sul disco rigido.

A volte devi identificare il messaggio infetto usando le informazioni fornite nel rapporto della scansione ed eliminarlo manualmente.

Ecco come rimuovere una minaccia presente in un archivio e-mail:

1. Esamina il database delle e-mail con Bitdefender.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
   b. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
   c. Nel **Avanzate** finestra, spegnere **Scudo di Bitdefender**.
3. Apri il rapporto della scansione e usa le informazioni d'identificazione (oggetto, da, a) dei messaggi infettati per localizzarli nel client e-mail.
4. Elimina i messaggi infetti. La maggior parte dei client e-mail spostano il messaggio eliminato in una cartella di recupero, dalla quale può

essere recuperato. Dovresti assicurarti che il messaggio sia eliminato anche da questa cartella di ripristino.

5. Compatta la cartella di memorizzazione del messaggio infetto.
   - In Microsoft Outlook 2007: nel menu File, clicca su Gestione file dati. Seleziona i file delle cartelle personali (.pst) che intendi compattare e clicca su Impostazioni. Clicca su Compatta ora.
   - In Microsoft Outlook 2010 / 2013/ 2016: nel menu File, clicca su Info e poi su Impostazioni account (Aggiungi e rimuovi account o cambia le impostazioni di connessione attuali). Poi clicca su File di dati, seleziona i file delle cartelle personali (.pst) che intendi compattare e clicca su Impostazioni. Clicca su Compatta ora.
6. Attiva la protezione antivirus in tempo reale di Bitdefender.

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 287).

Cosa fare se sospetti che un file possa essere pericoloso?

Puoi sospettare che un file del tuo sistema sia pericoloso, anche se il prodotto Bitdefender non l'ha rilevato.

Per assicurarti che il tuo sistema sia protetto:

1. Esegui una **Scansione sistema** con Bitdefender. Per scoprire come fare, fai riferimento a {3}{4}.
2. Se il risultato della scansione non segnala nulla, ma hai ancora dubbi e vuoi essere certo che il file sia pulito, contatta gli operatori del nostro supporto tecnico per ricevere assistenza.
   Per scoprire come fare, fai riferimento a Richiesta d'aiuto (pagina 287).

Quali sono i file protetti da password nel registro della scansione?

Questa è solo una notifica per indicare che Bitdefender ha rilevato che questi file sono protetti da una password o da una qualche forma di crittografia.

In genere gli elementi protetti da password sono:

- File che appartengono a un'altra soluzione di sicurezza.
- File che appartengono al sistema operativo.

Per poter controllare i contenuti, devi estrarre o quantomeno decriptare questi file.

Qualora tali contenuti venissero estratti, la scansione in tempo reale di Bitdefender li controllerebbe automaticamente per proteggere il tuo dispositivo. Se desideri controllare quei file con Bitdefender, devi contattare il produttore per ottenere maggiori informazioni sui file.

Ti consigliamo di ignorare quei file perché non sono una minaccia per il sistema.

Quali sono gli elementi ignorati nel registro della scansione?

Tutti i file che compaiono come Ignorati nel rapporto della scansione sono puliti.

Per prestazioni superiori, Bitdefender non controlla file che non sono stati modificati dall'ultima scansione.

Quali sono i file supercompressi nel registro della scansione?

Gli oggetti supercompressi sono elementi che non possono essere estratti dal motore di scansione o elementi per i quali la crittografia avrebbe impiegato troppo tempo, rendendo il sistema instabile.

Supercompresso significa che Bitdefender ha saltato la scansione di quell'archivio perché scompattarlo avrebbe richiesto troppe risorse di sistema. Se necessario, il contenuto sarà controllato solo durante l'accesso in tempo reale.

Perché Bitdefender ha eliminato automaticamente un file infetto?

Se viene rilevato un file infetto, Bitdefender tenterà di disinfettarlo automaticamente. Se la disinfezione dovesse fallire, il file sarà messo in quarantena per contenere l'infezione.

Per particolari tipi di minacce, la disinfezione non è possibile perché il file rilevato è interamente dannoso. In tali casi, il file infetto viene eliminato dal disco.

Questo di solito è il caso di file di installazione che vengono scaricati da siti web non attendibili. Se dovessi trovarti in tale situazione, scarica il file d'installazione dal sito web del produttore o da un altro sito web affidabile.

4. ANTIVIRUS PER MAC

4.1. Cos'è Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac è un potente scanner antivirus, che può rilevare e rimuovere ogni tipo di software dannoso ("minacce"), tra cui:

- ransomware
- adware
- virus
- spyware
- Trojan
- keylogger
- worm

Questa applicazione non solo rileva e rimuove le minacce per Mac, ma anche quelle per Windows, impedendo quindi di inviare accidentalmente file infetti a familiari, amici e colleghi che utilizzano un PC.

4.2. Installazione e rimozione

Questo capitolo include i seguenti argomenti:

- Requisiti di sistema (pagina 150)
- Installazione di Bitdefender Antivirus for Mac (pagina 151)
- Rimuovere Bitdefender Antivirus for Mac. (pagina 155)

4.2.1. Requisiti di sistema

Puoi installare Bitdefender Antivirus for Mac su computer Macintosh con OS X Yosemite (10.10) o versioni successive.

Il tuo Mac deve avere un minimo di 1 GB di spazio disponibile sul disco rigido.

Per registrare e aggiornare Bitdefender Antivirus for Mac è richiesta una connessione a Internet.

Nota
Bitdefender Anti-tracker e Bitdefender VPN possono essere installati solo su sistemi con macOS 10.12 o versioni successive.

Come scoprire la versione del tuo macOS e le informazioni hardware sul tuo Mac
Clicca sull'icona Apple nell'angolo in alto a sinistra dello schermo e seleziona Informazioni su **questo Mac**. Nella finestra che comparirà, potrai visualizzare la versione del tuo sistema operativo e altre informazioni utili. Clicca su **Resoconto di sistema** per informazioni più dettagliate sull'hardware.

4.2.2. Installazione di Bitdefender Antivirus for Mac

La app Bitdefender Antivirus for Mac può essere installata dal tuo account Bitdefender come segue:

1. Accedi come amministratore.
2. Vai in: https://central.bitdefender.com.
3. Accedi al tuo account Bitdefender utilizzando il tuo indirizzo e-mail e la tua password.
4. Seleziona il pannello **I miei dispositivi** e clicca su **INSTALLA PROTEZIONE**.
5. Seleziona una delle due opzioni disponibili:
   - **Proteggi questo dispositivo**
     a. Seleziona questa opzione e poi il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, clicca sul pulsante corrispondente.
     b. Salva il file di installazione.
   - **Proteggi altri dispositivi**
     a. Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.
     b. Clicca su **INVIA LINK DI DOWNLOAD**.
     c. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA E-MAIL**.

Nota che il link di download generato è valido solo per le prossime 24 ore. Se il link dovesse scadere, dovrai generarne uno nuovo seguendo gli stessi passaggi.

d. Sul dispositivo su cui vuoi installare il tuo prodotto Bitdefender, controlla l'account e-mail che hai digitato e poi clicca sul pulsante di download corrispondente.

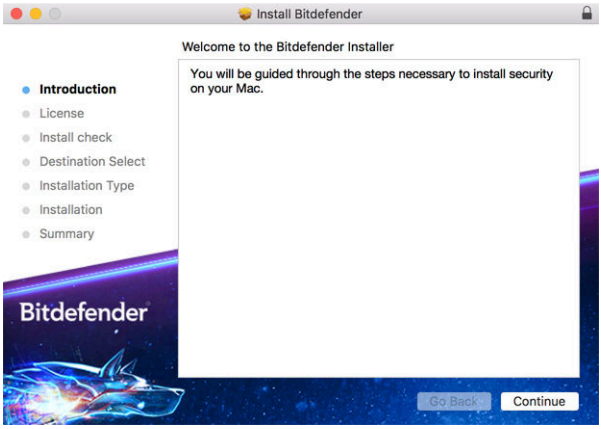
6. Esegui il prodotto Bitdefender che hai scaricato.
7. Completa tutti i passaggi dell'installazione.

Fase di installazione

Per installare Bitdefender Antivirus for Mac:

1. Clicca sul file scaricato. Sarà lanciato il programma d'installazione, che ti guiderà attraverso il processo d'installazione.
2. Segui la procedura guidata dell'installazione.

Passo 1 - Finestra di benvenuto



Clicca su **Continua**.

Passo 2 - Leggi l'Accordo di Abbonamento

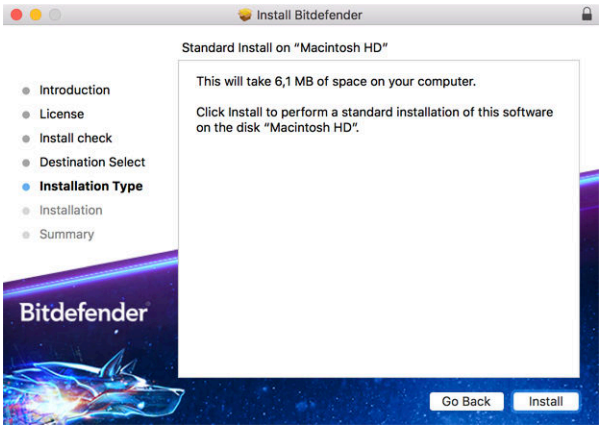
Prima di continuare con l'installazione, devi accettare l'Accordo di abbonamento. Prenditi qualche istante per leggere l'Accordo di abbonamento in quanto contiene i termini e le condizioni con cui è possibile utilizzare Bitdefender Antivirus for Mac.

Da questa finestra puoi anche selezionare la lingua con cui vuoi installare il prodotto.

Clicca su **Continua** e poi su **Accetto**.

> **Importante**
> Se non accetti i termini, clicca su **Continua** e poi su **Rifiuta** per annullare l'installazione e uscire dal relativo programma.

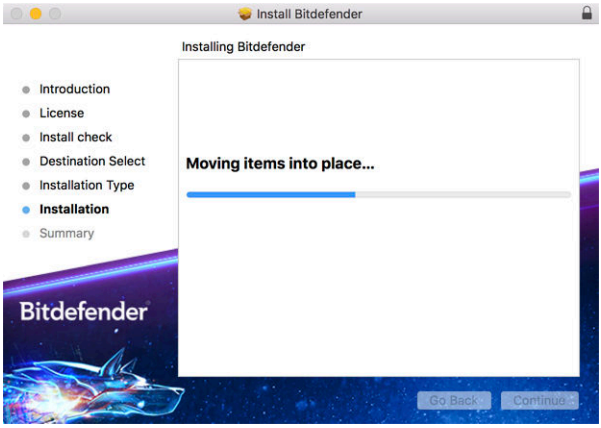
Passo 3 - Inizia l'installazione



Bitdefender Antivirus for Mac sarà installato in Macintosh HD/Library/Bitdefender. Non è possibile modificare il percorso di installazione.

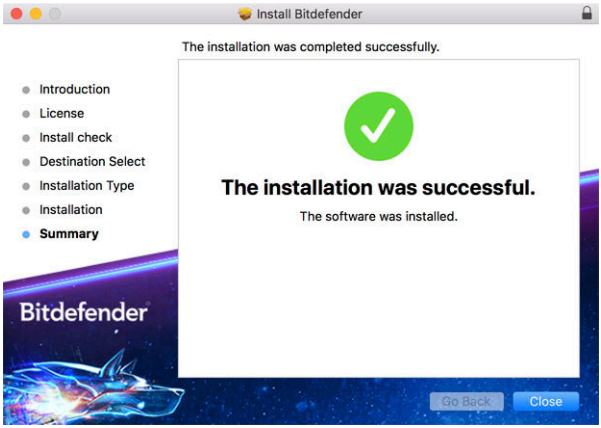
Clicca su **Installa** per avviare l'installazione.

Fase 4 - Installazione di Bitdefender Antivirus for Mac



Attendi la fine dell'installazione e clicca su **Continua**.

Passaggio 5 - Fine



Clicca su **Chiudi** per chiudere la finestra del programma d'installazione.

Ora hai completato la fase d'installazione.

Importante

- Se stai installando Bitdefender Antivirus for Mac su macOS High Sierra 10.13.0 o una versione successiva, comparirà la notifica **Estensione del sistema bloccata**. Questa notifica ti informa che le estensioni firmate da Bitdefender sono state bloccate e dovrai attivarle manualmente. Clicca su OK per continuare. Nella finestra di Bitdefender Antivirus for Mac che comparirà, clicca sul link **Security & Privacy**. Clicca su **Consenti** nella parte inferiore della finestra o seleziona Bitdefender SRL dall'elenco e clicca su **OK**.
- Se stai installando Bitdefender Antivirus for Mac su macOS Mojave 10.14 o una versione più recente, comparirà una nuova finestra, informandoti che devi **garantire a Bitdefender pieno accesso al disco** e **consentire il caricamento a Bitdefender**. Segui le istruzioni su schermo per configurare correttamente il prodotto.

4.2.3. Rimuovere Bitdefender Antivirus for Mac.

Essendo un'applicazione complessa, Bitdefender Antivirus for Mac non può essere rimossa in modo tradizionale, semplicemente trascinando l'icona dell'applicazione dalla cartella **Applicazioni** al Cestino.

Per rimuovere Bitdefender Antivirus for Mac, segui questi passaggi:

1. Apri una finestra di **Finder** e vai alla cartella **Applicazioni**.
2. Apri la cartella Bitdefender in **Applicazioni** e poi clicca due volte su **BitdefenderUninstaller**.
3. Seleziona l'opzione di disinstallazione preferita.

   Nota
   Se stai cercando di rimuovere solo la app Bitdefender VPN, seleziona solo **Disinstalla VPN**.

4. Clicca su **Disinstalla** e attendi il completamento del processo.
5. Clicca su **Chiudi** per terminare.

   Importante
   In caso di errore, puoi contattare il Servizio clienti di Bitdefender come descritto in Richiesta d'aiuto (pagina 287).

4.3. Iniziare

Questo capitolo include i seguenti argomenti:

4.3.1. Aprire Bitdefender Antivirus for Mac

Puoi aprire Bitdefender Antivirus for Mac in diversi modi.

- Clicca sull'icona di Bitdefender Antivirus nel Launchpad.
- Clicca sull'icona nella barra del menu e seleziona **Apri interfaccia Antivirus**.
- Apri una finestra di Finder, vai in Applicazioni e clicca due volte sull'icona di **Bitdefender Antivirus for Mac**.

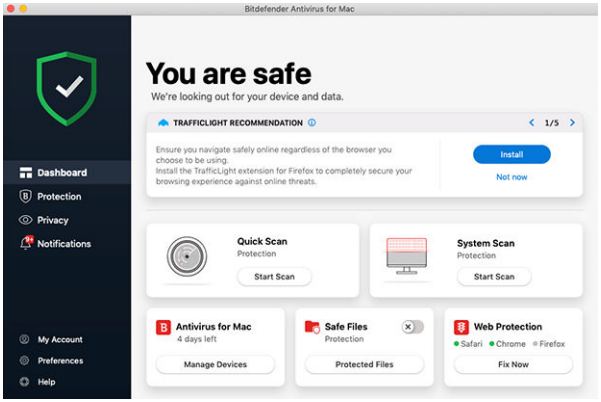
Importante

La prima volta che si apre Bitdefender Antivirus for Mac su macOS Mojave 10.14 o una versione più recente, comparirà un suggerimento di protezione. Tali suggerimenti compaiono perché ci servono i permessi per esaminare l'intero sistema alla ricerca di minacce. Per darci i permessi, devi accedere come amministratore e seguire questi passaggi:

1. Clicca sul link **Preferenze di sistema**.
2. Clicca sull'icona e poi inserisci le tue credenziali di amministratore.
3. Si aprirà una nuova finestra. Trascina il file **BDLDaemon** nell'elenco delle app autorizzate.

4.3.2. Finestra principale della app

Bitdefender Antivirus for Mac soddisfa sia le necessità degli utenti esperti che quelle dei principianti. L'interfaccia grafica è quindi stata progettata per essere adatta a qualsiasi categoria di utenti.



Per apprendere l'interfaccia di Bitdefender, in alto a sinistra comparirà una procedura guidata introduttiva contenente maggiori dettagli su come interagire con il prodotto e configurarlo correttamente. Scegli la giusta parentesi angolare per continuare con la guida, o **Salta il tour** per chiudere la procedura guidata.

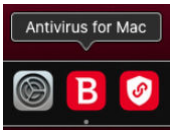
La barra di stato nella parte superiore della finestra ti informa sullo stato di sicurezza del sistema usando messaggi chiari e colori indicativi. Se Bitdefender Antivirus for Mac non ha alcun avviso, la scheda dello stato è verde. Quando viene rilevato un problema di sicurezza, la scheda dello stato diventa rossa. Per maggiori dettagli sui problemi e come risolverli, fai riferimento a Risoluzione problemi (pagina 172).

Per offrirti un funzionamento efficace e una maggiore protezione mentre esegui diverse attività, **Bitdefender Autopilot** agirà come tuo consulente di sicurezza personale. In base alle attività eseguite, sia che tu stia lavorando o effettuando pagamenti online, Bitdefender Autopilot ti fornirà suggerimenti contestuali basati sull'uso e le esigenze del tuo dispositivo. Ciò ti aiuterà a scoprire e usufruire dei vantaggi offerti dalle funzionalità incluse nella app Bitdefender Antivirus for Mac.

Dal menu di navigazione sul lato sinistro puoi accedere alle sezioni di Bitdefender per una configurazione dettagliata e attività amministrative avanzate (schede **Protezione** e **Privacy**), notifiche, il tuo **account Bitdefender** e la zona delle **Preferenze**. Inoltre, puoi contattarci (scheda **Aiuto**) se avessi delle domande o dovesse apparire qualcosa di inatteso.

4.3.3. Icona app nel Dock

L'icona di Bitdefender Antivirus for Mac può essere notata nel Dock non appena si apre la app. L'icona nel Dock ti fornisce un facile modo per esaminare file e cartelle alla ricerca di minacce. Basta trascinare e rilasciare il file o la cartella sull'icona del Dock e la scansione inizierà immediatamente.



4.3.4. Menu di navigazione

Sul lato sinistro dell'interfaccia di Bitdefender si trova il menu di navigazione, che ti consente di accedere rapidamente alle funzionalità di Bitdefender necessarie per la gestione del prodotto. In quest'area sono disponibili le seguenti schede:

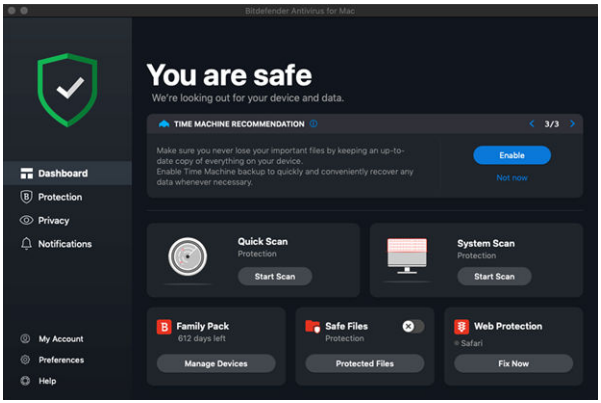
- **Dashboard**. Da qui puoi risolvere rapidamente eventuali problemi di sicurezza, visualizzare suggerimenti in base alle esigenze del tuo

sistema e l'utilizzo del prodotto, eseguire azioni rapide e andare al tuo account Bitdefender per gestire i dispositivi che hai aggiunto al tuo abbonamento Bitdefender.

- **Protezione**. Da qui, puoi eseguire attività di scansione antivirus, aggiungere file all'elenco delle eccezioni, proteggere file e app da attacchi ransomware, proteggere i tuoi backup Time Machine, e configurare la protezione durante la navigazione su Internet.
- **Privacy**. Da qui, puoi aprire la app Bitdefender VPN e installare l'estensione Anti-tracker nel tuo browser web.
- **Notifiche**. Da qui, puoi visualizzare maggiori dettagli sulle azioni intraprese sui file esaminati.
- **Il mio account**. Da qui, puoi visualizzare il tuo account Bitdefender e l'abbonamento con cui il tuo dispositivo è protetto, nonché cambiare il tuo account, se necessario.
- **Preferenze**. Da qui, puoi configurare le impostazioni di Bitdefender.
- **Aiuto**. Da qui, ogni volta che ti serve assistenza nel risolvere una situazione con il tuo prodotto Bitdefender, puoi contattare il Supporto tecnico. Puoi anche lasciarci un tuo feedback per aiutarci a migliorare il prodotto.

4.3.5. Modalità scura

Per proteggere gli occhi da bagliori e luci mentre si lavora di notte o in condizioni di scarsa luminosità, Bitdefender Antivirus for Mac supporta la modalità scura per Mojave 10.14 e versioni successive. I colori dell'interfaccia sono stati ottimizzati per poter usare il Mac senza sforzare gli occhi. L'interfaccia di Bitdefender Antivirus for Mac si regola automaticamente in base alle impostazioni video del tuo dispositivo.



4.4. Proteggersi da software dannoso

Questo capitolo include i seguenti argomenti:

4.4.1. Consigli

Per tenere il tuo sistema sempre privo di minacce e impedire un'infezione accidentale di altri sistemi, segui questi consigli:

- Mantieni attivato **Bitdefender Shield**, per consentire la scansione automatica dei file di sistema da parte di Bitdefender Antivirus for Mac.
- Mantieni il tuo prodotto Bitdefender Antivirus for Mac aggiornato con gli ultimi aggiornamenti del prodotto e delle informazioni delle minacce.
- Controlla regolarmente e risolvi i problemi segnalati da Bitdefender Antivirus for Mac. Per informazioni dettagliate, fai riferimento a Risoluzione problemi (pagina 172).
- Controlla il registro degli eventi riguardanti le attività di Bitdefender Antivirus for Mac sul tuo computer. Ogni volta che accade qualcosa di rilevante per la sicurezza del sistema o dei dati, viene aggiunto un nuovo messaggio nell'area delle notifiche di Bitdefender. Per maggiori dettagli, accedere a Notifiche (pagina 173).
- Dovresti seguire questi consigli:
  - Prendi l'abitudine di controllare i file che scarichi da periferiche di memorizzazione esterne (come una chiavetta USB o un CD), specialmente se non ne conosci l'origine.
  - Se hai un file DMG, montalo e poi controllane il contenuto (i file all'interno del volume/immagine montata).

  Il modo più semplice per controllare un file, una cartella o un volume è di trascinarli e lasciarli sulla finestra di Bitdefender Antivirus for Mac o nell'icona sul Dock.

Non è necessaria nessun'altra configurazione o azione. Tuttavia, se lo desideri, puoi modificare le impostazioni e le preferenze dell'applicazione in base alle tue esigenze. Per maggiori informazioni, fai riferimento a Configurare le preferenze (pagina 175).

4.4.2. Eseguire una scansione sul Mac

Oltre alla funzione **Bitdefender Shield**, che monitora regolarmente le app installate, cercando azioni simili a minacce e impedendo a nuove minacce di accedere al sistema, puoi eseguire una scansione sul tuo Mac o esaminare determinati file in qualsiasi momento.

Il modo più semplice per controllare un file, una cartella o un volume è di trascinarli e lasciarli sulla finestra di Bitdefender Antivirus for Mac o nell'icona sul Dock. Comparirà la procedura guidata della scansione, che ti guiderà attraverso il processo di scansione.

Puoi avviare una scansione anche in questo modo:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Seleziona la scheda **Antivirus**.
3. Clicca su uno dei tre pulsanti di scansione per avviare la scansione desiderata.
   - **Scansione veloce** - Cerca eventuali minacce nei punti più vulnerabili del sistema (per esempio nelle cartelle contenenti documenti, file scaricati, messaggi di posta e altri file temporanei di ciascun utente).
   - **Scansione di sistema** - Esegue un controllo dell'intero sistema alla ricerca di eventuali minacce. Saranno controllati anche tutti i mount connessi.

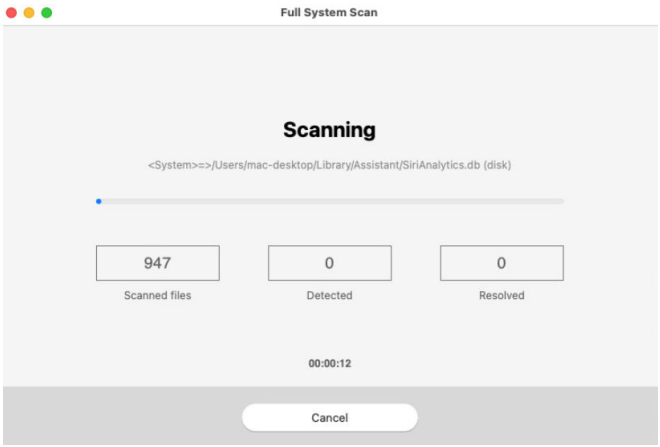
     > **Nota**
     > In base alla misura del disco fisso, controllare l'intero sistema potrebbe richiedere un po' di tempo (fino a un'ora o persino di più). Per ottenere prestazioni migliori, si consiglia di non avviare questa attività mentre se ne eseguono altre piuttosto esigenti in termini di risorse di sistema (come ad esempio una sessione di editing video).
     >
     > Se preferisci, puoi scegliere di non controllare determinati volumi montati, aggiungendoli all'elenco delle **Eccezioni** dalla finestra Protezione.

   - **Scansione personalizzata** - Ti aiuta a controllare file, cartelle o volumi particolari in cerca di eventuali minacce.

Puoi anche avviare una Scansione veloce o di sistema dalla Dashboard.

4.4.3. Procedura guidata per la scansione

Ogni volta che avvii una scansione, comparirà la relativa procedura guidata di Bitdefender Antivirus for Mac.



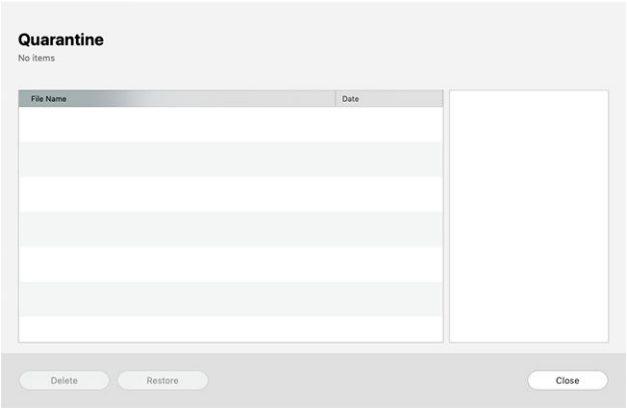
Durante ogni scansione, vengono mostrate informazioni in tempo reale sulle minacce eventualmente rilevate e risolte.

Attendere che Bitdefender Antivirus for Mac finisca la scansione.

> **Nota**
> La durata del processo dipende dalla complessità della scansione.

4.4.4. Quarantena

Bitdefender Antivirus for Mac consente di isolare i file infetti o sospetti in un'area sicura, chiamata quarantena. Quando una minaccia è in quarantena, non può più arrecare alcun danno, in quanto non può essere eseguita o letta.



La sezione Quarantena mostra tutti i file attualmente isolati nella cartella Quarantena.

Per eliminare un file dalla quarantena, selezionalo e clicca su **Elimina**. Se desideri ripristinare un file in quarantena alla sua ubicazione originale, selezionalo e clicca su **Ripristina**.

Per visualizzare un elenco con tutti gli elementi aggiunti alla quarantena:

1. Clic **Protezione** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Clicca su **Apri** nel pannello **Quarantena**.

4.4.5. Bitdefender Shield (protezione in tempo reale)

Bitdefender fornisce una protezione in tempo reale da una vasta gamma di minacce esaminando tutte le app installate, le loro versioni aggiornate e i file nuovi e modificati.

Per disattivare la protezione in tempo reale:

1. Clicca su **Preferenze** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Disattiva **Bitdefender Shield** nella finestra **Protezione**.

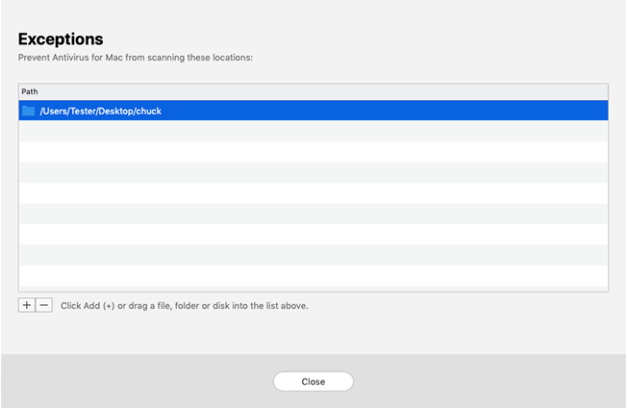
Avvertimento

È una questione di sicurezza piuttosto importante. Si consiglia di disattivare la protezione in tempo reale per il minimo tempo possibile. Se la protezione in tempo reale è disattivata, non si è protetti dalle minacce.

4.4.6. Scansione eccezioni

Se lo desideri, puoi configurare Bitdefender Antivirus for Mac per non controllare determinati file e cartelle o anche interi volumi. Per esempio, potresti voler escludere dalla scansione:

- File che sono stati identificati per errore come infetti (conosciuti come falsi positivi)
- File che causano errori di scansione
- Backup dei volumi



L'elenco delle eccezioni contiene i percorsi che sono stati esclusi dalla scansione.

Per accedere all'elenco delle eccezioni:

1. Clic **Protezione** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Clicca su **Apri** nel pannello **Eccezioni**.

Ci sono due modi per impostare un'eccezione di scansione:

- Trascina e rilascia un file, una cartella o un volume sull'elenco delle eccezioni.
- Clicca sul pulsante con il segno più (+), posizionato sotto l'elenco delle eccezioni. Poi, seleziona il file, la cartella o il volume da escludere dalla scansione.

Per rimuovere un'eccezione, selezionala dall'elenco e clicca sul pulsante con il segno meno (-), posizionato sotto l'elenco delle eccezioni.

4.4.7. Protezione web

Bitdefender Antivirus for Mac utilizza le estensioni di TrafficLight per proteggere completamente la tua navigazione web. Le estensioni di TrafficLight intercettano, elaborano e filtrano tutto il traffico web, bloccando eventuali contenuti dannosi.

Le estensioni funzionano e si integrano con i seguenti browser: Mozilla Firefox, Google Chrome e Safari.

Attivare le estensioni di TrafficLight

Per attivare le estensioni di TrafficLight:

1. Clicca su **Risolvi ora** nella scheda **Protezione web** nella Dashboard.
2. Si aprirà la finestra **Protezione web**.
   Comparirà il browser web rilevato che hai installato sul tuo sistema. Per installare l'estensione di TrafficLight sul tuo browser, clicca su **Ottieni estensione**.
3. Ora raggiungerai l'indirizzo:
   https://bitdefender.com/solutions/trafficlight.html
4. Seleziona **Free Download** (Scarica gratuitamente).
5. Segui i passaggi per installare l'estensione di TrafficLight corrispondente al tuo browser.

Gestire le impostazioni delle estensioni

Per proteggerti da ogni tipo di minaccia che potresti incontrare durante la tua navigazione web, è disponibile una vasta gamma di funzioni. Per accedervi, clicca sull'icona di TrafficLight accanto alle impostazioni del browser e poi clicca sul pulsante ⚙ **Impostazioni**:

- **Impostazioni di Bitdefender TrafficLight**
  - Protezione web - Ti impedisce di accedere a siti web utilizzati per attacchi di malware, tentativi di phishing e frodi.
  - Analisi risultati della ricerca - Segnala eventuali siti web rischiosi tra i risultati della tua ricerca.

- **Eccezioni**
  Se sei sul sito web che vuoi aggiungere alle eccezioni, clicca su **Aggiungi questo sito web all'elenco**.
  Se vuoi aggiungere un altro sito web, inserisci il suo indirizzo nel campo corrispondente, e clicca su .
  Non comparirà alcun avviso in caso di minacce presenti sulle pagine escluse. Ecco perché in questa lista devi indicare solo siti web affidabili.

Valutazione delle pagine e avvisi

In base a come TrafficLight classifica la pagina web che stai visualizzando, in quest'area sarà mostrata una delle seguenti icone:

Questa è pagina sicura da visitare. Puoi continuare il tuo lavoro.

Questa pagina web può contenere contenuti pericolosi. Presta la massima cautela se decidi di visitarla.

Dovresti abbandonare subito questo pagina web in quanto contiene malware o altre minacce.

In Safari, lo sfondo delle icone di TrafficLight è nero.

4.4.8. Anti-tracker

Molti siti web che visiti utilizzano tracker per ottenere informazioni sul tuo comportamento, per condividerle con aziende di terze parti o mostrarti pubblicità più rilevanti per te. Quindi, i possessori dei siti web guadagnano per essere in grado di fornirti contenuti gratuitamente o continuare a operare. Oltre a raccogliere informazioni, i tracker possono rallentare la tua esperienza di navigazione oppure occupare la tua banda.

Con l'estensione Bitdefender Anti-tracker attivata nel tuo browser web, puoi evitare la tracciatura così che i tuoi dati restino privati mentre navighi online, velocizzando il tempo necessario per caricare i siti web.

L'estensione di Bitdefender è compatibile con i seguenti browser web:

- Google Chrome
- Mozilla Firefox
- Safari

I tracker che rileviamo vengono raggruppati nelle seguenti categorie:

- **Pubblicità** - Usati per analizzare il traffico del sito web, il comportamento dell'utente o gli schemi di traffico dei visitatori.
- **Interazione del cliente** - Usati per misurare l'interazione dell'utente con diverse forme di input, come chat o supporto.
- **Essenziali** - Usati per monitorare funzionalità critiche della pagina web.
- **Analisi dei siti** - Usati per raccogliere dati relativi all'uso della pagina web.
- **Social media** - Usati per monitorare il pubblico dei social, attività e coinvolgimento degli utenti con diverse piattaforme di social media.

Attivare Bitdefender Anti-tracker

Per attivare l'estensione Bitdefender Anti-tracker nel tuo browser web:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Seleziona la scheda **Anti-tracker**.
3. Clicca su **Attiva estensione** accanto al browser web per cui vuoi attivare l'estensione.

Interfaccia di Anti-tracker

Quando l'estensione Bitdefender Anti-tracker viene attivata, compare l'icona accanto alla barra di ricerca nel tuo browser web. Ogni volta che visiti un sito web, sull'icona si può notare un contatore, che indica i tracker rilevati e bloccati. Per maggiori dettagli sui tracker bloccati, clicca sull'icona per aprire l'interfaccia. Accanto al numero dei tracker bloccati, puoi visualizzare il tempo richiesto per il caricamento della pagina e le categorie di appartenenza dei tracker rilevati. Per vedere l'elenco dei siti web che stanno usando la tracciatura, clicca sulla categoria desiderata.

Per impedire a Bitdefender di bloccare i tracker sul sito web che stai attualmente visitando, clicca su **Sospendi la protezione su questo sito web**. Questa applicazione si applica solo finché il sito web sarà aperto e sarà riportata allo stato iniziale quando lo chiuderai.

Per consentire ai tracker di una determinata categoria di monitorare le tue attività, clicca sull'attività desiderata e poi sul pulsante corrispondente. Se cambiassi idea, clicca sullo stesso pulsante un'altra volta.

Disattivare Bitdefender Anti-tracker

Per disattivare Bitdefender Anti-tracker dal tuo browser web:

1. Apri il tuo browser web.
2. Clicca sull'icona accanto alla barra dell'indirizzo nel tuo browser web.
3. Clicca sull'icona nell'angolo in alto a destra.
4. Usa l'interruttore corrispondente per disattivarlo.
   L'icona Bitdefender diventa grigia.

Consentire la tracciatura di un sito web

Se desideri lasciare attivata la tracciatura mentre visiti un determinato sito web, puoi aggiungere questo indirizzo alle eccezioni nel seguente modo:

1. Apri il browser web.
2. Clicca sull'icona accanto alla barra di ricerca.
3. Clicca il icona nell'angolo in alto a destra.
4. Se ti trovi sul sito Web che desideri aggiungere alle eccezioni, fai clic su **Aggiungi il sito web corrente all'elenco**.
   Se desideri aggiungere un altro sito web, digita il suo indirizzo nel campo corrispondente, quindi fai clic su .

4.4.9. Safe Files

Un Ransomware è un programma dannoso che colpisce i sistemi vulnerabili bloccandoli e chiedendo denaro agli utenti per riavere il controllo dei propri sistemi. Questo programma dannoso agisce in maniera molto scaltra, mostrando falsi messaggi per allarmare l'utente, spingendoli al pagamento delle cifre richieste.

Utilizzando le tecnologie più moderne, Bitdefender assicura l'integrità del sistema proteggendone le aree critiche da attacchi ransomware senza influenzarne le prestazioni. Tuttavia, potresti voler proteggere anche i tuoi file personali, come documenti, fotografie o filmati, impedendone l'accesso ad applicazioni non affidabili. Con Bitdefender Safe Files, puoi proteggere i tuoi file personali e configurare le app autorizzate a effettuare modifiche nei tuoi file protetti, bloccando tutte le altre.

Per aggiungere successivamente file all'ambiente protetto:

1. Clic **Protezione** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Anti-Ransomware**.
3. Clicca su **File protetti** nell'area Safe Files.
4. Clicca sul pulsante con il segno più (+), posizionato sotto l'elenco dei file protetti. Poi, seleziona un file, una cartella o un volume da proteggere da eventuali attacchi ransomware.

Per evitare rallentamenti al sistema, ti consigliamo di aggiungere un massimo di 30 cartelle, o salvare più file in una sola cartella.

Di norma, le cartelle Immagini, Documenti, Desktop e Download sono protette dagli attacchi di ogni minaccia.

> **Nota**
> Le cartelle personali possono essere protette solo per gli utenti attuali. Unità esterne, oltre a file di sistema e delle applicazioni, non possono essere aggiunti all'ambiente protetto.

Riceverai un avviso ogni volta che una app sconosciuta con un comportamento anomalo cercherà di modificare i file che hai aggiunto. Clicca su **Consenti** o **Blocca** per aggiungerla all'elenco delle **Applicazioni gestite**.

Accesso applicazioni

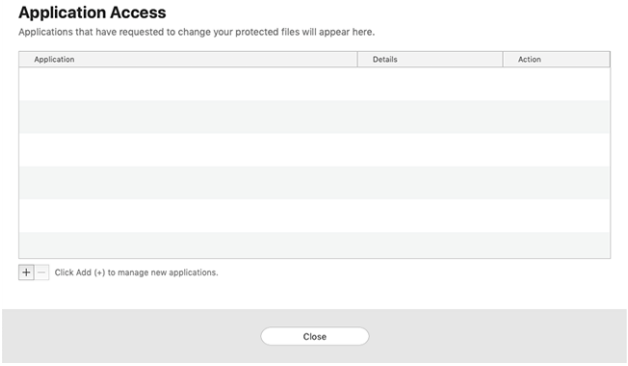
Le applicazioni che cercano di modificare o eliminare file protetti potrebbero essere segnalate come potenzialmente pericolose e aggiunte all'elenco delle "applicazioni bloccate". Se un'applicazione venisse bloccata ma hai la certezza che il suo comportamento sia assolutamente normale, puoi autorizzarla seguendo questi passaggi:

1. Clic **Protezione** nel menu di navigazione dell'interfaccia di Bitdefender.

2. Seleziona il **Anti ransomware** scheda.
3. Clicca su **Accesso applicazione** nell'area Safe Files.
4. Cambia lo stato in Consenti accanto alla app bloccata.

Anche le app impostate su Consenti possono essere bloccate.

Usa il metodo trascina e rilascia o clicca sul segno più (+) per aggiungere altre app all'elenco.



4.4.10. Time Machine Protection

Bitdefender Time Machine Protection serve come ulteriore livello di sicurezza per l'unità di backup, incluso tutti i file che hai deciso di archiviarci, bloccando l'accesso a qualsiasi fonte esterna. Nel caso in cui i file nella tua unità Time Machine venissero cifrati da un ransomware, potrai recuperarli senza dover cedere al ricatto.

Nel caso dovessi ripristinare degli elementi da un backup di Time Machine, controlla la pagina del supporto Apple per le istruzioni.

Attivare o disattivare Time Machine Protection

Per attivare o disattivare Time Machine Protection:

1. Clicca su **Protezione** nel menu di navigazione nell'**interfaccia di Bitdefender**.
2. Seleziona il **Anti ransomware** scheda.
3. Attiva o disattiva l'interruttore **Time Machine Protection**.

4.4.11. Risoluzione problemi

Bitdefender Antivirus for Mac rileva automaticamente e ti informa sui problemi che possono influenzare la sicurezza del sistema e dei dati. In questo modo, puoi risolvere facilmente e in maniera tempestiva ogni rischio per la sicurezza.

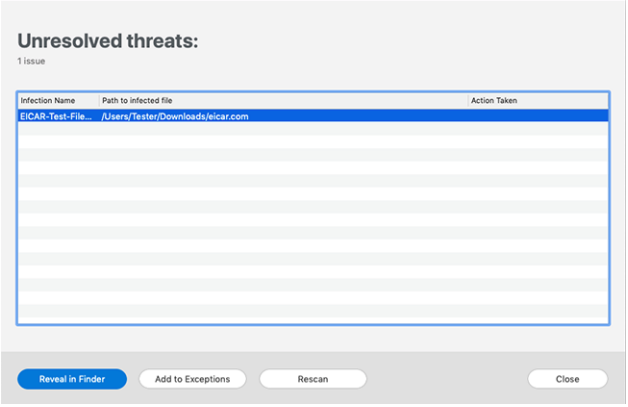
Risolvere i problemi indicati da Bitdefender Antivirus for Mac è un modo rapido e semplice per assicurare una protezione ottimale al tuo sistema e ai tuoi dati.

I problemi rilevati includono:

- Il nuovo aggiornamento sulle informazioni delle minacce non è stato scaricato dai nostri server.
- Sul tuo sistema sono state rilevate delle minacce e il prodotto non ha potuto disinfettarle automaticamente.
- La protezione in tempo reale è stata disattivata.

Per controllare e correggere i problemi rilevati:

1. Se Bitdefender non ha alcun avviso, la barra di stato è verde. Quando viene rilevato un problema di sicurezza, la barra di stato cambia il suo colore, diventando rossa.
2. Verifica la descrizione per maggiori informazioni.
3. Quando viene rilevato un problema, clicca sul pulsante corrispondente per intervenire.



L'elenco delle minacce non risolte viene aggiornato dopo ogni scansione del sistema, indipendentemente se la scansione è stata eseguita automaticamente in background o avviata da te.

Puoi scegliere di intraprendere le seguenti azioni sulle minacce non risolte:

- **Elimina manualmente**. Intraprendi questa azione per rimuovere le infezioni manualmente.
- **Aggiungi alle eccezioni**. Questa azione non è disponibile per le minacce trovate negli archivi.

4.4.12. Notifiche

Bitdefender conserva un registro dettagliato di eventi riguardanti la sua attività sul computer. Ogni volta che si verifica un evento rilevante per la sicurezza del sistema o dei dati, viene aggiunto un nuovo messaggio nelle Notifiche di Bitdefender, in modo simile a quando ricevi un nuovo messaggio nella casella di posta.

Le notifiche sono uno strumento molto importante per monitorare e gestire la tua protezione di Bitdefender. Per esempio, puoi controllare facilmente se l'aggiornamento è stato eseguito con successo, se sono state rilevate minacce o vulnerabilità sul computer, ecc. In aggiunta, se necessario, puoi intraprendere ulteriori azioni o modificare le azioni intraprese da Bitdefender.

Per accedere al rapporto delle notifiche, clicca su **Notifiche** nel menu di navigazione dell'interfaccia di Bitdefender. Ogni volta che si verifica un evento critico, sull'icona 2 compare un contatore.

In base al tipo e alla gravità, le notifiche sono suddivise in:

- Gli eventi **critici** indicano problemi importanti. Dovresti controllarli subito.
- Gli **Avvisi** indicano problemi non critici. Quando hai tempo, dovresti controllarli e risolverli.
- Gli eventi **informazione** indicano operazioni avvenute con successo.

Clicca su ogni scheda per scoprire maggiori dettagli sugli eventi generati. Cliccando una sola volta su ciascun titolo di un evento, vengono mostrati alcuni dettagli: una breve descrizione, l'azione intrapresa da Bitdefender quando è successo e la data e l'ora in cui si è verificato. Se necessario, possono essere fornite opzioni per intraprendere ulteriori azioni.

Per aiutarti a gestire facilmente gli eventi registrati, la finestra delle notifiche offre opzioni per eliminare o segnare come letti tutti gli eventi in quella sezione.

4.4.13. Aggiornamenti

Ogni giorno vengono trovate e identificate nuove minacce. Ecco perché è molto importante mantenere Bitdefender Antivirus for Mac sempre aggiornato con i nuovi aggiornamenti delle informazioni delle minacce.

Gli aggiornamenti delle informazioni delle minacce sono eseguiti al volo, ciò significa che i file da aggiornare sono sostituiti progressivamente. In questo modo, l'aggiornamento non interesserà l'operatività del prodotto, e, allo stesso tempo, ogni vulnerabilità sarà esclusa.

- Se Bitdefender Antivirus for Mac è aggiornato, può rilevare tutte le ultime minacce scoperte e pulire i file infetti.
- Se Bitdefender Antivirus for Mac non è aggiornato, non potrà rilevare e rimuovere le nuove minacce scoperte da Bitdefender Labs.

Richiedere un aggiornamento

Puoi richiedere un aggiornamento manualmente in qualsiasi momento.

Per controllare la disponibilità di aggiornamenti e scaricarli, è richiesta una connessione a Internet attiva.

Per richiedere un aggiornamento manualmente:

1. Clicca sul pulsante **Azioni** nella barra dei menu.
2. Seleziona **Aggiornamento database informazioni minacce**.

In alternativa, puoi richiedere un aggiornamento manuale, premendo CMD + U.

Puoi visualizzare l'avanzamento dell'aggiornamento e i file scaricati.

Ottenere gli aggiornamenti tramite server proxy

Bitdefender Antivirus for Mac può essere aggiornato solo attraverso server proxy che non richiedono autenticazione. Non è necessario configurare alcuna impostazione del programma.

Se ti connetti a Internet attraverso un server proxy che richiede l'autenticazione, devi passare a una normale connessione Internet diretta per ottenere gli aggiornamenti delle informazioni delle minacce.

Fare l'upgrade a una nuova versione

Occasionalmente, rendiamo disponibili aggiornamenti del prodotto per aggiungere nuove funzioni e miglioramenti, o per risolvere eventuali problemi. Tali aggiornamenti potrebbero richiedere un riavvio del sistema per avviare l'installazione dei nuovi file. Di norma, se un aggiornamento richiede un riavvio del computer, Bitdefender Antivirus for Mac continuerà a funzionare con i file precedenti fin quando il sistema non sarà riavviato. In questo caso, il processo di aggiornamento non interferirà con le attività dell'utente.

Quando l'aggiornamento di un prodotto viene completato, una finestra di pop-up ti informerà di riavviare il sistema. Se hai saltato questa notifica, puoi cliccare su **Riavvia per aggiornare** dalla barra dei menu oppure riavviare il sistema manualmente.

Trovare informazioni su Bitdefender Antivirus for Mac

Per trovare informazioni sulla versione di Bitdefender Antivirus for Mac che hai installato, accedi alla finestra **Info**. Nella stessa finestra puoi accedere e visualizzare l'Accordo di abbonamento, l'Informativa sulla privacy e le licenze open source.

Per accedere alla finestra Info:

1. Apri Bitdefender Antivirus for Mac.
2. Clicca su Bitdefender Antivirus for Mac nella barra dei menu e seleziona **Informazioni su Antivirus for Mac**.

4.5. Configurare le preferenze

Questo capitolo include i seguenti argomenti:

4.5.1. Accedere alle preferenze

Per aprire la finestra delle Preferenze di Bitdefender Antivirus for Mac:

- Esegui una delle seguenti azioni:
  - Clic **Preferenze** nel menu di navigazione dell'interfaccia di Bitdefender.
  - Clicca su Bitdefender Antivirus for Mac nella barra dei menu e seleziona **Preferenze**.

4.5.2. Preferenze di protezione

La finestra delle preferenze di protezione ti consente di configurare l'approccio generale alla scansione. Puoi configurare le azioni intraprese sui file infetti o sospetti, e altre impostazioni generali.

- **Bitdefender Shield.** Bitdefender Shield offre una protezione in tempo reale da una vasta gamma di minacce esaminando tutte le app installate, le loro versioni aggiornate e i file nuovi e modificati. Non ti consigliamo di disattivare Bitdefender Shield, ma se devi farlo, fallo per il minor tempo possibile. Se Bitdefender Shield è disattivato, non avrai più alcuna protezione dalle minacce.
- **Esamina solo i file nuovi e modificati.** Seleziona questa casella per fare in modo che Bitdefender Antivirus for Mac controlli solo i file che non sono stati già controllati o che sono stati modificati dall'ultima scansione.
  Puoi scegliere di non applicare questa impostazione per la scansione trascina e rilascia personalizzata, deselezionando la casella corrispondente.
- **Non esaminare i contenuti nei backup.** Seleziona questa casella per escludere i file dei backup dalla scansione. Se i file infetti vengono ripristinati più tardi, Bitdefender Antivirus for Mac li rileverà automaticamente, intraprendendo l'azione appropriata.

4.5.3. Preferenze avanzate

Puoi scegliere quale azione generale intraprendere per tutti i problemi ed elementi sospetti trovati durante un processo di scansione.

Azione per elementi infetti

- **Prova a disinfettare o spostare in quarantena** - Se vengono rilevati file infetti, Bitdefender tenterà di disinfettarli (rimuovendo il codice dannoso) o spostarli in quarantena.

- **Non fare nulla** - Nessuna azione verrà intrapresa sui file rilevati.

Azione per elementi sospetti

- **Sposta i file in quarantena** - Se vengono rilevati file sospetti, Bitdefender li sposterà in quarantena.
- **Non intraprendere alcuna azione** - Non verrà intrapresa alcuna azione sui file rilevati.

4.5.4. Offerte speciali

Quando sono disponibili eventuali offerte promozionali, Bitdefender è configurato per avvisarti attraverso una finestra pop-up. Ciò ti darà l'opportunità di usufruire di prezzi vantaggiosi e mantenere protetti i tuoi dispositivi per un periodo di tempo maggiore.

Per attivare o disattivare le notifiche sulle offerte speciali:

1. Clic **Preferenze** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Altro**.
3. Attiva o disattiva l'interruttore **Le mie offerte**.

> **Nota**
> Di norma, l'opzione **Le mie offerte** è attivata.

4.6. Domande frequenti

Come posso provare Bitdefender Antivirus for Mac prima di acquistare un abbonamento?

Sei un nuovo cliente di Bitdefender e vorresti provare il nostro prodotto prima di acquistarlo? Il periodo di prova dura 30 giorni ed è possibile continuare a utilizzare il prodotto installato, solo se acquisti un abbonamento a Bitdefender. Per provare Bitdefender Antivirus for Mac, devi:

1. Crea un account Bitdefender, seguendo questi passaggi:
   a. Vai a: https://central.bitdefender.com.
   b. Inserisci le informazioni richieste nei campi corrispondenti. I dati forniti resteranno riservati.

c. Prima di procedere ulteriormente devi accettare i Termini di utilizzo. Accedi ai Termini di utilizzo e leggili attentamente, in quanto contengono i termini e le condizioni con cui puoi utilizzare Bitdefender.
Inoltre, potrai accedere e leggere l'Informativa sulla privacy.

d. Clicca su **CREA ACCOUNT**.

2. Scarica Bitdefender Antivirus for Mac come segue:

a. Seleziona il **I miei dispositivi** pannello, quindi fare clic su **INSTALLA LA PROTEZIONE**.

b. Scegli una delle due opzioni disponibili:

- **Proteggi questo dispositivo**

i. Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.

ii. Salva il file di installazione.

- **Proteggi altri dispositivi**

i. Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.

ii. Clic **INVIA IL LINK PER IL DOWNLOAD**.

iii. Digita un indirizzo email nel campo corrispondente e fai clic **INVIA UNA EMAIL**.
Si noti che il collegamento per il download generato è valido solo per le prossime 24 ore. Se il link scade, dovrai generarne uno nuovo seguendo gli stessi passaggi.

iv. Sul dispositivo su cui desideri installare il tuo prodotto Bitdefender, controlla l'account e-mail che hai digitato, quindi fai clic sul pulsante di download corrispondente.

c. Esegui il prodotto Bitdefender che hai scaricato.

Ho un codice di attivazione. Come posso aggiungere la sua validità al mio abbonamento?

Se hai acquistato un codice di attivazione da uno dei nostri rivenditori o l'hai ricevuto in regalo, puoi aggiungere la sua disponibilità al tuo abbonamento a Bitdefender.

Per attivare un abbonamento utilizzando un codice di attivazione, attenersi alla seguente procedura:

1. Accesso Bitdefender centrale.
2. Seleziona il **le mie sottoscrizioni** pannello.
3. Clicca il **CODICE DI ATTIVAZIONE** pulsante, quindi digitare il codice nel campo corrispondente.
4. Clic **ATTIVARE** continuare.

Ora l'estensione è visibile nel tuo account Bitdefender e nel tuo prodotto Bitdefender Antivirus for Mac installato, nel lato in basso a destra della schermata.

Il registro della scansione indica che ci sono ancora alcuni elementi non risolti. Come posso rimuoverli?

Gli elementi non risolti nel registro della scansione possono essere:

- archivi ad accesso limitato (xar, rar, ecc.)
  Soluzione: usa l'opzione **Svela in Finder** per trovare il file ed eliminarlo manualmente. Assicurati di svuotare il Cestino.
- caselle di posta ad accesso limitato (Thunderbird, ecc.)
  Soluzione: usa l'applicazione per rimuovere l'elemento contenente il file infetto.
- Contenuti nei backup
  Soluzione: attiva l'opzione **Non esaminare i contenuti nei backup** nelle preferenze della Protezione o **Aggiungi a eccezioni** i file rilevati.
  Se i file infetti venissero ripristinati in un secondo momento, Bitdefender Antivirus for Mac li rileverà automaticamente, adottando tutti i provvedimenti necessari.

> **Nota**
> I file ad accesso limitato sono file che solo Bitdefender Antivirus for Mac può aprire, ma non può comunque modificarli.

Dove posso visualizzare maggiori dettagli sulle attività del prodotto?

Bitdefender salva un registro di tutte le azioni importanti, i cambiamenti di stato e gli altri messaggi critici relativi alle sue attività. Per accedere a tali

informazioni, clicca su **Notifiche** nel menu di navigazione nell'interfaccia di Bitdefender.

Posso aggiornare Bitdefender Antivirus for Mac attraverso un server proxy?

Bitdefender Antivirus for Mac può aggiornarsi solo tramite server proxy che non richiedono l'autenticazione. Non è necessario configurare alcuna impostazione del programma.

Se ti connetti a Internet tramite un server proxy che richiede l'autenticazione, devi passare regolarmente a una connessione Internet diretta per ottenere gli aggiornamenti delle informazioni sulle minacce.

Come posso rimuovere Bitdefender Antivirus for Mac?

Per rimuovere Bitdefender Antivirus for Mac, segui questi passaggi:

1. Apri una finestra di **Finder** e vai alla cartella Applicazioni.
2. Apri la cartella Bitdefender e poi clicca due volte su BitdefenderUninstaller.
3. Clic **Disinstalla** e attendere il completamento del processo.
4. Clic **Vicino** finire.

> **Importante**
> Se c'è un errore, puoi contattare l'assistenza clienti di Bitdefender come descritto in Richiesta d'aiuto (pagina 287).

Come posso rimuovere le estensioni di TrafficLight dal mio browser web?

- Per rimuovere le estensioni di TrafficLight da Mozilla Firefox, segui questi passaggi:
  1. Vai in **Strumenti** e seleziona **Add-on**.
  2. Seleziona **Estensioni** sulla colonna a sinistra.
  3. Seleziona l'estensione e clicca su **Rimuovi**.
  4. Riavvia il browser per completare il processo di rimozione.
- Per rimuovere le estensioni di TrafficLight da Google Chrome, segui questi passaggi:
  1. In alto a destra, clicca su **Altri** ⋮.

2. Vai in **Altri strumenti** e seleziona **Estensioni**.
3. Clicca sull'icona **Rimuovi** accanto all'estensione che desideri rimuovere.
4. Clicca su **Rimuovi** per confermare il processo di rimozione.

- Per rimuovere Bitdefender TrafficLight da Safari, segui questi passaggi:
  1. Vai in **Preferenze** o premi **Command-Comma(,)**.
  2. Seleziona **Estensioni**.
     Comparirà un elenco con le estensioni installate.
  3. Seleziona l'estensione Bitdefender TrafficLight e clicca su **Disinstalla**.
  4. Clicca nuovamente su **Disinstalla** per confermare il processo di rimozione.

Quando devo utilizzare Bitdefender VPN?

Devi fare sempre attenzione quando accedi, scarichi o invii contenuti su internet. Per assicurarti di essere sempre al sicuro mentre navighi sul web, ti consigliamo di utilizzare Bitdefender VPN quando:

- vuoi connetterti a reti wireless pubbliche
- vuoi accedere a contenuti che normalmente sono riservati a determinate aree, indipendentemente dal fatto che ti trovi a casa o all'estero
- vuoi mantenere i tuoi dati personali privati (nomi utente, password, informazioni della carta di credito, ecc.)
- vuoi nascondere il tuo indirizzo IP

Bitdefender VPN avrà un impatto negativo sulla durata della batteria del mio dispositivo?

Bitdefender VPN è progettato per proteggere i tuoi dati personali, nascondere il tuo indirizzo IP mentre ti connetti a reti wireless non sicure e accedere a contenuti inaccessibili in determinati paesi. Per evitare un consumo non necessario della batteria del tuo dispositivo, ti consigliamo di utilizzare VPN solo quando ne hai bisogno e disconnetterti quando sei offline.

Perché riscontro rallentamenti in Internet durante la connessione con Bitdefender VPN?

Bitdefender VPN è stato progettato per offrirti un'esperienza di navigazione sul web leggera; tuttavia, la tua connettività a Internet o la distanza del server a cui ti connetti potrebbero causare dei rallentamenti. In questo caso, se non è obbligatorio connetterti a un server ospitato molto distante (ad esempio negli Stati Uniti o in Cina), ti consigliamo di consentire a Bitdefender VPN di connettersi automaticamente al server più vicino o trovarne uno più vicino alla tua ubicazione attuale.

5. SICUREZZA MOBILE PER ANDROID

5.1. Cos'è Bitdefender Mobile Security

Attività online come pagare le bollette, prenotare le vacanze o acquistare beni o servizi, sono molto comode e pratiche. Ma come molte attività che si sono sviluppate su Internet, possono comportare dei rischi, se si ignorano alcune norme di sicurezza, che potrebbero condurre alla compromissione dei propri dati personali. E cosa c'è di più importante del proteggere i dati memorizzati negli account online e nel proprio smartphone?

Bitdefender Mobile Security ti consente di:

- Ottenere la migliore protezione per il tuo tablet e smartphone Android con un impatto minimo sulla durata della batteria
- Non cadere vittima delle truffe mobile basate sui link
- Accedere alla tua VPN sicura per un'esperienza di navigazione web sempre veloce, anonima e sicura
- Localizzare, bloccare e azzerare in remoto il tuo dispositivo Android in caso di furto o smarrimento
- Verificare se il tuo account di posta elettronica è stato coinvolto in violazioni o fughe di dati

5.2. Iniziare

5.2.1. Requisiti dispositivo

Bitdefender Mobile Security funziona su ogni dispositivo con Android 5.0 e una versione successiva. Per la scansione delle minacce nel cloud serve una connessione a Internet attiva.

5.2.2. Installare Bitdefender Mobile Security

- **Da Bitdefender Central**
  - Su Android
    1. Vai in: https://central.bitdefender.com.

2. Accedi al tuo account Bitdefender.
3. Seleziona la scheda **I miei dispositivi**.
4. Tocca **INSTALLA LA PROTEZIONE** e poi tocca **Proteggi questo dispositivo**.
5. Seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, tocca il pulsante corrispondente.
6. Sarai reindirizzato alla app su **Google Play**. Nella schermata di Google Play, tocca l'opzione di installazione.

- Su Windows, macOS e iOS
  1. Vai a: https://central.bitdefender.com.
  2. Accedi al tuo account Bitdefender.
  3. Seleziona il **I miei dispositivi** pannello.
  4. Premi **INSTALLA LA PROTEZIONE** e poi premi **Proteggi altri dispositivi**.
  5. Seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, premi il pulsante corrispondente.
  6. Premi **INVIA LINK DI DOWNLOAD**.
  7. Inserisci l'indirizzo e-mail nel campo corrispondente e premi **INVIA E-MAIL**. Nota che il link del download generato è valido solo per le prossime 24 ore. Se il link dovesse scadere, dovrai generarne uno nuovo seguendo gli stessi passaggi.
  8. Sul dispositivo su cui vuoi installare Bitdefender, controlla l'account e-mail che hai inserito e premi il pulsante di download corrispondente.

- **Da Google Play**
  Cerca Bitdefender Mobile Security per localizzare e installare la app.
  In alternativa, inquadra il codice QR:

  Prima di passare alle diverse fasi per la convalida, devi accettare l'Accordo di abbonamento. Prenditi qualche istante per leggere l'Accordo di abbonamento in quanto contiene i termini e le condizioni con cui è possibile utilizzare Bitdefender Mobile Security.

Tocca **CONTINUA** per passare alla finestra successiva.

5.2.3. Accedi al tuo account Bitdefender

Per usare Bitdefender Mobile Security, devi collegare il tuo dispositivo a un account di Bitdefender, Facebook, Google, Microsoft o Apple, accedendo all'account direttamente dalla app. La prima volta che apri l'applicazione, ti sarà chiesto di accedere a un account.

Se hai installato Bitdefender Mobile Security dal tuo account Bitdefender, la app tenterà di accedere automaticamente a tale account.

Per collegare il tuo dispositivo a un account di Bitdefender:

1. Inserisci l'indirizzo e-mail e la password del tuo account di Bitdefender nei campi corrispondenti. Se non hai un account di Bitdefender e vuoi crearne uno, seleziona il link corrispondente.
2. Tocca **ACCEDI**.

Per accedere utilizzando un account Facebook, Google o Microsoft, tocca il servizio che vuoi utilizzare dall'area O ACCEDI CON. Sarai reindirizzato alla pagina di accesso del servizio selezionato. Segui le istruzioni per collegare il tuo account a Bitdefender Mobile Security.

> **Nota**
> Bitdefender non accede ad alcuna informazione confidenziale, come la password dell'account con cui accedi o le informazioni personali dei tuoi amici e contatti.

5.2.4. Configurare la protezione

Una volta eseguito l'accesso alla app, comparirà la finestra Configura la protezione. Per proteggere il tuo dispositivo, ti consigliamo di seguire questi passaggi:

- **Stato dell'abbonamento**. Per ottenere la protezione da Bitdefender Mobile Security, devi attivare il prodotto con un abbonamento, che specifica per quanto tempo puoi utilizzarlo. alla scadenza, la app smette di eseguire le proprie funzioni e proteggere il tuo dispositivo.
  Se hai un codice di attivazione, tocca **HO UN CODICE** e poi tocca **ATTIVA**.

Se hai eseguito l'accesso con un nuovo account di Bitdefender e non hai un codice di attivazione, puoi usare il prodotto per 14 giorni gratuitamente.

- **Protezione web**. Se il tuo dispositivo richiede l'accessibilità per attivare Protezione web, tocca **ATTIVA**. Si aprirà il menu dell'accessibilità. Tocca Bitdefender Mobile Security e attiva l'interruttore corrispondente.
- **Scansione malware**. Esegui una scansione unica per assicurarti che il tuo dispositivo sia privo di minacce. Per avviare il processo di scansione, tocca **ESAMINA ORA**.
  Non appena il processo di scansione inizierà, comparirà la dashboard. Qui puoi visualizzare lo stato di sicurezza del tuo dispositivo.

5.2.5. Dashboard

Tocca l'icona di Bitdefender Mobile Security nell'app drawer del dispositivo per aprire l'interfaccia dell'applicazione.

La dashboard offre informazioni sullo stato di sicurezza del tuo dispositivo e tramite Autopilot ti aiuta a migliorare la sua sicurezza dandoti suggerimenti sulle varie funzionalità.

La scheda stato nella parte superiore della finestra ti informa sullo stato di sicurezza del dispositivo usando messaggi chiari e colori indicativi. Se Bitdefender Mobile Security non ha alcun avviso, la scheda dello stato è verde. Quando viene rilevato un problema di sicurezza, la scheda dello stato diventa rossa.

Per offrirti un funzionamento efficace e una maggiore protezione mentre esegui diverse attività, **Bitdefender Autopilot** agirà come tuo consulente di sicurezza personale. In base alle attività eseguite, sia che tu stia lavorando o effettuando pagamenti online, Bitdefender Autopilot ti fornirà suggerimenti contestuali basati sull'uso e le esigenze del tuo dispositivo. Ciò ti aiuterà a scoprire e usufruire dei vantaggi offerti dalle funzionalità incluse nella app Bitdefender Mobile Security.

Ogni volta che vi è un processo in esecuzione o una funzione richiede un tuo intervento, nell'interfaccia viene mostrata una scheda con maggiori informazioni e le possibili azioni.

Puoi accedere alle funzionalità di Bitdefender Mobile Security e selezionarle facilmente dalla barra di navigazione in basso:

Scansione malware

Ti consente di avviare una scansione a richiesta e attivare la funzione Esamina la memoria. Per maggiori informazioni, fai riferimento a Scansione malware (pagina 188).

Protezione web

Assicura una navigazione sicura, avvisandoti in caso di eventuali pagine web potenzialmente dannose. Per maggiori informazioni, fai riferimento a Protezione web (pagina 191).

VPN

Cifra le comunicazioni via Internet, aiutandoti a mantenere la tua privacy, indipendentemente dalla rete a cui ci si connette. Per maggiori informazioni, fai riferimento a VPN (pagina 192).

Allerta truffe

Ti mantiene al sicuro avvisandoti dell'arrivo di collegamenti dannosi ricevuti tramite SMS, applicazioni di messaggistica e qualsiasi tipo di notifica. Per maggiori informazioni, fai riferimento a Allerta truffe (pagina 195).

Anti-Theft

Ti consente di attivare o disattivare le funzioni antifurto e di configurarne le relative impostazioni. Per maggiori informazioni, fai riferimento a Funzioni Antifurto (pagina 198).

Privacy dell'account

Verifica se nei tuoi account online si è verificata un'eventuale violazione dei dati. Per maggiori informazioni, fai riferimento a Privacy dell'account (pagina 202).

Blocco App

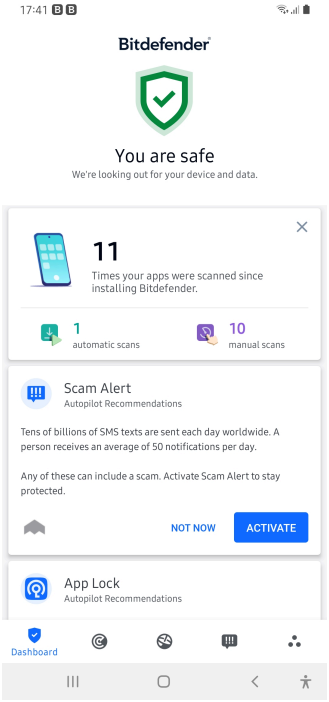
Ti consente di proteggere le applicazioni installate impostando un codice di accesso PIN. Per maggiori informazioni, fai riferimento a Blocco App (pagina 204).

Rapporti

Mantiene un registro di tutte le azioni importanti, i cambiamenti di stato e altri messaggi critici relativi alle attività del tuo dispositivo. Per maggiori informazioni, fai riferimento a Rapporti (pagina 208).

WearON

Comunica con il tuo smartwatch per aiutarti a trovare il telefono nel caso l'avessi smarrito o dimenticato dove l'hai lasciato. Per maggiori informazioni, fai riferimento a WearON (pagina 209).



5.3. Scansione malware

Bitdefender protegge il tuo dispositivo e i tuoi dati da applicazioni dannose usando una scansione all'installazione e a richiesta.

L'interfaccia dello scanner per malware fornisce un elenco di tutti i tipi di minacce cercate da Bitdefender, oltre alle loro definizioni. Tocca semplicemente una minaccia per visualizzarne la definizione.

Nota
Assicurati che il dispositivo mobile sia connesso a Internet. Se il dispositivo non è connesso a Internet, la scansione non inizierà.

- **Scansione all'installazione**

Ogni volta che si installa un'applicazione, Bitdefender Mobile Security esegue automaticamente una scansione utilizzando la tecnologia in-the-cloud. Lo stesso processo di scansione viene avviato ogni volta che le app installate sono aggiornate.

Se l'applicazione viene giudicata pericolosa, un avviso ti segnalerà di disinstallarla. Tocca **Disinstalla** per accedere alla schermata di disinstallazione dell'applicazione.

- **Scansione a richiesta**

  Ogni volta che vuoi assicurarti che le applicazioni installate sul dispositivo siano sicure, puoi avviare una scansione a richiesta.

  Per avviare una scansione a richiesta:

  1. Tocca **Scansione malware** nella barra di navigazione in basso.
  2. Tocca **AVVIA SCANSIONE**.

  > **Nota**
  > In Android 6, per la funzione Scansione malware sono richieste alcune autorizzazioni aggiuntive. Dopo aver toccato il pulsante **AVVIA SCANSIONE**, seleziona **Consenti** per le seguenti opzioni:
  >
  > - Consenti ad **Antivirus** di effettuare e gestire le chiamate?
  > - Consenti ad **Antivirus** di accedere a foto, filmati e file sul tuo dispositivo?

  Puoi visualizzare l'avanzamento della scansione ed eventualmente fermarla in qualsiasi momento.

Di norma, Bitdefender Mobile Security esaminerà la memoria di archiviazione interna del dispositivo, incluso eventuali schede SD inserite. In questo modo, qualsiasi applicazione pericolosa che potrebbe trovarsi sulla scheda può essere rilevata prima ancora di provocare danni.

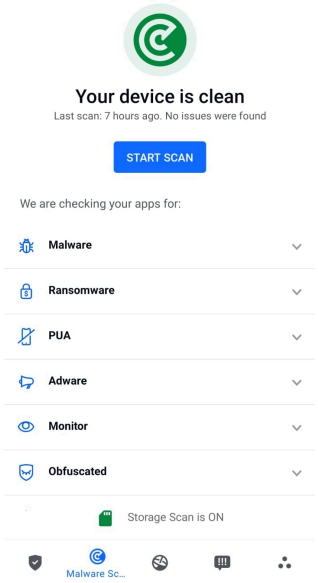
Per disattivare la funzione Esamina la memoria:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Impostazioni**.
3. Disattiva l'interruttore **Esamina la memoria** nell'area Scansione malware.

Se viene rilevata un'eventuale applicazione dannosa, saranno mostrate ulteriori informazioni e potrai rimuoverla, toccando il pulsante **DISINSTALLA**.

La scheda Scansione malware mostra lo stato del tuo dispositivo. Quando il dispositivo è protetto, la scheda è verde, mentre diventerà rossa, se il dispositivo richiede una scansione o in caso di eventuali azioni che necessitano di un tuo intervento.

Se la tua versione di Android è 7.1 o superiore, puoi accedere a un collegamento allo Scanner malware così da poter eseguire scansioni più velocemente, senza aprire l'interfaccia di Bitdefender Mobile Security. Per farlo, tieni premuta l'icona di Bitdefender nella schermata Home o nell'app drawer, e seleziona l'icona .



5.3.1. Rilevamento anomalie dell'app

Bitdefender App Anomaly Detection è una nuova tecnologia integrata nello scanner malware Bitdefender per fornire un ulteriore livello di protezione monitorando e rilevando continuamente eventuali

comportamenti dannosi e avvisando l'utente se vengono identificate attività sospette.

Il rilevamento anomalie dell'app Bitdefender protegge gli utenti anche quando hanno inconsapevolmente installato un'app pericolosa che rimane inattiva per un periodo di tempo o un'app apparentemente affidabile che ne interrompe la funzionalità e diventa canaglia.

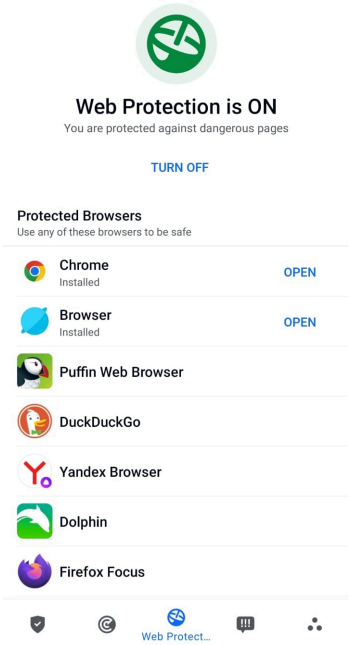
5.4. Protezione web

Utilizzando i servizi cloud di Bitdefender, Protezione web esamina le pagine web a cui accedi con il browser predefinito di Android, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser e Dolphin.

Nota

In Android 6, per la funzione Protezione web sono richieste alcune autorizzazioni aggiuntive.

Consenti di registrare il servizio di accessibilità e tocca **ATTIVA** quando richiesto. Tocca **Antivirus** e attiva l'interruttore, poi conferma di essere d'accordo con l'accesso all'autorizzazione del dispositivo.



Protezione web di Bitdefender è impostata per avvisarti di utilizzare Bitdefender VPN ogni volta che accedi a un sito bancario. La notifica compare nella barra di stato. Ti consigliamo di usare Bitdefender VPN mentre usi il tuo account bancario così da proteggere i tuoi dati da potenziali violazioni di sicurezza.

Per disattivare la notifica di Protezione web:

1. Rubinetto **Di più** nella barra di navigazione in basso.
2. Rubinetto **Impostazioni**.
3. disattiva il corrispondente interruttore nell'area Protezione web.

5.5. VPN

Con Bitdefender VPN puoi mantenere privati i tuoi dati ogni volta che ti connetti a reti wireless non protette mentre sei in aeroporti, centri commerciali, bar o alberghi. In questo modo, è possibile evitare situazioni spiacevoli, come furti di dati personali o tentativi di rendere accessibile il tuo indirizzo IP a pirati informatici.

Il VPN opera come una sorta di tunnel tra il tuo dispositivo e la rete a cui ti connetti, proteggendo la tua connessione, cifrando i dati usando una cifratura di tipo bancario e nascondendo il tuo indirizzo IP, ovunque ti trovi. Il tuo traffico viene reindirizzato a un server indipendente, rendendo quindi il tuo dispositivo quasi impossibile da identificare tra la miriade di altri dispositivi che stanno usando i nostri servizi. Inoltre, mentre ti connetti a Internet tramite VPN, puoi accedere a contenuti che normalmente sono limitati ad alcuni paesi.

> **Nota**
> Alcuni paesi applicano una censura di Internet e quindi l'utilizzo delle VPN sul loro territorio è proibito per legge. Per evitare conseguenze legali, potrebbe comparire un messaggio di avviso quando cerchi di usare la app Bitdefender VPN per la prima volta. Continuando a utilizzare la app, confermi di essere consapevole dei regolamenti applicabili nel paese in cui ti trovi e dei rischi a cui potresti andare incontro.

Ci sono due modi per attivare o disattivare Bitdefender VPN:

- Tocca **CONNETTI** nella scheda VPN della Dashboard.
  Viene mostrato lo stato di Bitdefender VPN.

- Tocca **VPN** nella barra di navigazione in basso e poi tocca **CONNETTI**.
  Tocca **CONNETTI** ogni volta che vuoi restare al sicuro mentre usi la connessione a reti wireless non affidabili.
  Tocca **DISCONNETTI** ogni volta che vuoi disattivare la connessione.

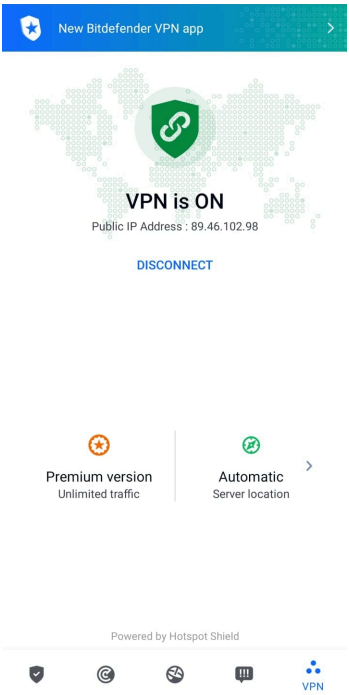
> **Nota**
> La prima volta che attivi VPN, ti verrà chiesto di consentire a Bitdefender di impostare una connessione VPN, che monitorerà il traffico di rete. Tocca **OK** per continuare.

Se la versione del tuo sistema Android è 7.1 o superiore, puoi accedere a una scorciatoia per Bitdefender VPN, senza aprire l'interfaccia di Bitdefender Mobile Security.

Per farlo, tieni premuta l'icona di Bitdefender nella schermata Home o nell'app drawer e seleziona l'icona .

Per risparmiare la batteria, ti consigliamo di disattivare la funzionalità VPN quando non ti serve.

Se hai un abbonamento premium e ti piacerebbe connetterti a un server a tuo piacimento, tocca Posizione server nella funzionalità VPN e poi seleziona l'ubicazione desiderata. Per maggiori dettagli sugli abbonamenti a VPN, fai riferimento a



5.5.1. Impostazioni VPN

Per una configurazione avanzata della tua VPN:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Impostazioni**.

Nell'area VPN, puoi configurare le seguenti opzioni:

- Accesso rapido a VPN - Nella barra di stato del tuo dispositivo comparirà una notifica per consentirti di attivare rapidamente VPN.

- Avviso rete Wi-Fi aperta - Ogni volta che ti connetti a una rete Wi-Fi aperta, ti verrà segnalato nella barra di stato del tuo dispositivo di usare VPN.

5.5.2. Abbonamenti

Bitdefender VPN offre gratuitamente una quota di traffico giornaliera di 200 MB per proteggere la tua connessione ogni volta che ti serve, connettendoti automaticamente all'ubicazione del server ottimale.

Per ottenere traffico illimitato e accesso senza restrizioni a contenuti in tutto il mondo scegliendo l'ubicazione del server che preferisci, fai l'upgrade alla versione premium.

Puoi fare l'upgrade a Bitdefender Premium VPN in qualsiasi momento toccando **Attiva Premium** nella finestra VPN.

L'abbonamento a Bitdefender Premium VPN è indipendente dall'abbonamento a Bitdefender Mobile Security, ciò significa che potrai utilizzarlo per tutta la sua disponibilità, indipendentemente dallo stato del tuo abbonamento di sicurezza. Nel caso l'abbonamento a Bitdefender Premium VPN fosse scaduto, ma quello a Bitdefender Mobile Security fosse ancora attivo, tornerai al piano gratuito.

Bitdefender VPN è un prodotto multipiattaforma, disponibile nei prodotti Bitdefender compatibili con Windows, macOS, Android e iOS. Una volta effettuato l'upgrade al piano premium, potrai usare il tuo abbonamento su tutti i prodotti, a condizione che tu acceda con lo stesso account Bitdefender.

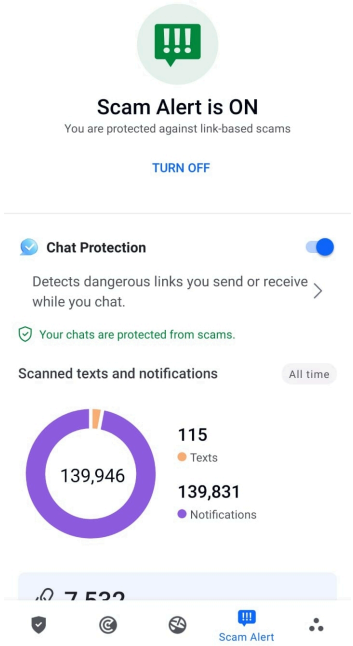
> **Nota**
> Bitdefender VPN funziona anche come applicazione indipendente su tutti i sistemi operativi supportati, ovvero Windows, macOS, Android e iOS.

5.6. Allerta truffe

La funzionalità Allerta truffe prende misure preventive in prima linea, affrontando situazioni potenzialmente pericolose prima ancora che abbiano la possibilità di diventare un problema, incluso le minacce malware. Allerta truffe monitora tutti i messaggi SMS in arrivo e le notifiche Android in tempo reale.

Quando un link pericoloso arriva in un messaggio sul tuo telefono, sul tuo schermo comparirà un avviso. Bitdefender ti offrirà due opzioni. La prima è ignorare le informazioni, mentre la seconda è **MOSTRA DETTAGLI**. Ciò ti fornisce maggiori informazioni sull'incidente, oltre a consigli essenziali, come:

- Non aprire o inoltrare il link rilevato.
- Per i messaggi di testo, se possibile, eliminali.
- Blocca il mittente se non è un contatto affidabile.
- Elimina la app che invia link pericolosi nelle notifiche.



Nota

A causa di alcune limitazioni del sistema operativo Android, Bitdefender non può eliminare i messaggi di testo, adottare misure dirette relative ai messaggi SMS o a qualsiasi altra fonte di notifiche dannose. Se ignori l'avviso di Allerta truffe e provi ad aprire il link pericoloso, la funzionalità Protezione web di Bitdefender lo bloccherà, impendendo l'infezione del tuo dispositivo.

5.6.1. Attivare Allerta truffe

Per attivare Allerta truffe, devi garantire alla app Bitdefender Mobile Security l'accesso ai messaggi SMS e al sistema di notifica:

1. Apri la app Bitdefender Mobile Security installata sul tuo telefono o tablet Android.
2. Nella schermata principale della app Bitdefender, tocca l'opzione **Allerta truffe** nella barra di navigazione in basso e premi **ATTIVA**.
3. Tocca il pulsante **CONSENTI**.
4. Nell'elenco Accesso alla notifica, imposta Bitdefender Security in posizione **ATTIVA**.
5. Conferma l'azione premendo **CONSENTI**.
6. Torna alla schermata di Allerta truffe e premi **CONSENTI** per garantire a Bitdefender la possibilità di esaminare i messaggi SMS.

5.6.2. Protezione chat in tempo reale

I messaggi in chat sono il nostro mezzo più comodo per restare in contatto, ma sono anche un modo semplice con cui i link pericolosi possono raggiungerti.

Con la funzionalità Protezione chat attiva, il modulo Allerta truffe si estende dalla protezione dei messaggi e delle notifiche alla protezione delle chat anche dagli attacchi basati sui link, rilevando i link pericolosi che invii o ricevi mentre chatti.

Per attivare Protezione chat:

1. Apri l'app Bitdefender Mobile Security installata sul tuo telefono o tablet Android.
2. Nella schermata principale della app Bitdefender, tocca l'opzione **Allerta truffe** nella barra di navigazione in basso.
3. Nella parte superiore della scheda Allerta truffe troverai la funzionalità Protezione chat. Imposta l'interruttore corrispondente sulla posizione **ATTIVA**.

Nota

Attualmente, Protezione chat è compatibile con le seguenti applicazioni:

- WhatsApp
- Facebook Messenger
- Telegram
- Discord

5.7. Scam Copilot

Questa funzionalità è essenzialmente un chatbot basato sull'IA e addestrato da Bitdefender per rilevare diverse truffe, tentativi di phishing, campagne di disinformazione e siti web fasulli.

Per attivare Scam Copilot:

1. Aprire la app Bitdefender Mobile Security. Nel pannello Dashboard, sarà presente una scheda dedicata a Scam Copilot. Toccare **Attiva**.
2. Attivare l'accessibilità a Bitdefender Mobile Security toccando il pulsante **ATTIVA**.
3. **Consentire** l'autorizzazione Notifiche.

Ora Scam Copilot è stato configurato correttamente sul dispositivo.

È possibile accedere a Scam Copilot dalla scheda dedicata. Qui sarà possibile trovare:

- **Chatbot per il rilevamento delle truffe:** è possibile chiedere al chatbot di verificare qualsiasi messaggio ritenuto sospetto.
- **Assistente per la prevenzione:** aiuta a saperne di più sulle truffe per individuarle sempre con certezza.
- Stato e pannello di controllo del**Rilevamento truffe automatico**.
- **Filtraggio SMS**: è possibile far filtrare i propri messaggi pericolosi direttamente nella app di messaggistica.

5.8. Funzioni Antifurto

Bitdefender può aiutarti a localizzare il tuo dispositivo e impedire che i tuoi dati personali finiscano nelle mani sbagliate.

Tutto ciò che devi fare è attivare Anti-Theft dal dispositivo e, quando necessario, accedere a **Bitdefender Central** da un qualsiasi browser web, ovunque ti trovi.

> **Nota**
> L'interfaccia di Anti-Theft include anche un link alla app Bitdefender Central su Google Play Store. Puoi utilizzarlo per scaricare la app, nel caso non lo avessi già fatto.

Bitdefender Mobile Security offre le seguenti funzionalità Anti-Theft:

Localizzazione remota

Scopri la posizione attuale del tuo dispositivo su Google Maps. La posizione è aggiornata ogni 5 secondi, in modo da poterlo rintracciare, se è in movimento.

L'accuratezza della posizione dipende da come Bitdefender può rilevarla:

- Se nel dispositivo il GPS è attivato, la sua posizione può essere determinata con un'accuratezza di un paio di metri, finché resta nel raggio dei satelliti GPS (ad esempio, non dentro a un edificio).
- Se il dispositivo è in un edificio, la sua posizione può essere determinata entro decine di metri, se il Wi-Fi è attivato e ci sono reti wireless disponibili nel suo raggio d'azione.
- Diversamente, la posizione sarà determinata usando solo le informazioni dalla rete mobile, che offrono un'accuratezza non superiore a diverse centinaia di metri.

Blocco remoto

Blocca lo schermo del dispositivo e imposta un codice PIN per sbloccarlo.

Cancellazione remota

Rimuovi tutti i dati personali dal dispositivo che hai smarrito.

Invia avviso al dispositivo (Allarme)

Invia un messaggio in remoto che comparirà sullo schermo del dispositivo oppure fallo suonare.

Se perdi il dispositivo, puoi indicare a chi lo trova come restituirlo, facendo comparire un messaggio sul suo schermo.

Se hai smarrito il tuo dispositivo e probabilmente non è molto lontano (ad esempio, da qualche parte in casa o in ufficio), quale modo migliore di

ritrovarlo, se non farlo suonare? Il dispositivo emetterà un suono, anche se è in modalità silenziosa.

5.8.1. Attivare Anti-Theft

Per attivare le funzioni di Anti-Theft, completa semplicemente la fase di configurazione dalla scheda Anti-Theft, disponibile nell'interfaccia.

In alternativa, puoi attivare Anti-Theft seguendo questi passaggi:

1. Rubinetto **Di più** nella barra di navigazione in basso.
2. Tocca **Anti-Theft**.
3. Tocca **ATTIVA**.
4. Per aiutarti ad attivare questa funzione, sarà attivata la seguente procedura:

   > **Nota**
   > In Android 6, la funzione Anti-Theft richiede alcuni permessi aggiuntivi.
   >
   > Per attivare l'opzione, segui questi passaggi:
   >
   > a. Tocca **Attiva Anti-Theft** e poi **ATTIVA**.
   >
   > b. Consenti all'**Antivirus** di accedere alla posizione del tuo dispositivo.

   a. **Dai privilegi di amministratore**
   Questi privilegi sono essenziali per il funzionamento del modulo Anti-Theft e per continuare è necessario assegnarli.

   b. **Imposta PIN applicazione**
   Per impedire l'accesso non autorizzato al tuo dispositivo, occorre impostare un codice PIN. A ogni tentativo di accesso, sarà necessario inserire il PIN. In alternativa, su dispositivi che supportano l'autenticazione tramite impronte digitali, potrà essere utilizzata una conferma tramite impronta digitale invece del codice PIN configurato.
   Lo stesso codice PIN viene usato da Blocco App per proteggere le tue applicazioni installate.

   c. **Attiva Scatta foto**

Ogni volta che qualcuno tenta di sbloccare il tuo dispositivo senza successo con l'opzione Scatta foto attiva, Bitdefender gli scatterà una foto.

Più precisamente, ogni volta che si sbaglia per tre volte di fila a digitare il codice PIN o la password o a confermare l'impronta digitale impostati per proteggere la app, la fotocamera frontale scatta una foto. La foto viene salvata con tanto di indicazione e ora e può essere vista quando si apre Bitdefender Mobile Security e si accede alla finestra di Anti-Theft.

In alternativa, puoi visualizzare la foto scattata nel tuo account di Bitdefender:

i. Vai a: https://central.bitdefender.com.

ii. Accedi al tuo account.

iii. Seleziona il **I miei dispositivi** pannello.

iv. Seleziona il tuo dispositivo Android, quindi la scheda **Anti-Theft**.

v. Tocca ⋮ accanto a **Controlla i tuoi scatti** per vedere le foto più recenti che sono state scattate.
Vengono salvate solo le due foto più recenti.

Una volta attivata la funzionalità Anti-Theft, puoi attivare o disattivare i comandi del Controllo web individualmente dalla finestra Anti-Theft toccando le opzioni corrispondenti.

5.8.2. Utilizzare le funzioni Anti-Theft da Bitdefender Central

> **Nota**
> Tutte le funzioni di Anti-Theft richiedono che l'opzione **Dati in background** sia attivata nelle impostazioni di utilizzo dei dati del dispositivo.

Per accedere alle funzionalità di Anti-Theft dal tuo account di Bitdefender:

1. Accedi a **Bitdefender Central**.
2. Seleziona il **I miei dispositivi** pannello.
3. Nella finestra **I MIEI DISPOSITIVI**, seleziona la scheda del dispositivo desiderata toccando il corrispondente pulsante **Mostra dettagli**.

4. Seleziona la scheda **Anti-Theft**.
5. Tocca il pulsante corrispondente della funzionalità che vuoi usare:
   Localizza - Mostra la posizione del dispositivo su Google Maps.
   Mostra IP - Mostra l'ultimo indirizzo IP per il dispositivo selezionato.
   Allerta - Digita un messaggio da far comparire sul dispositivo e/o fai suonare un allarme.
   Blocca - Blocca il tuo dispositivo e imposta un codice PIN per sbloccarlo.
   Elimina - Elimina tutti i dati dal tuo dispositivo.

   > **Importante**
   > Dopo aver cancellato il contenuto di un dispositivo, tutte le funzioni di Anti-Theft cessano di funzionare.

5.8.3. Impostazioni Anti-Theft

Se desideri attivare o disattivare i comandi remoti:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Antifurto**.
3. Attiva o disattiva le opzioni desiderate.

5.9. Privacy dell'account

Bitdefender Account Privacy rileva se una qualche violazione dei dati si è verificata negli account che utilizzi per effettuare pagamenti e acquisti online, o accedere a diverse app o siti web. I dati memorizzabili in un account possono essere password, informazioni sulle carte di credito o sul conto bancario. Se non protette correttamente, potrebbero verificarsi un furto d'identità o un'invasione alla privacy.

Lo stato della privacy di un account viene mostrato subito dopo la conferma.

Vengono impostati nuovi controlli automatici in background, ma è anche possibile eseguire scansioni manuali su base giornaliera.

Le notifiche saranno mostrate ogni volta che vengono scoperte nuove violazioni che includono uno degli account e-mail verificati.

Per iniziare a proteggere le informazioni personali:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Tocca **Privacy dell'account**.
3. Tocca **COME INIZIARE**.
4. Comparirà l'indirizzo e-mail utilizzato per creare il tuo account di Bitdefender e sarà aggiunto automaticamente all'elenco degli account monitorati.
5. Per aggiungere un altro account, tocca **AGGIUNGI ACCOUNT** nella finestra Privacy account e poi inserisci l'indirizzo e-mail.
   Tocca **AGGIUNGI** per continuare.
   Bitdefender deve confermare questo account prima di mostrare informazioni private. Inoltre, viene inviata un'e-mail con un codice di conferma all'indirizzo fornito.
   Controlla la tua casella di posta e inserisci il codice che hai ricevuto nella sezione **Privacy dell'account** della tua app. Se non riesci a trovare l'e-mail di conferma nei tuoi messaggi in arrivo, controlla la cartella dello Spam.
   Viene mostrato lo stato della privacy dell'account confermato.

Se in uno degli account viene rilevata una violazione, ti consigliamo di modificarne la password il prima possibile. Per creare una password sicura, segui questi suggerimenti:

- Deve contenere almeno otto caratteri.
- Includi sia caratteri minuscoli che maiuscoli.
- Aggiungi almeno un numero o simbolo, come #, @, % or !.

Una volta protetto un account coinvolto in una violazione della privacy, puoi confermare le modifiche spuntando le violazioni rilevate come Risolto. Per farlo:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Privacy dell'account**.
3. Tocca l'account che hai appena protetto.
4. Tocca la violazione da cui hai protetto l'account.
5. Tocca **RISOLTO** per confermare che l'account è protetto.

Quando tutte le violazioni rilevate sono state segnate come **Risolte**, l'account non apparirà più come violato, almeno fino al rilevamento di una nuova violazione.

Per smettere di essere avvisati ogni volta che vengono eseguite scansioni automatiche:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Impostazioni**.
3. Disattiva l'interruttore corrispondente nell'area Privacy account.

5.10. Blocco App

Le applicazioni installate, così come e-mail, foto o messaggi, possono includere dati personali che si desidera mantenere privati, limitando l'accesso ad essi in modo selettivo.

Blocco App consente di bloccare l'accesso non autorizzato alle applicazioni, impostando un codice di accesso PIN. Il codice PIN impostato deve essere di almeno 4 cifre ma non più lungo di 8, ed è richiesto ogni volta che si vuole accedere alle applicazioni con restrizioni selezionate.

Al posto del codice PIN configurato, è possibile utilizzare l'autenticazione biometrica (come la conferma tramite impronte digitali o riconoscimento facciale).

5.10.1. Attivare Blocco App

Per limitare l'accesso alle applicazioni selezionate, configura Blocco App dalla scheda visualizzata nell'interfaccia, dopo aver attivato l'Anti-Theft.

In alternativa, puoi attivare Blocco App seguendo questi passaggi:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Tocca **Blocco App**.
3. Rubinetto **ACCENDERE**.
4. Consenti l'accesso all'utilizzo dei dati per Bitdefender Security.
5. Consenti **trascinamento su altre app**.
6. Torna alla app, configura il codice d'accesso e poi tocca **IMPOSTA PIN**.

> **Nota**
> Questo passaggio è disponibile solo se non hai configurato in precedenza il PIN in Anti-Theft.

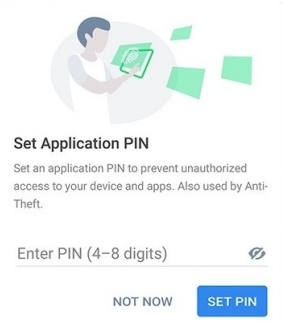
7. Attiva l'opzione Scatta foto per catturare un'immagine di chiunque cercherà di accedere ai tuoi dati privati.

> **Nota**
> In Android 6, per la funzione Scatta foto sono richiesti alcuni permessi aggiuntivi. Per attivarla, consenti all'**Antivirus** di scattare foto e registrare video.

8. Seleziona le app che vuoi proteggere.

Utilizzando un PIN o un'impronta digitale errata per cinque volte di fila, si attiverà una sessione di tempo massimo consentito di 30 secondi. In questo modo, sarà bloccato ogni tentativo di accedere alle app protette.

> **Nota**
> Lo stesso codice PIN viene usato da Anti-Theft per aiutarti a localizzare il tuo dispositivo.



5.10.2. Modalità Blocco

La prima volta che aggiungi una app a Blocco App, compare la schermata della modalità Blocco App. Qui puoi scegliere quando la funzione Blocco App deve proteggere le app installate sul tuo dispositivo.

Puoi selezionare una delle seguenti opzioni:

- **Richiede uno sblocco ogni volta** - Ogni volta che si accede alle app bloccate, dovrà essere utilizzato il codice PIN o l'impronta digitale impostati.
- **Mantieni sbloccato fino allo spegnimento dello schermo** - L'accesso alle tue app sarà valido fino a quando lo schermo non si spegnerà.
- **Blocca dopo 30 secondi** - Puoi uscire e accedere di nuovo alle app sbloccate entro 30 secondi.

Se vuoi cambiare l'impostazione selezionata:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Impostazioni**.
3. Tocca **Richiede uno sblocco ogni volta** nell'area Blocco App.
4. Scegli l'opzione desiderata.

5.10.3. Impostazioni Blocco App

Per una configurazione avanzata di Blocco App:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Impostazioni**.

Nell'area Blocco App, puoi configurare le seguenti opzioni:

- **Suggerimento app sensibile** - Ricevi una notifica di blocco ogni volta che hai installato una app sensibile.
- **Richiede una sblocco ogni volta** - Scegli una delle opzioni di blocco e sblocco disponibili.
- **Sblocco rapido** - Mantieni le app sbloccate finché sei connesso a una rete Wi-Fi affidabile.
- **Tastiera casuale** - Impedisce la lettura del PIN rendendo casuale le posizioni dei numeri.

5.10.4. Scatta foto

Con Bitdefender Snap Photo puoi cogliere sul fatto amici o familiari, evitando che i loro occhi curiosi sbircino i tuoi file personali o le app che utilizzi.

Il suo funzionamento è davvero semplice: ogni volta che si sbaglia per tre volte di fila a digitare il codice PIN o a confermare l'impronta digitale

impostati per proteggere la app, la fotocamera frontale scatta una foto. La foto viene salvata con tanto di indicazione e ora e può essere vista quando si apre Bitdefender Mobile Security e si accede alla funzione Blocco App.

> **Nota**
> Questa funzionalità è disponibile solo per telefoni dotati di una fotocamera frontale.

Per configurare la funzione Scatta foto di Blocco App:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Impostazioni**.
3. Attiva l'interruttore corrispondente nell'area Scatta foto.

Le foto scattate in caso di inserimento di un PIN errato sono mostrate nella finestra di Blocco App e possono essere visualizzate a schermo intero.

In alternativa, possono essere visualizzate nel tuo account di Bitdefender:

1. Vai a: https://central.bitdefender.com.
2. Accedi al tuo account.
3. Seleziona la scheda **Il mio dispositivo**.
4. Seleziona il tuo dispositivo Android, quindi il file **Antifurto** scheda.
5. Rubinetto accanto a **Controlla le tue istantanee** per visualizzare le ultime foto scattate.

Vengono salvate solo le due foto più recenti.

Per fermare l'invio delle foto scattate sul tuo account Bitdefender:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Impostazioni**.
3. Disattiva **Carica foto** nell'area Scatta foto.

5.10.5. Sblocco rapido

Per evitare che la funzione Blocco App richieda l'inserimento del codice PIN o la conferma dell'impronta digitale per le app protette ogni volta che si accede, basta attivare Sblocco rapido.

Con Sblocco rapido, puoi impostare come affidabili le reti Wi-Fi a cui ti connetti di solito e ogni volta che le userai, le impostazioni di blocco di Blocco App saranno disattivate per le app protette.

Per configurare la funzione Sblocco rapido:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Blocco app**.
3. Tocca il pulsante .
4. Tocca l'interruttore accanto a **Sblocca rapido**, se la funzionalità non è ancora stata attivata.
   Convalida usando la tua impronta digitale o il tuo PIN.
   La prima volta che attiverai la funzionalità, dovrai attivare le autorizzazioni locali. Tocca il pulsante **CONSENTI** e poi tocca ancora **CONSENTI**.
5. Tocca **AGGIUNGI** per impostare come affidabile la connessione Wi-Fi attualmente usata.

Nel caso si cambiasse idea, basterà disattivare la funzione e le reti Wi-Fi impostate come affidabili saranno trattate come se non lo fossero.

5.11. Rapporti

Nei Rapporti, è possibile trovare un registro dettagliato degli eventi inerenti le attività di scansione sul proprio dispositivo.

Ogni volta che si verifica qualcosa di rilevante per la sicurezza del dispositivo, un nuovo messaggio viene aggiunto ai Rapporti.

Per accedere alla sezione Rapporti:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Tocca **Rapporti**.

Nella finestra Rapporti, sono disponibili le seguenti schede:

- **RAPPORTI SETTIMANALI** - Qui puoi accedere allo stato della protezione e le attività eseguite nella settimana attuale e in quella precedente. Il rapporto della settimana attuale viene generato ogni domenica e riceverai una notifica ogni volta che sarà disponibile.

In questa sezione, ogni settimana troverai un nuovo suggerimento, perciò assicurati di visitarla regolarmente per sfruttare al massimo la tua app.

Per non ricevere più notifiche ogni volta che viene generato un rapporto:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Impostazioni**.
3. Disattiva l'interruttore **Notifica nuovo rapporto** nell'area Rapporti.

- **RAPPORTO ATTIVITÀ** - Qui puoi verificare maggiori informazioni sulle attività della tua app Bitdefender Mobile Security da quando è stata installata sul tuo dispositivo Android.

  Per eliminare il rapporto attività disponibile:

  1. Rubinetto **Di più** sulla barra di navigazione in basso.
  2. Rubinetto **Impostazioni**.
  3. Tocca **Cancella rapporto attività** e tocca **AZZERA**.

5.12. WearON

Con Bitdefender WearON, puoi localizzare facilmente il tuo smartphone sia che tu l'abbia lasciato in una sala riunioni dell'ufficio o sotto il cuscino del divano. Il dispositivo può essere localizzato persino se era attivata la modalità silenziosa.

Mantieni questa funzione attivata per assicurarti di avere il tuo smartphone sempre a portata di mano.

> **Nota**
> La funzione richiede Android 4.3 e Android Wear.

5.12.1. Attivare WearON

Per usare WearON, devi solo connettere il tuo smartwatch all'applicazione Bitdefender Mobile Security e attivare la funzione con il seguente comando vocale:

Inizia:<Dov'è il mio telefono>

Bitdefender WearON ha due comandi:

1. **Phone Alert**
   Con la funzione Phone Alert, puoi trovare rapidamente il tuo smartphone ogni volta che ti allontani troppo da lui.
   Se hai il tuo smartwatch con te, rileverà automaticamente la app sul tuo telefono vibrando ogni volta che sarà troppo distante e i dispositivi perderanno la connessione Bluetooth.
   Per attivare questa funzione, apri Bitdefender Mobile Security, tocca **Impostazioni generali** nel menu e seleziona l'interruttore corrispondente sotto la sezione WearON.
2. **Allarme**
   Trovare il tuo telefono non è mai stato così semplice. Ogni volta che hai dimenticato dove l'hai lasciato, tocca il comando Allarme sul tuo orologio, per far emettere un suono al tuo telefono.

5.13. Info

Per trovare informazioni sulla versione di Bitdefender Mobile Security che hai installato, accedere e consultare l'Accordo di abbonamento e l'Informativa sulla privacy, e visualizzare le licenze open source:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Impostazioni**.
3. Tocca l'opzione desiderata nell'area Informazioni.

5.14. Domande frequenti

Perché Bitdefender Mobile Security richiede una connessione a Internet?

L'applicazione deve comunicare con i server di Bitdefender per determinare lo stato della sicurezza delle applicazioni che controlla e delle pagine web visitate, ma anche per ricevere comandi dal tuo account Bitdefender, quando si utilizzano le funzioni Anti-Theft.

Per quali funzioni Bitdefender Mobile Security richiede un'autorizzazione?

- Accesso a Internet -> Usata per la comunicazione cloud.
- Valutazione dello stato del telefono e dell'identità -> Usata per rilevare se il dispositivo è connesso a Internet e per estrapolare determinate

informazioni necessarie a creare un ID univoco per comunicare con il cloud di Bitdefender.

- Lettura e scrittura segnalibri del browser -> Il modulo Protezione web elimina i siti dannosi dalla cronologia.
- Lettura dati del registro -> Bitdefender Mobile Security rileva tracce di attività delle minacce dai registri di Android.
- Posizione -> Richiesta per la localizzazione remota.
- Fotocamera -> Richiesta per Scatta foto.
- Memoria -> Usata per consentire a Scansione malware di esaminare la scheda SD.

Come posso smettere di inviare a Bitdefender informazioni sulle app sospette?

Di norma, Bitdefender Mobile Security invia rapporti ai server di Bitdefender su app sospette che stai installando. Queste informazioni sono essenziali per migliorare il rilevamento delle minacce e possono aiutarci a offrirti un'esperienza migliore in futuro. Nel caso volessi arrestare l'invio di tali informazioni su app sospette:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Impostazioni**.
3. Disattiva il **Rilevamento in-the-cloud** nell'area Scansione malware.

Dove posso vedere maggiori dettagli sulle attività dell'app?

Bitdefender Mobile Security salva un rapporto di tutte le azioni importanti, i cambiamenti di stato e gli altri messaggi critici relativi alle sue attività. Per accedere e visualizzare le attività della app:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Rapporti**.
   Nella finestra RAPPORTI SETTIMANALI puoi accedere ai rapporti che vengono generati ogni settimana, mentre nella finestra RAPPORTO ATTIVITÀ puoi visualizzare maggiori informazioni sulle attività della tua app di Bitdefender.

Ho dimenticato il codice PIN impostato per proteggere la mia applicazione. Che cosa posso fare?

1. Accesso Bitdefender centrale.
2. Seleziona il **I miei dispositivi** pannello.
3. Tocca la scheda del dispositivo desiderato e poi tocca ⋮ nell'angolo in alto a destra dello schermo.
4. Selezionare **Impostazioni**.
5. Recupera il codice PIN dal campo **PIN per l'applicazione**.

Come posso modificare il codice PIN impostato per Blocco App e Anti-Theft?

Se desideri modificare il codice PIN impostato per Blocco App e Anti-Theft:

1. Rubinetto **Di più** nella barra di navigazione in basso.
2. Rubinetto **Impostazioni**.
3. Tocca **CODICE PIN** di sicurezza nell'area Anti-Theft.
4. Inserisci il codice PIN attuale.
5. Inserisci il nuovo codice PIN che vuoi impostare.

Come posso disattivare la funzionalità Blocco App?

Non c'è un'opzione per disattivare direttamente l'opzione Blocco App, ma puoi facilmente disattivarla togliendo la spunta delle caselle accanto alle app, dopo aver confermato il PIN o le impronte digitali impostate.

Come posso impostare un'altra rete wireless come affidabile?

Per iniziare, devi connettere il tuo dispositivo alla rete wireless che vuoi impostare come affidabile. Poi segui questi passaggi:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Rubinetto **Blocco app**.
3. Tocca nell'angolo in alto a destra.
4. Tocca **AGGIUNGI** accanto alla rete che vuoi impostare come affidabile.

Come posso smettere di vedere le fotografie scattate dai miei dispositivi?

Per smettere di rendere visibili le fotografie scattate sui tuoi dispositivi:

1. Accesso Bitdefender centrale.
2. Tocca in alto a destra dello schermo.
3. Tocca **Impostazioni** nel menu scorrevole.
4. Disattiva l'opzione **Mostra/non mostrare le foto scattate sui tuoi dispositivi**.

Come posso mantenere sicuri i miei acquisti online?

Quando si ignorano alcuni dettagli, gli acquisti online possono comportare dei rischi elevati. Per non cadere vittima di una frode, ti consigliamo di seguire questi suggerimenti:

- Mantieni la tua app di sicurezza aggiornata.
- Invia pagamenti online solo con la protezione dell'acquirente.
- Usa una VPN quando ti connetti a internet da reti wireless pubbliche e non protette.
- Presta attenzione alle password che hai assegnato ai tuoi account online. Devono essere sicure, includendo sia lettere maiuscole che minuscole, numeri e simboli (@, !, %, #, ecc.).
- Assicurati di inviare le tue informazioni sempre con connessioni sicure. L'estensione del sito web online deve essere HTTPS:// e non HTTP://.

Quando devo utilizzare Bitdefender VPN?

Devi fare sempre attenzione quando accedi, scarichi o invii contenuti su internet. Per assicurarti di essere sempre al sicuro mentre navighi sul web, ti consigliamo di utilizzare Bitdefender VPN quando:

- vuoi connetterti a reti wireless pubbliche
- vuoi accedere a contenuti che normalmente sono riservati a determinate aree, indipendentemente dal fatto che ti trovi a casa o all'estero
- vuoi mantenere i tuoi dati personali privati (nomi utente, password, informazioni della carta di credito, ecc.)
- vuoi nascondere il tuo indirizzo IP

Bitdefender VPN avrà un impatto negativo sulla durata della batteria del mio dispositivo?

Bitdefender VPN è progettato per proteggere i tuoi dati personali, nascondere il tuo indirizzo IP mentre ti connetti a reti wireless non sicure

e accedere a contenuti inaccessibili in determinati paesi. Per evitare un consumo non necessario della batteria del tuo dispositivo, ti consigliamo di utilizzare VPN solo quando ne hai bisogno e disconnetterti quando sei offline.

Perché riscontro rallentamenti in Internet durante la connessione con Bitdefender VPN?

Bitdefender VPN è stato progettato per offrirti un'esperienza di navigazione sul web leggera; tuttavia, la tua connettività a Internet o la distanza del server a cui ti connetti potrebbero causare dei rallentamenti. In questo caso, se non è obbligatorio connetterti a un server ospitato molto distante (ad esempio negli Stati Uniti o in Cina), ti consigliamo di consentire a Bitdefender VPN di connettersi automaticamente al server più vicino o trovarne uno più vicino alla tua ubicazione attuale.

Posso cambiare l'account Bitdefender associato al mio dispositivo?

Sì, puoi facilmente modificare l'account di Bitdefender collegato al tuo dispositivo seguendo questi passaggi:

1. Rubinetto **Di più** sulla barra di navigazione in basso.
2. Tocca il tuo indirizzo e-mail.
3. Tocca **Esci dal tuo account**. Se è stato impostato un codice PIN, ti sarà chiesto di inserirlo.
4. Conferma la tua scelta.
5. Inserisci l'indirizzo email e la password del tuo account nei campi corrispondenti, e tocca **ACCEDI**.

In che modo Bitdefender Mobile Security influenza le prestazioni del dispositivo e l'autonomia della batteria?

Abbiamo mantenuto un basso impatto sulle prestazioni. L'applicazione si attiva solo quando serve, dopo aver installato un'applicazione, mentre si usa l'interfaccia o si esegue un controllo di sicurezza. Bitdefender Mobile Security non funziona in background mentre chiami gli amici, digiti un messaggio o giochi.

Che cos'è la funzione Amministratore dispositivo?

Amministratore dispositivo è una funzione di Android che dà a Bitdefender Mobile Security le autorizzazioni necessarie per eseguire determinati compiti in remoto. Senza questi privilegi, il Blocco remoto non

funzionerebbe e la cancellazione non potrebbe rimuovere completamente i tuoi dati. Se desideri rimuovere l'applicazione, assicurati di revocare tali privilegi prima della disinstallazione, andando in **Impostazioni > Sicurezza > Seleziona Amministratori dispositivo**.

Come risolvere l'errore "Nessun token Google" che compare quando ci si registra a Bitdefender Mobile Security.

Questo errore si verifica quando il dispositivo non è associato a un account Google, oppure se associato, un problema temporaneo impedisce la connessione a Google. Prova una delle seguenti soluzioni:

- Vai in Impostazioni Android > Applicazioni > Gestisci applicazioni > Bitdefender Mobile Security e tocca **Cancella dati**. Poi riprova ad accedere.
- Assicurati che il dispositivo sia associato con un account Google.
  Per controllare, vai in Impostazioni > Account per poi sincronizzare e verificare se un account Google è indicato sotto la voce **Gestione account**. Se non c'è, riavvia il dispositivo e riprova ad accedere a Bitdefender Mobile Security.
- Riavvia il dispositivo e riprova ad accedere.

In quali lingue è disponibile Bitdefender Mobile Security?

Attualmente, Bitdefender Mobile Security è disponibile nelle seguenti lingue:

- Brasiliano
- Ceco
- Olandese
- Inglese
- Francese
- Tedesco
- Greco
- Ungherese
- Italiano
- Giapponese
- Coreano

- Polacco
- Portoghese
- Romeno
- Russo
- Spagnolo
- Svedese
- Thai
- Turco
- Vietnamita

Altre lingue saranno aggiunte nei futuri aggiornamenti. Per cambiare la lingua dell'interfaccia di Bitdefender Mobile Security, vai alle impostazioni **Lingua e tastiera** del dispositivo e imposta la lingua che vuoi usare.

6. SICUREZZA MOBILE PER IOS

6.1. Che cos'è Bitdefender Mobile Security for iOS

Attività online come pagare le bollette, prenotare le vacanze o acquistare beni o servizi, sono molto comode e pratiche. Ma come molte attività che si sono sviluppate su Internet, possono comportare dei rischi, se si ignorano alcune norme di sicurezza, che potrebbero condurre alla compromissione dei propri dati personali. E cosa c'è di più importante del proteggere i dati memorizzati negli account online e nel proprio smartphone?

Bitdefender Mobile Security for iOS ti consente di:

- Offre la più potente protezione dalle minacce con il minimo impatto sulla batteria
- Proteggi i tuoi dati personali: password, indirizzo, informazioni finanziari e dei social
- Controlla facilmente la sicurezza del tuo telefono per rilevare e risolvere eventuali configurazioni errate che potrebbero esporlo
- Evita l'esposizione accidentale dei dati e l'uso improprio per tutte le app installate
- Esamina il tuo dispositivo per ottenere le impostazioni di privacy e sicurezza ottimali
- Ottieni informazioni dettagliate sull'utilizzo delle tue attività online e la cronologia degli incidenti impediti
- Verifica se i tuoi account online sono stati coinvolti in fughe o violazioni dei dati
- Cifra il traffico Internet con la VPN inclusa

Bitdefender Mobile Security for iOS è disponibile gratuitamente e richiede l'attivazione con un account Bitdefender. Tuttavia, l'accesso e l'utilizzo di alcune funzionalità importanti di Bitdefender, come il modulo "Protezione web", richiedono un abbonamento a pagamento.

6.2. Iniziare

6.2.1. Requisiti dispositivo

Bitdefender Mobile Security for iOS funziona su qualsiasi dispositivo con il sistema operativo iOS 12 o successivo e richiede una connessione attiva a Internet per essere attivato e rilevare se si è verificata una perdita di dati nei tuoi account online.

6.2.2. Installare Bitdefender Mobile Security for iOS

- **Da Bitdefender Central**
  - Su iOS
    1. Accedi a **Bitdefender Central**.
    2. Seleziona la scheda **I miei dispositivi**.
    3. Tocca **INSTALLA PROTEZIONE** e poi tocca **Proteggi questo dispositivo**.
    4. Seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, tocca il pulsante corrispondente.
    5. Sei stato reindirizzato alla app di **App Store**. Nella schermata di App Store, tocca l'opzione di installazione.
  - Su Windows, macOS, Android
    1. Accesso Bitdefender centrale.
    2. Seleziona il **I miei dispositivi** pannello.
    3. Premi **INSTALLA LA PROTEZIONE** e poi premi **Proteggi altri dispositivi**.
    4. Seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, premi il pulsante corrispondente.
    5. Premi **INVIA LINK DI DOWNLOAD**.
    6. Inserisci l'indirizzo email nel campo corrispondente e premi **INVIA EMAIL**. Nota che il link del download generato è valido solo per le prossime 24 ore. Se il link dovesse scadere, dovrai generarne uno nuovo seguendo gli stessi passaggi.

7. Sul dispositivo su cui vuoi installare Bitdefender, controlla l'account email che hai digitato e poi premi il pulsante di download corrispondente.

- **Da App Store**
  Cerca Bitdefender Mobile Security for iOS per localizzare e installare la app.

La prima volta che apri la app, viene visualizzata una finestra di introduzione contenente maggiori dettagli sulle funzionalità del prodotto. Tocca Iniziare per passare alla finestra successiva.

Prima di passare alle diverse fasi per la convalida, devi accettare l'Accordo di abbonamento. Prenditi qualche istante per leggere l'Accordo di abbonamento in quanto contiene i termini e le condizioni con cui è possibile utilizzare Bitdefender Mobile Security for iOS.

Tocca **Continua** per passare alla finestra successiva.

6.2.3. Accedi al tuo account Bitdefender

Per usare Bitdefender Mobile Security for iOS, devi collegare il tuo dispositivo a un account di Bitdefender, Facebook, Google, Apple o Microsoft, accedendo all'account direttamente dalla app. La prima volta che apri l'applicazione, ti sarà chiesto di accedere a un account.

Per collegare il tuo dispositivo a un account di Bitdefender:

1. Inserisci l'indirizzo e-mail del tuo account Bitdefender nel campo corrispondente e tocca **AVANTI**. Se non hai un account Bitdefender e vuoi crearne uno, seleziona il link corrispondente e segui le istruzioni sullo schermo fino all'attivazione dell'account.
   Per accedere utilizzando un account Facebook, Google, Apple, o Microsoft, tocca il servizio che vuoi utilizzare dall'area **O accedi con**. Sarai reindirizzato alla pagina di accesso del servizio selezionato. Segui le istruzioni per collegare il tuo account a Bitdefender Mobile Security for iOS.

> **Nota**
> Bitdefender non accede ad alcuna informazione confidenziale, come la password dell'account con cui accedi o le informazioni personali dei tuoi amici e contatti.

2. Inserisci la tua password e tocca **ACCEDI**.

Da qui puoi anche accedere all'Informativa sulla privacy di Bitdefender.

6.2.4. Dashboard

Tocca l'icona di Bitdefender Mobile Security for iOS nell'app drawer del dispositivo per aprire l'interfaccia dell'applicazione.

La prima volta che accedi alla app, ti sarà chiesto di consentire a Bitdefender di inviarti delle notifiche. Tocca **Consenti** per restare informato ogni volta che Bitdefender ha qualcosa da comunicarti di importante sulla app. Per gestire le notifiche Bitdefender, vai in Impostazioni > Notifiche > Mobile Security.

Per accedere alla sezione che ti serve, tocca l'icona corrispondente nella parte inferiore dello schermo.

Protezione web

Resta al sicuro mentre navighi sul web e ogni volta che app meno sicure cercheranno di accedere a domini non affidabili. Per maggiori informazioni, fai riferimento a Protezione web (pagina 225).

VPN

Ottieni sempre la massima privacy indipendentemente dalla rete a cui ti connetti, mantenendo la tua comunicazione Internet cifrata. Per maggiori informazioni, fai riferimento a VPN (pagina 226).

Privacy dell'account

Scopri se i tuoi account e-mail sono stati violati oppure no. Per maggiori informazioni, fai riferimento a Privacy dell'account (pagina 229).

Per vedere opzioni aggiuntive, tocca l'icona ••• sul tuo dispositivo nella schermata principale dell'applicazione. Compariranno le seguenti opzioni:

- **Ripristina acquisti** - Qui puoi ripristinare gli abbonamenti precedenti che hai acquistato tramite il tuo account di iTunes.
- **Impostazioni** - Qui puoi accedere a:
  - **Impostazioni VPN**
    - **Accordo** - è possibile consultare i termini in base ai quali utilizzi il servizio Bitdefender VPN. Toccando l'opzione **Non sono più**

d'accordo, non potrai utilizzare Bitdefender VPN almeno finché non toccherai **Accetto**.

- **Avviso Wi-Fi pubblico** - Puoi attivare o disattivare la notifica del prodotto che compare ogni volta che ti connetti a una rete Wi-Fi non sicura.
  Lo scopo di questa notifica è aiutarti a mantenere i tuoi dati sempre privati e protetti usando Bitdefender VPN.

- **Impostazioni Protezione web**
  - **Accordo** - è possibile consultare i termini in base ai quali utilizzi il servizio Protezione web di Bitdefender. Toccando **Non sono più d'accordo**, non potrai utilizzare Bitdefender VPN almeno finché non toccherai **Accetto**.
  - **Attiva notifica di Protezione web** - Ti avvisa che Protezione web può essere attivata dopo aver completato una sessione di VPN.

- **Rapporti sul prodotto**

- **Feedback** - Da qui puoi lanciare il client email predefinito per inviarci un tuo feedback sulla app.
- **Info app** - Da qui, puoi accedere a varie informazioni sulla versione installata e l'Accordo di abbonamento, l'Informativa sulla privacy e gli accordi per le licenze open-source.

6.3. Esamina

Bitdefender Mobile Security for iOS ti consente di esaminare il tuo dispositivo per rilevare eventuali vulnerabilità di sicurezza e potenziali minacce. Eseguendo la scansione controllerai:

- **Versione del SO:** controllo della versione di iOS per gli aggiornamenti più recenti.
- **Codice di sblocco/Biometrica:** controllo del livello di sicurezza per l'accesso al dispositivo.
- **Protezione web:** controllo dello stato del modulo Protezione web
- **Privacy dell'account:** controllo della presenza di account monitorati elencati nel modulo Privacy dell'account.

- **Scansione Wi-Fi:** controllo dello stato di sicurezza della rete a cui si è attualmente connessi.

Lo stato di protezione viene determinato dopo che esegui una scansione manuale.

Dopo aver eseguito la prima scansione, visualizzerai i suggerimenti di Autopilot di Bitdefender. Si tratta del tuo consulente di sicurezza personale, che ti fornisce suggerimenti contestuali e basati sull'uso e sulle esigenze del tuo dispositivo. In questo modo, potrai beneficiare di tutto ciò che la tua app ha da offrirti.

> **Nota**
> Quando accedi per la prima volta alla app, ti sarà chiesto di eseguire una scansione.

6.4. Avviso di truffa

La funzione Avviso truffa disponibile in Bitdefender Mobile Security for iOS protegge in modo proattivo gli utenti Apple dalle truffe di phishing. Scam Alert per iOS include due livelli di protezione che monitorano le truffe recapitate tramite messaggi SMS/MMS e inviti di calendario:

- **Filtro messaggi di testo (SMS, MMS)**
  Questa funzione identifica e filtra i messaggi SMS e MMS indesiderati.
  Un SMS/MMS dannoso (Short Message Service/Multimedia Messaging Service) si riferisce a un tipo di messaggio inviato a dispositivi mobili con intenti dannosi. Questi messaggi sono progettati per sfruttare vulnerabilità, ingannare i destinatari o causare danni al dispositivo, alle informazioni personali o alla sicurezza del bersaglio.
- **Scanner dei collegamenti di invito del calendario**
  Questa funzionalità rileva calendari ed eventi di spam che contengono collegamenti pericolosi. Il virus del calendario è un tipo di spam che colpisce l'app Calendario del tuo iPhone e può essere fastidioso e potenzialmente pericoloso:
  - Ricevi inviti di calendario o notifiche di eventi indesiderati quando accetti accidentalmente un invito di calendario falso inviato al tuo indirizzo email da hacker o spammer.

- Quando fai clic sul collegamento nell'invito, ti iscrivi inconsapevolmente al calendario del mittente, consentendogli di inviarti più eventi di spam.
- Gli eventi di spam possono contenere collegamenti o allegati che potrebbero portarti a pagine di phishing o altre minacce informatiche se le apri.

6.4.1. Come impostare l'avviso di truffa

Per abilitare Avviso truffa, devi concedere all'app Bitdefender Mobile Security l'accesso alle notifiche del calendario e ai messaggi SMS:

Come abilitare il filtraggio SMS:

Affinché Bitdefender possa iniziare a filtrare i messaggi, devi attivare manualmente l'opzione Filtra mittenti sconosciuti nelle impostazioni dell'app Messaggi:

1. Apri il **Impostazioni** app sul tuo iPhone o iPad.
2. Scorri verso il basso e seleziona **Messaggi** nella lista.
3. Clicca il **Sconosciuto e spam** sezione.
4. Attiva/disattiva **Filtra mittenti sconosciuti** alla posizione accesa.
5. Selezionare **Sicurezza mobile** nella sezione Filtraggio SMS e poi scegli **Abilitare**.

Bitdefender sarà ora in grado di filtrare i messaggi spazzatura sul tuo iPhone/iPad.

> **Nota**
> A causa delle restrizioni di iOS, il filtro SMS di Bitdefender può essere utilizzato solo per i messaggi SMS e MMS che provengono da persone che non hai salvato nei tuoi contatti. Ciò significa che non filtrerà i messaggi delle persone già presenti nel tuo elenco di contatti o i messaggi iMessage di nessuno.

Come abilitare la scansione del calendario:

1. Apri il **Bitdefender Mobile Security** app installata sul tuo iPhone o iPad.
2. Vai a **Avviso di truffa** opzione nella barra di navigazione in basso e premere **Configura ora**.

3. Rubinetto **Continua**, quindi toccare **Abilitare**.
4. Scegliere **OK** per concedere a Bitdefender l'accesso al tuo calendario. La scansione del calendario inizierà immediatamente.

6.5. Scam Copilot

Questa funzionalità è essenzialmente un chatbot basato sull'IA e addestrato da Bitdefender per rilevare diverse truffe, tentativi di phishing, campagne di disinformazione e siti web fasulli.

Per attivare Scam Copilot:

1. Aprire la app Bitdefender Mobile Security. Nel pannello Dashboard, sarà presente una scheda dedicata a Scam Copilot. Toccare **Attiva**.
2. Sarà necessario attivare il filtraggio SMS come indicato di seguito:
   a. Aprire **Impostazioni** sul dispositivo.
   b. Selezionare **Messaggi** dall'elenco.
   c. Selezionare **Sconosciuti e spam**.
   d. Attivare **Filtra mittenti sconosciuti**.
   e. Selezionare **Mobile Security** in Filtraggio SMS.
3. Una volta terminato, premere **Continua**.
4. Attivare la scansione del Calendario. Sullo schermo comparirà una finestra pop-up subito dopo aver premuto il pulsante **Attiva**. Toccare **Consenti accesso completo**.

Ora Scam Copilot è stato configurato correttamente sul dispositivo.

È possibile accedere a Scam Copilot dalla scheda dedicata. Qui sarà possibile trovare:

- **Chatbot per il rilevamento delle truffe:** è possibile chiedere al chatbot di verificare qualsiasi messaggio ritenuto sospetto.
- **Assistente per la prevenzione:** aiuta a saperne di più sulle truffe per individuarle sempre con certezza.
- Stato e pannello di controllo del**Rilevamento truffe automatico**.
- **Filtraggio SMS**: è possibile far filtrare i propri messaggi pericolosi direttamente nella app di messaggistica.

6.6. Protezione web

Protezione web di Bitdefender garantisce un'esperienza di navigazione sicura avvisandoti di pagine web potenzialmente dannose e quando app installate meno sicure cercheranno di accedere a domini non affidabili.

Quando un URL porta a un sito web noto per essere fraudolento o phishing, o a contenuti dannosi come spyware o virus, la pagina web viene bloccata, mostrando un avviso. La stessa cosa accade quando le app installate cercano di accedere a domini dannosi.

> **Importante**
> Se ti trovi in un'area in cui l'uso di un servizio VPN è vietato per legge, la funzionalità Protezione web non sarà disponibile.

Per attivare Protezione web:

1. Tocca l'icona nella parte inferiore dello schermo.
2. Tocca **Accetto**.
3. Attiva l'interruttore della Protezione web.

> **Nota**
> La prima volta che attivi Protezione web, ti viene chiesto di consentire a Bitdefender di impostare le configurazioni VPN che monitoreranno il traffico di rete. Tocca **Consenti** per continuare. Se per proteggere il tuo smartphone è stato impostato un metodo di autenticazione (come impronta digitale o codice PIN), dovrai utilizzarlo. Per rilevare l'accesso a domini non affidabili, Protezione web collabora con i servizi VPN.

> **Importante**
> Protezione web e VPN non possono funzionare contemporaneamente. Ogni volta che una delle due viene attivata, l'altra (se in quel momento è attiva) sarà disattivata.

6.6.1. Avvisi di Bitdefender

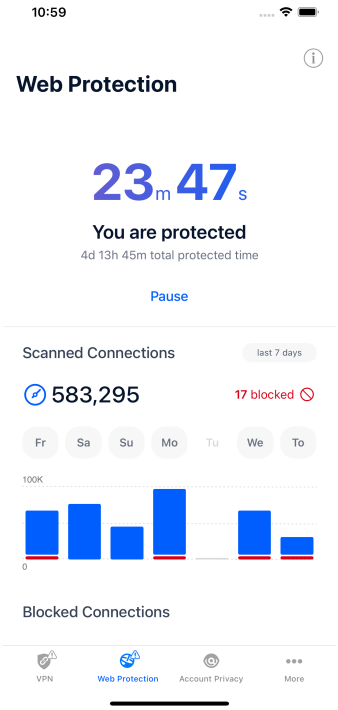
Ogni volta che visiti un sito web classificato come non sicuro, questo viene bloccato. Per informarti dell'evento, vieni avvisato da Bitdefender nel Centro notifiche e nel tuo browser. La pagina di avviso contiene informazioni come l'URL del sito web e la minaccia rilevata. Dunque, dovrai decidere cosa fare.

Inoltre, nel Centro notifiche sarai avvisato ogni volta che una app meno sicura prova ad accedere a domini non affidabili. Tocca la notifica mostrata per essere reindirizzato alla finestra dove potrai decidere cosa fare.

Le seguenti opzioni sono disponibili per entrambi i casi:

- Allontanati dal sito web toccando **RIPORTAMI ALLA PROTEZIONE**.
- Procedi al sito web, malgrado l'avviso, toccando la notifica mostrata e poi su **Voglio accedere alla pagina**.

Conferma la tua scelta.



6.7. VPN

Con Bitdefender VPN puoi mantenere privati i tuoi dati ogni volta che ti connetti a reti wireless non protette mentre sei in aeroporti, centri commerciali, bar o alberghi. In questo modo, è possibile evitare situazioni

spiacevoli, come furti di dati personali o tentativi di rendere accessibile il tuo indirizzo IP a pirati informatici.

Una VPN opera come una sorta di tunnel tra il tuo dispositivo e la rete a cui ti connetti, proteggendo la tua connessione, cifrando i dati usando una cifratura di livello militare e nascondendo il tuo indirizzo IP, ovunque ti trovi. Il tuo traffico viene reindirizzato a un server indipendente, rendendo quindi il tuo dispositivo impossibile da identificare dal tuo provider di servizi Internet tra la miriade di altri dispositivi che stanno usando i nostri servizi. Inoltre, mentre ti connetti a Internet tramite Bitdefender Password Manager, puoi accedere a contenuti che normalmente sono limitati in alcuni paesi.

> **Nota**
> Alcuni paesi applicano una censura di Internet e quindi l'utilizzo delle VPN sul loro territorio è proibito per legge. Per evitare conseguenze legali, potrebbe comparire un messaggio di avviso quando cerchi di usare la app Bitdefender VPN per la prima volta. Continuando a utilizzare la app, confermi di essere consapevole dei regolamenti applicabili del paese in cui ti trovi e dei rischi a cui potresti andare incontro.

Per attivare Bitdefender VPN:

1. Clicca il icona dalla parte inferiore dello schermo.
2. Tocca **Connetti** ogni volta che vuoi restare protetto mentre usi una connessione a reti wireless non affidabili.
   Tocca **Disconnetti** ogni volta che vuoi disattivare la connessione.

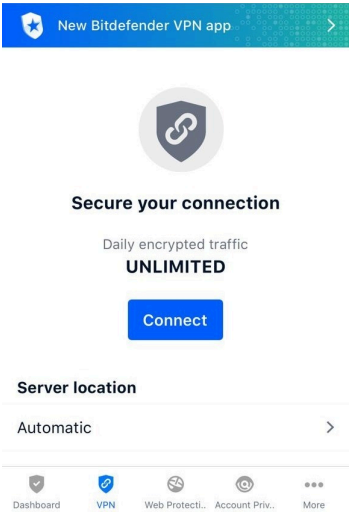
> **Nota**
> La prima volta che attivi VPN, ti viene chiesto di consentire a Bitdefender di impostare le configurazioni VPN che monitoreranno il traffico di rete. Tocca **Consenti** per continuare. Se per proteggere il tuo smartphone è stato impostato un metodo di autenticazione (come impronta digitale o codice PIN), dovrai utilizzarlo.

Quando la VPN è attiva, nella barra di stato compare l'icona VPN.

Per risparmiare la batteria, ti consigliamo di disattivare VPN quando non ti serve.

Se hai un abbonamento premium e ti piacerebbe connetterti a un server a tuo piacimento, tocca Automatico nell'interfaccia VPN e poi seleziona

l'ubicazione desiderata. Per maggiori dettagli sugli abbonamenti a VPN, fai riferimento a Abbonamenti (pagina 228).



6.7.1. Abbonamenti

Bitdefender VPN offre gratuitamente una quota di traffico giornaliera di 200 MB per proteggere la tua connessione ogni volta che ti serve, connettendoti automaticamente all'ubicazione del server ottimale.

Per ottenere traffico illimitato e accesso senza restrizioni a contenuti in tutto il mondo scegliendo l'ubicazione del server che preferisci, fai l'upgrade alla versione premium.

Puoi fare l'upgrade alla versione Bitdefender Premium VPN in qualunque momento toccando il pulsante **Attiva Premium VPN** disponibile nella finestra di VPN. Puoi scegliere fra due tipi di abbonamento: annuale e mensile.

L'abbonamento Bitdefender Premium a VPN è indipendente dall'abbonamento gratuito a Bitdefender Mobile Security for iOS, il che significa che potrai usarlo per la sua intera disponibilità. Se l'abbonamento Bitdefender Premium a VPN scadesse, sarai riportato automaticamente al piano gratuito.

Bitdefender VPN è un prodotto multipiattaforma, disponibile nei prodotti Bitdefender compatibili con Windows, macOS, Android e iOS. Una volta effettuato l'upgrade al piano premium, potrai usare il tuo abbonamento su tutti i prodotti, a condizione che tu acceda con lo stesso account Bitdefender.

> **Nota**
> Bitdefender VPN funziona anche come applicazione indipendente su tutti i sistemi operativi supportati, ovvero Windows, macOS, Android e iOS.

6.8. Privacy dell'account

Privacy dell'account di Bitdefender rileva se si sono verificate perdite di dati negli account che utilizzi per fare pagamenti e acquisti online, o per accedere a diversi siti web e app online. I dati che potrebbero essere stati memorizzati in un account possono essere password, dati della carta di credito o informazioni bancarie, e, se non protetti correttamente, potrebbero verificarsi furti d'identità o invasioni alla privacy.

Lo stato della privacy di un account viene mostrato subito dopo la conferma.

Per verificare se un account è stato violato, tocca **Scansione per violazioni**.

Per iniziare a proteggere le informazioni personali:

1. Clicca il icona dalla parte inferiore dello schermo.
2. Tocca **Aggiungi account**.
3. Inserisci il tuo indirizzo e-mail nel campo corrispondente e tocca **Avanti**.
   Bitdefender deve confermare questo account prima di mostrare informazioni private. Inoltre, viene inviata un'e-mail con un codice di conferma all'indirizzo fornito.
4. Controlla la tua casella di posta e inserisci il codice che hai ricevuto nella sezione **Privacy dell'account** della tua app. Se non riesci a trovare l'e-mail di conferma nei tuoi messaggi in arrivo, controlla anche la cartella dello Spam.
   Viene mostrato lo stato della privacy dell'account confermato.

Se in uno degli account viene rilevata una violazione, ti consigliamo di modificarne la password il prima possibile. Per creare una password sicura, segui questi suggerimenti:

- Deve contenere almeno otto caratteri.
- Includi sia caratteri minuscoli che maiuscoli.
- Aggiungi almeno un numero o simbolo, come #, @, % or !.

Una volta protetto un account coinvolto in una violazione della privacy, puoi confermare le modifiche spuntando le fughe rilevate come **Risolto**. Per farlo:

1. Tocca ··· accanto alla violazione che hai risolto.
2. Tocca **Segna come risolto**.

Quando tutte le violazioni rilevate sono state segnate come Risolte, l'account non apparirà più come violato, almeno fino al rilevamento di una nuova violazione.

6.9. Domande frequenti

In che modo Bitdefender Mobile Security for iOS mi protegge da virus e minacce informatiche?

Bitdefender Mobile Security for iOS fornisce una protezione assoluta da tutte le minacce informatiche ed è stato progettato appositamente per mantenere i tuoi dati al sicuro da occhi indiscreti.

Ottieni una vasta gamma di funzioni avanzate di sicurezza e privacy per il tuo iPhone e iPad, oltre a molte funzioni bonus, tra cui VPN e Protezione web.

Bitdefender Mobile Security for iOS reagisce subito ai virus e malware senza compromettere le prestazioni del sistema.

Che tipo di dispositivi e sistemi operativi sono protetti da Bitdefender Mobile Security for iOS?

Bitdefender Mobile Security per iOS proteggerà i tuoi smartphone e tablet con iOS da tutte le minacce informatiche.

Perché mi serve Bitdefender Mobile Security per iOS su Apple OS?

Alcuni dei tuoi dati più personali sono memorizzati sul tuo iPhone o iPad, e devi sempre avere la certezza che siano al sicuro. Bitdefender Mobile

Security for iOS fornisce una protezione totale dalle minacce informatiche e si prende cura della tua privacy online e delle tue informazioni private senza interferire nelle tue attività quotidiane.

Ottengo una VPN con il mio abbonamento a Bitdefender Mobile Security per iOS?

Bitdefender Mobile Security for iOS ha una versione base di Bitdefender VPN, che include una generosa quantità di traffico gratuito (200 MB/giorno, per un totale di 6 GB/mese).

7. VPN

7.1. Cos'è Bitdefender Password Manager

La VPN funge da tunnel tra il tuo dispositivo e la rete a cui ti connetti per proteggere la tua connessione, crittografare i dati utilizzando una crittografia di livello militare e nascondere il tuo indirizzo IP ovunque tu sia. Il tuo traffico viene reindirizzato attraverso un server separato; rendendo così impossibile l'identificazione del tuo dispositivo da parte del tuo ISP, attraverso la miriade di altri dispositivi che utilizzano i nostri servizi. Inoltre, mentre sei connesso a Internet tramite Bitdefender VPN, puoi accedere a contenuti che normalmente sono limitati in aree specifiche.

> **Nota**
> Alcuni paesi censurano Internet e quindi l'utilizzo di una VPN sul loro territorio è vietato per legge. Per evitare conseguenze legali, potrebbe comparire un messaggio di avviso quando provi a utilizzare la funzionalità di Bitdefender Password Manager per la prima volta. Continuando a utilizzare tale funzionalità, confermi di essere a conoscenza dei regolamenti applicabili nel paese in cui ti trovi e dei rischi in cui potresti incorrere.

7.1.1. Protocolli di cifratura

I set di pacchetti di cifratura predefiniti abilitati sul server e sul client Hydra sono indicati di seguito. Tutti gli altri pacchetti di cifratura sono disabilitati.

Pacchetti di cifratura del client Hydra:

- 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

> **Nota**
> Il set lato server è molto più restrittivo e sia il server che il client Hydra rifiuteranno modalità diverse da GCM tramite AES. Il server Hydra assegna una priorità lato server a pacchetti di cifratura più severi e rifiuterà handshake TLS in caso di richieste di suite meno restrittive da parte di un client. L'elenco può anche essere configurato in runtime lato server.

7.2. Installazione

7.2.1. Prepararsi all'installazione

Prima di installare Bitdefender Password Manager, completa questi passaggi preliminari per assicurarti che l'installazione funzioni senza problemi:

- Assicurati che il dispositivo su cui desideri installare Bitdefender soddisfi i requisiti di sistema. Se il dispositivo non soddisfa tutti i requisiti di sistema, Bitdefender non sarà installato, o, nel caso venisse installato, non funzionerà correttamente e causerà rallentamenti e instabilità.
  Per un elenco completo di tutti i requisiti di sistema, fai riferimento a Requisiti di sistema (pagina 233)
- Accedi al dispositivo utilizzando un account Amministratore.
- Assicurati che il dispositivo sia connesso a Internet durante l'installazione, anche se l'hai avviata da un CD/DVD. Se sono disponibili versioni più recenti dei file dell'applicazione inclusi nel pacchetto d'installazione, Bitdefender può scaricarli e installarli.

7.2.2. Requisiti di sistema

- **Per utenti Windows**
  - **Sistemi operativi:** Windows 7 con Service Pack 1, Windows 8, Windows 8.1 Windows 10 e Windows 11
  - **Memoria (RAM):** 1 GB
  - **Spazio disponibile su disco fisso:** 500 MB
  - **Net Framework:** versione minima 4.5.2

> **Importante**
> Le prestazioni del sistema potrebbero essere influenzate su dispositivi dotati di CPU di vecchia generazione.

- **Per utenti macOS**
  - **Sistema operativo:** macOS Sierra (10.12) o versione successiva
  - **Spazio disponibile su disco fisso:** 100 MB
- **Per utenti Android**
  - **Sistema operativo:** Android 5.0 o versione successiva
  - **Spazio di archiviazione:** 100 MB
  - Una connessione Internet attiva
- **Per utenti iOS**
  - **Sistema operativo:** iOS 12 o versione successiva
  - **Spazio su archiviazione su iPhone:** 50 MB
  - **Spazio di archiviazione su iPad:** 100 MB
  - Una connessione Internet attiva

7.2.3. Installazione di Bitdefender Password Manager

Per avviare l'installazione, segui le istruzioni relative al sistema operativo in uso:

- **Per utenti Windows**
  1. Per avviare l'installazione di Bitdefender Password Manager su un PC Windows, inizia a scaricare il kit di installazione da https://www.bitdefender.com/solutions/vpn/download o dall'e-mail ricevuta dopo il tuo acquisto.
  2. Clicca due volte sul programma d'installazione scaricato per eseguirlo.
  3. Se appare la finestra di dialogo Controllo dell'account utente, seleziona Sì.
  4. Attendi il completamento del download.

5. Tramite il menu a discesa del programma di installazione, seleziona la lingua per il prodotto.
6. Seleziona la casella "Confermo di aver letto e di accettare l'Accordo di abbonamento e l'Informativa sulla privacy, poi clicca su **INIZIA L'INSTALLAZIONE**.
7. Attendi il completamento dell'installazione.
8. **ACCEDI** con il tuo account Bitdefender Central. Se non hai un account Central, clicca sul pulsante **CREA UN ACCOUNT**.
9. Seleziona **Ho un codice di attivazione** se hai acquistato un abbonamento a Premium VPN.
   In alternativa, puoi selezionare **AVVIA PROVA** per provare il prodotto gratuitamente per 7 giorni prima di decidere di pagarlo.
10. Digita il codice che hai ricevuto via e-mail, poi clicca sul pulsante **ATTIVA PREMIUM**.
11. Dopo una breve attesa, Bitdefender Password Manager sarà installato e pronto per essere utilizzato sul tuo computer.

❍ **Per utenti macOS**

1. Per avviare l'installazione di Bitdefender Password Manager su macOS, inizia a scaricare il kit di installazione da https://www.bitdefender.com/solutions/vpn/download o dall'e-mail ricevuta dopo il tuo acquisto.
2. Il programma di installazione viene salvato sul Mac. Nella cartella dei download, fai doppio clic sul file del pacchetto .
3. Segui le istruzioni a schermo. Scegli **Continua**.
4. Ti guiderà attraverso i passaggi necessari per installare Bitdefender Password Manager sul tuo Mac. Clicca due volte sul pulsante **Continua**.
5. Dopo aver letto e accettato i termini del contratto di licenza del software, clicca su **Accetto**.
6. Clicca su **Installa**.
7. Inserisci un nome utente e una password amministratore, poi clicca su **Installa software**.
8. Riceverai una notifica con l'informazione che un'estensione di sistema firmata da Bitdefender è stata bloccata. Non si tratta di un

errore, solo di un controllo di sicurezza. Clicca su **Apri preferenze di sicurezza**.

9. Clicca sull'icona a forma di lucchetto per sbloccarla.
   Inserisci un nome e una password amministratore, poi premi **Sblocca**.
10. Clicca su **Consenti** per caricare l'estensione di sistema di Bitdefender Bitdefender. Poi chiudi la finestra Sicurezza e privacy e il programma di installazione.
11. Accedi all'icona a forma di scudo sulla barra dei menu, poi **effettua l'accesso** con il tuo account Bitdefender Central. Se non hai un account Central, creane uno.
12. Se hai acquistato un abbonamento a Premium VPN, seleziona Ho un **codice di attivazione**.
    Altrimenti puoi scegliere **INIZIA LA PROVA** per testare il prodotto gratuitamente per 7 giorni prima di impegnarsi a pagarlo.
13. Digita il codice ricevuto via e-mail, quindi fai clic su **Attiva codice** pulsante.
14. Dopo una breve attesa, Bitdefender Password Manager sarà installato e pronto per essere utilizzato sul tuo Mac.

- **Per utenti Android**

1. Per installare Bitdefender Password Manager su Android, apri l'app **Google Play Store** sul tuo smartphone o tablet.
2. Cerca {1}{2} e seleziona questa app.
3. Tocca il pulsante **Installa** e attendi il completamento del download.
4. Tocca {1}Apri{2} per eseguire l'app.
5. Seleziona la casella "Accetto l'Accordo di abbonamento e l'Informativa sulla privacy" e poi tocca **CONTINUA**.
6. **Accedi** con il tuo account Bitdefender Central. Se non hai un account Central, tocca **Crea un account** per crearne uno.
7. Se hai acquistato un abbonamento a Premium VPN, seleziona {1}Ho un codice di attivazione{2}.

In alternativa, puoi selezionare Inizia la prova di 7 giorni per provare il prodotto gratuitamente per 7 giorni prima di decidere di pagarlo.

8. Digita il codice che hai ricevuto via e-mail, poi tocca {1}Attiva codice{2}.

- **Per utenti iOS**

1. Per installare Bitdefender Password Manager su iOS, prima apri l'**App Store** sul tuo iPhone o iPad.
2. Cercare Bitdefender Password Manager e seleziona questa app.
3. Tocca l'icona **Scarica** e attendi il completamento del download.
4. Rubinetto **Aprire** per eseguire l'app.
5. Seleziona la casella **Accetto l'Accordo di abbonamento e l'Informativa sulla privacy**, poi tocca **Continua**.
6. **Accedi** con il tuo account Bitdefender Central. Se non hai un account, tocca **Crea un account** per crearne uno.
7. Tocca **Consenti** se desideri ricevere le notifiche di Bitdefender Password Manager.
8. Scegliere **Ho un codice di attivazione** se hai acquistato un abbonamento Premium VPN.
   Altrimenti, puoi scegliere Avvia 7 giorni di prova per testare il prodotto gratuitamente per 7 giorni prima di impegnarti a pagarlo.
9. Digita il codice ricevuto via e-mail, quindi tocca **Attiva il codice**.

7.3. Utilizzare Bitdefender VPN

7.3.1. Aprire Bitdefender VPN

- **Per Windows**

  Per accedere all'**interfaccia principale di Bitdefender VPN**, usa uno dei seguenti metodi:

  - **Dalla barra di sistema**

    Clicca con il pulsante destro sull'icona a forma di scudo rosso nella barra di sistema e seleziona **Mostra** nel menu.

- **Dall'interfaccia di Bitdefender**
  Se un prodotto di sicurezza Bitdefender come Bitdefender Total Security o Bitdefender Antivirus Plus (o altri) sono già installati sul tuo computer Windows, puoi aprire Bitdefender VPN direttamente da questi software:

  1. Clicca su **Privacy** nella barra laterale a sinistra dell'interfaccia di Bitdefender.
  2. Clicca su **Apri VPN** nel pannello VPN.

- **Dal tuo desktop**
  Clicca due volte sull'icona di Bitdefender VPN sul desktop.

- **Per macOS**

  Puoi aprire la app Bitdefender VPN cliccando sull'icona nella barra del menu in alto a destra dello schermo.
  Se non riesci a localizzare lo scudo di Bitdefender nella barra del menu, usa Launchpad o Finder del Mac per riportarlo indietro:

  - **Da Launchpad**

    1. Premi **F4** sulla tastiera per accedere al Launchpad nel tuo Mac.
    2. Sfoglia le pagine delle app installate finché non trovi la app Bitdefender VPN. In alternativa, puoi inserire **Bitdefender VPN** in Launchpad per filtrare i tuoi risultati.
    3. Una volta trovata la app Bitdefender VPN, clicca sulla sua icona per fissarla alla barra del menu.

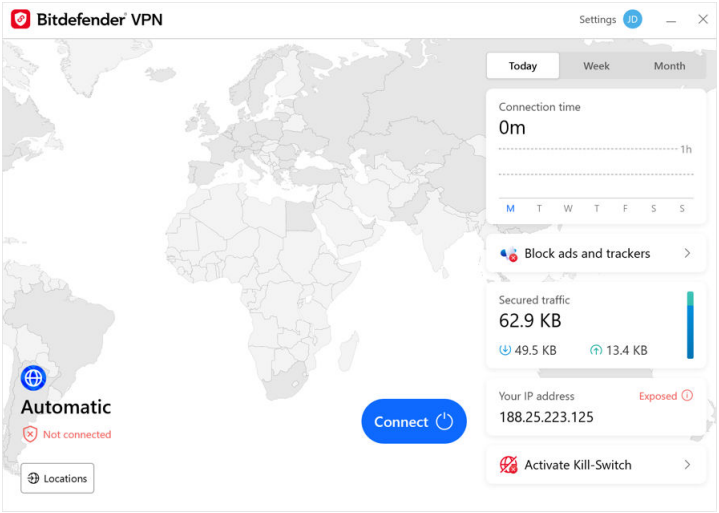
  - **Da Finder**

    1. Clicca su **Finder** in basso a sinistra del Dock (Il Finder è l'icona che sembra un quadrato blu con una faccina sorridente).
    2. Poi, clicca **Vai** in alto a sinistra dello schermo nella barra del menu.
    3. Seleziona **Applicazioni** dal menu per inserire la cartella Applicazioni sul tuo Mac.
    4. Dalla cartella Applicazioni, apri la cartella **Bitdefender** e poi clicca due volte sulla app **Bitdefender VPN**.

> **Nota**
> Per accedere a Bitdefender VPN sui tuoi dispositivi mobili Android o iOS, apri semplicemente l'applicazione VPN dopo averla installata.

7.3.2. Come connettersi a Bitdefender Password Manager

L'interfaccia di VPN mostra lo stato della app: connessa o disconnessa. L'ubicazione del server per gli utenti con la versione gratuita viene impostata automaticamente da Bitdefender sul server più appropriato, mentre gli utenti premium hanno la possibilità di modificare la posizione del server a cui desiderano connettersi, selezionandola dall'elenco Posizioni virtuali. Per connettersi o disconnettersi, basta cliccare sul pulsante di accensione nell'interfaccia di VPN.



- **Per Windows:** l'icona della barra di sistema mostra una spunta di colore verde quando la VPN è connessa e una spunta di colore nero quando è disconnessa. Durante la connessione a una posizione selezionata manualmente, l'indirizzo IP viene mostrato nell'interfaccia principale.
- **Per macOS:** l'icona della barra del menu diventa nera quando la VPN è connessa e in bianco quando è disconnessa. Clicca sul pulsante circolare al centro dell'interfaccia e attendi che venga stabilita la connessione.

- **Per Android e iOS:** per connetterti a Bitdefender VPN per Android, iOS e iPadOS:
  - **Nella app Bitdefender VPN:** per connetterti o disconnetterti tocca semplicemente il pulsante di accensione nell'interfaccia di VPN. Verrà così mostrato lo stato di Bitdefender VPN.
  - **Nella app Bitdefender Mobile Security:**
    1. Accedi all'icona VPN nella barra di navigazione inferiore di Bitdefender Mobile Security.
    2. Tocca **CONNETTI** ogni volta che vuoi ottenere protezione mentre ti connetti a reti wireless non protette. Tocca **DISCONNETTI** ogni volta che vuoi disattivare la connessione a VPN.

7.3.3. Come connettersi a un server diverso

Con un abbonamento Premium, Bitdefender Password Manager ti consente di connetterti a qualsiasi dei nostri server in tutto il mondo e in qualunque momento. Per farlo, dovrai:

1. Apri la app Bitdefender Password Manager.
2. Sul lato inferiore dell'interfaccia, tocca il pulsante **Posizione virtuale**.
3. Seleziona il paese che preferisci.
4. Nel lato inferiore dell'interfaccia, clicca sul pulsante **Connetti a [paese scelto]**.

- L'icona nella barra delle applicazioni visualizza un segno di spunta verde quando la VPN è connessa.
- L'indirizzo IP del server virtuale viene mostrato nella schermata principale mentre sei connesso a Bitdefender VPN.
- Nella dashboard principale vengono visualizzati anche un riepilogo del tempo di connessione, della quantità di traffico protetto e delle ultime 5 posizioni a cui ti sei connesso.

7.4. Bitdefender Password Manager Impostazioni e funzionalità

7.4.1. Accedere alle impostazioni

Per accedere alle impostazioni di Bitdefender Password Manager, segui questi passaggi:

- **In Windows**
  1. Apri l'app Bitdefender Password Manager sul tuo dispositivo. Per farlo, clicca due volte sulla relativa icona nella barra delle applicazioni o clicca con il pulsante destro e seleziona Mostra.
  2. Sul lato sinistro dell'interfaccia, clicca sul pulsante delle **Impostazioni** (rappresentato da un ingranaggio).

- **In macOS**
  1. Per aprire l'app Bitdefender Password Manager sul tuo dispositivo macOS, tocca la sua icona nella barra dei menu.
  2. Nell'angolo in alto a destra dell'interfaccia di Bitdefender Password Manager, tocca il pulsante a forma di ingranaggio e seleziona Impostazioni.

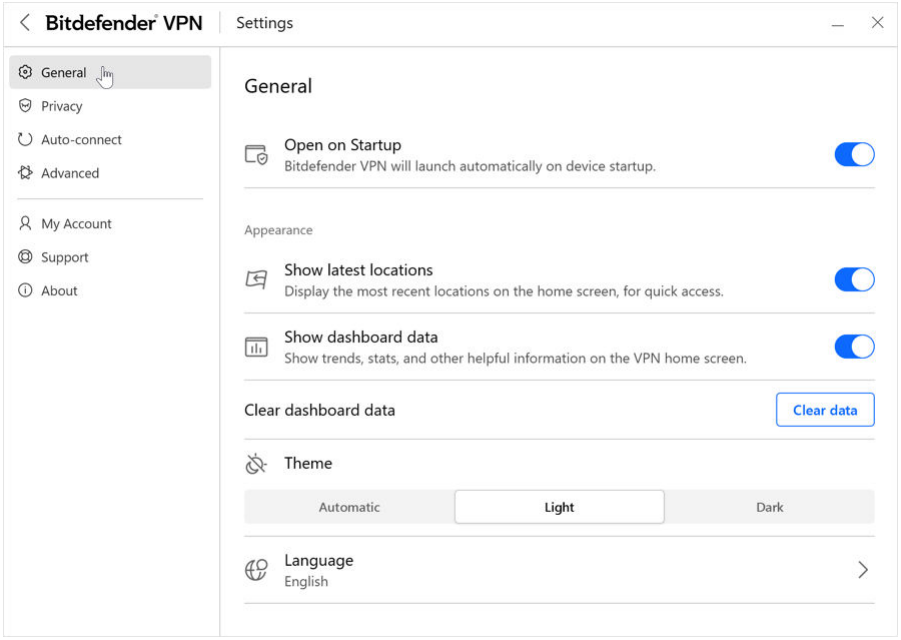
- **Su Android**
  1. Apri la app Bitdefender Password Manager sul tuo dispositivo.
  2. Nell'angolo in alto a destra dell'interfaccia di Bitdefender Password Manager, tocca il pulsante a forma di ingranaggio.

- **Su iOS**
  1. Apri il Bitdefender Password Manager app sul tuo dispositivo.
  2. Fare clic sul pulsante della ruota dentata nell'angolo in alto a destra del Bitdefender Password Manager interfaccia.

7.4.2. Generale

Qui puoi modificare quanto segue:

- **Apri all'avvio**– Bitdefender VPN si avvierà automaticamente all'avvio del dispositivo.
- **Mostra le ultime posizioni**– Visualizza le posizioni più recenti sulla schermata principale, per un accesso rapido.
- **Mostra i dati del dashboard** – Mostra tendenze, statistiche e altre informazioni utili sulla schermata iniziale della VPN.
- **Cancella i dati della dashboard**– Tutti i dati della dashboard verranno cancellati e tutti i contatori verranno ripristinati.
- **Tema**– Tema chiaro/scuro
- **Lingua**– Cambia la lingua di Bitdefender VPN.
- **Notifiche**– Gestisci le tue preferenze di notifica.
- **Aiutaci a migliorare Bitdefender VPN**– Invia report anonimi sui prodotti per aiutarci a migliorare la tua esperienza.
- **Resettare tutte le impostazioni**– Ripristina la VPN alle impostazioni originali senza reinstallarla.



7.4.3. Caratteristiche

Privacy

Interruzione Internet

L'Interruzione Internet è una nuova funzionalità di Bitdefender Password Manager. Quando è attiva, sospende temporaneamente tutto il traffico Internet qualora la connessione VPN si interrompa. Non appena ritorni online, viene ristabilita la connessione VPN.

Per attivare l'Interruzione Internet:

- **Su Windows**
  1. Apri la app Bitdefender Password Manager sul tuo dispositivo cliccando due volte sulla sua icona nella barra di sistema o cliccando con il pulsante destro su di essa e selezionando **Mostra**.
  2. Clicca sul **Impostazioni** pulsante (rappresentato da una ruota dentata) sul lato sinistro dell'interfaccia.
  3. Seleziona **Avanzate**.
  4. Attiva l'opzione **Interruzione Internet**.
- **Su Android**
  1. Apri il Bitdefender Password Manager app sul tuo dispositivo.
  2. Fare clic sul pulsante della ruota dentata nell'angolo in alto a destra del Bitdefender Password Manager interfaccia.
  3. In **Impostazioni**, attiva l'opzione **Interruzione Internet**.
- **Su iOS**
  1. Apri il Bitdefender Password Manager app sul tuo dispositivo.
  2. Fare clic sul pulsante della ruota dentata nell'angolo in alto a destra del Bitdefender Password Manager interfaccia.
  3. Sotto **Impostazioni**, abilita il **Kill-Switch** opzione.

> **Nota**
> Questa funzionalità è disponibile anche per i dispositivi macOS con sistema operativo 10.15.4 o successivo.

Ad blocker e Anti-tracker

Queste funzionalità sono state sviluppate per assisterti nel mantenere la tua privacy e utilizzare il web senza pubblicità fastidiose o aziende che ti spiano. Ti aiutano a bloccare gli annunci pubblicitari e bloccare i tracker online.

Ad blocker

Ad blocker viene usato per bloccare annunci, pop-up, video pubblicità o banner mentre navighi. Ciò aiuterà i siti web a caricarsi più velocemente e ad essere più leggeri, nonché più sicuri nell'interazione.

Per attivare Ad blocker:

1. Localizza le funzionalità **Ad blocker e Antitracker** nelle **Impostazioni**.
2. Imposta l'interruttore sulla posizione **ATTIVATO**.

Anti-tracker

L'**Anti-tracker** viene usato per bloccare i tracker impostati dagli inserzionisti per seguirti e profilarti online. Alcuni siti web potrebbero non funzionare correttamente quando si bloccano i tracker, ma aggiungendo i loro URL alla whitelist dovrebbe essere possibile usarli normalmente.

Per attivare Anti-tracker:

1. Individua il **Blocco pubblicità e Antitracker** funzionalità in **Impostazioni**.
2. Sposta l'interruttore su **SU** posizione.

Whitelist

Alcuni siti web potrebbero non caricarsi correttamente se blocchi il loro codice tracker e gli annunci. Aggiungere gli URL di questi domini alla whitelist potrebbe risolvere il problema, ma ricordati che, mentre navigherai su questi siti web, visualizzerai le pubblicità e il loro codice di tracker sarà attivo.

Aggiungi i siti web a cui desideri consentire la visualizzazione delle pubblicità e l'utilizzo dei tracker:

1. Individua il **Blocco pubblicità e Antitracker** funzionalità in **Impostazioni**.

2. Clicca sul link **Gestisci**. Poi, vai nella sezione Whitelist della finestra e clicca sul link **Gestisci** corrispondente.
3. Clicca su **Aggiungi sito web** e inserisci l'URL desiderato.

Connetti automaticamente

Mentre sei in viaggio, lavorando in un bar o aspettando all'aeroporto, connettersi a una rete wireless pubblica per effettuare pagamenti, controllare le e-mail o gli account dei social network può essere la soluzione più rapida. Ma potrebbero esserci alcuni occhi indiscreti che cercheranno di ottenere i tuoi dati personali, sfruttando ogni falla nella rete per sottrarre informazioni.

Per proteggerti dai rischi derivanti dall'utilizzo di hotspot non sicuri o non crittografati, Bitdefender Password Manager include una funzionalità di connessione automatica. Questo significa che in alcune situazioni Bitdefender Password Manager può essere attivato automaticamente, in base alle tue preferenze e al sistema operativo che usi.

- In **Windows**, è possibile attivare la funzionalità di connessione automatica per le seguenti situazioni:
  - **Avvio:** connettiti a VPN all'avvio di Windows.
  - **Rete Wi-Fi non protetta:** usa VPN ogni volta che ti connetti a reti Wi-Fi pubbliche o non protette.
  - **App peer-to-peer:** connettiti a VPN quando avvii una app di condivisione file peer-to-peer.
  - **App e domini:** utilizza sempre VPN per determinate app e pagine web.

    Nota

    1. Clicca sul link **Gestisci**.
    2. Raggiungi l'ubicazione della app per cui vuoi utilizzare VPN, seleziona il nome della app e clicca su **Aggiungi**.
  - **Categorie siti web:** connettiti a VPN quando visiti determinate categorie di siti web. Bitdefender VPN può connettersi automaticamente per le seguenti categorie di siti web:
    - Finanza

- Pagamenti online
- Salute
- Condivisione file
- Incontri online
- Contenuti per adulti

> **Nota**
> Per ogni categoria, puoi selezionare un diverso server a cui VPN si connetterà.

- In **macOS**, è possibile attivare la funzionalità di connessione automatica per le seguenti situazioni:
  - **Avvio:** connettiti a VPN all'avvio di macOS.
  - **Wi-Fi non protetto:** Usa la VPN ogni volta che ti connetti a reti Wi-Fi pubbliche o non protette.
  - **App peer-to-peer:** Connettiti alla VPN quando avvii un'app di condivisione file peer-to-peer.
  - **Applicazioni:** connettiti sempre a VPN per determinate app.
- In **Android** e **iOS** Bitdefender Password Manager può essere impostato per connettersi automaticamente solo quando stai utilizzando una rete Wi-Fi pubblica o non protetta.

Avanzate

Split tunneling

Lo split tunneling della Virtual private network (VPN) ti consente d'indirizzare parte del traffico del tuo dispositivo o delle tue applicazioni attraverso una VPN cifrata, mentre le altre applicazioni o gli altri dispositivi avranno accesso diretto a Internet. Ciò è particolarmente utile se vuoi beneficiare di servizi che funzionano meglio quando la tua posizione è nota, ottenendo anche un accesso sicuro a comunicazioni e dati potenzialmente sensibili.

Attivando la funzionalità **Split tunneling**, le app e i siti web selezionati bypasseranno la VPN accedendo direttamente a Internet.

Per gestire le applicazioni e i siti web che bypassano la VPN:

1. Clicca sul link **Gestisci** una volta attivata la funzionalità.
2. Clicca sul pulsante **Aggiungi**.
3. Raggiungi la posizione della app in questione o inserisci l'URL del sito web desiderato, poi clicca su **Aggiungi**.

> **Nota**
> Aggiungendo un sito web, l'intero dominio, incluso tutti i sottodomini, saranno bypassati.

> **Importante**
> Nei dispositivi **macOS**, la funzionalità Split tunneling è disponibile solo per i siti web.

App Traffic Optimizer

App Traffic Optimizer di Bitdefender Password Manager ti consente di assegnare la priorità al traffico delle app più importanti sul dispositivo senza esporre la tua connessione a pericoli per la privacy. Le VPN reindirizzano il traffico Internet attraverso un tunnel sicuro usando potenti algoritmi di cifratura per proteggerlo.

Tuttavia, questa combinazione di tecniche può avere alcuni svantaggi, principalmente per quanto riguarda la velocità della connessione. Diversi fattori possono causare rallentamenti nella connessione, i più comuni sono la distanza dal server a cui ci si connette, la congestione della rete e l'elevato utilizzo della banda. Se hai la sensazione che a volte Bitdefender Password Manager causi un carico non necessario alla tua connessione e ottieni costantemente dei rallentamenti, potrebbe essere una risposta migliore alla disconnessione.

Come funziona App Traffic Optimizer?

Alcune app e determinati servizi, come piattaforme di streaming, client torrent e videogiochi, richiedono più banda. Utilizzarli costantemente potrebbe influenzare la velocità della tua connessione a Internet. Indirizzare il tuo traffico attraverso un tunnel VPN già sottopone la tua connessione a un rallentamento. Mettere a dura prova la tua connessione può seriamente degradare la tua esperienza online.

La funzionalità App Traffic Optimizer di Bitdefender Password Manager può aiutarti ad affrontare i rallentamenti di connessione di VPN dando la priorità alle app di tua scelta. La funzionalità ti consente di

decidere quali app dovrebbero ricevere la maggior parte del tuo traffico, successivamente assegna le risorse di conseguenza. Per esempio, se sei in una riunione e noti che la qualità della tua chiamata è scadente, App Traffic Optimizer ti consente di dare la priorità al traffico per la app di videoconferenza ottenendo risultati migliori.

In genere, gli utenti di VPN chiuderebbero tutti i processi che interferiscono sul proprio dispositivo o addirittura disattiverebbero la propria connessione VPN per ottenere una maggiore velocità di Internet. App Traffic Optimizer ti consente di ottenere una protezione alla privacy ininterrotta senza compromettere la tua velocità di connessione.

Utilizzare App Traffic Optimizer

Attualmente, la funzionalità è disponibile solo sui dispositivi Windows e ti consente di assegnare la priorità al traffico per un massimo di 3 applicazioni.

Segui questi passaggi per attivarla e configurarla senza problemi:

1. Lancia l'applicazione Bitdefender VPN sul tuo computer Windows.
2. Clicca sul pulsante nella barra laterale per accedere alle impostazioni di VPN.
3. Raggiungi la scheda **Generali** e attiva la funzionalità **App Traffic Optimizer**. Il colore dell'interruttore cambierà da grigio a blu.

Per gestire le applicazioni prioritarie per questa funzionalità

1. Clicca il**Maneggio**collegamento.
2. Raggiungi la posizione della app per la quale vuoi ottimizzare il traffico, seleziona il nome della app e clicca su **Aggiungi**. La app comparirà nella sezione **Prioritaria**.

> **Nota**
> In alternativa, se di recente hai aperto l'applicazione a cui vuoi assegnare la priorità, premi il pulsante + nella finestra App Traffic Optimizer.

3. Disconnettiti e riconnettiti a Bitdefender VPN dopo aver aggiunto o rimosso le app dall'elenco.

Per rimuovere una app da App Traffic Optimizer, clicca semplicemente sull'icona accanto al nome della app.

Nota
L'ottimizzatore del traffico dell'app non è disponibile su macOS.

Protocollo

Qui puoi scegliere il tipo di protocollo che desideri utilizzare per il trasferimento dei dati. Sono disponibili le seguenti opzioni:

- **Automatico** - Bitdefender VPN selezionerà il protocollo ottimale per il tuo dispositivo e la tua rete specifici.
- **Catapulta dell'Idra** - Veloce e sicuro, ideale per streaming e giochi.
- **OpenVPNUDP** - Ottimizzato per velocità elevate. Tuttavia, questo protocollo non è affidabile in termini di perdita di dati come altri protocolli nell'elenco.
- **Apri VPN TCP** - Progettato per l'affidabilità. Garantisce che i tuoi dati vengano consegnati interamente, ma non è veloce come OpenVPN UDP.
- **Wireguard** - Protocollo più recente, che fornisce una forte sicurezza e un elevato livello di prestazioni.

Doppio salto

Con questa funzionalità puoi gestire i server attraverso i quali inviare e crittografare doppiamente il tuo traffico internet. I tuoi dati passeranno attraverso due server VPN anziché uno, rendendo più difficile monitorare la tua attività su Internet.

Nota
Puoi aggiungere solo un totale di 5 posizioni a doppio salto. Tuttavia, puoi eliminare i doppi hop personalizzati nel tuo elenco e crearne altri in qualsiasi momento.

Importante
L'utilizzo di server situati in continenti diversi nello stesso double-hop potrebbe rallentare la velocità di connessione.

7.5. Disinstallare Bitdefender Password Manager

La procedura di rimozione di Bitdefender Password Manager è simile a quella che useresti per rimuovere qualsiasi altro programma dal computer:

- **Disinstallare Bitdefender Password Manager dai dispositivi Windows**
  - In **Windows 7**:
    1. Clicca su **Inizia**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
    2. Trova **Bitdefender Password Manager** e seleziona **Disinstalla**.
       Attendere che il processo di disinstallazione sia terminato.
  - In **Windows 8** e **Windows 8.1**:
    1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
    2. Clicca su **Disinstalla un programma** o **Programmi e funzionalità**.
    3. Trovare **Bitdefender Password Manager** e seleziona **Disinstalla**.
       Attendere il completamento del processo di disinstallazione.
  - In **Windows 10** e **Windows 11**:
    1. Clicca su **Inizia** e poi su **Impostazioni**.
    2. Clicca sull'icona **Sistema** e seleziona **App installate**.
    3. Trovare **Bitdefender Password Manager** e seleziona **Disinstalla**.
    4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
       Attendere il completamento del processo di disinstallazione.
- **Disinstallare dai dispositivi macOS**
  1. Clicca su **Vai** nella barra del menu e seleziona **Applicazioni**.

2. Clicca due volte sulla cartella **Bitdefender**.
3. Esegui **BitdefenderUninstaller**.
4. Nella nuova finestra, seleziona la casella accanto a **Bitdefender Password Manager**, poi clicca su **Disinstalla**.
5. Digita un nome utente e una password amministratore validi, poi clicca su **OK**.
6. Riceverai la conferma che Bitdefender Password Manager è stato disinstallato correttamente. Clicca su **Chiudi**.

- **Disinstallare dai dispositivi Android**
  1. Apri l'app **Play Store**.
  2. Cerca **Bitdefender Password Manager**.
  3. Nella pagina dello store della app Bitdefender Password Manager, seleziona **Disinstalla**.
  4. Conferma toccando **OK**.
- **Disinstallare dai dispositivi iOS**
  1. Mantieni il dito sulla app Bitdefender Password Manager.
  2. Seleziona **Elimina app**.
  3. Tocca **Elimina**.

7.6. Domande frequenti

Quando devo utilizzare Bitdefender VPN?

Devi fare sempre attenzione quando accedi, scarichi o invii contenuti su Internet. Per assicurarti di essere sempre al sicuro durante la navigazione, ti consigliamo di utilizzare la VPN quando:

- vuoi connetterti a reti wireless pubbliche
- vuoi accedere a contenuti che normalmente sono riservati a determinate aree, indipendentemente dal fatto che ti trovi a casa o all'estero
- vuoi mantenere i tuoi dati personali privati (nomi utente, password, indirizzi e-mail, informazioni della carta di credito, ecc.)

- vuoi nascondere il tuo indirizzo IP

Posso scegliere una città con Bitdefender VPN?

Sì. Attualmente, Bitdefender VPN for Windows, macOS, Android e iOS può essere utilizzato per selezionare una determinata città. Ecco l'elenco delle città attualmente disponibili:

- **Stati Uniti:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, New York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Canada:** Montreal, Toronto, Vancouver
- **Regno Unito:** Londra, Manchester

Bitdefender VPN può essere installato come app indipendente?

La app VPN viene installata automaticamente insieme alla tua soluzione di sicurezza Bitdefender. Può anche essere installata come app indipendente dalla pagina del prodotto, da Google Play Store e App Store.

Bitdefender condividerà il mio indirizzo IP e i miei dati personali con terze parti?

No, con Bitdefender VPN la tua privacy è sicura al 100%. Nessuno (agenzie pubblicitarie, ISP, compagnie d'assicurazione, ecc.) avrà accesso ai tuoi registri online.

Quale algoritmo di cifratura utilizza?

Bitdefender VPN utilizza il protocollo Hydra su tutte le piattaforme, una cifratura AES a 256 bit o la cifratura più alta disponibile supportata sia dal client che dal server, con Perfect Forward Secrecy. Ciò significa che le chiavi di cifratura vengono generate per ogni nuova sessione VPN ed eliminate dalla memoria una volta terminata la sessione.

Posso accedere a contenuti con restrizioni regionali?

Con Premium VPN hai accesso a una vasta rete di posizioni virtuali in tutto il mondo.

Avrà un impatto negativo sulla vita della batteria del mio dispositivo?

Bitdefender VPN è stato sviluppato per proteggere i tuoi dati personali, nascondere il tuo indirizzo IP mentre ti connetti a reti wireless non protette e accedere a contenuti vietati in determinati paesi. Per evitare un consumo non necessario della batteria del tuo dispositivo, ti consigliamo

di utilizzare VPN solo quando ne hai bisogno e disconnetterti quando sei offline.

Perché la VPN rallenta la mia connessione a Internet?

Bitdefender VPN è stato progettato per offrirti una migliore esperienza di navigazione del web. In base alla distanza tra la tua ubicazione attuale e la posizione del server a cui scegli di connetterti, è possibile aspettarsi una certa penalizzazione nella velocità, tuttavia, è quasi sempre sufficientemente ridotta da non notarsi durante le normali attività online. Inoltre, ci affidiamo a una delle infrastrutture VPN più veloci al mondo. Se non è necessario connettersi dalla propria ubicazione a un server ospitato lontano (ad esempio dagli Stati Uniti alla Francia), ti consigliamo di consentire alla VPN di connetterti automaticamente al server più vicino o di trovare un server più vicino alla tua ubicazione attuale.

8. GESTORE DELLE PASSWORD

8.1. Cos'è Bitdefender Password Manager

Bitdefender Password Manager è un servizio multipiattaforma sviluppato per aiutare gli utenti a memorizzare e organizzare tutte le proprie password online. Si basa sui più potenti algoritmi di cifratura noti per il massimo livello di protezione e sicurezza digitale. Funziona come un'estensione del browser e una soluzione app mobile per la gestione di identità e password, dati bancari e qualsiasi altro tipo di informazioni sensibili sui vari dispositivi.

Bitdefender Password Manager può salvare, compilare e generare automaticamente, nonché gestire le tue password per tutti i siti web e i servizi online con l'aiuto di una sola password principale, rendendo così la tua intera identità digitale più facile da gestire.

8.1.1. Sicurezza e come funziona

Alla base del software {1}{2} ci sono alcuni dei più recenti algoritmi di cifratura che garantiscono la più elevata sicurezza dei dati a cui gli utenti possano aspirare, come AES-256-CCM, SH512, BCRYPT e i protocolli HTTPS e WSS per la trasmissione dei dati. Tutti i dati coinvolti vengono cifrati e decifrati localmente. Ciò fa in modo che solo il titolare dell'account possa avere accesso alle informazioni memorizzate nell'account stesso, nonché alla password principale utilizzata per accedervi, così da poter poi usare i relativi dati.

8.2. Come iniziare

8.2.1. Requisiti di sistema

È possibile utilizzare la versione più recente di Bitdefender Password Manager solo su dispositivi con i seguenti sistemi operativi:

- **Per gli utenti PC:**
  - Windows 7 con Service Pack 1
  - Windows 8
  - Windows 8.1

- Windows 10
- Windows 11

- **Per gli utenti macOS:**
  - macOS 10.14 (Mojave) e versioni successive

> **Nota**
> Ricordati che le prestazioni del sistema potrebbero risentirne su dispositivi dotati di CPU di vecchia generazione.

- **Per gli utenti iOS:**
  - iOS 11.0 o versioni successive

- **Per gli utenti Android:**
  - Android 5.1 e versioni successive

> **Nota**
> - La funzionalità di sblocco con le impronte digitali è supportata da **Android 6.0** e versioni successive.
> - La funzionalità di compilazione automatica è supportata da **Android 8.0** e versioni successive, compatibile con iPhone, iPad e iPod touch.

Requisiti software

Per poter usare Bitdefender Password Manager e tutte le sue funzionalità, i tuoi dispositivi Windows o macOS devono soddisfare i seguenti requisiti software:

- **Microsoft Edge** (basato su Chromium 80 e successivi)
- **Mozilla Firefox** (versione 65 o successiva)
- **Google Chrome** (versione 72 o successiva)
- **Safari** (versione 12 o successiva)

> **Nota**
> I requisiti software non sono applicabili per Android e iOS.

Avvertimento

Se i requisiti di sistema indicati sopra non vengono soddisfatti, non sarà possibile installare Bitdefender Password Manager o il prodotto potrebbe non funzionare correttamente.

8.2.2. Installazione

Questo capitolo ti illustrerà come installare Bitdefender Password Manager sia sul tuo browser web sul tuo PC Windows e macOS, nonché sui tuoi dispositivi mobili Android o iOS.

Importante

Prima dell'installazione, assicurati di avere un abbonamento valido a Password Manager nel tuo account **Bitdefender Central**, così che l'estensione del browser possa recuperarne la validità dal tuo account.

Gli abbonamenti attivi sono indicati nella sezione **I miei abbonamenti** in Bitdefender Central.

Installazione su dispositivi Windows e macOS

A differenza della maggior parte delle applicazioni desktop e dei software che devono essere installati e impostati su questi dispositivi, Bitdefender Password Manager è disponibile come estensione del browser, anche nota come add-on, che può essere aggiunta e attivata nel tuo browser preferito.

I browser attualmente supportati per il prodotto sono: **Google Chrome**, **Mozilla Firefox**, **Microsoft Edge** e **Safari**.

1. Vai in https://central.bitdefender.com/ e accedi al tuo account.
   Se non hai già un account, seleziona **CREA ACCOUNT** e inserisci il tuo nome completo, un indirizzo e-mail e una password.
2. Seleziona **I miei dispositivi** nella barra laterale sinistra dello schermo.
3. Nella sezione **I miei dispositivi**, continua selezionando **+ Aggiungi dispositivo**.
4. Si aprirà una nuova finestra. Scegli **Password Manager** nella schermata di selezione.
5. Scegli **questo dispositivo**.

Se stai cercando di installarlo su un altro dispositivo, seleziona Altri dispositivi. Potrai successivamente inviare un link di download al rispettivo dispositivo o copiare direttamente l'URL per l'installazione.

6. Ora scegli su quale browser vuoi installare l'estensione di Password Manager.
7. Ogni pulsante corrispondente ti reindirizzerà al Negozio delle estensioni del browser. Da qui, segui semplicemente le istruzioni sullo schermo come mostrato di seguito:

   Microsoft Edge

   - Seleziona il pulsante **Ottieni**
   - Seleziona **Aggiungi estensione** nel prompt che compare sullo schermo

   Google Chrome

   - Seleziona il pulsante **Aggiungi a Chrome**
   - Nella casella di conferma, seleziona **Aggiungi estensione**

   Mozilla Firefox

   - Seleziona il pulsante **Aggiungi a Firefox**
   - Seleziona il pulsante **Installa** nell'angolo in alto a destra dello schermo

   Safari

   - Seleziona il pulsante **Ottieni** e seleziona su **Installa**
   - Apri Safari e seleziona **Preferenze** nella barra superiore del menu
   - Nella finestra Preferenze, seleziona la scheda **Estensioni**
   - Seleziona la casella accanto a Password Manager per attivarlo

Una volta seguiti questi passaggi, imposta una password principale sicura e premi il pulsante **Salva la password principal**e dopo aver letto e accettato i **Termini e le condizioni**.

> **Importante**
> Ricordati che la password principale ti servirà per sbloccare tutte le password, i dati delle carte di credito e gli appunti salvati in Bitdefender Password Manager. È la chiave che consente al proprietario di usare il prodotto.

Avvertimento

Dopo aver creato la password principale, riceverai un **codice di recupero di 24 cifre**. **Annota il tuo codice di recupero in un luogo sicuro e non perderlo**. Il codice è l'unico modo per accedere alle tue password salvate in Password Manager nel caso dovessi **dimenticare la password principale** impostata in precedenza per il tuo account.

❍ Una volta fatto, puoi premere **Chiudi**.

Installazione su dispositivi Android

Il modo più facile per installare Bitdefender Password Manager per telefoni e tablet Android è scaricare l'applicazione direttamente da Google Play.

GET IT ON Google Play

Si può installare la app Bitdefender Password Manager anche tramite il tuo account **Bitdefender Central**:

1. Accedi al tuo account Bitdefender Central sul tuo dispositivo mobile Android tramite https://login.bitdefender.com/central/login.
2. Selezionare **I miei dispositivi** nella barra laterale sinistra dello schermo.
3. Nel **I miei dispositivi** sezione, procedere cliccando su **+ Aggiungi dispositivo**.
4. Questa azione farà apparire una nuova finestra. Scegliere **Gestore di password** nella schermata di selezione.
5. Scegliere **Questo dispositivo**.
   Se stai cercando di installarlo su un altro dispositivo, seleziona **Altri dispositivi**. Potrai successivamente inviare un link di download al rispettivo dispositivo o copiare direttamente l'URL per l'installazione.
6. L'installazione ti reindirizzerà a **Google Play**. Tocca **Installa** per scaricare Bitdefender Password Manager su Android.
7. Una volta completato il download, apri l'applicazione Password Manager.
8. Se non accedi automaticamente al tuo account, fallo inserendo il tuo nome utente e la tua password.

Dopo aver seguito questi passaggi, imposta una password principale sicura, quindi premi il tasto **Salva password principale** pulsante dopo aver letto e concordato con il **Termini e Condizioni**.

> **Importante**
> Tieni presente che avrai bisogno di questa password principale per sbloccare tutte le password, le informazioni sulla carta di credito e le note salvate in Bitdefender Password Manager. Questa è essenzialmente la chiave che consente al proprietario di utilizzare questo prodotto.

> **Avvertimento**
> Dopo aver creato la password principale, riceverai a **Chiave di ripristino a 24 cifre**. Prendi nota della chiave di ripristino in un luogo sicuro e non perderla. Questa chiave è l'unico modo per accedere alle tue password salvate in Password Manager nel caso in cui ti capitasse **dimenticare la password principale** precedentemente impostato per il tuo account.
>
> ❍ Puoi premere **Vicino** quando fatto.

9. Crea un **PIN di 4 cifre**, così se dovessi passare a un'altra app e poi tornare a Password Manager, non dovrai inserire nuovamente la password principale che hai impostato in precedenza. Se disponibile, potrai anche attivare il riconoscimento facciale o l'autenticazione tramite l'impronta digitale.
10. Tocca **Compilazione automatica** per configurare le impostazioni della compilazione automatica di Android.

> **Nota**
> Se salti questo passaggio, potrai attivare e personalizzare le funzionalità di compilazione automatica di Android successivamente seguendo le istruzioni disponibili in Compilazione automatica intelligente (pagina 269).

11. Ti sarà presentato un elenco di app che possono compilare automaticamente le password.
    Seleziona **Password Manager** e successivamente il dispositivo ti chiederà di confermare se ritieni affidabile questa app.
    Tocca **OK**.

12. Inserisci il PIN impostato nel **passaggio 9** per confermare questa azione.

L'installazione sui tuoi dispositivi Android è ora completata.

Installazione sui dispositivi iOS

Il modo più facile per installare Bitdefender Password Manager per i dispositivi iOS e iPadOS è scaricare l'applicazione da App Store di Apple.

Download on the App Store

L'installazione dell'app Bitdefender Password Manager può essere eseguita anche tramite il tuo Bitdefender centrale account:

1. Sul tuo iPhone o iPad accedi al tuo account Bitdefender Central tramite https://login.bitdefender.com/central/login.
2. Selezionare **I miei dispositivi** nella barra laterale sinistra dello schermo.
3. Nel **I miei dispositivi** sezione, procedere cliccando su **+ Aggiungi dispositivo**.
4. Questa azione farà apparire una nuova finestra. Scegliere **Gestore di password** nella schermata di selezione.
5. Scegliere **Questo dispositivo**.
   Se stai cercando di installare su un dispositivo diverso, seleziona **Altri dispositivi**. È quindi possibile inviare tramite e-mail un collegamento per il download al rispettivo dispositivo o copiare direttamente l'URL per l'installazione.
6. L'installazione ti reindirizzerà all'**App Store**. Tocca l'icona della nuvola con una freccia che punta verso il basso per scaricare Bitdefender Password Manager per iOS.
7. Una volta che l'applicazione è stata installata, aprila e spunta la piccola casella sulla schermo. Seleziona **Continua** dopo aver letto e accettato l'**Accordo di abbonamento**.
8. Se non accedi automaticamente al tuo account, accedi utilizzando il tuo nome utente e password.

Dopo aver seguito questi passaggi, imposta una password principale sicura, quindi premi il tasto **Salva password principale** pulsante dopo aver letto e concordato con il **Termini e Condizioni**.

> **Importante**
> Tieni presente che avrai bisogno di questa password principale per sbloccare tutte le password, le informazioni sulla carta di credito e le note salvate in Bitdefender Password Manager. Questa è essenzialmente la chiave che consente al proprietario di utilizzare questo prodotto.

> **Avvertimento**
> Dopo aver creato la password principale, riceverai a **Chiave di ripristino a 24 cifre**. Prendi nota della chiave di ripristino in un luogo sicuro e non perderla. Questa chiave è l'unico modo per accedere alle tue password salvate in Password Manager nel caso in cui ti capitasse **dimenticare la password principale** precedentemente impostato per il tuo account.
>
> ❍ Puoi premere **Vicino** quando fatto.

9. Creare un **PIN a 4 cifre**, quindi se passi a un'altra app e poi torni a Password Manager, non dovrai reinserire la password principale che hai impostato in precedenza. Se disponibile, puoi anche abilitare il riconoscimento facciale o l'autenticazione delle impronte digitali.

L'installazione sul tuo dispositivo iOS / iPadOS è ora completata!

8.2.3. Piano condiviso

Bitdefender Password Manager Shared Plan consente a più utenti di accedere e utilizzare lo stesso abbonamento. Fornisce un approccio centralizzato all'accesso, all'amministrazione e al supporto del software, offrendo una soluzione economica per la condivisione del servizio di password manager tra più utenti.

- ❍ Il responsabile del piano di abbonamento condiviso, denominato Responsabile del Piano, può condividere il servizio tra gli iscritti.
- ❍ Ogni membro riceve un account Bitdefender Central unico, collegato al proprio indirizzo e-mail e all'accesso al servizio Password Manager.

Condivisione di Bitdefender Password Manager con più utenti

Invito di membri

Per aggiungere uno o più utenti all'abbonamento condiviso, il gestore del piano deve seguire questi passaggi:

1. Accedere al proprio account Bitdefender Central all'indirizzo https://central.bitdefender.com/.
2. Accedere al menu **I miei abbonamenti** situato sul lato sinistro della pagina.
3. Scegliere **Invita membro** nel pannello **Bitdefender Password Manager Shared Plan**.
4. Inserire l'e-mail di ogni persona con cui si desidera condividere l'abbonamento, quindi fare clic su **Invia**. È possibile aggiungere un massimo di 3 membri alla volta.
5. Le istruzioni per l'installazione vengono inviate subito via e-mail ai nuovi membri. Cliccare su **Chiudi** per uscire dalla finestra di conferma.

> **Nota**
> I membri hanno 24 ore per accettare il tuo invito una volta ricevuto via email.
>
> - I membri invitati appariranno con lo stato "Invitato".
> - Li vedrai come membri "Attivi" dopo che avranno accettato l'invito. Riceverai inoltre una notifica via e-mail per ogni invito accettato.

Rimozione di membri

L'accesso al piano condiviso di Bitdefender Password Manager viene perso per i membri che vengono rimossi. Quando il gestore del piano decide di rimuovere un membro dell'abbonamento, il membro riceve una notifica via e-mail. Per i 30 giorni successivi, l'ex membro passa a una versione di prova di Bitdefender Password Manager di 30 giorni con tutte le funzionalità. Il servizio verrà poi disattivato.

Il responsabile del piano può eliminare gli utenti dal piano condiviso nel seguente modo:

1. Accedere al proprio account Bitdefender Central all'indirizzo https://central.bitdefender.com/.
2. Accedere al menu **I miei abbonamenti** situato sul lato sinistro della pagina.

3. Nel pannello del **Bitdefender Password Manager Shared Plan**, fare clic su **Gestisci**, quindi scegliere **Modifica membri** nel menu.
4. Fare clic sul pulsante **Rimuovi** per togliere un membro dal piano condiviso.
5. Scegliere **Sì, rimuovi membro** e cliccare sul pulsante **Termina modifica** per rendere effettive le modifiche.

> **Nota**
> Quando un membro viene eliminato dal piano condiviso, il suo stato viene modificato in **In attesa di rimozione** fino alla sua completa eliminazione.

Accettare un invito

Riceverai un'e-mail quando qualcuno ti invita a diventare un membro dell'abbonamento al piano condiviso di Bitdefender Password Manager. Hai 24 ore per accettare un invito una volta che ti è stato inviato.

Per accettare l'invito e ottenere l'accesso alle funzionalità del gestore password, l'utente deve seguire questi passaggi:

1. Aprire l'e-mail ricevuta intitolata **[Inizia a usare il tuo abbonamento Bitdefender come membro]** e fare clic sul pulsante **ATTIVA IN CENTRAL**.
2. La pagina Bitdefender Central si aprirà quindi nel tuo browser.
   - Se hai già un account utente Bitdefender associato all'e-mail con cui è stato inviato l'invito, **accedi** per richiedere l'abbonamento condiviso.
   - Se non hai un account utente Bitdefender, clicca su **Crea** e registrati con la stessa e-mail con cui ti è stato inviato l'invito per richiedere l'abbonamento condiviso.
     - Inserisci il tuo nome e cognome
     - Inserisci il tuo indirizzo email
     - Inserisci la tua password
     - Clicca sul pulsante Crea account e sarai iscritto.

3. Dopo aver effettuato l'accesso, fare clic su **Inizia** nella schermata di benvenuto che informa che l'abbonamento a Bitdefender Password Manager è ora attivo.
4. Seguire i passaggi sullo schermo descritti anche in Installazione (pagina 256).

> **Nota**
> L'e-mail del gestore del piano viene visualizzata nel tuo account Bitdefender Central nella parte superiore del menu Password Manager e sulla scheda di abbonamento, sotto I miei abbonamenti.
>
> Se hai bisogno di assistenza con il piano condiviso, contattali.

8.3. Importare ed esportare le tue password

Bitdefender Password Manager è stato sviluppato in modo tale da facilitare con efficacia la comunicazione e il trasferimento di dati con fonti esterne, piattaforme e strumenti software. Questo è il motivo principale per cui è possibile importare o esportare password da o verso Bitdefender Password Manager con estrema facilità.

8.3.1. Compatibilità

Bitdefender Password Manager può trasferire facilmente dati dal seguente elenco di applicazioni:

- **1Password**
- **Bitwarden**
- **Bitdefender Password Manager**
- **ByePass**
- **Chrome browser**
- **Claro**
- **Dashlane**
- **Edge browser**
- **ESET Password Manager v2**
- **ESET Password Manager v3**
- **StickyPassword**

- **Watchguard**
- **Firefox browser**
- **Gestor de contraseñas – Claro**
- **Gestor de contraseñas – SIT**
- **Gestor de contraseñas – Telnor**
- **KeePass 2.x**
- **LastPass**
- **Panda Dome Passwords**
- **PassWatch**
- **Saferpass**
- **SFR Cybersécurité**
- **SIT**
- **F-Secure**
- **Telnor**

> **Nota**
> Se il nome del browser o dello strumento di gestione delle password da cui stai cercando di trasferire i dati non è indicato nell'elenco fornito sopra, puoi seguire la nostra guida online che illustra come modificare un file CSV da un password manager non supportato così da importarne i dati in **Bitdefender Password Manager**: https://www.bitdefender.it/consumer/support/answer/22167/

Questo trasferimento di dati tra Bitdefender Password Manager e altri software di gestione degli account può essere effettuato con i seguenti formati di dati:

CSV, **JSON**, **XML**, **TXT**, **1pif** e **FSK**.

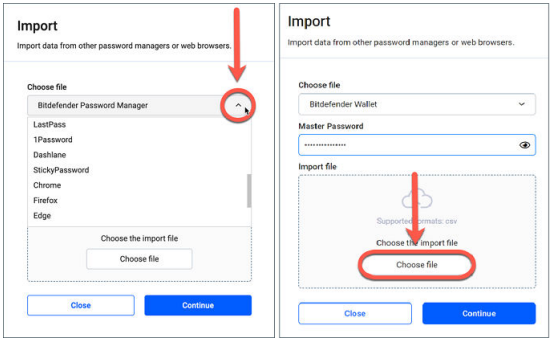
8.3.2. Importazione in Password Manager

Bitdefender Password Manager ti consente di importare facilmente le password da altri browser e password manager. Se attualmente stai cercando di passare a Bitdefender Password Manager da un altro servizio di gestione delle password, molto probabilmente hai memorizzato una notevole quantità di credenziali, come nomi utente, password e altri dati d'accesso richiesti per tutti i tuoi account.

Ora che hai scelto Bitdefender Password Manager, cercherai d'importarci quei dati salvati.

Ecco come importare le tue informazioni salvate da altre app e browser web in Bitdefender Password Manager, **indipendentemente dal sistema operativo** su cui ha scelto d'installare il prodotto:

1. Seleziona l'icona di Password Manager nel tuo browser web (su Windows o macOS) o lancia l'applicazione di Password Manager (su Android o iOS). Se richiesto, inserisci la tua **password principale**.
2. Apri il menu di Password Manager per espandere la barra laterale a sinistra e seleziona la voce **Impostazioni**.
3. Scorri in basso fino alla sezione **Dati** e seleziona l'opzione **Importa dati**.
4. Usa il menu a discesa per selezionare il nome del browser o della app di gestione delle password da cui vuoi importare i tuoi account. Inserisci la tua **password principale** nel campo corrispondente e seleziona **Scegli file**.



5. Naviga nelle cartelle per trovare il percorso in cui hai salvato il file contenente i tuoi nomi utenti e le tue password, esportato dal tuo attuale browser web o password manager, e premi **Continua**.

Una volta importate, le tue password saranno accessibili su ogni dispositivo in cui è stata installata l'applicazione o l'estensione del browser di Bitdefender Password Manager.

8.3.3. Esportazione da Password Manager

Bitdefender Password Manager ti consente di esportare facilmente le tue password salvate (incluso le credenziali di accesso per l'account, note protette, ecc.) in un file CSV (valori separati da una virgola) o un file cifrato se vuoi passare a un altro servizio di gestione delle password, così che la tua partenza da Bitdefender Password Manager non sarà un processo troppo complicato.

> **Importante**
> Un file CSV **non** è cifrato e contiene nomi utenti e password in formato di testo normale, il che significa che le tue informazioni private possono essere lette da chiunque abbia accesso al tuo dispositivo. Ti consigliamo quindi di seguire le istruzioni in basso su un dispositivo affidabile.

Ecco come puoi esportare i tuoi dati da Bitdefender Password Manager:

1. Fai clic sull'icona Password Manager nel tuo browser web (su Windows o macOS) o avvia l'applicazione Password Manager (su Android o iOS). Se richiesto, inserisci il tuo Password principale.
2. Apri il menu di Password Manager per espandere la barra laterale a sinistra e seleziona la voce **Impostazioni**.
3. Scorri in basso fino alla sezione **Dati** e seleziona l'opzione **Esporta dati**.
4. Ora dovresti ricevere le seguenti due opzioni:
   - **CSV**
   - **File protetti da password**

   Seleziona la tua opzione preferita e inserisci la tua password principale, quindi seleziona il pulsante **Esporta dati**.

   > **Nota**
   > Se scegli l'opzione file protetto da password, ti sarà chiesto di cifrare i dati contenenti l'elenco degli account con una password, così che solo tu possa accedervi in caso di necessità.

5. La tua app e/o il tuo browser web procederanno salvando un file chiamato Bitdefender Password Manager_exported_data_current-date

nel tuo sistema nella cartella predefinita di download. Contiene tutti i dati memorizzati in Bitdefender Password Manager.

Dopo aver esportato i tuoi dati, potrai caricarli nel password manager che preferisci.

8.4. Caratteristiche e funzionalità

Questo capitolo ti guiderà attraverso tutte le caratteristiche e le funzionalità di Bitdefender Password Manager, illustrando la loro utilità e come sfruttarle con la massima efficacia.

8.4.1. Gestione delle password

Generatore di password

La regola d'oro relativa alla sicurezza online è utilizzare sempre sequenze casuali e univoche per ogni servizio che richiede la creazione di un account. Il riutilizzo delle password in più piattaforme è la prima causa di furti d'identità e perdite associate alla sottrazione di un account.

Questa funzionalità aiuta gli utenti con la generazione di password uniche, sicure e complesse per ogni nuovo account che creano online. Ciò elimina la necessità degli utenti di inventare password complesse da soli o fare attenzione a non riutilizzare la stessa password per più account.

Si può accedere a **Password Generator** tramite la scheda in alto nell'interfaccia di Password Manager.

Il generatore può essere impostato per generare password **comprese tra 4 e 32 caratteri**.

Si possono anche specificare le tipologie di caratteri che dovrebbero o non dovrebbero essere presenti nella password generata casualmente spuntando o deselezionando le caselle corrispondenti. **(Minuscole, maiuscole, numeri, caratteri speciali)**

Premendo il pulsante alla destra della password mostrata, il generatore modificherà la password suggerita.

Per usare la password mostrata, premi **Usa la password**, un'azione che salverà la stringa di caratteri nei tuoi appunti.

> **Nota**
> Le tue password generate in precedenza saranno memorizzate temporaneamente nella cronologia delle password, accessibile tramite il pulsante **Cronologia password**.

Acquisizione delle password

Con questa funzionalità di Password Manager, ti sarà chiesto di memorizzare tutte le tue nuove password subito dopo averle create. Password Manager chiederà agli utenti di memorizzare le loro nuove password appena create, in modo che possano essere aggiunte subito all'ambiente ultra sicuro fornito da Bitdefender.

Compilazione automatica intelligente

Bitdefender Password Manager può essere impostato in modo tale da compilare automaticamente tutte le tue credenziali di accesso e le password più importanti. Algoritmi proprietari possono rilevare e pre-compilare le credenziali sui siti web visitati in precedenza, facendo risparmiare tempo agli utenti ogni volta che accedono a un servizio.

1. Su Windows o macOS, clicca sull'icona **Password Manager** nel tuo browser web.

   Su Android o iOS, esegui l'applicazione **Password Manager**.
   Se richiesto, inserisci la tua **password principale**.

2. Apri il menu di Password Manager per espandere la barra laterale sinistra e seleziona la voce **Impostazioni**.

3. Seleziona **Impostazioni dispositivo**.

4. Qui noterai un pulsante che mostra le opzioni **Disattiva compilazione automatica** o **Attiva compilazione automatica**. Questa impostazione controlla lo stato operativo della funzionalità di compilazione automatica intelligente.

Rapporto di sicurezza

Il Rapporto di sicurezza è uno strumento che genererà rapporti basati su un numero di funzionalità pensate per rafforzare la tua sicurezza digitale. Ti farà sapere se una password richiede la tua attenzione immediata determinando il suo livello di sicurezza. Rileverà i duplicati

delle password, chiedendoti di modificarle di conseguenza, evitando i pericoli derivanti dal riutilizzare le stesse password per più account.

Il rapporto si concentrerà nel fornire informazioni sull'igiene generale delle password: in particolare se ci sono password duplicate e deboli, o password o indirizzi e-mail trapelati.

Ciò viene fatto confrontando l'elenco degli hash cifrati dalla pagina web di Troy localmente sul tuo dispositivo per verificare se contiene gli hash corrispondenti delle tue password. Se viene trovata una corrispondenza, riceverai un avviso per incoraggiarti a modificare le tue password o altre credenziali d'accesso.

Per accedere al **rapporto di sicurezza**, accedi all'interfaccia di Password Manager e seleziona il suo pulsante corrispondente nella barra superiore.

Sincronizzazione con altre piattaforme

Salvare le tue password una volta in Bitdefender Password Manager ti consentirà di memorizzarle e accedervi in modo sicuro su tutti i tuoi dispositivi Windows, Mac, Android o iOS da Chrome, Safari, Firefox ed Edge o nelle app mobile.

> **Nota**
> Bitdefender è dotato anche di una **modalità offline** per accedere alle tue password nel caso non disponessi momentaneamente di una connessione a Internet. Ciò rende le tue password accessibili in qualsiasi momento e da qualsiasi luogo.

Eliminare una voce

Per eliminare prima le password salvate, premi l'icona di modifica accanto alla voce che vuoi rimuovere, localizzata nella scheda **Account**. Scorri in basso e seleziona **Elimina**. Quando ti viene chiesto, se hai la certezza di voler rimuovere l'account, seleziona **Rimuovi**.

8.4.2. Gestione dell'account

Autenticazione

L'autenticazione in Bitdefender Password Manager viene fatta attraverso il **PIN** impostato nella fase di installazione del prodotto. (Nota che la

funzionalità di **Blocco automatico** bloccherà il password manager o uscirà dopo un periodo di inattività a livello del browser o chiudendo la app mobile)

Inoltre, se disponibili, può essere fatto anche sfruttando alcuni dati biometrici, come l'**impronta digitale** o il **riconoscimento facciale**.

Per **attivare o disattivare** l'autenticazione basata sui dati biometrici:

1. Su Windows o macOS, fai clic su **Password Manager** icona nel tuo browser web.

   Su Android o iOS, avvia il file **Password Manager** applicazione.
   Se richiesto, inserisci il tuo Password principale.

2. Apri il menu Gestore password per espandere la barra laterale a sinistra e fare clic su **Impostazioni** elemento del menu.
3. Clicca su **Impostazioni del dispositivo**.
4. Qui noterai un pulsante che mostra le opzioni **Disattiva dati biometrici** o **Attiva dati biometrici**. Questa impostazione controlla lo stato operativo della funzionalità di autenticazione basata sui dati biometrici.

Reimpostazione della password principale

> **Importante**
> La funzionalità **Cambia password principale** non è disponibile sui dispositivi mobili. L'unico modo per cambiare o recuperare la tua password principale è tramite l'estensione del browser Bitdefender Password Manager su Windows PC o un dispositivo macOS.

Ecco come cambiare la tua **password principale** come misura precauzionale e crearne una nuova in Bitdefender Password Manager:

1. Una volta installata l'estensione del browser, clicca sull'icona **Password Manager** nella barra degli strumenti del browser web.
2. Inserisci la tua attuale password principale per sbloccare il vault.

> **Importante**
> Se non ricordi la tua attuale password principale, seleziona l'opzione **Ho dimenticato la mia password** nella stessa schermata. Inserisci il **codice di recupero di 24 cifre** fornito durante la configurazione iniziale di Bitdefender Password Manager e digita una nuova password principale. **Se hai dimenticato o smarrito** sia la **password principale** che il **codice di recupero**, come ultima possibilità, **contatta un responsabile di Bitdefender per aiutarti a reimpostare il tuo account**. Reimpostare il tuo account **eliminerà tutti i tuoi dati e le tue password** salvati in Bitdefender Password Manager.

3. Apri il menu Gestore password per espandere la barra laterale a sinistra e fare clic su **Impostazioni** elemento del menu.
4. Seleziona il pulsante **Il mio account** nella sezione **Account**.
5. Si aprirà una finestra con alcune informazioni sul tuo abbonamento di Password Manager.
   Seleziona il pulsante **Cambia password principale**.
6. Si aprirà una nuova finestra dove potrai selezionare una nuova password principale. Inserisci la tua attuale password principale e digitane una nuova. La nuova password principale deve contenere un minimo di 8 caratteri, almeno una lettera minuscola, una maiuscola e un numero.
7. Premi il pulsante **Cambia** una volta fatto.
8. Attendi alcuni istanti finché Bitdefender non resetta la vecchia password principale.
   Non uscire dal tuo browser web!
9. Successivamente, ti sarà fornito un nuovo **codice di recupero di 24 cifre**. Annotati il codice di recupero in un posto sicuro e **non perderlo**. Il codice è l'unico modo per accedere alle tue password salvate in Password Manager nel caso avessi dimenticato la password principale.
   Premi **Chiudi** una volta fatto.
10. Sarà effettuata la disconnessione da Bitdefender Password Manager.
    Per sbloccare il vault, usa la nuova password principale che hai appena impostato.

8.4.3. Altre funzionalità

Gestione delle identità

Questa funzionalità consente agli utenti di memorizzare più identità e permette a Password Manager di compilare automaticamente i dettagli nei moduli web prima di effettuare un acquisto in modo sicuro, facile e veloce.

Come tutto il resto in Password Manager, tutti i dati sensibili contenuti all'interno di queste identità memorizzate sono cifrati e disponibili solo per il dispositivo dell'utente.

Per aggiungere un'identità a Password Manager:

1. Su Windows o macOS, fai clic su **Password Manager** icona nel tuo browser web.

   Su Android o iOS, avvia il file **Password Manager** applicazione.
   Se richiesto, inserisci il tuo Password principale.

2. Apri il menu di Password Manager per espandere la barra laterale sinistra e seleziona la voce **Identità**.
3. Premi il pulsante **Aggiungi identità** in fondo.
4. Completa le informazioni che desideri vengano memorizzate e premi **Salva**.

Gestione delle carte di credito

Questa funzionalità ti consente di salvare e compilare i dati delle carte di credito per un'esperienza di acquisto più facile, veloce e sicura.

Per aggiungere una carta di credito a Password Manager:

1. Su Windows o macOS, fai clic su **Password Manager** icona nel tuo browser web.

   Su Android o iOS, avvia il file **Password Manager** applicazione.
   Se richiesto, inserisci il tuo Password principale.

2. Apri il menu di Password Manager per espandere la barra laterale sinistra e seleziona la voce **Carte di credito**.
3. Premere sul **Aggiungi identità** pulsante in basso.

4. Completare i dettagli che si desidera memorizzare, quindi premere **Salva**.

Proteggimi

La funzionalità Proteggimi ti consente di disconnettersi da remoto o eliminare la cronologia di navigazione di computer, tablet o dispositivi mobili. Se stai condividendo un dispositivo con altre persone, ti consigliamo vivamente di attivare questa funzionalità.

Per localizzare e attivare questa funzionalità:

1. Su Windows o macOS, fai clic su **Password Manager** icona nel tuo browser web.

   Su Android o iOS, avvia il file **Password Manager** applicazione.
   Se richiesto, inserisci il tuo Password principale.

2. Apri il menu di Password Manager per espandere la barra laterale sinistra e seleziona la voce **Proteggimi**.

3. Premi il pulsante **Proteggi tutte le sessioni**.
   Sei stai cercando di proteggere solo un dispositivo in particolare, individualo nell'elenco dei dispositivi su cui è stato installato o attivato su un determinato browser Password Manager.

Note

Secure Notes è una funzionalità che agisce come un taccuino segreto in cui puoi memorizzare dati sensibili, ordinarli e usare una codifica a colori per visualizzarli meglio. Non solo manterrà tutte le informazioni in ordine, ma anche al sicuro.

Per individuare e abilitare questa funzione:

1. Su Windows o macOS, fai clic su **Gestore di password** icona nel tuo browser web.

   Su Android o iOS, avvia il file **Gestore di password** applicazione.
   Se richiesto, inserisci il tuo Password principale.

2. Apri il menu di Password Manager per espandere la barra laterale sinistra e seleziona la voce **Note**.

3. Premi il pulsante **Aggiungi nota**.

Una volta indicate tutte le informazioni che vuoi conservare, premi **Salva**.

8.5. Domande frequenti

Alcune domande comuni su Bitdefender Password Manager tendono a ripetersi. Noi abbiamo le risposte! Qui potrai scoprire maggiori dettagli sul tuo account Bitdefender, su come importare le password, sui protocolli di sicurezza dei dati e altri argomenti importanti per i nostri clienti.

Domande generali su Bitdefender Password Manager

Come posso bloccare la finestra pop-up di Password Manager nella mia soluzione di sicurezza Bitdefender?

La notifica di Password Manager mostrata da Bitdefender Total Security, Internet Security e Antivirus Plus ad agosto 2022 può essere eliminata selezionando il pulsante "x". La finestra "Gestisci le tue password con Bitdefender Password Manager" comparirà un paio di volte prima di scomparire del tutto. Puoi interrompere questo messaggio promozionale disattivando le **Notifiche di suggerimento** nelle Impostazioni di Bitdefender.

Cosa succede alla scadenza di Bitdefender Password Manager?

Una volta scaduto l'abbonamento a Password Manager, avrai un massimo di 90 giorni per esportare le tue password. Verrà eseguito il backup delle tue password per altri 30 giorni. Durante questi 90 giorni, potrai solo esportare i tuoi dati. Non potrai continuare a usare Password Manager. La funzionalità di compilazione automatica smetterà di funzionare, così come la possibilità di generare password.

Al termine del periodo di proroga di 90 giorni, avrai altri 30 giorni per contattare il supporto di Bitdefender e richiedere di ripristinare le tue password nel database live. Successivamente, potrai esportarle da Bitdefender Password Manager.

I tuoi dati saranno conservati nel database live solo fino alla fine del giorno in cui sono stati ripristinati su richiesta. Alla mezzanotte, il database sarà eliminato e, se non avrai ancora superato il periodo aggiuntivo di 30 giorni, le password potranno essere nuovamente ripristinate dal backup. I dati grezzi del database dal backup possono essere forniti su richiesta all'utente, ma il database è cifrato e le informazioni non sono accessibili.

Cos'è la password principale e perché devo ricordarmela?

La password principale è la chiave che apre la porta a tutte le password memorizzate nel tuo account di Bitdefender Password Manager. La password principale deve avere almeno 8 caratteri. Quindi crea una password principale sicura, memorizzala e non condividerla mai con nessuno. Per creare una password principale sicura, ti consigliamo di usare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

Come posso indicare a Bitdefender di non chiedermi più la mia password principale ogni volta che apro il browser?

Se blocchi il tuo dispositivo senza chiudere il browser, Password Manager non si chiuderà e potrai accedere ai tuoi dati quando tornerai. Come misura di sicurezza, ogni volta che apri il browser dovrai accedere al tuo account di Bitdefender Central e poi inserire la tua password principale.

- Per bloccare la richiesta di accesso di Central, vai in Impostazioni e seleziona "Disattiva la scheda di accesso all'avvio".
- Per bloccare la richiesta della password principale, seleziona la casella "Ricordami" nella schermata Sblocca il tuo vault.

Perché non memorizzate la mia password principale e cosa succede se me la dimentico?

Il motivo per cui non memorizziamo la tua password principale sui nostri server è per essere certi che solo tu possa accedere al tuo account. È il modo più sicuro. Se Bitdefender Password Manager non riconosce la tua password principale, assicurati di digitarla correttamente e che il tasto Blocca maiuscole non sia attivo sulla tastiera.

Se hai dimenticato la password principale, puoi sempre usare il codice di recupero per sbloccare Password Manager. Durante la fase di registrazione, Bitdefender Password Manager ti fornisce un {1}codice di recupero{2} che può essere usato per riottenere l'accesso al tuo account senza perdere i tuoi dati.

Se hai dimenticato o smarrito sia la password principale che il codice di recupero, come ultima possibilità, contatta un responsabile di Bitdefender per reimpostare il tuo account.

> **Importante**
> Reimpostare il tuo account eliminerà tutte le tue password e i tuoi dati salvati in Bitdefender Password Manager.

È possibile per più utenti condividere un abbonamento a Bitdefender Password Manager?

Per ora, non è possibile avere più utenti con lo stesso abbonamento di Password Manager, ma stiamo lavorando per attivare questa funzionalità in un prossimo futuro.

Cos'è la modalità offline e come funziona?

La modalità offline viene attivata automaticamente quando cade la connessione Internet mentre si usa Bitdefender Password Manager. Se hai già effettuato l'accesso e hai inserito la tua password principale, la modalità offline ti consente di accedere alle tue password quando non è possibile utilizzare una connessione a Internet.

Come disinstallo Bitdefender Password Manager?

Per disinstallare Bitdefender Password Manager:

- Su Windows e macOS:
  Rimuovi l'estensione di Password Manager dal tuo browser web. Clicca con il pulsante destro sull'icona di Bitdefender e seleziona "Rimuovi".
- Su Android:
  Tocca e tieni premuto la app Password Manager, poi trascinala nella parte superiore dello schermo dove dice "Disinstalla".
- Su iOS e iPadOS:
  Tocca e tieni premuto la app Password Manager finché tutte le app sul tuo schermo iniziano a vibrare, poi tocca la X nell'angolo in alto a sinistra dell'icona di Bitdefender.

Domande su privacy e sicurezza su Bitdefender Password Manager

I dipendenti di Bitdefender possono visualizzare le mie password?

Assolutamente no. La tua privacy è la nostra massima priorità. Questo è il motivo principale per cui non memorizziamo la tua password principale sui nostri server per i dati: in modo che nessuno abbia accesso al tuo account, nemmeno i dipendenti dell'azienda. Ogni password e account sono altamente cifrati con gli algoritmi di sicurezza dei dati più potenti e il codice che vediamo appare come una semplice stringa casuale di numeri e lettere mescolati tra loro.

Cosa succede se i server di Password Manager vengono violati?

Ogni password è cifrata a livello locale sul tuo dispositivo prima che si avvicini ai nostri server, così se degli hacker entrassero nel nostro sistema, riceverebbero solo pagine di lettere e numeri casuali senza il tuo codice per decifrarli. Ciò significa che sia tu che i dettagli del tuo account sarete sempre al sicuro con noi.

9. PROTEZIONE DELL'IDENTITÀ DIGITALE

9.1. Cos'è Bitdefender Password Manager

Oggigiorno la sicurezza e la privacy online sono solo alcuni degli obiettivi principali degli utenti di Internet. E ci sono alcune ottime ragioni. Con gravi violazioni dei dati che si verificano il più delle volte, è assolutamente fondamentale assicurarsi che le tue informazioni di identificazione personale (PII) sia al sicuro e protette.

Ma cosa può essere classificato come informazione di identificazione personale? Tradizionalmente, informazioni sensibili come il nome completo, il codice fiscale, il numero della patente, l'indirizzo e-mail o i dati della carta di credito erano considerate PII. In seguito, anche informazioni meno sensibili, come i codici postali, gli indirizzi IP o gli ID di accesso sono state incluse in questa categoria. Col tempo, la tua traccia digitale, ovvero i dati che ti lasci alle spalle come risultato della tua navigazione Internet, potrebbe arrivare a includere alcuni di questi dati.

Bitdefender Password Manager rappresenta una vita privata per la libertà online, consentendoti di riottenere il controllo della tua vita digitale. E richiede solo il tuo nome, l'indirizzo e-mail più usato e il tuo numero di telefono. In base a questi dati, cerca sia sul web ufficiale che sul dark web le informazioni personali che sono state esposte pubblicamente.

Bitdefender Password Manager offre i seguenti:

- **Servizi di monitoraggio e rilevamento:** monitora più di 100 informazioni di identificazione personale come codici fiscali, numeri di carta di credito o indirizzi domestici, e mostra tutti i dati trovati sulla tua traccia online.

  > **Nota**
  > Bitdefender non memorizza o elabora informazioni di identificazione personale. Vengono conservati solo i riferimenti di potenziali violazioni dei dati senza includere dati sensibili.

- **Allerte in tempo reale:** ricevi notifiche su violazioni dei dati e dati esposti nel dark web, informazioni personali nel web ufficiale e potenziali impersonificatori sui social media.
- **Soluzioni:** i nostri servizi suggeriscono azioni chiare necessarie per risolvere i problemi e forniscono promemoria se un problema non

viene risolto completamente. Possono fornire anche istruzioni su come rimuovere annunci personalizzati, esportare i tuoi dati o disattivare la tracciatura.

9.2. Come iniziare

9.2.1. Attivare Digital Identity Protection

Attiva l'abbonamento a Bitdefender Digital Identity Protection una volta effettuato e pagato il tuo ordine.

1. Apri l'e-mail di conferma ricevuta subito dopo aver completato il tuo ordine e clicca su **COME INIZIARE**.
2. Passerai alla pagina https://central.bitdefender.com.
   Accedi con il tuo account di Bitdefender Central. Se non ne hai uno, scegli di crearlo.
3. Dopo aver effettuato l'accesso, l'abbonamento sarà collegato automaticamente al tuo account di Central e inizierà la fase di introduzione.

In alternativa:

- accedi al pannello **I miei abbonamenti** da Central, localizzato sul lato sinistro della finestra e clicca su **+ Attiva con codice**.
- digita il codice a 10 cifre trovato nell'e-mail di conferma e premi **ATTIVA**.
- se richiesto, seleziona come usare il codice e clicca su **ATTIVA**.

9.2.2. Configurare Digital Identity Protection

1. Vai in https://central.bitdefender.com/ e accedi al tuo account.
   Se non hai già un account, seleziona **CREA ACCOUNT** e inserisci il tuo nome completo, un indirizzo e-mail e una password.
2. Seleziona il pannello Digital Identity Protection.
   Comparirà una schermata di benvenuto.
3. Clicca su **INIZIA**.
4. Ora ti saranno illustrate le informazioni che devi fornire. I tuoi dati saranno sempre cifrati e protetti.
   Clicca su **AVANTI**.

5. Inserisci il tuo nome, secondo nome (se ne hai uno) e cognome negli spazi corrispondenti, poi clicca su **AVANTI**.
6. Inserisci il tuo indirizzo e-mail e clicca su **AVANTI**.
   Assicurati che sia un indirizzo e-mail valido a cui puoi accedere.
7. Un codice di sicurezza viene inviato all'indirizzo che hai fornito.
   Apri il messaggio, copia il codice e incollalo nello spazio corrispondente.
   Poi, clicca su **VERIFICA**.
8. Seleziona il paese e inserisci il tuo numero di telefono, poi clicca su **AVANTI**.
9. Poco dopo dovresti ricevere un codice di sicurezza.
   Inserisci il codice e seleziona **VERIFICA**.
10 Una volta eseguita la verifica iniziale, clicca su **TERMINA**.
.

> **Nota**
> Riceverai una notifica se durante il primo controllo venisse rilevata una qualsiasi vuolazione, oltre a informazioni di identificazione personale o potenziali impersonificazioni.

Ora Bitdefender Password Manager è stato configurato.

9.2.3. Controllare la tua traccia digitale, le violazioni dei dati e le possibili impersonificazioni

Una volta completata la configurazione, Bitdefender Password Manager esegue una verifica online per scoprire potenziali impersonificazioni, violazioni dei dati e informazioni di identificazione personale sull'open web. Ti consigliamo di verificare ogni singola informazione inclusa nelle schede **TRACCIA DIGITALE**, **VIOLAZIONI DEI DATI** e **CONTROLLO D'IMPERSONIFICAZIONE**.

- Verificare la tua traccia digitale (pagina 283)
- Verificare le violazioni dei dati (pagina 284)
- Verificare le impersonificazioni possibili (pagina 285)

9.2.4. Migliora il tuo controllo

Usiamo i dati che ci fornisci per monitorare il web superficiale e il Dark web per rilevare qualsiasi attività che possa influenzare la tua privacy o la reputazione del tuo brand personale.

Se vuoi aggiungere un altro indirizzo e-mail o numero di telefono, clicca su ⊕, poi clicca su **AGGIUNGI INDIRIZZO E-MAIL ADDRESS** o **AGGIUNGI NUMERO DI TELEFONO**, e segui le istruzioni.

9.3. Dashboard

La dashboard riunisce le informazioni incluse nelle sezioni **TRACCIA DIGITALE**, **VIOLAZIONI DEI DATI** e **CONTROLLO D'IMPERSONIFICAZIONE**.

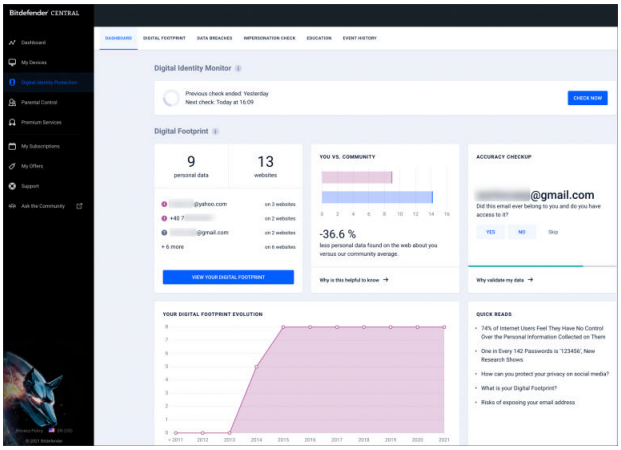
Include le seguenti:

- I tuoi dati esposti e le loro fonti web
- L'ammontare medio di dati esposti per l'intera community
- L'evoluzione della tua traccia digitale
- Contenuti relativi alla privacy
- Violazioni di dati
- Il numero medio di violazioni dei dati nella community

9.3.1. Monitoraggio identità digitale

Utilizzando solo informazioni accurate, il sistema di Bitdefender cerca nuovi dati personali esposti sull'Open Web e il Dark Web, ed esamina tutte le principali piattaforme dei social media per cercare qualsiasi segno di un tentativo di impersonificazione.

Clicca su **CONTROLLA ORA** per eseguire una scansione online.



9.4. Traccia digitale

Le tue informazioni di identificazione personale e le loro fonti compaiono qui. Sta a te valutare se avere tali informazioni a livello pubblico sul web rappresenti o no una minaccia.

Il nostro monitoraggio guidato dall'IA fa molto affidamento sui dati corretti per rilevare nuove minacce, perciò indicaci se le informazioni sono corrette o poco precise.

Una volta confermato che una parte delle informazioni sono tue, le aggiungiamo al nostro sistema di monitoraggio, migliorando le probabilità di scoprirne altre in futuro.

9.4.1. Verificare la tua traccia digitale

Per rivedere la tua traccia digitale:

1. Vai alla scheda **TRACCIA DIGITALE**.
2. Le informazioni non ancora verificate compariranno con la dicitura **Verifica** sul lato destro. Clicca su **Verifica** e seleziona Sì o No, a seconda dei casi.

> **Nota**
> Ogni parte di informazione confermata viene aggiunta al nostro algoritmo di monitoraggio, migliorando i risultati mostrati dai nostri servizi. Le informazioni scartate non saranno più visualizzate. Ma, resteranno comunque disponibili sul web.

9.5. Violazioni dei dati

Le violazioni si verificano quando gli hacker riescono a bypassare le misure di sicurezza di una società e ottengono le tue informazioni personali per venderle sul dark web. In genere, i criminali informatici puntano a dati d'accesso, informazioni di identificazione personale (PII), cartelle cliniche e dati bancari.

Qualsiasi organizzazione o servizio può cadere vittima di una violazione dei dati, ma quelli con un'ampia base di utenti sono bersagli sicuramente più interessanti. Le violazioni incluse normalmente sono nomi, indirizzi e-mail, nomi utente, password, indirizzi postali, numeri di telefono, codici fiscali e dati delle carte di credito (numero, data di scadenza, codice CVV).

9.5.1. Verificare le violazioni dei dati

Per verificare le tue violazioni dei dati:

1. Vai alla scheda **VIOLAZIONI DEI DATI**.
2. Sotto alcune voci, troverai un elenco di azioni necessarie per proteggere il tuo account. Dopo aver eseguito un'azione, clicca sulla casella accanto a essa per confermarla.
   Se non hai la certezza su come eseguire un'attività, puoi sempre cliccare sul link incluso nella descrizione dell'attività e arriverai a una pagina dove troverai tutti i passaggi necessari.
   Non tutte le violazioni possono essere affrontate in questo modo. Alcune, come **Raccolta #1** non includeranno passaggi. Invece, arriverai ad alcuni articoli disponibili online, dove trovera maggiori aiuto.

   Nota
   Bitdefender non memorizza o elabora informazioni di identificazione personale. Vengono mantenuti solo i riferimenti a potenziali violazioni dei dati, senza includere i dati sensibili.

9.6. Controllo impersonificazione

I criminali noti come "impersonificatori" usano l'arte dell'impersonificazione in molti modi, vestendo i panni di un individuo fidato per ingannare le proprie vittime e ottenere accesso a dati sensibili. La pratica del "pretesto" viene definita come presentare sé stessi come

qualcun altro per ingannare un destinatario nel fornire dati sensibili come password, numeri di carta di credito o altre informazioni sensibili.

Bitdefender Password Manager monitora 25 piattaforme social e ti avvisa subito se trovasse un profilo che potrebbe essere un tentativo di impersonificazione.

9.6.1. Verificare le impersonificazioni possibili

La scheda **CONTROLLO D'IMPERSONIFICAZIONE** è dove saranno mostrati tutti i possibili tentativi. Per ogni rilevamento, puoi scegliere una delle tre possibilità:

- È un tentativo di impersonificazione
- È il tuo profilo personale
- È un profilo differente

In base alla scelta, Bitdefender Password Manager suggerirà determinati passaggi suggeriti per affrontare il problema. Ogni volta che completi un passaggio, puoi marcarlo come **Fatto**.

9.7. Istruzione

La scheda Istruzione funziona come una knowledge base in cui l'utente può trovare più informazioni su come proteggere la sua identità digitale.

Gli articoli indicati qui possono essere ordinati in base a diverse categorie:

- Violazioni
- Esposizioni
- Controllo della rappresentazione

Per accedere alla versione completa di un articolo, clicca sul link **Leggi altro** corrispondente.

9.8. Cronologia evento

La sezione Cronologia degli eventi è il mezzo tramite cui comunichiamo costantemente con i nostri utenti. Rappresenta un elenco ordinato cronologicamente di eventi relativi alla protezione della tua traccia digitale.

Oltre alle minacce appena rilevate (nel caso esistessero), puoi tornare a questa pagina per suggerimenti preziosi su come comportarti

correttamente online per aumentare le tue probabilità di non incappare in problemi della privacy.

Nella sezione Cronologia degli eventi, puoi trovare le seguenti informazioni:

- Azioni eseguite
- Aggiornamenti del servizio
- Violazioni dei dati

10. OTTENERE AIUTO

10.1. Richiesta d'aiuto

Bitdefender offre ai suoi clienti un livello impareggiabile di supporto rapido e accurato. Se dovessi riscontrare un qualche problema o se avessi domande sul tuo prodotto Bitdefender, potrai usare diverse risorse online per trovare una soluzione o una risposta. Allo stesso tempo, potrai contattare il servizio clienti di Bitdefender. I nostri responsabili del supporto risponderanno alle tue domande in maniera tempestiva e ti forniranno tutto l'aiuto necessario.

10.2. Risorse online

Sono disponibili diverse risorse online per aiutarti a risolvere i tuoi problemi e le tue domande relative a Bitdefender.

- Centro di supporto di Bitdefender:
  https://www.bitdefender.it/consumer/support/
- La community di esperti di Bitdefender:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Puoi anche usare il tuo motore di ricerca preferito per trovare più informazioni sulla sicurezza del computer, i prodotti Bitdefender e la società.

10.2.1. Centro di supporto di Bitdefender

Il Centro di supporto di Bitdefender è un archivio online di informazioni sui prodotti Bitdefender. Conserva, in un formato facilmente accessibile, le notifiche sui risultati delle attività di risoluzioni bug e problemi del supporto tecnico di Bitdefender e dei team di sviluppo, oltre ad articoli più generali sulla prevenzione delle minacce, la gestione delle soluzioni di Bitdefender con spiegazioni dettagliate e molti altri articoli.

Il Centro di supporto di Bitdefender è aperto al pubblico e gratuitamente esplorabile. Le ricche informazioni che contiene sono un altro modo per fornire ai clienti di Bitdefender le conoscenze tecnologiche e le

informazioni necessarie. Tutte le richieste di informazioni o i rapporti sui difetti, provenienti dai clienti di Bitdefender, prima o poi arrivano al Centro di supporto di Bitdefender, come rapporti di disinfezione, metodi per aggirare le truffe, o articoli informativi, per integrare i file di aiuto dei prodotti.

Il Centro assistenza di Bitdefender è disponibile in qualsiasi momento al seguente indirizzo: https://www.bitdefender.it/consumer/support/.

10.2.2. La community di esperti di Bitdefender

La community di esperti è un ambiente in cui gli utenti di Bitdefender, oltre a fan e appassionati, possono interagire, scambiare idee, supportarsi a vicenda e condividere le proprie conoscenze e soluzioni. È anche un luogo creativo e fornisce feedback preziosi ai nostri team di sviluppo. I membri della community sono utenti esperti di Bitdefender, felici di aiutare altri utenti nel proprio tempo libero. Grazie al loro immenso contributo e sforzi volontari, abbiamo creato una knowledge base dove gli utenti possono trovare risposte e aiuto, ma con un tocco più umano di una semplice risposta automatizzata.

Qui potrai trovare molte conversazioni utili con utenti che utilizzano Bitdefender sui propri dispositivi. La community offre una vera connessione con i nostri membri e fa sentire la loro voce. Ti invitiamo a parteciparvi sapendo che la tua opinione e le tue informazioni saranno rispettate e apprezzate. In qualità di fornitore stimato, ci sforziamo di offrire un livello senza precedenti di supporto sempre rapido e preciso, sperando di avvicinare sempre più i nostri utenti. Abbiamo progettato la nostra community con questo obiettivo sempre in mente.

Puoi trovare la pagina web della nostra community di esperti qui:

https://community.bitdefender.com/en/

10.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia include tutte le informazioni necessarie sulle minacce informatiche più recenti. È anche dove gli esperti Bitdefender condividono trucchi e suggerimenti su come restare protetti da hacker, violazioni, furti d'identità e tentativi d'impersonificazione dei social.

La pagina web di Bitdefender Cyberpedia è disponibile qui:

https://www.bitdefender.com/cyberpedia/.

10.3. Informazioni di contatto

Una comunicazione efficiente è la chiave per un business di successo. Dal 2001 BITDEFENDER ha stabilito una reputazione indiscutibile impegnandosi costantemente per una migliore comunicazione in modo da superare le aspettative dei nostri clienti e partner. In caso di domande, non esitate a contattarci direttamente tramite il ns Centro di supporto di Bitdefender (pagina 287).

https://www.bitdefender.it/consumer/support/

10.3.1. Distributori locali

I distributori locali di Bitdefender sono pronti a rispondere a ogni richiesta inerente le loro zone operative, sia in ambito commerciale sia generale.

Per trovare un distributore di Bitdefender nel tuo paese:

1. Vai a https://www.bitdefender.com/partners/partner-locator.html.
2. Seleziona il tuo paese e la tua città, utilizzando le opzioni corrispondenti.

GLOSSARIO

Codice di attivazione

È una chiave unica che può essere acquistata dal rivenditore e usata per attivare un servizio o un prodotto specifico. Un codice di attivazione consente l'attivazione di un abbonamento valido per un determinato periodo di tempo e un certo numero di dispositivi. Inoltre, può anche essere utilizzato per estendere un abbonamento, a condizione che venga generato per lo stesso prodotto o servizio.

ActiveX

ActiveX è un modello per la scrittura di programmi in modo che altri programmi e il sistema operativo possano chiamarli. La tecnologia ActiveX viene utilizzata con Microsoft Internet Explorer per creare pagine Web interattive che sembrano e si comportano come programmi per computer, piuttosto che come pagine statiche. Con ActiveX, gli utenti possono porre o rispondere a domande, utilizzare pulsanti e interagire in altri modi con la pagina web. I controlli ActiveX vengono spesso scritti utilizzando Visual Basic. Active X si distingue per una completa mancanza di controlli di sicurezza; gli esperti di sicurezza informatica ne scoraggiano l'uso su Internet.

Minaccia persistente avanzata

Advanced Persistent Threat (APT) sfrutta le vulnerabilità dei sistemi per rubare informazioni importanti per consegnarle alla fonte. Grandi gruppi come organizzazioni, aziende o governi sono presi di mira da questa minaccia. L'obiettivo di una minaccia persistente avanzata è rimanere inosservato per lungo tempo essendo in grado di monitorare e raccogliere informazioni importanti senza danneggiare le macchine mirate. Il metodo utilizzato per iniettare la minaccia nella rete è attraverso un file PDF o un documento di Office che sembra innocuo in modo che ogni utente possa eseguire i file.

Adware

L'adware è spesso combinato con un'app host fornita gratuitamente a condizione che l'utente accetti l'adware. Poiché le app adware vengono generalmente installate dopo che l'utente ha accettato un contratto di licenza che stabilisce lo scopo dell'app, non viene commesso alcun reato. Tuttavia, le pubblicità pop-up possono diventare fastidiose e in alcuni casi

degradare le prestazioni del sistema. Inoltre, le informazioni raccolte da alcune di queste app possono causare problemi di privacy per gli utenti che non erano pienamente a conoscenza dei termini del contratto di licenza.

Archivio

Un disco, un nastro o una cartella che contiene file memorizzati.

Un file che contiene uno o più file in un formato compresso.

Porta sul retro

Un buco nella sicurezza di un sistema deliberatamente lasciato in essere da progettisti o manutentori. La motivazione di tali buchi non è sempre sinistra; alcuni sistemi operativi, ad esempio, escono dalla confezione con account privilegiati destinati all'uso da parte dei tecnici dell'assistenza sul campo o dei programmatori di manutenzione del fornitore.

Settore di avvio

Un settore all'inizio di ogni disco che identifica l'architettura del disco (dimensione del settore, dimensione del cluster e così via). Per i dischi di avvio, il settore di avvio contiene anche un programma che carica il sistema operativo.

Avvio virus

Una minaccia che infetta il settore di avvio di un disco fisso o floppy. Un tentativo di avvio da un dischetto infettato da un virus del settore di avvio causerà l'attivazione della minaccia nella memoria. Ogni volta che avvierai il tuo sistema da quel momento in poi, avrai la minaccia attiva in memoria.

Botnet

Il termine “botnet” è composto dalle parole “robot” e “network”. Le botnet sono dispositivi connessi a Internet infettati da minacce e possono essere utilizzati per inviare e-mail di spam, rubare dati, controllare da remoto dispositivi vulnerabili o diffondere spyware, ransomware e altri tipi di minacce. Il loro obiettivo è quello di infettare il maggior numero possibile di dispositivi connessi, come PC, server, dispositivi mobili o IoT appartenenti a grandi aziende o industrie.

Navigatore

Abbreviazione di browser Web, un'app software utilizzata per individuare e visualizzare pagine Web. I browser più diffusi includono Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Questi sono browser

grafici, il che significa che possono visualizzare grafica e testo. Inoltre, la maggior parte dei browser moderni può presentare informazioni multimediali, inclusi audio e video, sebbene richiedano plug-in per alcuni formati.

Attacco di forza bruta

Attacco di indovinazione della password utilizzato per irrompere in un sistema informatico inserendo possibili combinazioni di password, per lo più a partire dalla password più facile da indovinare.

Riga di comando

In un'interfaccia a riga di comando, l'utente digita i comandi nello spazio fornito direttamente sullo schermo utilizzando il linguaggio dei comandi.

Biscotti

Nell'industria di Internet, i cookie sono descritti come piccoli file contenenti informazioni su singoli computer che possono essere analizzati e utilizzati dagli inserzionisti per tenere traccia dei tuoi interessi e gusti online. In questo ambito, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di indirizzare gli annunci direttamente a ciò che hai dichiarato di essere i tuoi interessi. È un'arma a doppio taglio per molte persone perché, da un lato, è efficiente e pertinente in quanto si vedono solo annunci su ciò che ti interessa. cosa clicchi. Comprensibilmente, c'è un dibattito sulla privacy e molte persone si sentono offese dall'idea di essere viste come un "numero SKU" (sai, il codice a barre sul retro dei pacchi che viene scansionato alla cassa della drogheria) . Sebbene questo punto di vista possa essere estremo, in alcuni casi è accurato.

Cyber bullismo

Quando coetanei o estranei commettono atti violenti contro i bambini apposta per ferirli fisicamente. Per danneggiare emotivamente, gli aggressori inviano messaggi meschini o foto poco lusinghiere, isolando così le loro vittime dagli altri o sentendosi frustrate.

Dizionario Attacco

Attacchi di indovinazione della password utilizzati per irrompere in un sistema informatico inserendo una combinazione di parole comuni per generare potenziali password. Lo stesso metodo viene utilizzato per indovinare le chiavi di decrittazione di messaggi o documenti crittografati.

Gli attacchi con dizionario hanno successo perché molte persone tendono a scegliere password brevi e con parole singole facili da indovinare.

Unità disco

È una macchina che legge e scrive dati su un disco. Un disco rigido legge e scrive dischi rigidi. Un'unità floppy accede ai dischi floppy. Le unità disco possono essere interne (alloggiate all'interno di un computer) o esterne (alloggiate in una scatola separata che si collega al computer).

Scaricamento

Per copiare i dati (di solito un intero file) da una fonte principale a un dispositivo periferico. Il termine è spesso usato per descrivere il processo di copia di un file da un servizio online al proprio computer. Il download può anche riferirsi alla copia di un file da un file server di rete a un computer in rete.

E-mail

Mail elettronica. Un servizio che invia messaggi sui computer tramite reti locali o globali.

Eventi

Un'azione o un evento rilevato da un programma. Gli eventi possono essere azioni dell'utente, come fare clic su un pulsante del mouse o premere un tasto, o occorrenze di sistema, come l'esaurimento della memoria.

Exploit

Un modo per sfruttare diversi bug o vulnerabilità presenti in un computer (software o hardware). Pertanto, gli hacker possono ottenere il controllo di computer o reti.

Falso positivo

Si verifica quando uno scanner identifica un file come infetto quando in realtà non lo è.

Estensione del nome file

La parte di un nome di file, dopo il punto finale, che indica il tipo di dati memorizzati nel file. Molti sistemi operativi utilizzano estensioni di file, ad esempio Unix, VMS e MS-DOS. Di solito sono da una a tre lettere (alcuni tristi vecchi sistemi operativi non supportano più di tre). Gli esempi includono "c" per codice sorgente C, "ps" per PostScript, "txt" per testo arbitrario.

Euristico

Un metodo basato su regole per identificare nuove minacce. Questo metodo di scansione non si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione euristica è che non viene ingannata da una nuova variante di una minaccia esistente. Tuttavia, potrebbe occasionalmente segnalare codice sospetto nei normali programmi, generando il cosiddetto "falso positivo".

Vaso di miele

Un sistema informatico esca impostato per attirare gli hacker per studiare il modo in cui agiscono e identificare i metodi eretici che utilizzano per raccogliere informazioni di sistema. Le aziende e le aziende sono più interessate a implementare e utilizzare gli honeypot per migliorare il proprio stato di sicurezza generale.

IP

Protocollo Internet - Un protocollo instradabile nella suite di protocolli TCP/IP responsabile dell'indirizzamento IP, del routing e della frammentazione e riassemblaggio dei pacchetti IP.

Applet Java

Un programma Java progettato per essere eseguito solo su una pagina Web. Per utilizzare un'applet su una pagina Web, devi specificare il nome dell'applet e la dimensione (lunghezza e larghezza, in pixel) che l'applet può utilizzare. Quando si accede alla pagina Web, il browser scarica l'applet da un server e la esegue sulla macchina dell'utente (il client). Le applet differiscono dalle app in quanto sono governate da un rigido protocollo di sicurezza.

Ad esempio, anche se le applet vengono eseguite sul client, non possono leggere o scrivere dati sulla macchina del client. Inoltre, le applet sono ulteriormente limitate in modo che possano solo leggere e scrivere dati dallo stesso dominio da cui sono servite.

Registratore di tasti

Un keylogger è un'app che registra tutto ciò che digiti. I keylogger non sono di natura dannosa. Possono essere utilizzati per scopi legittimi, come il monitoraggio dell'attività dei dipendenti o dei bambini. Tuttavia, vengono sempre più utilizzati dai criminali informatici per scopi dannosi (ad esempio, per raccogliere dati privati, come credenziali di accesso e numeri di previdenza sociale).

Virus a macroistruzione

Un tipo di minaccia informatica codificata come macro incorporata in un documento. Molte app, come Microsoft Word ed Excel, supportano potenti linguaggi macro. Queste app ti consentono di incorporare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Cliente di posta

Un client di posta elettronica è un'app che consente di inviare e ricevere e-mail.

Memoria

Aree di archiviazione interne nel computer. Il termine memoria identifica l'archiviazione dei dati sotto forma di chip e la parola archiviazione viene utilizzata per la memoria che esiste su nastri o dischi. Ogni computer viene fornito con una certa quantità di memoria fisica, solitamente indicata come memoria principale o RAM.

Non euristico

Questo metodo di scansione si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione non euristica è che non si lascia ingannare da quella che potrebbe sembrare una minaccia e non genera falsi allarmi.

Predatori online

Individui che cercano di attirare minori o adolescenti in conversazioni apposta per coinvolgerli in attività sessuali illegali. I social network sono il luogo ideale in cui i bambini vulnerabili possono essere facilmente cacciati e indotti a commettere attività sessuali, online o faccia a faccia.

Programmi confezionati

Un file in un formato di compressione. Molti sistemi operativi e app contengono comandi che consentono di comprimere un file in modo che occupi meno memoria. Ad esempio, supponi di avere un file di testo contenente dieci caratteri spazio consecutivi. Normalmente, ciò richiederebbe dieci byte di archiviazione.

Tuttavia, un programma che comprime i file sostituirà i caratteri di spazio con uno speciale carattere di serie di spazi seguito dal numero di spazi da sostituire. In questo caso, i dieci spazi richiederebbero solo due byte. Questa è solo una delle tecniche di confezionamento, ce ne sono molte altre.

Sentiero

Le indicazioni esatte per un file su un computer. Queste direzioni sono solitamente descritte per mezzo del sistema di archiviazione gerarchico dall'alto verso il basso.

Il percorso tra due punti qualsiasi, ad esempio il canale di comunicazione tra due computer.

Phishing

L'atto di inviare un'e-mail a un utente che afferma falsamente di essere un'impresa legittima e consolidata nel tentativo di indurre l'utente a cedere informazioni private che verranno utilizzate per il furto di identità. L'e-mail indirizza l'utente a visitare un sito Web in cui viene chiesto di aggiornare le informazioni personali, come password e numeri di carta di credito, previdenza sociale e conto bancario, che l'organizzazione legittima già possiede. Il sito Web, tuttavia, è fasullo e impostato solo per rubare le informazioni dell'utente.

Fotone

Photon è una tecnologia di Bitdefender innovativa e discreta, progettata per minimizzare l'impatto della tua soluzione di sicurezza sulle prestazioni del sistema. Monitorando in background l'attività del PC, crea degli schemi di utilizzo, per ottimizzare i processi di avvio e scansione.

Virus polimorfo

Una minaccia che modifica la propria forma con ogni file che infetta. Non avendo caratteristiche binarie costanti, queste minacce sono difficili da identificare.

Porta

Un'interfaccia su un computer alla quale puoi connettere un supporto. I PC hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, schermi e tastiere. Esternamente hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

Nelle reti TCP/IP e UDP, un endpoint per una connessione logica. Il numero della porta identifica di che tipo di porta si tratta. Ad esempio, la porta 80 viene usata per il traffico HTTP.

Ransomware

Un ransomware è un programma dannoso che prova a sottrarre illecitamente denaro agli utenti bloccando i loro sistemi vulnerabili.

CryptoLocker, CryptoWall e TeslaWall sono solo alcune delle varianti che cercano di bloccare i sistemi personali degli utenti.

L'infezione può partire, aprendo e-mail di spam, scaricando gli allegati di un messaggio o installando determinate applicazioni, il tutto lasciando l'utente ignaro di ciò che sta accadendo sul suo sistema. Gli autori di ransomware puntano a colpire soprattutto gli utenti normali e le aziende.

File di rapporto

File che elenca le azioni avvenute. Bitdefender mantiene un file di rapporto che elenca i percorsi esaminati, le cartelle, il numero di archivi e i file esaminati, oltre a quanti file infetti e sospetti sono stati trovati.

Rootkit

Un rootkit è una serie di strumenti software che offre accesso a livello di amministratore a un sistema. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la propria presenza in modo da non dover essere visti dai veri amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, i login e i log. Possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche, se incorporano il software adeguato.

I rootkit non sono dannosi per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando i rootkit. Comunque, vengono principalmente utilizzati per nascondere minacce o per celare la presenza di un intruso nel sistema. Se combinati alle minacce, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e registri, ed evitare il rilevamento.

Script

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Spam

Messaggi di posta elettronica o newsgroup indesiderati. Generalmente conosciuti come e-mail non desiderate.

Spyware

Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessione a Internet, senza che questo se ne accorga, di solito per scopi pubblicitari. Le applicazioni spyware in genere sono incluse come componente nascosta di programmi freeware o shareware, che possono essere scaricati da Internet. Tuttavia, occorre segnalare che la maggioranza delle applicazioni shareware o freeware non includono alcun programma spyware. Una volta installato, uno spyware monitora le attività dell'utente su Internet e trasmette di nascosto tali informazioni a qualcun altro. Gli spyware possono anche raccogliere informazioni su indirizzi e-mail o addirittura password e numeri di carta di credito.

Gli spyware sono simili a un Trojan che gli utenti installano inconsapevolmente installando altre applicazioni. Un modo comune per diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli spyware utilizzano memoria e risorse del sistema, le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

Articoli di avvio

Qualsiasi file posizionato in questa cartella si aprirà all'avvio del computer. Ad esempio, una schermata di avvio, un file audio da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure app che possono essere elementi di avvio. Normalmente in questa cartella viene posizionato un alias di un file, al posto del file stesso.

Abbonamento

Un accordo di acquisto che offre all'utente il diritto di utilizzare un particolare prodotto o servizio su un numero specifico di dispositivi e per un certo periodo di tempo. Un abbonamento scaduto può essere rinnovato automaticamente, utilizzando le informazioni fornite dall'utente con il primo acquisto.

Area di notifica

Introdotta con Windows 95, la barra degli strumenti è situata nella barra delle applicazioni di Windows (in genere in basso vicino all'orologio) e contiene icone miniaturizzate per un accesso veloce a funzioni di sistema come fax, stampante, modem, volume e molto altro. Clicca due volte o

clicca con il pulsante destro su un'icona per visualizzare e accedere a dettagli e controlli.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di rete largamente utilizzati su Internet, che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il relativo traffico.

Minaccia

Un programma o parte di codice caricato sul computer a propria insaputa e che viene eseguito contro la propria volontà. La maggior parte delle minacce è anche in grado di auto replicarsi. Tutte le minacce informatiche sono state create dall'uomo. È relativamente facile produrre una semplice minaccia in grado di copiare sé stessa innumerevoli volte. Persino una minaccia così semplice è pericolosa in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di minaccia ancora più pericolosa è quella in grado di trasmettere sé stessa attraverso le reti superando i sistemi di sicurezza.

Aggiornamento delle informazioni sulle minacce

Lo schema binario di una minaccia, usato dalla soluzione di sicurezza per rilevare ed eliminare la minaccia.

Troiano

Un programma distruttivo che si maschera da applicazione benevola. A differenza di programmi software dannosi e worm, i trojan non si replicano ma possono essere altrettanto distruttivi. Un tipo di minaccia Trojan particolarmente insidiosa è un programma che dichiara di pulire le minacce dal computer, ma al contrario le introduce.

Il termine deriva dalla storia dell'Iliade di Omero, dove i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, durante la notte, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

Aggiornamento

Una nuova versione di un prodotto software o hardware creato per sostituire una versione precedente dello stesso prodotto. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul computer; diversamente non sarà possibile installare l'aggiornamento.

Bitdefender dispone della propria funzionalità di aggiornamento, che consente la verifica manuale degli aggiornamenti, oppure l'aggiornamento automatico del prodotto.

Virtual Private Network (VPN)

È una tecnologia che consente una connessione diretta temporanea e cifrata a una determinata rete su una rete meno sicura. In questo modo, la ricezione e l'invio dei dati sono sempre sicuri e cifrati, ma soprattutto più difficili da intercettare dai pirati informatici. Una prova di sicurezza è l'autenticazione, che può essere fatta solo usando un nome utente e una password.

Verme

Programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.