MANUALE D'USO

Bitdefender Antivirus Free
Manuale d'uso

Data di pubblicazione 27/04/2022

Avvertenze legali

Bitdefender

Indice

INSTALLAZIONE

1. PREPARARSI ALL'INSTALLAZIONE

Prima di installare Bitdefender Antivirus Free, 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*» (p. 3).
- Accedere al dispositivo utilizzando un account Amministratore.
- Rimuovi qualsiasi altro programma simile dal dispositivo. Se dovesse rilevarne una durante l'installazione di Bitdefender, ti sarà chiesto di disinstallarla. 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.

2. REQUISITI DI SISTEMA

Puoi installare Bitdefender Antivirus Free solo su dispositivo con i seguenti sistemi operativi:

- Windows 7 con Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

- 2,5 GB di spazio disponibile su disco rigido (almeno 800 MB sull'unità di sistema)
- 2 GB di memoria (RAM)
- An active internet connection

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 su **Computer** nel desktop e poi seleziona **Proprietà** nel menu.
- In **Windows 8**, dal menu Start di Windows, localizza l'opzione **Computer** (per esempio, puoi 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 attività e clicca sulla sua icona. Individua la sezione **Sistema** per trovare maggiori informazioni sul tuo sistema.

2.1. 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 11 e superiore
- Mozilla Firefox 51 e superiore
- Google Chrome 34 e superiore

3. INSTALLARE IL TUO PRODOTTO BITDEFENDER

You can install Bitdefenderusing the web installer downloaded on your device from the Bitdefender Antivirus Free page on Bitdefender Website.

3.1. Install from Bitdefender Website

From Bitdefender Website you can download the Bitdefender Antivirus Free installation kit. Once the installation process is complete, Bitdefender Antivirus Free is activated.

To download Bitdefender Antivirus Free from Bitdefender Website:

1. Access https://www.bitdefender.com/toolbox/ .
2. Click download on Bitdefender Antivirus Free.
3. Attendi il completamento del download e poi esegui il programma d'installazione.

Convalidare l'installazione

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

Se il tuo sistema non soddisfa i requisiti di sistema per installare Bitdefender, sarai informato delle aree 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 Antivirus Free è aggiornato costantemente.

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

Una volta convalidata l'installazione, comparirà la relativa procedura guidata. Segui tutti i passaggi per installare Bitdefender Antivirus Free.

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 utilizzare Bitdefender Antivirus Free.

Se non accetti questi 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, scegliere se desideri essere informato oppure no del termine della scansione.

Una volta completata la scansione, clicca su **Crea account di Bitdefender**.

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

Fase 5 - Account Bitdefender

Dopo aver completato la configurazione iniziale, comparirà la finestra Account di Bitdefender. Per attivare il prodotto e utilizzare le sue funzioni online, è necessario avere un account Bitdefender. Per maggiori informazioni, fai riferimento a «*Bitdefender Central*» (p. 21).

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 di Bitdefender**

  1. Fare clic 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. Inserisci la nuova password che vuoi impostare e ridigitala ancora una volta. Clicca su **SALVA**.

   Nota
   Se hai già un account MyBitdefender, puoi usarlo per accedere al tuo account Bitdefender. Se hai dimenticato la password, prima devi andare su https://my.bitdefender.com per ripristinarla. 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.

If you already have an active subscription on your account, that subscription will be used to protect your device.

If you do not have an active subscription, your Bitdefender Antivirus Free will be activated. You can also opt-in for a 30 days Bitdefender Total Security trial.

Fase 7 - Come iniziare

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

Clicca su **FINE** per accedere all'interfaccia di Bitdefender Antivirus Free.

3.2. Installare su altre soluzioni di sicurezza

Avere più soluzioni di sicurezza sul dispositivo può causare alcuni malfunzionamenti del sistema, come rallentamenti o blocchi.

Per assicurarti che il tuo dispositivo non abbia più soluzioni di sicurezza installate, nella fase di installazione di Bitdefender Antivirus Free ti guideremo attraverso la disinstallazione delle soluzioni di sicurezza esistenti rilevate.

INIZIARE

4. INTERFACCIA DI BITDEFENDER

Bitdefender Antivirus Free soddisfa le necessità di persone esperte e di principianti. L'interfaccia grafica dell'utente 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.

L'icona nell'area di notifica di Bitdefender è sempre disponibile, non importa se si desidera aprire la finestra principale, eseguire un aggiornamento del prodotto o visualizzare informazioni sulla versione installata.

La finestra principale ti fornisce informazioni sul tuo stato di sicurezza. In base all'uso e alle esigenze del tuo dispositivo, Autopilot qui mostrerà diversi tipi di suggerimento per aiutarti a migliorare la sicurezza e le prestazioni del tuo dispositivo. Inoltre, puoi aggiungere azioni veloci che usi più spesso, così da averle sempre a portata di mano ogni volta che ti servono.

Dal menu di navigazione sul lato sinistro puoi accedere all'area di impostazioni, notifiche e sezioni di Bitdefender per una configurazione dettagliata e attività amministrative avanzate.

Dalla parte superiore dell'interfaccia principale, puoi accedere al tuo account di Bitdefender. Inoltre, puoi contattarci per richiedere supporto nel caso avessi domande o si verificasse qualcosa di inatteso.

Se vuoi tenere sotto controllo le informazioni più importanti sulla sicurezza e accedere rapidamente alle impostazioni principali, aggiungi il Widget sicurezza al tuo desktop.

4.1. Icona area di notifica

Per gestire tutto il prodotto più velocemente, puoi utilizzare l'icona di Bitdefender nell'area di notifica.

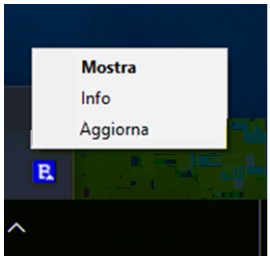
Nota
L'icona di Bitdefender potrebbe non essere sempre visibile. Per far apparire l'icona in modo permanente:

- In **Windows 7, Windows 8 e Windows 8.1**:

1. Clicca sulla freccia nell'angolo in basso a destra dello schermo.
2. Clicca su **Personalizza...** per aprire la finestra delle icone dell'area di Notifica.
3. Seleziona l'opzione **Mostra icone e notifiche** per l'**icona dell'agente di Bitdefender**.

- In **Windows 10**:
  1. Clicca con il pulsante destro sulla barra delle applicazioni e seleziona **Impostazioni barra delle applicazioni**.
  2. Scorri in basso e clicca sul link **Seleziona le icone che compaiono sulla barra delle applicazioni** nell'**Area di notifica**.
  3. Attiva l'interruttore accanto a **Bitdefender Agent**.

Se si fa doppio clic su questa icona, Bitdefender si aprirà. Inoltre, facendo clic con il pulsante destro sull'icona, apparirà un menu contestuale che consentirà una rapida gestione del prodotto Bitdefender.



Tray Icon

- **Mostra** - Apre la finestra principale di Bitdefender.
- **Info** - Apre una finestra in cui puoi visualizzare maggiori informazioni su Bitdefender, dove cercare aiuto nel caso dovesse verificarsi qualcosa di inaspettato, oltre ad accedere e rivedere l'Accordo di abbonamento, i componenti di terze parti e l'Informativa sulla privacy.
- **Nascondi / Mostra widget sicurezza** - Attiva / disattiva il widget sicurezza.
- **Aggiorna ora** - Inizia un aggiornamento immediato. Puoi seguire lo stato di aggiornamento nel pannello Aggiornamento della finestra principale di Bitdefender.

L'icona di Bitdefender nell'area di notifica fornisce informazioni relative ai problemi del dispositivo o al funzionamento del prodotto, visualizzando un simbolo speciale come segue:

Nessun problema sta influenzando la sicurezza del tuo sistema.
Si sono verificati dei problemi critici per la sicurezza del sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.

Se Bitdefender non è in funzione, l'icona nell'area di notifica appare su uno sfondo grigio: . Questo si verifica normalmente quando l'abbonamento è scaduto. Può anche verificarsi quando i servizi di Bitdefender non rispondono o quando altri errori interferiscono con il normale funzionamento di Bitdefender.

4.2. Menu di navigazione

Sul lato sinistro dell'interfaccia di Bitdefender c'è il menu di navigazione, che ti consente di accedere rapidamente alle funzionalità e gli strumenti di Bitdefender necessari per gestire il prodotto. Le schede disponibili in quest'area sono:

- **Dashboard**. Da qui, puoi risolvere rapidamente eventuali problemi di sicurezza, visualizzare suggerimenti in base alle esigenze del tuo sistema e modalità d'uso, ed eseguire azioni rapide.
-
- **Protezione**. Da qui, potrai lanciare e configurare scansioni antivirus, ripristinare i dati nel caso venissero cifrati da un ransomware e configurare la protezione mentre si naviga su Internet.

  Nota
  Some features are not available on the free version.

- **Privacy**. Da qui, puoi creare gestori di password per i tuoi account online, effettuare pagamenti online in un ambiente sicuro e aprire la app VPN.

  Nota
  Some features are not available on the free version.

- **Utilities**. Da qui, puoi gestire i profili e accedere alla funzionalità Protezione dati.

  Nota
  Some features are not available on the free version.

- **Notifiche**. Da qui, puoi accedere alle notifiche già generate.
- **Impostazioni**. Da qui, puoi accedere alle impostazioni generali.

Sul lato superiore dell'interfaccia principale, troverai le funzionalità **Il mio account** e **Supporto**.

- **Supporto**. Da qui, se hai bisogno di assistenza per risolvere un determinato problema con Bitdefender Antivirus Free, puoi contattare l'assistenza tecnica di Bitdefender.
- **Il mio account**. Da qui, puoi accedere al tuo account di Bitdefender per verificare i tuoi abbonamenti ed eseguire le attività di sicurezza sui dispositivi che gestisci. Sono anche disponibili maggiori dettagli sull'account Bitdefender e l'abbonamento in uso.

4.3. Dashboard

La finestra Dashboard ti consente di eseguire le attività più comuni, risolvere rapidamente problemi di sicurezza, visualizzare informazioni sulle attività del prodotto e accedere ai vari pannelli da cui puoi configurare le impostazioni.

Tutto è a pochi clic di distanza.

La finestra è organizzata in tre sezioni principali:

Area stato di sicurezza
: Qui è dove controllare lo stato di sicurezza del tuo dispositivo.

Autopilot
: Qui è dove puoi controllare i suggerimenti dell'Autopilot per assicurare una funzionalità adeguata del sistema.

Azioni rapide
: Da qui puoi eseguire diverse attività per mantenere sempre protetto il tuo sistema.

> **Nota**
> Some tasks are not available on the free version.

4.3.1. Area stato di sicurezza

Bitdefender utilizza un sistema di identificazione dei problemi per rilevare e fornire informazioni relative ai problemi che potrebbero avere effetto sulla sicurezza del dispositivo e dei dati. I problemi rilevati includono importanti impostazioni di protezione che sono disattivate e altre condizioni che possono rappresentare un rischio per la sicurezza.

Ogni volta che i problemi incidono sulla sicurezza del tuo dispositivo, lo stato visualizzato nella parte superiore dell'interfaccia di Bitdefender diventa rosso. Lo stato visualizzato indica la natura dei problemi che influenzano il tuo sistema. Inoltre, l'icona dell'area di notifica diventa e se sposti il cursore del mouse sull'icona, un pop-up confermerà l'esistenza di problemi in sospeso.

Poiché i problemi rilevati possono impedire a Bitdefender di proteggerti dalle minacce o rappresentano un importante rischio per la sicurezza, ti consigliamo di prestarvi attenzione e risolverli il prima possibile. Per risolvere un problema, clicca sul pulsante accanto al problema rilevato.

4.3.2. Autopilot

Per offrirti un funzionamento efficace e una maggiore protezione, eseguendo diverse attività, Bitdefender Autopilot si comporterà come un consulente di sicurezza personale. In base alle attività eseguite, come lavorare, effettuare pagamenti online, guardare un film o giocare a videogiochi, Bitdefender Autopilot fornirà alcuni suggerimenti contestuali in base all'uso e alle esigenze del dispositivo. I suggerimenti proposti possono essere anche relativi ad azioni che devi intraprendere per far funzionare il prodotto al massimo delle sue capacità.

Per iniziare a usare una funzionalità suggerita o effettuare miglioramenti nel tuo prodotto, clicca sul pulsante corrispondente.

Disattivare le notifiche di Autopilot

Per portare la tua attenzione ai suggerimenti di Autopilot, il prodotto Bitdefender viene impostato per informarti tramite una finestra di pop-up.

Per disattivare le notifiche di Autopilot:

1. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.

2. Nella finestra **Generale**, disattiva **Notifiche suggerimenti**.

4.3.3. Azioni rapide

Usando le azioni rapide puoi lanciare rapidamente attività che consideri importanti per mantenere protetto il tuo sistema e migliorare il modo in cui lavori.

Di norma, Bitdefender è dotato di alcune azioni rapide che possono essere sostituite da altre che usi più spesso. Per sostituire un'azione rapida:

1. Clicca sull'icona nell'angolo in alto a destra della scheda che vuoi rimuovere.
2. Punta l'attività che vuoi aggiungere all'interfaccia principale e poi clicca su **AGGIUNGI**.

Le attività che puoi aggiungere all'interfaccia principale sono:

- **Scansione veloce**. Esegui una scansione veloce per rilevare prontamente possibili minacce eventualmente presenti sul tuo dispositivo.
- **Scansione di sistema**. Esegui una scansione di sistema per assicurarti che il tuo dispositivo sia privo di minacce.

To start protecting additional Windows devices:

1. Clicca su **Installa Bitdefender su un altro dispositivo**.

   Sul tuo schermo comparirà una nuova finestra.
2. Clicca su **CONDIVIDI LINK DI DOWNLOAD**.
3. Follow the on-screen steps to install Bitdefender Antivirus Free on Windows-based devices.

4.4. Le sezioni di Bitdefender

4.4. Le sezioni di Bitdefender

Il prodotto Bitdefender include tre sezioni divise con funzionalità utili per garantirti la massima sicurezza mentre lavori, navighi sul web o esegui pagamenti online, migliorare la velocità del tuo sistema e molto altro.

Quando vuoi utilizzare le funzionalità di una determinata sezione o iniziare a configurare il prodotto, accedi alle seguenti icone situate nel menu di navigazione dell'interfaccia di Bitdefender:

-  Protezione
-  Privacy
-  Utility

4.4.1. Protezione

In the Protection section you can configure security settings or configure and run scan tasks.

Le funzionalità che puoi gestire nella sezione Protezione sono:

ANTIVIRUS

La protezione antivirus è la base della tua sicurezza. Bitdefender ti protegge in tempo reale e su richiesta da ogni sorta di minaccia, come malware, trojan, spyware, adware, ecc.

Dalla funzionalità Antivirus, puoi accedere facilmente alle seguenti attività di scansione:

- Scansione veloce
- Scansione sistema
- Gestisci scansioni

Per maggiori informazioni sulle attività di scansione e su come configurare la protezione antivirus, fai riferimento a «*Protezione antivirus*» (p. 57).

PREVENZIONE MINACCE ONLINE

La Prevenzione minacce online ti aiuta a proteggerti da attacchi phishing, tentativi di frode e fughe di dati personali, durante la navigazione su Internet.

Per maggiori informazioni su come configurare Bitdefender per proteggere le tue attività sul web, fai riferimento a «*Prevenzione minacce online*» (p. 77).

ADVANCED THREAT DEFENSE

Advanced Threat Defense protegge attivamente il tuo sistema da minacce come ransomware, spyware e trojan, analizzando il comportamento delle app installate. I processi sospetti vengono identificati e, se necessario, bloccati.

Per maggiori informazioni su come tenere il sistema al sicuro dalle minacce, fai riferimento a «*Advanced Threat Defense*» (p. 74).

4.5. Security Widget

Il **widget sicurezza** è un modo semplice e veloce per monitorare e controllare Bitdefender Antivirus Free. Aggiungendo questo piccolo e discreto widget sul desktop, puoi visualizzare tutte le informazioni critiche ed eseguire le attività principali in qualsiasi momento:

- apri la finestra principale di Bitdefender.
- Monitorare le attività di scansione in tempo reale.
- Monitorare lo stato di sicurezza del sistema e risolvere ogni eventuale problema.
- mostra quando è in corso un aggiornamento.
- Visualizzare le notifiche e accedere agli ultimissimi eventi segnalati da Bitdefender.
- Eseguire una scansione di file o cartelle, trascinando e rilasciando uno o più elementi sul widget.

Security Widget

Lo stato di sicurezza generale del computer è indicato **al centro** del widget. Lo stato è indicato dal colore e dalla forma dell'icona che compare in quest'area.

Al momento il tuo sistema è a rischio.

Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile. Clicca sull'icona di stato per iniziare a risolvere i problemi segnalati.

I servizi Bitdefender non rispondono.

Il tuo sistema è protetto.

 Quando è in corso un'attività di scansione, viene mostrata questa icona animata.

 Questa icona indica che il tuo abbonamento a Bitdefender è scaduto.

 Quando è in corso un aggiornamento, viene mostrata questa icona.

In caso di problemi, clicca sull'icona di stato per lanciare la procedura guidata della risoluzione problemi.

Il lato inferiore del widget mostra il contatore degli eventi non letti (il numero di eventi rilevanti segnalati da Bitdefender, in caso ve ne fossero). Clicca sul contatore degli eventi, per esempio 1, nel caso di un evento non letto, per aprire la finestra delle Notifiche. Per maggiori informazioni, fai riferimento a ???.

4.5.1. Eseguire la scansione di file e cartelle

Puoi utilizzare il widget sicurezza per eseguire una scansione veloce di file e cartelle. Trascina un file o una cartella che desideri controllare e rilascialo sopra al **widget sicurezza**.

Comparirà la procedura guidata scansione antivirus e ti guiderà attraverso il processo di scansione. Le opzioni di scansione sono preconfigurate per ottenere i migliori risultati di rilevamento e non possono essere modificate. Quando viene rilevato un file infetto, Bitdefender cerca di pulirlo, rimuovendo il codice dannoso). Se la disinfezione fallisce, la procedura guidata della scansione antivirus ti consentirà di indicare altre azioni da intraprendere sui file infetti.

4.5.2. Nascondi / mostra widget sicurezza

Se non desideri più visualizzare il widget, clicca su ⊗.

Per ripristinare il widget sicurezza, usa uno dei seguenti metodi:

- Dall'area di notifica:
  1. Clicca con il pulsante destro del mouse sull'icona Bitdefender nell'area di stato.
  2. Clicca su **Mostra widget sicurezza** nel menu contestuale che apparirà.

- Dall'interfaccia di Bitdefender:
  1. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
  2. Nella finestra **Generale**, attiva il **Widget sicurezza**.

Di norma, il widget sicurezza di Bitdefender è disattivato.

4.6. Modificare la lingua del prodotto

L'interfaccia di Bitdefender è disponibile in varie lingue e può essere modificata seguendo questi passaggi:

1. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella finestra **Generali**, clicca su **Cambia lingua**.
3. Seleziona la lingua desiderata nell'elenco e clicca su **SALVA**.
4. Attendi qualche istante finché non vengono applicate le impostazioni.

5. BITDEFENDER CENTRAL

Bitdefender Central è la piattaforma che consente di accedere alle funzioni e ai servizi online del prodotto, oltre a eseguire in remoto alcune importanti funzioni sui dispositivi in cui è stato installato Bitdefender. Puoi accedere al tuo account Bitdefender da qualsiasi dispositivo connesso a Internet andando in https://central.bitdefender.com, o direttamente dalla app Bitdefender Central sui dispositivi Android e iOS.

Per installare la app Bitdefender Central sui tuoi dispositivi:

- **Su Android** - Cerca Bitdefender Central su Google Play e poi scarica e installa la app. Segui i passaggi richiesti per completare l'installazione.
- **Su iOS** - Cerca Bitdefender Central su App Store, e poi scarica e installa la app. Segui i passaggi richiesti per completare l'installazione.

Una volta eseguito l'accesso, puoi utilizzare le seguenti attività:

- Download and install Bitdefender on Windows based devices.
- Aggiungi nuovi dispositivi alla tua rete e gestiscili ovunque ti trovi.

5.1. Accedere a Bitdefender Central

Ci sono diversi modi per accedere a Bitdefender Central:

- Dall'interfaccia principale di Bitdefender:
  1. Clicca sull'icona  nell'angolo in alto a destra dell'interfaccia di Bitdefender.
  2. Clicca su **Vai a Bitdefender Central**.
  3. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
- Dal tuo browser web:
  1. Apri un browser web su un dispositivo con accesso a internet.
  2. Vai a: https://central.bitdefender.com.
  3. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
- Dal tuo dispositivo Android o iOS:

  Apri la app Bitdefender Central che hai installato.

Nota
In questo materiale vengono fornite le opzioni e le istruzioni disponibili sulla piattaforma web.

5.2. Autenticazione a due fattori

Il metodo dell'autenticazione a due fattori aggiunge un ulteriore livello di sicurezza al tuo account di Bitdefender, richiedendo un codice di autenticazione oltre alle tue credenziali di accesso. In questo modo, potrai impedire il furto del tuo account e proteggerlo da altri tipi di attacchi informatici, come keylogger, forza bruta o attacchi a dizionario.

Attivare l'autenticazione a due fattori

Attivando l'autenticazione a due fattori, renderai il tuo account di Bitdefender molto più sicuro. La tua identità sarà verificata ogni volta che accederai a dispositivi diversi per installare uno dei prodotti Bitdefender, verificare lo stato del tuo abbonamento o eseguire attività in remoto sui tuoi dispositivi.

Per attivare l'autenticazione a due fattori:

1. Accedi a Bitdefender Central.
2. Clicca sull'icona nell'angolo in basso a destra dello schermo.
3. Clicca su **account di Bitdefender** nel menu scorrevole.
4. Seleziona la scheda **Password e sicurezza**.
5. Clicca su **Autenticazione a due fattori**.
6. Clicca su **COME INIZIARE**.

   Scegli uno dei seguenti metodi:

   - **App Autenticatore** - Usa una app Autenticatore per generare un codice ogni volta che accedi al tuo account di Bitdefender.

     Se vuoi usare una app Autenticatore, ma non sai quale scegliere, è disponibile un elenco con le app di autenticazione consigliate.

     a. Clicca su **USA APP AUTENTICATORE** per iniziare.

     b. Per accedere a un dispositivo Android o iOS, usa il tuo dispositivo per esaminare il codice QR.

        Per accedere su un portatile o un computer desktop, puoi aggiungere manualmente il codice mostrato.

Clicca su **CONTINUA**.

c. Inserisci il codice fornito dalla app o quello mostrato nel passaggio precedente e poi clicca su **ATTIVA**.

- **E-mail** - ogni volta che accedi al tuo account di Bitdefender, un codice di verifica sarà inviato alla tua casella di posta. Controlla il tuo account e-mail e poi inserisci il codice che hai ricevuto.

  a. Clicca su **USA E-MAIL** per iniziare.

  b. Controlla il tuo account e-mail e inserisci il codice fornito.

  Ricordati che hai cinque minuti per controllare il tuo account di posta e inserire il codice generato. Se il tempo dovesse scadere, dovrai generare un nuovo codice seguendo gli stessi passaggi.

  c. Clicca su **ATTIVA**.

  d. Ti vengono forniti dieci codici di attivazione. Puoi copiare, scaricare o stampare l'elenco e usarlo se dovessi perdere il tuo indirizzo e-mail o non potrai accedere. Ogni codice può essere usato solo una volta.

  e. Clicca su **FINE**.

Nel caso non volessi più usare l'autenticazione a due fattori:

1. Clicca su **DISATTIVA L'AUTENTICAZIONE A DUE FATTORI**.
2. Controlla la tua app o il tuo account e-mail e inserisci il codice che hai ricevuto.

   Se hai scelto di ricevere il codice di autenticazione via e-mail, hai cinque minuti per controllare il tuo account e-mail e inserire il codice generato. Se il tempo dovesse scadere, dovrai generare un nuovo codice seguendo gli stessi passaggi.
3. Conferma la tua scelta.

5.2.1. Aggiungere dispositivi affidabili

Per assicurarti che solo tu possa accedere al tuo account di Bitdefender, potrebbe servirti un codice. Se vuoi saltare questo passaggio ogni volta che ti connetti allo stesso dispositivo, ti consigliamo di inserirlo tra i dispositivi affidabili.

Per aggiungere dispositivi ai dispositivi affidabili:

1. Accedi a Bitdefender Central.

2. Clicca sull'icona nell'angolo in basso a destra dello schermo.
3. Clicca su **account di Bitdefender** nel menu scorrevole.
4. Seleziona la scheda **Password e sicurezza**.
5. Clicca su **Dispositivi affidabili**.
6. Viene mostrato l'elenco con i dispositivi su cui è stato installato Bitdefender. Clicca sul dispositivo desiderato.

Puoi aggiungere quanti dispositivi desideri, a patto che abbiano installato Bitdefender e che il tuo abbonamento sia valido.

5.3. I miei abbonamenti

The Bitdefender Central platform gives you the possibility to easily see the subscriptions you have for all your devices.

5.3.1. Controllare gli abbonamenti disponibili

Per controllare gli abbonamenti disponibili:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **I miei abbonamenti**.

Qui puoi avere maggiori informazioni sulla disponibilità degli abbonamenti che possiedi e il numero di dispositivi che li utilizza.

Nota
Puoi avere uno o più abbonamenti sul tuo account, a condizione che siano per piattaforme differenti (Windows, macOS, iOS o Android).

5.3.2. Aggiungi un nuovo dispositivo

Se l'abbonamento copre più di un dispositivo, è possibile aggiungerne un altro e installare Bitdefender Antivirus Free su di esso, come segue:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **I miei dispositivi** e clicca sull'icona .
3. Seleziona una delle due opzioni disponibili:
   - **Proteggi questo dispositivo**

Seleziona questa opzione e poi il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, clicca sul pulsante corrispondente.

- **Proteggi altri dispositivi**

  Seleziona questa opzione e poi il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, clicca sul pulsante corrispondente.

  Clicca su **INVIA LINK DI DOWNLOAD**. 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.

  Sul dispositivo su cui vuoi installare il tuo prodotto Bitdefender, controlla l'account email che hai digitato e poi clicca sul pulsante di download corrispondente.

4. Attendi il completamento del download e poi esegui il programma d'installazione.

5.3.3. Attiva abbonamento

A paid subscription can be activated during the installation process by using your Bitdefender account. Together with the activation process, its validity starts to count-down.

Se hai acquistato un codice di attivazione da uno dei nostri rivenditori o l'hai ricevuto come o e

Ora l'abbonamento è attivato. Vai al pannello **I miei dispositivi** e clicca sull'icona per installare il prodotto su uno dei tuoi dispositivi.

Nota
If you activate a subscription with activation code, the existing free subscription will be replaced with the paid subsctiption.

5.4. I miei dispositivi

La sezione **I miei dispositivi** in Bitdefender Central ti consente d'installare, gestire e utilizzare in remoto il tuo prodotto Bitdefender su qualsiasi dispositivo, a condizione che sia acceso e connesso a Internet. Le schede dei dispositivi mostrano il nome del dispositivo, il sistema operativo, il prodotto installato, lo stato della protezione e l'eventuale presenza di rischi che ne influenzano la protezione.

Per visualizzare un elenco dei tuoi dispositivi ordinati in base al loro stato o agli utenti, clicca sulla freccia a tendina nell'angolo in alto a destra dello schermo.

Per identificare facilmente i tuoi dispositivi, puoi personalizzarne il nome:

1. Accedi a Bitdefender Central.
2. Seleziona la scheda **I miei dispositivi**.
3. Clicca su **MOSTRA DETTAGLI** sulla scheda del dispositivo desiderato e poi sull'icona nell'angolo in alto a destra dello schermo.
4. Seleziona **Impostazioni**.
5. Inserisci un nuovo nome nel campo **Nome dispositivo**, e clicca su **SALVA**.

Puoi creare e assegnare un proprietario a ogni dispositivo per una gestione migliore:

1. Accedi a Bitdefender Central.
2. Seleziona la scheda **I miei dispositivi**.
3. Clicca su **MOSTRA DETTAGLI** sulla scheda del dispositivo desiderato e poi sull'icona nell'angolo in alto a destra dello schermo.
4. Seleziona **Profilo**.

5. Clicca su **Aggiungi proprietario**, poi compila i campi corrispondenti. Personalizza il profilo aggiungendo una foto e selezionando una data di nascita.
6. Clicca su **AGGIUNGI** per salvare il profilo.
7. Seleziona il proprietario desiderato dall'elenco **Proprietario dispositivo** e clicca su **ASSEGNA**.

Per aggiornare Bitdefender in remoto su un dispositivo Windows:

1. Accedi a Bitdefender Central.
2. Seleziona la scheda **I miei dispositivi**.
3. Clicca su **MOSTRA DETTAGLI** sulla scheda del dispositivo desiderato e poi sull'icona ⋮ nell'angolo in alto a destra dello schermo.
4. Seleziona **Aggiorna**.

Per maggiori informazioni e altre azioni in remoto riguardo il tuo Bitdefender su un determinato dispositivo, clicca su **MOSTRA DETTAGLI** sulla scheda del dispositivo desiderato.

Una volta cliccato su **MOSTRA DETTAGLI** sulla scheda di un dispositivo, saranno disponibili le seguenti voci:

- **Dashboard**. In this window you can view details about the selected device, check its protection status and how many threats have been blocked in the last seven days. The protection status can be green, when there is no issue affecting your device, yellow when the device needs your attention or red when the device is at risk. When there are issues affecting your device, click the drop-down arrow in the upper status area to find out more details. From here you can manually fix issues that are affecting the security of your devices.
- **Protezione**. Da questa finestra, puoi eseguire in remoto una Scansione veloce o una Scansione di sistema sui tuoi dispositivi. Clicca sul pulsante **CONTROLLA** per avviare il processo. Puoi anche verificare quanto è stata eseguita l'ultima scansione sul dispositivo e visualizzare un rapporto della scansione più recente con tutte le informazioni più importanti.Per maggiori informazioni sui due processi di scansione, fai riferimento a Sezione 11.2.3, «*Eseguire una scansione del sistema*» e «*Eseguire una Scansione veloce*» (p. 59).

5.5. Attività

Nella sezione Attività hai accesso a informazioni sui dispositivi con Bitdefender installato.

Una volta eseguito l'accesso alla finestra **Attività**, saranno disponibili le seguenti schede:

- **I miei dispositivi**. Qui puoi visualizzare il numero dei dispositivi connessi insieme al loro stato di protezione. Per risolvere i problemi in remoto sui dispositivi rilevati, clicca su **Risolvi problemi** e poi clicca su **ESAMINA E RISOLVI I PROBLEMI**.

  Per vedere altri dettagli sui problemi rilevati, clicca su **Vedi problemi**.

  Le informazioni sulle minacce rilevate non possono essere recuperate da dispositivi iOS.

- **Minacce bloccate**. Qui puoi visualizzare un grafico che mostra alcune statistiche generali tra cui informazioni sulle minacce bloccate nelle ultime 24 ore e sette giorni. Le informazioni mostrate vengono recuperate in base al comportamento dannoso rilevato su file, app e URL a cui si accede.
- **Principali utenti con minacce bloccate**. Qui puoi visualizzare un elenco con gli utenti a cui sono state trovate la maggior parte delle minacce.
- **Principali dispositivi con minacce bloccate**. Qui puoi visualizzare un elenco con i dispositivi in cui sono state trovate la maggior parte delle minacce.

5.6. Notifiche

Per aiutarti a essere sempre informato su ciò che succede sui dispositivi associati al tuo account, l'icona 🔔 è sempre a portata di mano. Cliccandoci sopra, ottieni un'immagine che riassume maggiori informazioni sulle attività dei prodotti Bitdefender installati sui tuoi dispositivi.

6. MANTENERE AGGIORNATO BITDEFENDER

Tutti giorni vengono trovate e identificate nuove minacce. Ecco perché è molto importante mantenere Bitdefender aggiornato con il database delle informazioni delle minacce più recente.

Se siete connessi a Internet con una linea a banda larga o ADSL, Bitdefender si prenderà cura di sé da solo. Di norma, verifica la presenza di aggiornamenti all'accensione del dispositivo e in seguito ad ogni **ora**. Se vi è un aggiornamento disponibile, viene scaricato e installato automaticamente sul dispositivo.

Il processo di aggiornamento viene eseguito direttamente, ciò significa che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto e, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Importante
Per essere sempre protetti contro le minacce più recenti, mantieni attivato l'Aggiornamento automatico.

In alcune situazioni particolari, è necessario il tuo intervento per mantenere aggiornata la protezione di Bitdefender:

- Se il tuo dispositivo si collega a Internet tramite un server proxy, devi configurare le impostazioni proxy come descritto nella sezione *«Come posso configurare Bitdefender per usare una connessione a Internet tramite proxy?»* (p. 50).
- Se sei connesso a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di Bitdefender su richiesta dell'utente. Per maggiori informazioni, fai riferimento a *«Eseguire un aggiornamento»* (p. 30).

6.1. Verificare se Bitdefender è aggiornato

Per controllare la data dell'ultimo aggiornamento del tuo Bitdefender:

1. Clicca su **Notifiche** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella scheda **Tutto**, seleziona la notifica relativa all'ultimo aggiornamento.

Puoi sapere quando gli aggiornamenti sono stati lanciati e avere maggiori informazioni al riguardo (se hanno avuto successo o meno, e se richiedono

di riavviare il computer per completare l'installazione). Se necessario, riavvia il sistema al più presto.

6.2. Eseguire un aggiornamento

Per poter eseguire gli aggiornamenti, serve una connessione a Internet.

Per avviare un aggiornamento, clicca con il pulsante destro sull'icona di Bitdefender nell'area delle notifiche e poi seleziona **Aggiorna ora**.

La funzionalità Aggiornamento si connetterà al server di aggiornamento di Bitdefender per cercare eventuali aggiornamenti. Se viene rilevato un aggiornamento, ti sarà chiesto di confermare l'aggiornamento oppure sarà eseguito automaticamente, secondo le impostazioni di aggiornamento.

Importante
Potrebbe essere necessario riavviare il dispositivo, una volta completato l'aggiornamento. Si raccomanda di farlo il prima possibile.

Puoi anche eseguire gli aggiornamenti in remoto sui tuoi dispositivi, purché siano accesi e connessi a Internet.

Per aggiornare Bitdefender in remoto su un dispositivo Windows:

1. Accedi a Bitdefender Central.
2. Seleziona la scheda **I miei dispositivi**.
3. Clicca su **MOSTRA DETTAGLI** sulla scheda del dispositivo desiderato e poi sull'icona nell'angolo in alto a destra dello schermo.
4. Seleziona **Aggiorna**.

6.3. Attivare o disattivare l'aggiornamento automatico

Per attivare o disattivare l'aggiornamento automatico:

1. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Aggiorna**.
3. Attiva o disattiva l'interruttore corrispondente.
4. Comparirà una finestra di avviso. Devi confermare la tua scelta selezionando dal menu per quanto tempo desideri disattivare

l'aggiornamento automatico. Puoi disattivare l'aggiornamento automatico per 5, 15 o 30 minuti, per un'ora, o fino a un riavvio del sistema.

Avvertimento

È una questione di sicurezza piuttosto importante. Si consiglia di disattivare l'aggiornamento automatico per il minimo tempo possibile. Se Bitdefender non verrà aggiornato regolarmente non sarà in grado di proteggerti dalle minacce più recenti.

6.4. Modificare le impostazioni di aggiornamento

Gli aggiornamenti possono essere eseguiti dalla rete locale, su Internet, direttamente o attraverso un server proxy. Di norma, Bitdefender controllerà la disponibilità di aggiornamenti su Internet ogni ora e installerà gli aggiornamenti disponibili senza avvisarti.

Le impostazioni predefinite di aggiornamento sono adatte alla maggior parte degli utenti e normalmente non serve modificarle.

Per regolare le impostazioni dell'aggiornamento:

1. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Aggiorna** e regola le impostazioni in base alle tue preferenze.

Frequenza d'aggiornamento

Bitdefender è configurato per verificare la presenza di aggiornamenti ogni ora. Per cambiare la frequenza di aggiornamento, trascina il cursore scorrevole lungo la barra per impostare il lasso di tempo desiderato in cui effettuare l'aggiornamento.

Regole di esecuzione dell'aggiornamento

Ogni volta che è disponibile un aggiornamento, Bitdefender lo scaricherà e implementerà automaticamente senza mostrare alcuna notifica. Disattiva l'opzione **Aggiornamento silenzioso** se vuoi essere informato ogni volta che è disponibile un aggiornamento.

Per completare l'installazione di alcuni aggiornamenti devi riavviare il sistema.

Come impostazione predefinita, se un aggiornamento richiede un riavvio, Bitdefender continuerà a funzionare con i file precedenti finché l'utente non

riavvia volontariamente il dispositivo. Questo per impedire che il processo di aggiornamento di Bitdefender interferisca con il lavoro dell'utente.

Se vuoi essere informato quando un aggiornamento richiede un riavvio, attiva **Notifica di riavvio**.

6.5. Aggiornamenti costanti

Per assicurarsi che stai usando la versione più recente, Bitdefender cercherà automaticamente eventuali aggiornamenti del prodotto. Questi aggiornamenti potrebbero portare nuove funzionalità e miglioramenti, risolvere eventuali problemi del prodotto o fare l'upgrade automaticamente a una nuova versione. Quando la nuova versione di Bitdefender viene installata tramite un aggiornamento, le impostazioni personalizzate vengono salvate ed è possibile evitare le procedure di disinstallazione e reinstallazione.

Tali aggiornamenti richiedono un riavvio del sistema per avviare l'installazione di nuovi file. Quando l'aggiornamento di un prodotto viene completato, una finestra di pop-up ti informerà di riavviare il sistema. Se perdessi la notifica, puoi cliccare **RIAVVIA ORA** nella finestra Notifiche, dove viene indicato l'aggiornamento più recente o riavviare manualmente il sistema.

COME FARE

7. INSTALLAZIONE

7.1. Come installo Bitdefender su un secondo dispositivo?

If the subscription covers more than one device, you can use your Bitdefender account to activate a second PC.

Per installare Bitdefender su un secondo dispositivo:

1. Clicca su **Installa Bitdefender su un altro dispositivo** nell'angolo in basso a sinistra dell'interfaccia di Bitdefender.

   Sul tuo schermo comparirà una nuova finestra.

2. Clicca su **CONDIVIDI LINK DI 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.

7.2. 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.

Nel caso in cui una delle situazioni indicate sia il tuo caso, segui questi passaggi:

- In **Windows 7**:
  1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
  2. Trova **Bitdefender Antivirus Free** 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 su **Programmi e funzionalità**.
3. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
4. Clicca su **REINSTALLA** nella finestra che comparirà.
5. Devi riavviare il dispositivo per completare il processo.

- In **Windows 10**:

1. Clicca su **Start** e poi su Impostazioni.
2. Clicca sull'icona **Sistema** nelle Impostazioni e seleziona **App e funzioni**.
3. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
5. Clicca su **REINSTALLA**.
6. Devi 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.

7.3. Where can I download Bitdefender Antivirus Free from?

You can download Bitdefender Antivirus Free form the Bitdefender Website. Once the installation process is complete, Bitdefender Antivirus Free is activated.

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.

To download Bitdefender Antivirus Free from Bitdefender Website::

1. Access https://www.bitdefender.com/toolbox/.
2. Click download on Bitdefender Antivirus Free.

3. Attendi il completamento del download e poi esegui il programma d'installazione.
4. Esegui il prodotto Bitdefender che hai scaricato.

7.4. Come posso modificare la lingua del mio prodotto Bitdefender?

L'interfaccia di Bitdefender è disponibile in varie lingue e può essere modificata seguendo questi passaggi:

1. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella finestra **Generali**, clicca su **Cambia lingua**.
3. Seleziona la lingua desiderata nell'elenco e clicca su **SALVA**.
4. Attendi qualche istante finché non vengono applicate le impostazioni.

8. BITDEFENDER CENTRAL

8.1. Come posso accedere all'account di Bitdefender con un altro account?

Hai creato un nuovo account Bitdefender che desideri utilizzare da qui in avanti.

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. Inserisci l'indirizzo e-mail nel campo corrispondente e clicca su **AVANTI**.
4. Inserisci la tua password e clicca su **ACCEDI**.

Nota
Il prodotto Bitdefender dal tuo dispositivo cambia automaticamente in base all'abbonamento associato al nuovo account Bitdefender.
Se non ci fosse alcun abbonamento disponibile associato al nuovo account Bitdefender o si volesse trasferirlo dall'account precedente, contattare il supporto tecnico di Bitdefender, come descritto nella sezione *«Chiedere aiuto»* (p. 100).

8.2. Come posso disattivare 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. Accedi a Bitdefender Central.
2. Clicca sull'icona nell'angolo in basso 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 d'aiuto**.

8.3. 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:

- Dall'interfaccia di Bitdefender:

  1. Clicca sull'icona  nell'angolo in alto a destra dell'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**.

     Comparirà una nuova finestra.
  4. Clicca su **Hai dimenticato la password?**.
  5. Clicca su **AVANTI**.
  6. 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.
  7. Inserisci la nuova password che vuoi impostare e ridigitala ancora una volta. Clicca su **SALVA**.

- Dal tuo browser web:

  1. Vai a: https://central.bitdefender.com.
  2. Clicca su **ACCEDI**.
  3. Inserisci il tuo indirizzo e-mail e clicca su **AVANTI**.
  4. Clicca su **Hai dimenticato la password?**.
  5. Clicca su **AVANTI**.
  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.

8.4. 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. Accedi a Bitdefender Central.
2. Clicca sull'icona nell'angolo in basso a destra dello schermo.
3. Clicca su **Sessioni** nel menu scorrevole.
4. Nella sezione **Sessioni attive**, seleziona l'opzione **ESCI** accanto al dispositivo in cui vuoi terminare la sessione di accesso.

9. SCANSIONE CON BITDEFENDER

9.1. 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'oggetto che desideri controllare, selezionare Bitdefender e poi **Controlla 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.

9.2. Come posso eseguire una scansione del mio sistema?

Per eseguire una scansione completa del sistema:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Clicca sul pulsante **Esegui scansione** accanto a **Scansione di 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 «*Procedura guidata scansione antivirus*» (p. 64).

9.3. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Clicca su ••• accanto al tipo di scansione che vuoi programmare, Scansione di 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 **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
   - Giornalmente
   - Settimanalmente
   - Mensilmente

   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.

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.

9.4. 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 pannello **ANTIVIRUS**, clicca su **Apri**.
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:
   - **Scansiona solo le applicazioni**. Puoi impostare Bitdefender per esaminare solo le app a cui si accede.
   - **Priorità attività scansione**. Puoi scegliere l'impatto che il processo di scansione dovrebbe avere sulle prestazioni del 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.
   - **Azioni di post scansione**. Seleziona quale azione Bitdefender dovrebbe intraprendere se non venisse rilevata alcuna minaccia:
     - Mostra la finestra del sommario
     - Spegni il dispositivo
     - Chiudi la finestra di scansione
5. Se vuoi configurare le opzioni di scansione nel dettaglio, clicca su **Mostra impostazioni avanzate**.

   Clicca su **Avanti**.
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
- 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.

7. 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.

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

9.5. Come posso escludere una cartella dalla scansione?

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

Le eccezioni devono essere utilizz

3. Cliccare sul tasto **Impostazioni**.
4. Clicca su **Gestisci eccezioni**.
5. Clicca su **+Aggiungi un'eccezione**.
6. 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**.
7. 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
8. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

9.6. Cosa fare quando Bitdefender rileva un file pulito come infetto?

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

1. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
   b. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
   c. Nella finestra **Avanzate**, disattiva **Protezione di Bitdefender**.

      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 elementi nascosti in Windows. Per scoprire come fare, fai riferimento a «*Come posso visualizzare gli elementi nascosti in Windows?*» (p. 52).

3. Ripristina il file dalla quarantena:
   a. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
   b. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
   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?*» (p. 43).

   Per impostazione predefinita, Bitdefender aggiunge automaticamente i file ripristinati nell'elenco delle eccezioni.
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 «*Chiedere aiuto*» (p. 100).

9.7. 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.

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. Clicca su **Notifiche** nel menu di navigazione dell'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 un registro di scansione, clicca su **Guarda registro**.

10. INFORMAZIONI UTILI

10.1. 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

4. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

- 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 su **Programmi e funzionalità**.
3. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
4. Clicca su **RIMUOVI** nella finestra che comparirà.
5. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

- In **Windows 10**:

1. Clicca su **Start** e poi su Impostazioni.
2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni**.
3. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
5. Clicca su **RIMUOVI** nella finestra che comparirà.
6. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

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

10.3. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Scansioni**, clicca su ••• accanto a Scansione veloce o Scansione di sistema, e seleziona **Modifica**.
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 Giornalmente, Mensilmente o Settimanalmente, trascina il cursore lungo la scala per impostare il periodo di tempo desiderato in cui dovrebbe iniziare la scansione programmata.
6. Clicca su **Salva**.

Per spegnere il dispositivo al termine di una scansione personalizzata:

1. Clicca su ••• accanto alla scansione personalizzata che hai creato.
2. Clicca su **Avanti** e poi di nuovo su **Avanti**.
3. Seleziona la casella accanto a **Scegli quando programmare questa attività** e poi seleziona quando l'attività dovrà iniziare.
4. Clicca su **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*» (p. 64).

10.4. 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. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Avanzate**.
3. Attiva il **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 indicarli nei rispettivi campi.

     > **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 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.

10.5. 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. Individua **Risorse del 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.
- Per **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.

     In **Windows 8.1**, localizza **Questo PC**.
  2. Seleziona **Proprietà** nel menu inferiore.
  3. Controlla in Sistema per verificare il tipo di sistema.
- In **Windows 10**:
  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.

10.6. 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 poi seleziona **Pannello di controllo**.

   In **Windows 8 e Windows 8.1**: dal menu Start di Windows, localizza il **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 poi su **OK**.

In **Windows 10**:

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. Deseleziona **Nascondi estensioni per i file conosciuti**.
4. Deseleziona **Nascondi file protetti del sistema operativo**.
5. Clicca su **Applica** e poi su **OK**.

10.7. 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 Antivirus Free

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. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
  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. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
- 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 su **Programmi e funzionalità**.
  3. Attendi per qualche istante, finché non compare l'elenco del software installato.
  4. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
  5. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
- In **Windows 10**:
  1. Clicca su **Start** e poi su Impostazioni.
  2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni**.
  3. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
  4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
  5. Attendi che il processo di disinstallazione sia completo e riavvia 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.

10.8. 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 e Windows 10**:
  1. Esegui **Configurazione di sistema** in Windows, premendo contemporaneamente i tasti **Windows + R** sulla tastiera.
  2. Digita **msconfig** nella finestra di dialogo **aperta** e clicca su **OK**.
  3. Seleziona la scheda **Avvio**.
  4. Nella sezione **Opzioni di avvio**, seleziona la casella **Modalità provvisoria**.
  5. Clicca su **Rete** e poi su **OK**.

6. Clicca su **OK** nella finestra **Configurazione di sistema**, che ti informerà della necessità di riavviare il sistema per effettuare le modifiche selezionate.

   Il sistema sarà riavviato in modalità provvisoria con supporto di rete.

Per riavviarlo in modalità normale, cambia le impostazioni, eseguendo nuovamente la **Configurazione di sistema** e togliendo la spunta dalla casella **Modalità provvisoria**. Clicca su **OK** e poi su **Riavvia**. Attendi che le nuove impostazioni vengano applicate.

GESTIRE LA PROPRIA SICUREZZA

11. PROTEZIONE ANTIVIRUS

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

- Scansione all'accesso - Impedisce che nuove minacce entrino nel tuo sistema. Ad esempio, Bitdefender esaminerà un documento Word, quando sarà aperto, e un'e-mail, quando verrà ricevuta.

  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 antivirus avviata dall'utente. Si sceglie quale unità, cartella o file Bitdefender deve controllare e Bitdefender li esamina, su 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*» (p. 68).

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*» (p. 70).

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*» (p. 72).

Se il tuo dispositivo è stato infettato da una minaccia, fai riferimento a «*Rimuovere le minacce dal sistema*» (p. 93).

11.1. 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.

11.1.1. 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 **Protezione di Bitdefender**.
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.

11.1.2. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Avanzate**, scorri verso il basso nella finestra finché non trovi l'opzione **Reimposta impostazioni avanzate**. Seleziona questa opzione per riportare le impostazioni dell'antivirus ai valori predefiniti.

11.2. 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.

11.2.1. Controllare un file o una cartella alla ricerca di minacce

Dovresti controllare i file e le cartelle ogni volta che sospetti che possano essere stati infettati. Clicca con il pulsante destro del mouse sul file o la cartella che desideri controllare, seleziona **Bitdefender** e poi **Controlla con Bitdefender**. Comparirà la procedura guidata scansione antivirus e ti guiderà attraverso il processo di scansione. Al termine della scansione, ti sarà chiesto di scegliere quali azioni intraprendere sui file rilevati, se presenti.

11.2.2. 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 **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.

2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
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.

11.2.3. 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 aggiornato Bitdefender*» (p. 29).
- 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*» (p. 61).

Per eseguire una scansione del sistema:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Scansioni**, clicca sul pulsante **Esegui scansione** accanto a **Scansione di 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 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.

11.2.4. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Scansioni**, clicca su **+Crea scansione**.
4. Nel campo **Nome 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 per esaminare solo le app a cui si accede.
   - **Priorità attività scansione**. Puoi scegliere l'impatto che il processo di scansione dovrebbe avere sulle prestazioni del 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.

- **Azioni di post scansione**. Seleziona quale azione Bitdefender dovrebbe intraprendere se non venisse rilevata 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

Questa informazione potrebbe esserti utile:

- Se non conosci alcuni termini, verificali nel glossario. Puoi anche trovare informazioni utili cercando su Internet.

- **Scansiona 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 fornito con un software freeware, che mostrerà pop-up o installerà una barra di strumenti nel browser predefinito. Alcuni modificheranno la homepage o il motore di ricerca, altri eseguiranno diversi processi in background rallentando il PC o mostreranno numerose pubblicità. Tali programmi possono essere installati senza il tuo consenso (vengono anche chiamati adware) o sono spesso inclusi in modo predefinito nei kit di installazione rapida (ad-supported).
- **Scansiona archivi.** Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del sistema. La minaccia può colpire il sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la protezione in tempo reale. Tuttavia, si consiglia di usare questa opzione per rilevare e rimuovere ogni minaccia potenziale, anche se non è 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.

- **Esamina solo file nuovi e modificati.**nu

impostazioni e le opzioni di configurazione delle componenti del sistema operativo Windows, oltre a quelle delle applicazioni installate.

- **Scansiona i cookie.** Seleziona questa opzione per controllare i cookie memorizzati dai browser sul tuo dispositivo.
- **Scansione keylogger.** Seleziona questa opzione per eseguire una scansione del sistema alla ricerca di applicazioni keylogger. I keylogger registrano ciò che digiti sulla tastiera per poi inviare queste informazioni tramite Internet a un hacker. L'hacker può trovare informazioni sensibili nei dati rubati, come numeri e password di un conto corrente, e usarle per ottenere benefici personali.

11.2.5. Procedura guidata scansione antivirus

Ogni volta che si inizia una scansione su richiesta (ad esempio, cliccando con il pulsante destro su una cartella, selezionando Bitdefender e poi **Controlla con Bitdefender**), apparirà la procedura guidata Scansione antivirus di Bitdefender. Segui la procedura guidata per completare la scansione.

Nota

Se non compare la procedura guidata di scansione, potrebbe darsi che la procedura guidata sia configurata per un'esecuzione in background. Cerca l'icona di avanzamento della scansione nell'area di notifica. Clicca sull'icona per aprire la finestra di scansione e visualizzarne l'avanzamento.

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).

Attendi che Bitdefender termini la scansione. La durata del processo dipende dalla complessità della scansione.

Arrestare o mettere in pausa la scansione. Puoi fermare la scansione in qualsiasi momento, cliccando su **FERMA** Verrete portati all'ultimo passo dell'assistente. Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **PAUSA**. Per riprendere la scansione, dovrai cliccare su **RIPRENDI**.

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

- **Password.** Se desideri che Bitdefender controlli l'archivio, seleziona questa opzione e digita la password. Se non si conosce la password, scegliere un'altra opzione.
- **Non chiedere una password e ignora questo elemento per la scansione.** Seleziona questa opzione per non controllare questo archivio.
- **Ignora tutti gli elementi protetti da password senza controllarli.** Seleziona questa opzione se non desideri ricevere ulteriori domande sugli archivi protetti da password. Bitdefender non sarà in grado di controllarli, ma saranno annotati 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 in base al tipo di file rilevato:

- **File infetti.** I file rilevati come infetti corrispondono a una parte delle 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 è denominata 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*» (p. 72).

  ### Importante

  Per alcune particolari tipologie di minacce, non è possibile usare la disinfezione perché il file rilevato è interamente dannoso. In questi alcu

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 termina la risoluzione dei problemi, i risultati della scansione compariranno 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*» (p. 93).

11.2.6. 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. Clicca su **Notifiche** nel menu di navigazione dell'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**.

11.3. 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.

11.3.1. 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.

Un'icona di scansione di Bitdefender comparirà nell'area di notifica. Clicca sull'icona per aprire la finestra di scansione e visualizzarne l'avanzamento.

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 dispone dei 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*» (p. 93).

11.3.2. Gestire la scansione di supporti rimovibili

Per gestire la scansione automatica di supporti rimovibili:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
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.

11.4. 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 la cartella che desideri controllare e seleziona **Controlla con Bitdefender**.

11.4.1. Escludere file e cartelle dalla scansione

Per escludere determinati file e cartelle dalla scansione:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Impostazioni**, clicca su **Gestisci 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.

11.4.2. Escludere estensioni di 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Impostazioni**, clicca su **Gestisci eccezioni**.
4. Clicca su **+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**.

11.4.3. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.

3. Nella finestra **Impostazioni**, clicca su **Gestisci 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**.

11.5. 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.

Di norma, i file in quarantena sono inviati automaticamente ai laboratori di Bitdefender per essere analizzati dai ricercatori di Bitdefender. Se la presenza di una minaccia viene confermata, viene rilasciato un aggiornamento delle informazioni per consentirne la rimozione.

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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
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 di nuovo quarantena dopo agg. informazioni 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**.

12. ADVANCED THREAT DEFENSE

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.

12.1. Attivare o disattivare Advanced Threat Defense

Per attivare o disattivare Advanced Threat Defense:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ADVANCED THREAT DEFENSE**, clicca su **Apri**.
3. Vai alla finestra **Impostazioni** e clicca sull'interruttore acanto 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.

12.2. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ADVANCED THREAT DEFENSE**, clicca su **Apri**.
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.

12.3. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ADVANCED THREAT DEFENSE**, clicca su **Apri**.
3. Nella finestra **Impostazioni**, clicca su **Gestisci 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 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. Clicca su **Salva**.

12.4. 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:

- Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
- Nel pannello **ADVANCED THREAT DEFENSE**, clicca su **Apri**.

- 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.

13. PREVENZIONE MINACCE ONLINE

La Prevenzione minacce online di Bitdefender 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **PREVENZIONE MINACCE ONLINE**, 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. Se decidi di visitarlo, usa la massima cautela.

  Questa è una 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

- 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.

RISOLUZIONE DEI PROBLEMI

14. RISOLVERE I PROBLEMI PIÙ COMUNI

Questo capitolo illustra alcuni problemi che potresti incontrare utilizzando Bitdefender e ti fornisce alcune soluzioni possibili per questi problemi. La maggior parte di questi problemi può essere risolta attraverso la configurazione appropriata delle impostazioni del prodotto.

Se non riesci a trovare il problema qui, o se la soluzione fornita non lo risolve, puoi contattare un operatore del supporto tecnico di Bitdefender come indicato nel capitolo «*Chiedere aiuto*» (p. 100).

14.1. 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?*» (p. 52).

- **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*» (p. 3).

- **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 un'applicazione sia essenziale per il sistema operativo, non rimuoverla e contatta il supporto clienti di Bitdefender.

- **Il tuo sistema potrebbe essere infetto**.

  La velocità del tuo sistema e le sue prestazioni generali possono essere anche influenzate dalle minacce. Spyware, malware, Trojan e adware contribuiscono a diminuire le prestazioni del dispositivo. Assicurati di controllare periodicamente il tuo sistema, almeno una volta alla settimana. Si consiglia di usare la Scansione completa di sistema di Bitdefender perché controlla tutti i tipi di minacce che mettono in pericolo la sicurezza del tuo sistema.

  Per avviare la scansione del sistema:

  1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
  2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
  3. Nella finestra **Scansioni**, clicca su **Esegui scansione** accanto a **Scansione di sistema**.
  4. Segui i passaggi della procedura guidata.

14.2. 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. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
    2. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
    3. Clicca su **REINSTALLA** nella finestra che comparirà.
    4. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.

  - 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 su **Programmi e funzionalità**.
    3. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
    4. Clicca su **REINSTALLA** nella finestra che comparirà.
    5. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.

  - In **Windows 10**:

    1. Clicca su **Start** e poi su Impostazioni.
    2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
    3. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
    4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
    5. Clicca su **REINSTALLA** nella finestra che comparirà.
    6. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.

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.

- **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?*» (p. 52).
  2. Reinstalla Bitdefender:
     - In **Windows 7**:
       a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
       b. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
       c. Clicca su **REINSTALLA** nella finestra che comparirà.
       d. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.
     - In **Windows 8 e Windows 8.1**:
       a. 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.
       b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
       c. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
       d. Clicca su **REINSTALLA** nella finestra che comparirà.
       e. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.
     - In **Windows 10**:
       a. Clicca su **Start** e poi su Impostazioni.
       b. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
       c. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.

d. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.

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

f. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.

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.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 100).

14.3. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.

2. Nel pannello **ADVANCED THREAT DEFENSE**, clicca su **Apri**.
3. Nella finestra **Impostazioni**, clicca su **Gestisci eccezioni**.
4. Clicca su **+Aggiungi un'eccezione**.
5. Inserisci il percorso dell'eseguibile che vuoi 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. Clicca su **Salva**.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 100).

14.4. Che 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 sicura filtrando tutto il traffico web e bloccando ogni contenuto potenzialmente dannoso. Tuttavia, è possibile che Bitdefender consideri un sito web, un dominio, un indirizzo IP o un'applicazione online attendibili come non sicuri, perciò la scansione del traffico HTTP di Bitdefender li bloccherà immediatamente.

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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **PREVENZIONE MINACCE ONLINE**, clicca su **Impostazioni**.
3. Clicca su **Gestisci eccezioni**.
4. Clicca su **+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. Clicca su **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 questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 100).

14.5. 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. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Aggiorna**.
3. Disattiva l'interruttore **Aggiornamento silenzioso**.
4. La prossima volta, quando sarà disponibile un aggiornamento, ti sarà chiesto di selezionare quale aggiornamento scaricare. Seleziona solo **Aggiornamento firme**.
5. Bitdefender scaricherà e installerà solo il database delle informazioni sulle minacce.

14.6. I servizi 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 di Bitdefender nell'area di notifica è grigia e una finestra ti informa 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?*» (p. 52).

Se l'errore persiste, contatta i nostri operatori del supporto tecnico per ricevere assistenza, come indicato nella sezione «*Chiedere aiuto*» (p. 100).

14.7. 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. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
  2. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
  3. Clicca su **RIMUOVI** nella finestra che comparirà.

4. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

- 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 su **Programmi e funzionalità**.
  3. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
  4. Clicca su **RIMUOVI** nella finestra che comparirà.
  5. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

- In **Windows 10**:

  1. Clicca su **Start** e poi su Impostazioni.
  2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
  3. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
  4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
  5. Clicca su **RIMUOVI** nella finestra che comparirà.
  6. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

14.8. 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 avevi Bitdefender e non l'hai disinstallato 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?*» (p. 54).
2. Rimuovi Bitdefender dal tuo sistema:
   - In **Windows 7**:
     a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
     b. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
     c. Clicca su **RIMUOVI** nella finestra che comparirà.
     d. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
     e. Riavvia il sistema in modalità normale.
   - In **Windows 8 e Windows 8.1**:
     a. 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.
     b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
     c. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
     d. Clicca su **RIMUOVI** nella finestra che comparirà.
     e. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
     f. Riavvia il sistema in modalità normale.
   - In **Windows 10**:
     a. Clicca su **Start** e poi su Impostazioni.
     b. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
     c. Trova **Bitdefender Antivirus Free** e seleziona **Disinstalla**.
     d. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
     e. Clicca su **RIMUOVI** nella finestra che comparirà.
     f. Attendi che il processo di disinstallazione sia completo e riavvia 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:

  1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a «*Come posso riavviare in modalità provvisoria?*» (p. 54).
  2. Rimuovi l'altra soluzione di sicurezza dal sistema:
     - In **Windows 7**:
       a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
       b. Trova il nome del programma che desideri rimuovere e seleziona **Rimuovi**.
       c. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
     - In **Windows 8 e Windows 8.1**:
       a. 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.
       b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
       c. Trova il nome del programma che desideri rimuovere e seleziona **Rimuovi**.
       d. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
     - In **Windows 10**:
       a. Clicca su **Start** e poi su Impostazioni.
       b. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
       c. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.

d. Attendi che il processo di disinstallazione sia completo e riavvia 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:

1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a «*Come posso riavviare in modalità provvisoria?*» (p. 54).
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 «*Chiedere aiuto*» (p. 100).

15. 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.

- ???
- «*Cosa fare quando Bitdefender trova delle minacce sul tuo dispositivo?*» (p. 93)
- «*Come posso rimuovere una minaccia in un archivio?*» (p. 95)
- «*Come posso rimuovere una minaccia in un archivio di e-mail?*» (p. 96)
- «*Cosa fare se sospetti che un file possa essere pericoloso?*» (p. 97)
- «*Quali sono i file protetti da password nel registro della scansione?*» (p. 97)
- «*Quali sono gli elementi ignorati nel registro della scansione?*» (p. 98)
- «*Quali sono i file supercompressi nel registro della scansione?*» (p. 98)
- «*Perché Bitdefender ha eliminato automaticamente un file infetto?*» (p. 98)

Se non riesci a trovare il problema qui, o se la soluzione fornita non lo risolve, puoi contattare un operatore del supporto tecnico di Bitdefender come indicato nel capitolo «*Chiedere aiuto*» (p. 100).

15.1. 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 il Servizio 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
   b. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
   c. Nella finestra **Avanzate**, disattiva **Protezione di Bitdefender**.
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a *«Come posso visualizzare gli elementi nascosti in Windows?»* (p. 52).
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 scoprire come fare, fai riferimento a *«Come posso riavviare in modalità provvisoria?»* (p. 54).
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a *«Come posso visualizzare gli elementi nascosti in Windows?»* (p. 52).
3. Trova l'ubicazione del file infetto (controlla il registro della scansione) ed eliminalo.
4. Riavvia il sistema ed entra in modalità normale.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 100).

15.2. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
   b. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
   c. Nella finestra **Avanzate**, disattiva **Protezione 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 questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 100).

15.3. 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. Controlla il database e-mail con Bitdefender.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
   b. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
   c. Nella finestra **Avanzate**, disattiva **Protezione 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.
   - Per Microsoft Outlook 2007: Nel menu File, clicca su Gestione file dati. Seleziona i file delle cartelle personali (.pst) che desideri compattare e clicca su Impostazioni. Clicca su Compatta.
   - Per Microsoft Outlook 2007 / 2013/ 2016: Nel menu File, clicca su Info e poi su Impostazioni account (Consente di aggiungere e rimuovere account o di modificare le impostazioni di connessione esistenti). Poi

clicca su File di dati, seleziona i file delle cartelle personali (.pst) che desideri compattare e clicca su Impostazioni. Clicca su Compatta.

6. Attiva la protezione antivirus in tempo reale di Bitdefender.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 100).

15.4. 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 del sistema** con Bitdefender. Per scoprire come fare, fai riferimento a «*Come posso eseguire una scansione del mio sistema?*» (p. 40).
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 «*Chiedere aiuto*» (p. 100).

15.5. 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.

15.6. 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.

15.7. 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.

15.8. 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 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.

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.

CONTACT US

16. CHIEDERE AIUTO

Bitdefender fornisce ai suoi clienti un supporto veloce e preciso assolutamente senza pari. Se dovessi riscontrare un problema o se avessi una qualche domanda relativa al tuo prodotto Bitdefender, puoi utilizzare una delle tante risorse online per trovare una soluzione o una risposta. Oppure, puoi contattare il Servizio clienti di Bitdefender. Gli operatori del nostro supporto risponderanno alle tue domande in modo tempestivo e ti forniranno l'assistenza necessaria.

La sezione «*Risolvere i problemi più comuni*» (p. 81) fornisce le informazioni necessarie sui problemi più frequenti che potresti incontrare usando questo prodotto.

Se non dovessi trovare la soluzione al tuo problema nelle risorse fornite, puoi contattarci direttamente:

- «Contattaci direttamente da Bitdefender Antivirus Free» (p. 100)
- «Contattaci tramite il nostro Centro di supporto online» (p. 101)

Contattaci direttamente da Bitdefender Antivirus Free

Se hai una connessione a Internet funzionante, puoi contattare Bitdefender per ricevere assistenza direttamente dall'interfaccia del prodotto.

Segui questi passaggi:

1. Clicca sul pulsante **Supporto**, rappresentato da un **punto di domanda** nella parte superiore dell'interfaccia di Bitdefender.
2. Hai le seguenti opzioni:
   - **MANUALE D'USO**

     Accedi al nostro database e cerca le informazioni necessarie.
   - **CENTRO DI SUPPORTO**

     Accedi ai nostri articoli e tutorial video online.
   - **ASK THE COMMUNITY**

     Click **ASK THE COMMUNITY** to access the Bitdefender community where you can get answers and guidance from other Bitdefender users.

Contattaci tramite il nostro Centro di supporto online

Se non puoi accedere alle informazioni necessarie usando il prodotto Bitdefender, fai riferimento al nostro Centro di supporto online:

1. Visitare https://www.bitdefender.it/support/consumer.html.

   Il Centro di supporto di Bitdefender include molti articoli che contengono soluzioni ai problemi inerenti Bitdefender.

2. Utilizza la barra di ricerca nella parte superiore della finestra per trovare gli articoli che possono fornire una soluzione al tuo problema. Per effettuare una ricerca, digita un termine nella barra di ricerca e clicca su **Cerca**.

3. Leggi gli articoli o i documenti rilevanti e prova le soluzioni proposte.

4. Se la soluzione non dovesse risolvere il tuo problema, vai a

   http://www.bitdefender.it/support/contact-us.htmle contatta gli operatori del nostro supporto tecnico.

17. 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/support/consumer.html

- Forum del supporto di Bitdefender:

  https://forum.bitdefender.com

- Il portale di sicurezza informatica HOTforSecurity:

  https://www.hotforsecurity.com

Puoi anche usare il tuo motore di ricerca preferito per trovare più informazioni sulla sicurezza del computer, i prodotti Bitdefender e la società.

17.1. 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 liberamente esplorabile. Le molte informazioni contenute sono un altro mezzo per fornire ai clienti di Bitdefender le conoscenze tecniche che gli servono. Tutte le richieste di informazioni o segnalazioni di bug dai clienti di Bitdefender arrivano al Centro di supporto di Bitdefender, così come segnalazioni e informazioni su bug risolti o articoli tecnici per integrare i file di supporto del prodotto.

Il Centro di supporto di Bitdefender è disponibile in qualsiasi momento su

https://www.bitdefender.it/support/consumer.html.

17.2. Forum supporto di Bitdefender

Il forum del supporto di Bitdefender fornisce agli utenti di Bitdefender un modo semplice per ottenere aiuto e aiutare gli altri.

Se il tuo prodotto Bitdefender non funziona bene e non riesce a rimuovere minacce specifici dal dispositivo o se hai qualche domanda sul suo funzionamento, pubblica il tuo problema o la tua domanda sul forum.

I tecnici del supporto di Bitdefender controllano le nuove discussioni sul forum per poterti assistere. Potresti ricevere una risposta o una soluzione anche da un utente di Bitdefender più esperto.

Prima di postare il tuo problema o la tua domanda, cerca nel forum un'eventuale discussione simile o collegata.

Il forum del supporto di Bitdefender è disponibile all'indirizzo https://forum.bitdefender.com in 5 lingue diverse: inglese, tedesco, francese, spagnolo e rumeno. Clicca sul link **Protezione Casa/Ufficio** per accedere alla sezione dedicata ai prodotti per utenti standard.

17.3. Portale HOTforSecurity

Il portale HOTforSecurity è una ricca fonte di informazioni sulla sicurezza informatica. Qui puoi apprendere le varie minacce a cui il dispositivo è esposto quando ti connetti a Internet (malware, phishing, spam, cyber-criminali).

Vengono pubblicati regolarmente nuovi articoli per mantenerti sempre aggiornato sulle ultime minacce scoperte oltre alle tendenze attuali in fatto di sicurezza e altre informazioni sulla protezione del computer.

La pagina web HOTforSecurity è raggiungibile all'indirizzo https://www.hotforsecurity.com.

18. CONTACT INFORMATION

Una comunicazione efficiente è la chiave di un business di successo. Dal 2001, BITDEFENDER ha acquisito una reputazione inestimabile superando le aspettative di clienti e partner, e sforzandosi costantemente per una comunicazione sempre più efficiente. Se hai delle domande o richieste, non esitare a contattarci.

18.1. Indirizzi web

Dipartimento vendite: sales@bitdefender.com
Centro di supporto:https://www.bitdefender.it/support/consumer.html
Documentazione: documentation@bitdefender.com
Distributori locali:http://www.bitdefender.it/partners
Programma partner: partners@bitdefender.com
Contatti stampa: pr@bitdefender.com
Lavoro: jobs@bitdefender.com
Invio minaccia: virus_submission@bitdefender.com
Invio spam: spam_submission@bitdefender.com
Segnala abuso: abuse@bitdefender.com
Sito web:https://www.bitdefender.it

18.2. 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. Visitare http://www.bitdefender.it/partners/partner-locator.html.
2. Seleziona il tuo paese e la tua città, utilizzando le opzioni corrispondenti.
3. Se non dovessi trovare un distributore di Bitdefender nel tuo paese, contattaci via email all'indirizzo sales@bitdefender.com. Scrivi la tua e-mail in inglese per permetterci di assisterti prontamente.

18.3. Uffici di Bitdefender

Gli uffici di Bitdefender sono sempre pronti a rispondere a ogni richiesta inerente le loro competenze, sia in ambito commerciale sia generale. I loro rispettivi indirizzi e contatti sono elencati sotto.

USA

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefono (ufficio e vendite): 1-954-776-6262
Vendite: sales@bitdefender.com
Supporto tecnico: https://www.bitdefender.com/support/consumer.html
Web: https://www.bitdefender.com

Regno Unito e Irlanda

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
Email: info@bitdefender.co.uk
Phone: (+44) 2036 080 456
Vendite: sales@bitdefender.co.uk
Supporto tecnico: https://www.bitdefender.co.uk/support/
Web: https://www.bitdefender.co.uk

Germania

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Ufficio: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Vendite: vertrieb@bitdefender.de
Supporto tecnico: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

Danimarca

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Ufficio: +45 7020 2282
Supporto tecnico: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

Spagna

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Phone: +34 902 19 07 65
Vendite: comercial@bitdefender.es
Supporto tecnico: https://www.bitdefender.es/support/consumer.html
Sito web: https://www.bitdefender.es

Romania

BITDEFENDER SRL
Orhideea Towers Building, 15A Orhideelor Street, 11th fllor, district 6
Bucharest
Fax: +40 21 2641799
Telefono vendite: +40 21 2063470
E-mail vendite: sales@bitdefender.ro
Supporto tecnico: https://www.bitdefender.ro/support/consumer.html
Sito web: https://www.bitdefender.ro

Emirati Arabi Uniti

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefono vendite: 00971-4-4588935 / 00971-4-4589186
E-mail vendite: mena-sales@bitdefender.com
Supporto tecnico: https://www.bitdefender.com/support/consumer.html
Sito web: https://www.bitdefender.com

Glossario

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.

ActiveX

ActiveX è una tecnologia per lo sviluppo di programmi che possano essere richiamati da altri programmi e sistemi operativi. La tecnologia ActiveX è utilizzata in Microsoft Internet Explorer per generare pagine web interattive che appaiano e si comportino come applicazioni invece che come pagine statiche. Con ActiveX, gli utenti possono chiedere o rispondere a domande, adoperare pulsanti e interagire in altri modi con la pagina web. I controlli ActiveX sono spesso scritti utilizzando il linguaggio Visual Basic.

Gli ActiveX sono noti per una totale mancanza di controlli di sicurezza; gli esperti di sicurezza dei computer scoraggiano il loro utilizzo attraverso Internet.

Adware

La modalità adware è spesso combinata con un'applicazione che viene fornita gratuitamente se l'utente accetta l'adware. Considerando che le applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove viene spiegato il proposito dell'applicazione, non viene commessa alcuna infrazione.

Comunque, le finestre pop-up di avvertimento possono essere fastidiose e in alcuni casi ridurre le prestazioni del sistema. Inoltre, le informazioni che vengono raccolte da alcune di queste applicazioni possono causare inconvenienti riguardo la privacy degli utenti, non sempre completamente informati sui termini dell'accordo di licenza.

Aggiornamento

Una nuova versione di un prodotto software o hardware creato per sostituire la versione precedente. 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.

Aggiornamento informazioni minacce

Lo schema binario di una minaccia, usato dalla soluzione di sicurezza per rilevare ed eliminare la minaccia.

Applet Java

Un programma Java concepito per funzionare solo su pagine web. Per utilizzare un applet su una pagina web, bisogna specificare il nome dell'applet e la dimensione (lunghezza e larghezza in pixel) che può utilizzare. Quando si accede alla pagina web, il browser scarica l'applet dal server e lo esegue sulla macchina dell'utente (il client). Gli applet differiscono dalle applicazioni in quanto sono governati da un rigido protocollo di sicurezza.

Ad esempio, anche se gli applet vengono lanciati sul client, non possono leggere o scrivere dati nella macchina dell'utente. Inoltre, gli applet sono ulteriormente limitati in modo che possano leggere e scrivere dati solo dallo stesso dominio dai quali provengono.

Archivio

Un Disco, un nastro o una cartella che contiene file memorizzati.

Un file che contiene uno o più file in forma compressa.

Area di notifica

Introdotta con Windows 95, l'area di notifica 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 ai dettagli e i controlli.

Attacco a dizionario

Gli attacchi per indovinare le password in genere penetrano in un sistema informatico inserendo una combinazione di parole comuni per generare potenziali password. Lo stesso metodo viene usato per indovinare chiavi

di decifrazione per messaggi o documenti cifrati. Gli attacchi a dizionario riescono perché molte persone tendono a scegliere password brevi o composte da poche parole, che sono piuttosto facili da indovinare.

Attacco di forza bruta

Gli attacchi per indovinare le password in genere penetrano in un sistema informatico inserendo diverse possibili combinazioni di password, iniziando principalmente dalle più facili da indovinare.

Backdoor

Una breccia nella sicurezza di un sistema deliberatamente lasciata dal programmatore o dal manutentore. La presenza di tali “brecce” non sempre è dolosa: su alcuni sistemi operativi, ad esempio, vengono utilizzate per l’accesso con utenze privilegiate per servizi tecnici o per i programmatori del produttore a scopo di manutenzione.

Boot sector

Un settore all’inizio di ogni disco che ne identifica l’architettura (dimensione del settore, dimensione del cluster, ecc.). Nei dischi di avvio, il settore di boot contiene anche un programma che carica il sistema operativo.

Botnet

Il termine "botnet" è composto dalle parole "robot" e "network". I botnet sono dispositivi connessi a Internet e infettati con minacce, che possono essere utilizzati per inviare e-mail spam, sottrarre dati, controllare in remoto dispositivi vulnerabili o diffondere spyware, ransomware e altri tipi di minacce. Il loro obiettivo è infettare il maggior numero di dispositivi connessi possibile, come PC, server, dispositivi mobile o IoT che appartengono a grandi organizzazioni o aziende.

Browser

Abbreviazione di browser web, un'applicazione software utilizzata per localizzare e visualizzare pagine web. I browser più diffusi sono Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Questi sono browser grafici, ovvero in grado di visualizzare sia elementi grafici che il testo. Inoltre, i browser più moderni possono presentare informazioni multimediali, inclusi suoni e animazioni, anche se per alcuni formati, richiedono dei plug-in.

Client mail

Un client e-mail è un'applicazione che ti consente di inviare e ricevere e-mail.

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.

Cookie

Nell'industria di Internet, i cookie vengono descritti come piccoli file contenenti informazioni relative ai computer individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia di interessi e gusti online degli utenti. In questo settore, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire offerte pubblicitarie personalizzate in base agli interessi degli utenti. Per molte persone è una lama a doppio taglio, poiché da una parte è efficace e consente di far vedere solo ciò che viene dichiarato interessante. Ma dall'altra, implica in effetti un "tracciamento" di dove si va e di cosa si seleziona. In considerazione di questo è in atto un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come un "codice SKU" (il codice a barre sul retro delle confezioni che viene letto dalle casse). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

Cyberbullismo

Quando compagni o estranei commettono abusi nei confronti di bambini intenzionati a ferirli fisicamente. Per ferire a livello emotivo, gli aggressori inviano messaggi meschini o fotografie poco lusinghiere, cercando di isolare le proprie vittime dagli altri o farle sentire frustrate.

E-mail

Posta elettronica. Un servizio che invia messaggi ai computer attraverso reti locali o globali.

Elementi 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.

Estensione del nome di un file

Porzione del nome di un file che segue il punto finale e che indica il tipo di dati inclusi nel file.

Molti sistemi operativi utilizzano estensioni di file, come Unix, VMS e MS-DOS. Sono normalmente composti da una a tre lettere (alcuni vecchi sistemi operativi non ne supportano più di tre). Esempi: "c" per codici sorgente C, "ps" per PostScript, "txt" per testi semplici.

Euristico

Un metodo basato su regole per l'identificazione di nuove minacce. Questo metodo di scansione non si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione euristica è di non essere ingannata dalle nuove varianti di minacce esistenti. Tuttavia, può occasionalmente segnalare una parte di codice sospetto in programmi normali, generando i cosiddetti "falsi positivi".

Eventi

Un'azione oppure un evento segnalato da un programma. Gli eventi possono essere azioni dell'utente, come cliccare con il mouse o premere un tasto sulla tastiera, oppure del 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 prendere il controllo di computer e reti.

Falso positivo

Appare quando un prodotto di analisi antivirus individua un documento come infettato quando di fatto non lo è.

File di rapporto

Un file che elenca le azioni avvenute. Bitdefender crea un rapporto che elenca i percorsi controllati, le cartelle, il numero di archivi e file esaminati, oltre a quanti file infetti e sospetti sono stati trovati.

Honeypot

Un sistema trappola usato per attirare i pirati informatici in modo da studiare come agiscono e identificare i metodi che utilizzano per ottenere informazioni sul sistema. Aziende e organizzazioni sono sempre più interessate a implementare e utilizzare gli honeypot per migliorare il loro stato di sicurezza generale.

IP

Internet Protocol – protocollo di instradamento nella suite di protocollo TCP/IP, responsabile dell'indirizzamento IP, dell'instradamento, della frammentazione e della ricomposizione dei pacchetti IP.

Keylogger

Un keylogger è una app che registra ogni cosa che digiti.

I keylogger non sono dannosi di natura. Possono essere usati anche per scopi legittimi, come monitorare le attività di dipendenti o bambini. Tuttavia, sono utilizzati anche dai criminali informatici per scopi dannosi (per esempio, ottenere dati personali, come credenziali o codici di accesso).

Linea di comando

In un'interfaccia a linea di comando, l'utente digita i comandi nello spazio previsto direttamente sullo schermo, utilizzando il linguaggio di comando.

Macro virus

Un tipo di minaccia informatica, codificata come macro all'interno di un documento. Molte applicazioni, come ad esempio Microsoft Word ed Excel, supportano potenti linguaggi macro.

Queste applicazioni consentono di codificare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Memoria

Aree di archiviazione interne al computer. Il termine memoria identifica la memorizzazione dei dati sotto forma di chip, mentre la parola archiviazione viene utilizzata per la memoria su nastri o dischi. Ogni

computer dispone di un certo quantitativo di memoria fisica, solitamente chiamata memoria principale oppure RAM.

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.

Minaccia avanzata persistente

Una minaccia avanzata persistente (in inglese, Advanced Persistent Threat o APT) sfrutta le vulnerabilità dei sistemi per sottrarre informazioni importanti e inviarle alla fonte. Questa minaccia prende di mira alcuni grandi gruppi, come organizzazioni, società o governi.

L'obiettivo di una minaccia persistente avanzata è restare nascosta per molto tempo, in modo da monitorare e raccogliere informazioni importanti, senza danneggiare i computer colpiti. Il metodo utilizzato per inserire la minaccia nella rete è tramite un file PDF o un documento Office, in apparenza innocuo, in modo che ogni utente lo utilizzi senza problemi.

Non euristico

Questo metodo di scansione si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione non-euristica è di non essere ingannata da ciò che potrebbe sembrare una minaccia, e quindi non genera falsi allarmi.

Pacchetti di programmi

Un file in un formato compresso. Molti sistemi operativi e molte applicazioni contengono comandi che vi consentono di compattare un file in modo da occupare meno memoria. Ad esempio, supponiamo di avere un file di testo che contenga dieci caratteri spazio consecutivi. Normalmente occuperebbe dieci byte di memoria.

Un programma che compatta i file potrebbe sostituire gli spazi dei caratteri con un carattere speciale seguito dal numero di spazi sostituiti. In questo caso i dieci spazi occuperebbero solo due byte. Questa è solo una tecnica di compattazione, ma ce ne sono molte altre.

Percorso

I percorsi esatti per raggiungere un file su un computer. Questi percorsi vengono solitamente descritti attraverso il file system gerarchico dall'alto verso il basso.

La strada tra due punti qualsiasi, come ad esempio il canale di comunicazioni tra due computer.

Phishing

L'atto d'inviare un'e-mail a un utente fingendo di essere una società legittima e affermata, nel tentativo di truffarlo, facendogli cedere informazioni private che saranno usate per furti d'identità. L'e-mail invita gli utenti a visitare una pagina web, dove gli sarà chiesto di aggiornare determinate informazioni personali, come password e numero di carta di credito, codice fiscale o coordinate bancarie. In ogni caso, la pagina web è falsa e creata solo per rubare i dati personali dell'utente.

Photon

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.

Porta

Un'interfaccia su un computer dalla quale è possibile connettere un dispositivo. I personal computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, monitor e tastiere. Esternamente i personal computer 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 ne identifica il tipo. Ad esempio, la porta 80 viene usata per il traffico HTTP.

Predatori online

Individui che cercano di attirare minori o adolescenti in conversazioni per coinvolgerli in attività sessuali illegali. I social network sono il luogo ideale in cui è possibile predare e sedurre minori vulnerabili per coinvolgerli in attività sessuali, online o di persona.

Ransomware

Un Ransomware è un programma dannoso che cerca di sottrarre denaro agli utenti, bloccando i loro sistemi vulnerabili. CryptoLocker, CryptoWall e TeslaWall sono solo alcune delle varianti in grado di violare 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.

Rete privata virtuale (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.

Rootkit

Un rootkit è una serie di strumenti software che consente di accedere a un sistema come amministratore. 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 essere visti dagli amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, gli accessi e i registri. Se incorporano il software adeguato, possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche.

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.

Scarica

Per copiare dati (solitamente un file intero) da una fonte principale su un dispositivo periferico. Il termine viene spesso utilizzato per descrivere un processo di copia di un documento da un servizio online al computer di un utente. Si può inoltre riferire al processo di copiatura di un file da un file server di rete a un computer della rete.

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 conosciuto come e-mail non desiderate.

Spyware

Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessone 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.

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.

Trojan

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 da una storia dell'Iliade di Omero, in cui 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, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

Unità disco

È un dispositivo che legge e scrive dei dati su un disco.

Un drive di disco rigido legge e scrive dischi rigidi.

Un drive di floppy accede i dischi floppy.

Le unità disco possono essere interne (incorporate all'interno di un computer) oppure esterne (collocate in un meccanismo separato e connesso al computer).

Virus di boot

Una minaccia che infetta il settore di avvio di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infettato con un virus di boot, farà sì che la minaccia venga attivata nella memoria. Da quel momento in poi, ogni volta che si esegue il boot del sistema, la minaccia sarà attiva nella memoria.

Virus polimorfico

Una minaccia che modifica la propria forma con ogni file che infetta. Non avendo caratteristiche binarie costanti, queste minacce sono difficili da identificare.

Worm

Un programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.