GUIDA DELL'UTENTE

Bitdefender CONSUMER SOLUTIONS

Antivirus Plus

Bitdefender Antivirus Plus

Guida dell'utente

Data di pubblicazione 04/12/2023
Diritto d'autore © 2023 Bitdefender

Avviso legale

Tutti i diritti riservati. Nessuna parte di questo libro può essere riprodotta o trasmessa in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, incluse fotocopie, registrazioni o qualsiasi sistema di memorizzazione e recupero di informazioni, senza il permesso scritto di un rappresentante autorizzato di Bitdefender. L'inserimento di brevi citazioni nelle recensioni può essere possibile solo con la menzione della fonte citata. Il contenuto non può essere modificato in alcun modo.

Avviso e dichiarazione di non responsabilità. Questo prodotto e la relativa documentazione sono protetti da copyright. Le informazioni contenute in questo documento sono fornite "così come sono", senza garanzia. Sebbene ogni precauzione sia stata presa nella preparazione di questo documento, gli autori non avranno alcuna responsabilità nei confronti di alcuna persona o entità rispetto a qualsiasi perdita o danno causato o presumibilmente causato direttamente o indirettamente dalle informazioni contenute in questo lavoro.

Questo libro contiene collegamenti a siti Web di terze parti che non sono sotto il controllo di Bitdefender, pertanto Bitdefender non è responsabile del contenuto di alcun sito collegato. Se accedi a un sito Web di terze parti elencato in questo documento, lo farai a tuo rischio. Bitdefender fornisce questi collegamenti solo per comodità e l'inclusione del collegamento non implica che Bitdefender approvi o accetti alcuna responsabilità per il contenuto del sito di terze parti.

Marchi. I nomi dei marchi possono apparire in questo libro. Tutti i marchi registrati e non registrati in questo documento sono di esclusiva proprietà dei rispettivi proprietari e sono rispettosamente riconosciuti.

Bitdefender

Indice

INFORMAZIONI SU QUESTA GUIDA

Scopo e pubblico previsto

Questa guida è destinata a tutti gli utenti Windows che hanno scelto Bitdefender Antivirus Plus come soluzione di sicurezza per i propri computer. Le informazioni presentate in questo libro sono adatte non solo agli esperti di computer, ma sono accessibili a tutti coloro che sono in grado di lavorare con un PC Windows.

Scoprirai come configurare e utilizzare Bitdefender Antivirus Plus per proteggersi da minacce e altri software dannosi. Imparerai come ottenere il meglio dal tuo Bitdefender.

Vi auguriamo una lezione piacevole e utile.

Come usare questa guida

Questa guida è organizzata attorno a diversi argomenti principali:

Come iniziare (pagina 15)

Inizia con Bitdefender Antivirus Plus e la sua interfaccia utente.

Gestire la tua sicurezza (pagina 36)

Scopri come usare Bitdefender Antivirus Plus per proteggerti dai software dannosi.

Come fare (pagina 90)

Scopri di più su Bitdefender Antivirus Plus.

Ottenere aiuto (pagina 137)

Dove cercare e dove chiedere aiuto se appare qualcosa di inaspettato.

Convenzioni usate in questo manuale

Convenzioni tipografiche

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

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

Avvertenze

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

Nota

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

Importante

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

Avvertimento

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

Richiesta di commenti

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

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

1. INSTALLAZIONE

1.1. Prepararsi all'installazione

Prima di Bitdefender Antivirus Plusinstallare , completa questi passaggi preliminari per assicurarti che l'installazione funzioni senza problemi:

- Assicurati che il dispositivo su cui desideri installare Bitdefender soddisfi i requisiti di sistema. Se il dispositivo non soddisfa tutti i requisiti di sistema, Bitdefender non sarà installato, o, nel caso venisse installato, non funzionerà correttamente e causerà rallentamenti e instabilità. Per un elenco completo dei requisiti di sistema, consultare la sezione Requisiti di sistema (pagina 4).
- Accedi al dispositivo utilizzando un account Amministratore.
- Rimuovi qualsiasi altro programma simile dal dispositivo. Se dovesse rilevarne uno durante l'installazione di Bitdefender, ti sarà chiesto di disinstallarlo. L'esecuzione simultanea di due programmi di sicurezza può influenzarne il funzionamento e causare problemi seri al sistema. Durante l'installazione Windows Defender sarà disattivato.
- Disabilita o rimuovi qualsiasi programma firewall che possa essere in esecuzione sul dispositivo. L'esecuzione simultanea di due programmi firewall può influenzarne il funzionamento e causare problemi seri al sistema. Durante l'installazione il firewall di Windows sarà disattivato.
- Assicurati che il dispositivo sia connesso a Internet durante l'installazione, anche se l'hai avviata da un CD/DVD. Se sono disponibili versioni più recenti dei file dell'applicazione inclusi nel pacchetto d'installazione, Bitdefender può scaricarli e installarli.

1.2. Requisiti di sistema

Puoi installare Bitdefender Antivirus Plus solo su dispositivi con i seguenti sistemi operativi:

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

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

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

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

1.3. Requisiti software

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

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

1.4. Installare il tuo prodotto Bitdefender

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

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

1.4.1. Installare da Bitdefender Central

Da Bitdefender Central puoi scaricare il kit d'installazione corrispondente all'abbonamento acquistato. Una volta completato il processo d'installazione, Bitdefender Antivirus Plus viene attivato.

Per scaricare Bitdefender Antivirus Plus da Bitdefender Central:

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

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

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

Convalidare l'installazione

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

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

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

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

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

Una volta confermata l'installazione, compare la procedura guidata di configurazione. Segui i passaggi indicati per installare Bitdefender Antivirus Plus.

Fase 1 - Installazione di Bitdefender

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

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

In questa fase possono essere eseguite due attività aggiuntive:

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

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

Fase 2 - Installazione in corso

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

Fase 3 - Fine dell'installazione

Il tuo prodotto Bitdefender è stato installato con successo.

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

Fase 4 - Analisi del dispositivo

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

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

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

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

Fase 5 - Come iniziare

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

Clicca su **TERMINA** per accedere all'interfaccia di Bitdefender Antivirus Plus.

1.4.2. Installa dal disco di installazione

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

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

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

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

Convalidare l'installazione

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

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

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

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

Nota

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

Una volta confermata l'installazione, compare la procedura guidata di configurazione. Segui i passaggi indicati per installare Bitdefender Antivirus Plus.

Fase 1 - Installazione di Bitdefender

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

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

In questa fase è possibile eseguire due attività aggiuntive:

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

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

Passaggio 2: installazione in corso

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

Passaggio 3: installazione completata

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

Passaggio 4: analisi del dispositivo

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

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

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

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

Fase 5 - Account di Bitdefender

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

Procedi in base alla tua situazione.

- **Voglio creare un account Bitdefender**

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

Nota

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

- **Ho già un account Bitdefender**

  1. Clicca su **Accedi**.
  2. Inserisci l'indirizzo e-mail nel campo corrispondente e clicca su **AVANTI**.
  3. Inserisci la tua password e clicca su **ACCEDI**.
     Se hai dimenticato la password per il tuo account o vuoi semplicemente modificare quella già impostata:
     a. Clicca su **Hai dimenticato la password?**.
     b. Inserisci il tuo indirizzo e-mail e clicca su **AVANTI**.
     c. Controlla la tua casella di posta, inserisci il codice di sicurezza che hai ricevuto e clicca su **AVANTI**.
     In alternativa, puoi cliccare su **Cambia password** nella e-mail che ti abbiamo inviato.
     d. Digita la nuova password che vuoi impostare e inseriscila nuovamente. Clicca su **SALVA**.

     Nota

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

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

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

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

Fase 6 - Attiva il prodotto

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

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

Procedi secondo la tua situazione:

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

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

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

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

Fase 7 - Come iniziare

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

Clic **FINE** per accedere al Bitdefender Antivirus Plus interfaccia.

2. COME INIZIARE

2.1. Le basi

Una volta installato Bitdefender Antivirus Plus, il tuo dispositivo sarà protetto da ogni tipo di minaccia (come malware, spyware, ransomware, exploit, botnet e Trojan) e minacce web (come hacker, phishing e spam).

L'applicazione utilizza la tecnologia Photon per migliorare la velocità e le prestazioni del processo di scansione delle minacce. Funziona apprendendo i modelli di utilizzo delle applicazioni del sistema per sapere quando avviare la scansione e cosa esaminare, minimizzando l'impatto sulle prestazioni del sistema.

Protezione webcam Impedisce alle app non affidabili di accedere alla tua videocamera, bloccando così ogni tentativo di prenderne il controllo. In base alle scelte degli utenti di Bitdefender, l'accesso delle app più popolari alla tua webcam sarà consentito o bloccato.

Per proteggerti da potenziali occhi indiscreti, quando il dispositivo è connesso a una rete wireless non protetta, Bitdefender analizza il suo livello di sicurezza e, se necessario, fornisce suggerimenti per aumentare la sicurezza delle tue attività online. Per maggiori istruzioni su come proteggere i tuoi dati personali, fai riferimento al Wi-Fi Security Advisor (pagina 64).

Ora i file cifrati dai ransomware possono essere ripristinati senza dover spendere il denaro del riscatto. Per maggiori informazioni su come ripristinare i dati cifrati, fai riferimento a Risanamento da ransomware (pagina 68).

Mentre lavori, usi un videogioco o guardi un film, Bitdefender può offrirti un'esperienza continuativa, posticipando eventuali attività di manutenzione, eliminando ogni interruzione e regolando gli effetti visivi del sistema. Puoi beneficiare di tutte queste opzioni, attivando e configurando i Profili (pagina 82).

Bitdefender prenderà la maggior parte delle decisioni in materia di sicurezza per conto tuo, mostrandoti raramente delle finestre pop-up di avviso. Nella finestra Notifiche sono disponibili maggiori dettagli sulle azioni intraprese e sulle operazioni dei programmi. Per maggiori informazioni, fai riferimento a Notifiche (pagina 16).

Di tanto in tanto, dovresti aprire Bitdefender e risolvere i problemi esistenti. Devi configurare le componenti di Bitdefender o prendere azioni preventive per proteggere i tuoi dispositivo e i tuoi dati.

Per utilizzare le funzioni online di Bitdefender Antivirus Plus e gestire i tuoi abbonamenti e dispositivi, accedi al tuo account Bitdefender. Per maggiori informazioni, fai riferimento a Bitdefender Central.

Nella sezione Come fare (pagina 90) troverai le istruzioni passo passo su come eseguire le attività più comuni. Se dovessi riscontrare problemi mentre utilizzi Bitdefender, consulta la sezione Risolvere i problemi più comuni (pagina 118) per trovare possibili soluzioni ai problemi più comuni.

2.1.1. Notifiche

Bitdefender conserva un registro dettagliato di eventi riguardanti le sue attività sul dispositivo. Ogni volta che si verifica un evento rilevante per la sicurezza del sistema o dei dati, viene aggiunto un nuovo messaggio nelle Notifiche di Bitdefender, in modo simile a quando ricevi un nuovo messaggio nella casella di posta.

Le notifiche sono uno strumento molto importante per monitorare e gestire la tua protezione di Bitdefender. Per esempio, puoi controllare facilmente se l'aggiornamento è stato eseguito con successo, se sono state rilevate minacce o vulnerabilità sul dispositivo, ecc. In aggiunta, se necessario, puoi intraprendere ulteriori azioni o modificare le azioni intraprese da Bitdefender.

Per accedere al registro delle **Notifiche**, clicca su Notifiche nel menu di navigazione dell'**interfaccia di Bitdefender**. Ogni volta che si verifica un evento critico, sull'icona 2 compare un contatore.

In base al tipo e alla gravità, le notifiche sono suddivise in:

- Gli eventi **critici** indicano problemi importanti. Dovresti controllarli subito.
- Gli **Avvisi** indicano problemi non critici. Quando hai tempo, dovresti controllarli e risolverli.
- Gli eventi **informazione** indicano operazioni avvenute con successo.

Clicca su ogni scheda per scoprire maggiori dettagli sugli eventi generati. Cliccando una sola volta su ciascun titolo di un evento, vengono mostrati alcuni dettagli: una breve descrizione, l'azione intrapresa da Bitdefender

quando è successo e la data e l'ora in cui si è verificato. Se necessario, possono essere fornite opzioni per intraprendere ulteriori azioni.

Per aiutarti a gestire facilmente gli eventi registrati, la finestra delle notifiche offre opzioni per eliminare o segnare come letti tutti gli eventi in quella sezione.

2.1.2. Profili

Alcune attività del computer, come giochi online o presentazioni video, richiedono una maggiore prontezza del sistema, prestazioni più elevate e nessuna interruzione. Quando il portatile funziona a batterie, si consiglia di rimandare eventuali operazioni superflue, che consumano energia aggiuntiva, fino a quando il portatile non sarà connesso all'alimentazione CA.

I Profili di Bitdefender assegnano più risorse di sistema alle app in esecuzione, modificando temporaneamente le impostazioni di protezione e cambiando la configurazione del sistema. Di conseguenza, l'impatto del sistema sulle tue attività viene minimizzato.

Per adattarsi alle diverse attività, Bitdefender offre i seguenti profili:

Profilo Lavoro

Ottimizza la tua efficienza lavorativa identificando e modificando le impostazioni del prodotto e del sistema.

Profilo Film

Migliora gli effetti visivi ed elimina le interruzioni durante la visione di film.

Profilo Gioco

Migliora gli effetti visivi ed elimina le interruzioni durante l'uso di videogiochi.

Profilo Wi-Fi pubblico

Vengono applicate le impostazioni del prodotto per usufruire di una protezione totale mentre si è connessi a una rete wireless non sicura.

Profilo Modalità Batteria

Vengono applicate le impostazioni del prodotto, bloccando ogni attività in background per risparmiare il consumo della batteria.

Configura l'attivazione automatica dei profili

Per un'esperienza più intuitiva, puoi configurare Bitdefender per gestire i tuoi profili operativi. In questo caso, Bitdefender rileva automaticamente l'attività eseguita e applica le impostazioni di ottimizzazione del sistema e del prodotto.

La prima volta che accedi ai **Profili** ti sarà chiesto di attivare i profili automatici. Per farlo, clicca semplicemente su **ATTIVA** nella finestra visualizzata.

Puoi cliccare su **NON ORA** se desideri attivare la funzionalità in un secondo momento.

Per consentire a Bitdefender di attivare i profili automaticamente:

1. Clicca su **Utility** nel menu di navigazione nell'**interfaccia di Bitdefender**.
2. Nella scheda **Profili**, clicca su **Impostazioni**.
3. Usa l'interruttore corrispondente per attivare **Attiva i profili automaticamente**.

Se non desideri che i Profili siano attivati automaticamente, disattiva l'interruttore.

Per attivare manualmente un profilo, attiva l'interruttore corrispondente. Dei primi tre profili, solo uno alla volta può essere attivato manualmente.

Per maggiori informazioni sui Profili, fai riferimento a Profili (pagina 82).

2.1.3. Impostazioni protette da password di Bitdefender

Se non sei l'unica persona a utilizzare questo dispositivo, ti consigliamo di proteggere le tue impostazioni di Bitdefender con una password.

Per configurare la protezione password per le impostazioni di Bitdefender:

1. Clicca su **Impostazioni** nel menu di navigazione nell'**interfaccia di Bitdefender**.
2. Nella finestra **Generali**, attiva **Protezione password**.
3. Inserisci la password nei due campi e poi clicca su OK. La password deve essere composta da almeno 8 caratteri.

Una volta impostata una password, chiunque cerchi di cambiare le impostazioni di Bitdefender dovrà prima inserirla.

Importante
Assicurati di non dimenticare la tua password o conservane una copia in un luogo sicuro. Se hai dimenticato la password, dovrai reinstallare il programma o contattare il supporto di Bitdefender.

Per rimuovere la protezione della password:

1. Clic **Impostazioni** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nella finestra **Generali**, disattiva **Protezione password**.
3. Inserisci la password e clicca su **OK**.

Nota
Per modificare la password del tuo prodotto, clicca su **Modifica password**. Digita la tua password attuale e clicca su **OK**. Nella nuova finestra che comparirà, digita la nuova password che vuoi utilizzare d'ora in poi per limitare l'accesso alle tue impostazioni di Bitdefender.

2.1.4. Rapporti prodotto

I rapporti sul prodotto contengono informazioni su come utilizzi il prodotto Bitdefender che hai installato. Queste informazioni sono essenziali per migliorare il prodotto e possono aiutarci a offrire una migliore esperienza in futuro.

Nota che i rapporti non includono dati confidenziali, come nome o indirizzo IP, e non saranno utilizzati per scopi commerciali.

Se durante la fase di installazione, hai scelto di inviare tali rapporti ai server di Bitdefender e ora vuoi interrompere tale processo:

1. Clic **Impostazioni** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Seleziona la scheda **Avanzate**.
3. Disattiva **Rapporti prodotto**.

2.1.5. Notifiche offerte speciali

Quando sono disponibili eventuali offerte promozionali, Bitdefender è configurato per avvisarti attraverso una finestra pop-up. Ciò ti darà l'opportunità di usufruire di prezzi vantaggiosi e mantenere protetti i tuoi dispositivi per un periodo di tempo maggiore.

Per attivare o disattivare le notifiche sulle offerte speciali:

1. Clic **Impostazioni** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nella finestra **Generale**, attiva o disattiva l'interruttore corrispondente.

Di norma, l'opzione offerte speciali e notifiche sul prodotto è attivata.

2.2. Interfaccia di Bitdefender

Bitdefender Antivirus Plus 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.

2.2.1. Icona area di notifica

Per gestire l'intero prodotto più velocemente, puoi utilizzare l'icona Bitdefender nella barra delle applicazioni.

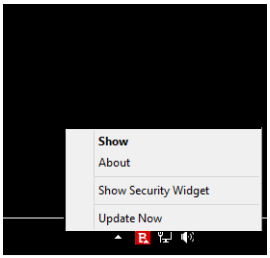
Nota

L'icona Bitdefender potrebbe non essere sempre visibile. Per farla comparire in maniera 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 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 **agente di Bitdefender**.

Se si clicca due volte su questa icona, si aprirà Bitdefender. Inoltre, cliccando con il pulsante destro sull'icona, apparirà un menu contestuale che consentirà di gestire rapidamente il prodotto Bitdefender.

- **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.
- **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 funziona, l'icona nella barra delle applicazioni compare su uno sfondo grigio: . In genere, ciò si verifica quando l'abbonamento è scaduto. Può anche verificarsi quando i servizi di Bitdefender non stanno rispondendo o quando altri errori influenzano il normale funzionamento di Bitdefender.

2.2.2. 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 alle modalità d'uso, eseguire azioni rapide e installare Bitdefender su altri dispositivi.
- **Protezione**. Da qui, potrai lanciare e configurare scansioni antivirus, accedere alle impostazioni del firewall, ripristinare i dati nel caso venissero cifrati da un ransomware e configurare la protezione mentre si naviga su Internet.
- **Privacy**. Da qui, puoi creare gestori di password per i tuoi account online, proteggere l'accesso alla tua webcam da occhi indiscreti, effettuare pagamenti online in un ambiente sicuro, aprire la app VPN e proteggere i tuoi bambini visualizzando e limitando le loro attività online.
- **Utility**. Da qui, puoi migliorare la velocità del sistema e configurare la funzionalità Anti-theft per i tuoi dispositivi.
- **Notifiche**. Da qui, puoi accedere alle notifiche già generate.

- **Settings**. Da qui, puoi accedere alle impostazioni generali.
- **Supporto**. Da qui, ogni volta che hai bisogno di assistenza per risolvere un problema con Bitdefender Antivirus Plus, puoi contattare il supporto tecnico 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.

2.2.3. 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:

Zona dello 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

Qui è dove puoi eseguire diverse attività per mantenere protetto il sistema e mantenerlo alla velocità ottimale. Puoi anche installare Bitdefender su altri dispositivi, sempre che il tuo abbonamento abbia abbastanza slot disponibili.

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 della **barra delle applicazioni** 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.

Autopilot

Per garantirti un funzionamento efficace e una maggiore protezione mentre esegui diverse attività, Bitdefender Autopilot agirà come tuo consulente di sicurezza personale. In base alle attività eseguite, sia che tu stia lavorando, effettuando pagamenti online, guardando un film o giocando a un videogioco, Bitdefender Autopilot ti fornirà suggerimenti contestuali basati sull'uso e le esigenze del tuo 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. Clic **Impostazioni** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nella finestra **Generali**, disattiva **Notifiche suggerimenti**.

Azioni rapide

Usando le azioni rapide puoi lanciare rapidamente attività che consideri importanti per mantenere protetto il tuo sistema e usarlo alla velocità ottimale.

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 individuare tempestivamente possibili minacce eventualmente presenti sul tuo dispositivo.
- **Scansione sistema**. Esegui una scansione di sistema per assicurarti che il dispositivo sia privo di minacce.
- **Scansione vulnerabilità**. Esegui una scansione del dispositivo alla ricerca di vulnerabilità per assicurarti che tutte le app installate, incluso il sistema operativo, siano aggiornate e funzionino correttamente.
- **Wi-Fi Security Advisor**. Apri la finestra di Wi-Fi Security Advisor nel modulo Vulnerabilità.
- **Apri Safepay**. Apri Bitdefender Safepay™ per proteggere i tuoi dati sensibili durante l'elaborazione delle transazioni online.
- **Distruttore di file**. Esegui lo strumento Distruttore di file per rimuovere ogni traccia di dati sensibili dal tuo dispositivo.

2.2.4. Le soluzioni 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**

Protezione

Nella sezione Protezione puoi configurare le impostazioni di sicurezza avanzate, gestire amici e spammer, visualizzare e modificare le impostazioni della connessione di rete, impostare le funzioni di prevenzione delle minacce online, controllare e risolvere potenziali vulnerabilità del sistema e valutare la sicurezza delle reti wireless a cui ti connetti.

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
- Ambiente di soccorso

Per maggiori informazioni sulle attività di scansione e su come configurare la protezione antivirus, fai riferimento a Protezione antivirus (pagina 36).

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 delle minacce online (pagina 58).

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 Difesa avanzata dalle minacce (pagina 56).

VULNERABILITÀ

Il modulo Vulnerabilità ti aiuta a mantenere costantemente aggiornati il sistema operativo e le applicazioni che usi regolarmente, oltre a identificare le reti wireless poco sicure a cui ti connetti. Clicca su **Apri** nel modulo Vulnerabilità per accedere alle sue funzionalità.

La funzionalità **Scansione vulnerabilità** ti consente di identificare gli aggiornamenti critici di Windows, gli aggiornamenti delle applicazioni, le password non sicure appartenenti agli account di Windows e le reti wireless pericolose. Clicca su **Avvia scansione** per eseguire una scansione sul tuo dispositivo.

Clicca su **Wi-Fi Security Advisor** per visualizzare l'elenco delle reti wireless a cui ti connetti, oltre alla nostra valutazione della reputazione per ciascuna di esse e le azioni che puoi intraprendere per restare protetto da potenziali intrusioni non autorizzate.

Per maggiori informazioni sulla configurazione della protezione dalle vulnerabilità, fai riferimento a Vulnerabilità (pagina 60).

RISANAMENTO DA RANSOMWARE

La funzionalità Risanamento da ransomware ti aiuta a recuperare i file nel caso venissero cifrati da un ransomware.

Per maggiori informazioni su come ripristinare i file cifrati, fai riferimento a Risanamento da ransomware (pagina 68).

Privacy

Nella sezione Privacy, puoi aprire la app Bitdefender VPN, cifrare i tuoi dati privati, proteggere le tue transazioni online, mantenere sicura la tua esperienza di navigazione e con la webcam, e proteggere i tuoi bambini, monitorando e limitando le loro attività online.

Le funzionalità che puoi gestire nella sezione Privacy sono:

PROTEZIONE AUDIO E VIDEO

Protezione audio e video tiene la webcam lontana da ogni pericolo bloccando l'accesso di app non affidabili e avvisandoti quando le app cercheranno di accedere al tuo microfono.

Per maggiori informazioni su come mantenere la tua webcam protetta da accessi indesiderati e come impostare Bitdefender per avvisarti sulle attività del microfono, fai riferimento a Protezione audio e video.

SAFEPAY

Il browser Bitdefender Safepay™ ti aiuta a mantenere le tue transazioni bancarie e i tuoi acquisti online sempre privati e sicuri.

Per maggiori informazioni su Bitdefender Safepay™, fai riferimento a Safepay: sicurezza per le transazioni online (pagina 76).

PARENTAL CONTROL

Bitdefender Parental Control ti consente di monitorare le attività dei bambini sui loro dispositivi. In caso di contenuti inappropriati, potrai decidere di limitare l'accesso a Internet o a determinate app.

Clicca su **Configura** nel pannello Controllo genitori per configurare i dispositivi dei bambini e monitorare le loro attività ovunque ti trovi.

Per maggiori informazioni sulla configurazione del Controllo genitori, fai riferimento a Controllo Genitori.

Utility

Nella sezione Utilities puoi migliorare la velocità del sistema e gestire i tuoi dispositivi.

Protezione dati

Il Distruttore di file di Bitdefender ti aiuta a eliminare in modo permanente i dati rimuovendoli fisicamente dal tuo disco rigido.

Per ulteriori informazioni a riguardo, fare riferimento a Protezione dati (pagina 88).

Profili

Le attività quotidiane, guardare un film o usare un videogioco, possono causare rallentamenti al sistema, in particolare se sono eseguite contemporaneamente ai processi di aggiornamento di Windows o alle attività di manutenzione.

Con Bitdefender, ora puoi scegliere e applicare il tuo profilo preferito, che adatta le impostazioni del sistema in modo da incrementare le prestazioni di determinate applicazioni installate.

Per ulteriori informazioni su questa funzione, fare riferimento a Profili (pagina 82).

2.2.5. Modificare la lingua del prodotto

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

1. Clic **Impostazioni** nel menu di navigazione sul 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.

2.3. Mantenere Bitdefender aggiornato

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 .
- 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 .

2.3.1. Verificare se Bitdefender è aggiornato

Per controllare quando si è verificato l'ultimo aggiornamento del tuo Bitdefender:

1. Clicca su **Notifiche** nel menu di navigazione nell'**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.

2.3.2. Eseguire un aggiornamento

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

Per avviare un aggiornamento, clicca con il pulsante destro del mouse sull'icona Bitdefender nella **barra delle applicazioni** e seleziona **Aggiorna**.

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. Accesso Bitdefender centrale.
2. Seleziona il **I miei dispositivi** pannello.
3. Fare clic sulla scheda del dispositivo desiderato, quindi su icona nell'angolo in alto a destra dello schermo.
4. Selezionare **Aggiornamento**.

2.3.3. Attivare o disattivare l'aggiornamento automatico

Per attivare o disattivare l'aggiornamento automatico:

1. Clic **Impostazioni** nel menu di navigazione sul 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 critica di sicurezza. Ti consigliamo 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.

2.3.4. 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. Clic **Impostazioni** nel menu di navigazione sul 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**.

2.3.5. 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.

> **Nota**
> Gli aggiornamenti, che includono nuove funzionalità e miglioramenti, saranno consegnati solo agli utenti che hanno Bitdefender 2020 installato.

2.4. Assistenza vocale intelligente

Se usi uno smart speaker di Amazon Alexa o la app Google Assistant, puoi avviare i comandi vocali per eseguire un set di attività o controllare informazioni sui dispositivi che hanno Bitdefender installato. Quindi, potrai eseguire attività di scansione e ottimizzazione, mettere in pausa la connessione a Internet sui dispositivi connessi, controllare lo stato del tuo abbonamento attuale, o controllare la posizione o le attività online dei bambini. Per visualizzare l'elenco completo dei comandi vocali che è possibile avviare, fai riferimento a Comandi vocali per interagire con Bitdefender (pagina 34).

2.4.1. Impostare i comandi vocali

I comandi vocali di Bitdefender possono essere configurati per:

- **Attivazione app Google Home**
  - Android 5.0 e sup.
  - iOS 10.0 o superiore
  - Chromebooks
- **Attivazione app Amazon Alexa**
  - Echo
  - Echo Dot
  - Echo Show
  - Echo Spot
  - Fire TV Cube

Impostare i comandi vocali di Amazon Alexa per Bitdefender

Per configurare i comandi vocali di Bitdefender su Amazon Alexa:

1. Apri la app Amazon Alexa.
2. Tocca l'icona **Menu** e vai in **Abilità**.
3. Cerca Bitdefender.
4. Tocca **Bitdefender** e tocca **ATTIVA**.
5. Ti sarà chiesto di accedere al tuo account Bitdefender.

Inserisci il tuo nome utente e la tua password, infine, tocca **ACCEDI**.

Non appena viene completata la sincronizzazione di Bitdefender con il tuo Amazon Alexa, ti saranno presentati i comandi vocali che potrai usare per avviare le attività o controllare le informazioni sui dispositivi con Bitdefender installato.

Ogni volta che l'assistente ti fornirà l'elenco di tutti i comandi vocali o le abilità disponibili, pronuncia **AIUTAMI**.

Impostare i comandi vocali di Google Home per Bitdefender

Per impostare i comandi vocali su Google Home:

1. Apri la app Google Home.
2. Tocca Menu nell'angolo in alto a sinistra della schermata Home e tocca **Esplora**.
3. Cerca Bitdefender.
4. Tocca **Bitdefender** e tocca **Collega**.
5. Ti viene chiesto di accedere al tuo account Bitdefender.
   Digita il nome utente e la password, quindi tocca **REGISTRAZIONE**.

Non appena viene completata la sincronizzazione di Bitdefender con Google Home, ti saranno presentati i comandi vocali che potrai usare per avviare le attività o controllare le informazioni sui dispositivi con Bitdefender installato.

Ogni volta che hai bisogno che l'assistente ti fornisca l'elenco di tutti i comandi vocali o le abilità disponibili, ad esempio **AIUTAMI**.

2.4.2. Comandi vocali per interagire con Bitdefender

Per aprire i comandi vocali di Bitdefender:

- In Amazon Alexa: **Alexa, apri Bitdefender**
- In Google Home: **OK, Google, parla con Bitdefender**

Per lanciare i comandi vocali di Bitdefender:

- In Amazon Alexa: **Alexa, chiedi a Bitdefender**
- In Google Home: **OK, Google, chiedi a Bitdefender**

Le domande e le attività che puoi avviare una volta aperto l'assistente di Bitdefender sono:

- Quali sono le mie attività di oggi?
- Qual è lo stato del mio abbonamento?
- Esegui una scansione veloce sul mio [tipo di dispositivo]. (Come tipo di dispositivo puoi indicare il tuo portatile, computer, telefono o tablet).

Se hai configurato Parental Control sui dispositivi dei bambini, le domande e le attività che potrai avviare una volta aperto l'assistente di Bitdefender sono:

- Interrompi la connessione a Internet per [nome del profilo].
- Riprendi la connessione a Internet per [nome del profilo].
- Localizza il bambino.
- Dov'è il bambino?
- Quando tempo ha trascorso il bambino sui suoi dispositivi?
- Quanto tempo ha trascorso oggi il bambino su Facebook?
- Quanto tempo ha trascorso oggi il bambino su Instagram?

Se hai più profili di Parental Control, puoi pronunciare il nome del bambino nel comando. Per esempio, **Localizza Sarah**.

3. GESTIRE LA TUA SICUREZZA

3.1. Protezione antivirus

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

- **Scansione all'accesso** - Impedisce a nuove minacce di accedere al tuo sistema. Per esempio, Bitdefender esaminerà un documento Word alla ricerca di minacce note quando lo apri, e un messaggio e-mail quando lo ricevi.

  La scansione all'accesso garantisce una protezione in tempo reale dalle minacce, essendo una componente essenziale di ogni programma di sicurezza informatica.

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

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

Bitdefender controlla automaticamente ogni supporto rimovibile che è collegato al dispositivo per assicurarti di accedervi in sicurezza. Per maggiori informazioni, fai riferimento a Scansione automatica di supporti rimovibili (pagina 50).

Gli utenti più esperti possono configurare le eccezioni della scansione, se non desiderano controllare determinati file o estensioni. Per maggiori informazioni, fai riferimento a Configurare le eccezioni della scansione (pagina 52).

Quando rileva una minaccia, Bitdefender tenterà automaticamente di rimuovere il codice dannoso dal file infetto, ricostruendo il file originale. Questa operazione è denominata disinfezione. I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione. Per maggiori informazioni, fai riferimento a Gestire i file in quarantena (pagina 54).

Se il tuo dispositivo è stato infettato da una minaccia, fai riferimento a Rimuovere le minacce dal sistema (pagina 129). Per aiutarti a ripulire il tuo dispositivo dalle minacce che non possono essere rimosse dal sistema operativo Windows, Bitdefender ti offre una Ambiente di salvataggio (pagina 130). Si tratta di un ambiente sicuro, realizzato specificatamente per la rimozione delle minacce, che ti consente di avviare il tuo dispositivo in modo indipendente da Windows. Quando il dispositivo è nell'Ambiente di soccorso, le minacce Windows sono inattive, rendendo quindi più semplice la loro rimozione.

3.1.1. 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.

Attivare o disattivare la protezione in tempo reale

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

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

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

Configurare le impostazioni avanzate della protezione in tempo reale

Gli utenti avanzati possono trarre vantaggio dalle impostazioni di scansione offerte da Bitdefender. Puoi configurare le impostazioni della

protezione in tempo reale in ogni dettaglio, creando un livello di protezione personalizzato.

Per configurare le impostazioni avanzate della protezione in tempo reale:

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

Informazioni sulle opzioni di scansione

Questa informazione potrebbe esserti utile:

- **Esamina solo le applicazioni**. Puoi impostare Bitdefender per esaminare solo le app a cui accedi.
- **Esamina le applicazioni potenzialmente indesiderate**. Seleziona questa opzione per esaminare le applicazioni indesiderate. Un'applicazione potenzialmente indesiderata (PUA) o un programma potenzialmente indesiderato (PUP) è un software in genere abbinato a un altro software freeware che mostra finestre di pop-up o installa una barra degli strumenti nel browser predefinito. Alcuni di questi programmi modificheranno la homepage o il motore di ricerca predefinito, altri eseguiranno diversi processi in background che rallentano il PC oppure mostreranno numerosi annunci pubblicitari. Tali programmi possono essere installati senza il tuo consenso (sono chiamati anche adware) o saranno inclusi in modo predefinito nel kit di installazione rapida (supportato da pubblicità).
- **Esamina script**. La funzionalità Esamina script consente a Bitdefender di esaminare gli script di Powershell e i documenti Office che potrebbero contenere malware basati su script.
- **Scansiona condivisioni di rete**. Per accedere in remoto in modo sicuro a una rete remota dal tuo dispositivo, ti consigliamo di mantenere attivata l'opzione Scansiona condivisioni di rete.
- **Scansiona memoria del processo**. Una scansione per rilevare attività dannose nella memoria dei processi in esecuzione.
- **Scansiona riga di comando**. Esamina la riga di comando di applicazioni appena eseguite per impedire gli attacchi privi di file.

- **Scansiona gli archivi**. Esaminare gli archivi è un processo lento e che richiede molte risorse, che pertanto non è consigliato per una protezione in tempo reale. Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del tuo sistema. La minaccia può interessare il tuo sistema solo se il file infetto viene estratto dall'archivio ed eseguito senza avere una protezione in tempo reale attivata.

  Se decidi di usare questa opzione, attivala, e trascina il cursore lungo la scala per escludere dalla scansione gli archivi superiori a un determinato valore di MB (Megabytes).

- **Scansiona i settori di avvio**. Puoi impostare Bitdefender per esaminare i settori di avvio del tuo disco rigido. Questo settore del disco rigido contiene il codice informatico necessario per iniziare la fase di avvio. Quando una minaccia infetta il settore di avvio, l'unità potrebbe diventare inaccessibile e potresti non poter più avviare il sistema e accedere ai dati.

- **Esamina solo file nuovi e modificati**. Esaminando solo i file nuovi o modificati, puoi migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.

- **Scansiona keylogger**. Seleziona questa opzione per esaminare il tuo sistema alla ricerca di app keylogger. I keylogger registrano tutto ciò che digiti con la tastiera e inviano rapporti su Internet a un eventuale aggressore (hacker). L'hacker può scoprire molte informazioni sensibili dai dati sottratti, come numeri di conti bancari e password, e usarli per il proprio tornaconto personale.

- **Scansione immediata all'avvio**. Seleziona l'opzione **Scansione immediata all'avvio** per esaminare il sistema all'avvio non appena vengono caricati i sistemi critici. L'obiettivo di questa funzionalità è migliorare il rilevamento delle minacce all'avvio del sistema.

Azioni intraprese sulle minacce rilevate

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

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

3. Nella finestra **Avanzate**, scorri verso il basso nella finestra finché non trovi l'opzione **Azioni minaccia**.
4. Configura le impostazioni della scansione come necessario.

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

Esegui azioni appropriate

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

- **File infetti**. I file rilevati come infetti corrispondono a una parte delle informazioni sulle minacce trovate nel Bitdefender Threat Information Database. Bitdefender tenterà di rimuovere automaticamente il codice dannoso dal file infetto e ricostruire il file originale. Questa operazione viene definita disinfezione.
  I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Per maggiori informazioni, fai riferimento a Gestire i file in quarantena (pagina 54).

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

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

Sposta in quarantena

Sposta i file infetti nella quarantena. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Per maggiori informazioni, fai riferimento a Gestire i file in quarantena (pagina 54).

Nega l'accesso

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

Ripristinare le impostazioni predefinite

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

Per ripristinare le impostazioni predefinite della protezione in tempo reale:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Nella finestra **Avanzate**, scorri in basso fino a visualizzare l'opzione **Reimposta impostazioni avanzate**. Selezionala per riportare le impostazioni dell'antivirus ai valori predefiniti.

3.1.2. 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.

Controllare un file o una cartella alla ricerca di minacce

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

Eseguire una Scansione veloce

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

Per eseguire una scansione veloce:

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

Eseguire una scansione del sistema

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

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

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

- Assicurati che Bitdefender sia aggiornato con il suo database delle informazioni delle minacce. Eseguire la scansione con un database delle informazioni delle minacce obsoleto può impedire a Bitdefender di rilevare nuove minacce, trovate dopo l'ultimo aggiornamento. Per maggiori informazioni, fai riferimento a Mantenere Bitdefender aggiornato (pagina 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 (pagina 43).

Per eseguire una scansione del sistema:

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

Configurare una scansione personale

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

Per configurare una nuova scansione personalizzata nei dettagli:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Nella finestra **Scansioni**, clicca su **+Crea scansione**.

4. Nel campo **Nome dell'attività**, inserisci un nome per la scansione, seleziona i percorsi che vorresti esaminare e clicca su **Avanti**.
5. Configura queste opzioni generali:
   - **Scansiona solo le applicazioni.** Puoi impostare Bitdefender in modo che controlli solo le app a cui si accede.
   - **Priorità dell'attività di scansione.** Puoi scegliere l'impatto che un processo di scansione dovrebbe avere sulle prestazioni del tuo sistema.
     - Automatico - La priorità del processo di scansione dipenderà dalle attività del sistema. Per assicurarsi che la fase di scansione non influenzi le attività del sistema, Bitdefender deciderà se eseguire la scansione con una maggiore o minore priorità.
     - Alta - La priorità della fase di scansione sarà elevata. Scegliendo questa opzione, consentirai ad altri programmi di funzionare più lentamente, diminuendo il tempo necessario per completare la scansione.
     - Bassa - La priorità della fase di scansione sarà bassa. Scegliendo questa opzione, consentirai ad altri programmi di funzionare più velocemente, aumentando il tempo necessario per completare la scansione.
   - **Pubblica azioni di scansione.** Scegli quale azione Bitdefender dovrebbe intraprendere nel caso non venisse trovata alcuna minaccia:
     - Mostra la finestra del sommario
     - Spegni il dispositivo
     - Chiudi la finestra di scansione
6. Se vuoi configurare le opzioni di scansione nel dettaglio, clicca su **Mostra impostazioni avanzate**. Puoi trovare informazioni sulle scansioni elencate al termine di questa sezione.
   Clicca su **Avanti**.
7. Se lo desideri, puoi attivare **Programma attività di scansione** e poi scegli quando dovrebbe iniziare la scansione personalizzata che hai creato.

- All'avvio del sistema
- Giornalmente
- Mensilmente
- Settimanalmente

Se scegli Giornalmente, Mensilmente o Settimanalmente, trascina il cursore lungo la scala per impostare il periodo di tempo desiderato in cui dovrebbe iniziare la scansione programmata.

8. Clicca su **Salva** per salvare le impostazioni e chiudere la finestra di configurazione.
   In base ai percorsi da controllare, la scansione potrebbe richiedere un po' di tempo. Se durante la scansione venissero rilevate delle minacce, ti sarà chiesto di scegliere le azioni da intraprendere sui file rilevati.

Informazioni sulle opzioni di scansione

Potresti trovare utili queste informazioni:

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

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

- **Scansiona solo i file nuovi e modificati.** Analizzando solo i file nuovi e modificati, è possibile migliorare notevolmente la reattività complessiva del sistema con un compromesso minimo in termini di sicurezza.
- **Scansiona i settori di avvio.** Puoi impostare Bitdefender in modo che esegua la scansione dei settori di avvio del tuo disco rigido. Questo settore del disco rigido contiene il codice del computer necessario per avviare il processo di avvio. Quando una minaccia infetta il settore di avvio, l'unità potrebbe diventare inaccessibile e potresti non essere in grado di avviare il sistema e accedere ai tuoi dati.
- **Scansiona memoria.** Seleziona questa opzione per esaminare i programmi in esecuzione nella memoria di sistema.
- **Scansiona registro.** Seleziona questa opzione per esaminare le chiavi del registro. Il registro di Windows è un database che memorizza le impostazioni e le opzioni di configurazione per i componenti del sistema operativo Windows, nonché per le app installate.
- **Scansiona i cookie.** Seleziona questa opzione per esaminare i cookie memorizzati dai browser sul tuo dispositivo.
- **Scansiona i keylogger.** Seleziona questa opzione per scansionare il tuo sistema alla ricerca di app keylogger. I keylogger registrano ciò che digiti sulla tastiera e inviano rapporti su Internet a una persona malintenzionata (hacker). L'hacker può scoprire informazioni sensibili dai dati rubati, come numeri di conto bancario e password, e utilizzarle per ottenere vantaggi personali.

Procedura guidata scansione antivirus

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

Nota

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

Fase 1 - Eseguire la scansione

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

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

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

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

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

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

Fase 2 - Scegliere le azioni

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

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

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

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

Esegui azioni appropriate

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

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

  I file che non possono essere disinfettati vengono spostati in quarantena per contenere l'infezione. I file in quarantena non possono essere eseguiti o aperti; quindi, il rischio di contrarre l'infezione scompare. Per ulteriori informazioni, fare riferimento a Gestire i file in quarantena (pagina 54).

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

- **Documenti sospetti.** I file vengono rilevati come sospetti dall'analisi euristica. I file sospetti non possono essere disinfettati perché non è disponibile alcuna routine di disinfezione. Saranno spostati in quarantena per prevenire una potenziale infezione.

- **Archivi contenenti file infetti.**
  - Gli archivi che contengono solo file infetti vengono eliminati automaticamente.
  - Se un archivio contiene sia file infetti che file puliti, Bitdefender tenterà di eliminare i file infetti a condizione che possa ricostruire l'archivio con i file puliti. Se la ricostruzione dell'archivio non è possibile, verrai informato che non è possibile intraprendere alcuna azione per evitare di perdere file puliti.

Elimina

Rimuove i file rilevati dal disco.

Se i file infetti sono memorizzati in un archivio con altri file puliti, Bitdefender tenterà di eliminarli e di riformare l'archivio con i file puliti. Se la ricostruzione dell'archivio non è possibile, sarai informato del fatto che non può essere intrapresa alcuna azione in modo da evitare la perdita di file puliti.

Non fare nulla

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

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

Fase 3 - Sommario

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

> **Importante**
> Nella maggior parte dei casi BitDefender disinfetta con successo i file infetti che rileva o isola l'infezione. Tuttavia, ci sono problemi che non possono essere risolti automaticamente. Se richiesto, riavvia il sistema per completare il processo di pulizia. Per maggiori informazioni e istruzioni su come rimuovere una minaccia manualmente, fai riferimento a Rimuovere le minacce dal sistema (pagina 129).

3.1.3. Controllare i registri di scansione

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

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

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

1. Clic **Notifiche** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nella scheda **Tutto**, seleziona la notifica relativa all'ultima scansione. Qui puoi trovare tutti gli eventi della scansione anti-minacce, incluso le minacce rilevate dalla scansione all'accesso, le scansioni avviate dall'utente e le variazioni di stato per le scansioni automatiche.
3. Nell'elenco delle notifiche, puoi verificare quali scansioni sono state eseguite di recente. Clicca su una notifica per visualizzare maggiori dettagli al riguardo.
4. Per aprire il registro della scansione, clicca su **Guarda registro**.

3.1.4. Scansione automatica di supporti rimovibili

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

I dispositivi rilevati rientrano in una di queste categorie:

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

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

Come funziona?

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

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

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

Nella maggior parte dei casi, Bitdefender rimuove automaticamente le minacce rilevate o isola i file infetti mettendoli in quarantena. Se dopo la scansione ci sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

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

Queste informazioni potrebbero esserti utili:

- Fai attenzione a usare un CD/DVD infettato da una minaccia, perché le minacce non possono essere rimosse dal disco (è un supporto di sola lettura). Assicurati che la protezione in tempo reale sia attivata per impedire la diffusione di minacce nel tuo sistema. Si consiglia di copiare tutti i dati importanti dal disco al proprio sistema e poi eliminare il disco.
- In alcuni casi, Bitdefender può non essere in grado di rimuovere le minacce da file specifici a causa di vincoli legali o tecnici. Un esempio sono i file archiviati con una tecnologia proprietaria (questo perché l'archivio non può essere ricreato correttamente).
  Per scoprire come comportarsi con le minacce, fai riferimento a Rimuovere le minacce dal sistema (pagina 129).

Gestire la scansione di supporti rimovibili

Per gestire la scansione automatica di supporti rimovibili:

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

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

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

3.1.5. Esamina file hosts

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

Per configurare la scansione del file hosts:

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

3.1.6. Configurare le eccezioni della scansione

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

Puoi configurare le eccezioni da applicare solo alla scansione all'accesso o su richiesta, oppure a entrambe. Gli oggetti esclusi dalla scansione

all'accesso non saranno esaminati, non importa se sono stati visitati da te o da un'applicazione.

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

Escludere file e cartelle dalla scansione

Per escludere determinati file e cartelle dalla scansione:

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

Escludere estensioni dei file dalla scansione

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

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

Per escludere estensioni di file dalla scansione:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Nel **Impostazioni** finestra, fare clic **Gestisci eccezioni**.
4. Clic **+ Aggiungi un'eccezione**.
5. Inserisci le estensioni che vuoi escludere dalla scansione con un punto prima di loro e separate da punto e virgola (;).
   `txt;avi;jpg`
6. Attiva l'interruttore accanto alla funzione di protezione che non deve esaminare l'estensione.
7. Clicca su **Salva**.

Gestire le eccezioni della scansione

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

Per gestire le eccezioni della scansione:

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

3.1.7. Gestire i file in quarantena

Bitdefender isola i file infettati da minacce che non può disinfettare e i file sospetti in un'area sicura chiamata quarantena. Quando una minaccia è in

quarantena, non può più arrecare alcun danno, in quanto non può essere eseguita o letta.

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

Per controllare e gestire i file in quarantena:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Vai alla finestra **Impostazioni**.
   Qui puoi visualizzare il nome dei file in quarantena, la loro posizione originale e il nome delle minacce rilevate.
4. I file in quarantena sono gestiti automaticamente da Bitdefender in base alle impostazioni di quarantena predefinite.
   Anche se non consigliato, puoi modificare le impostazioni della quarantena in base alle tue preferenze, cliccando su **Vedi impostazioni**.
   Clicca sugli interruttori per attivare o disattivare:
   Esamina nuovamente la quarantena dopo l'aggiornamento delle informazioni delle minacce
   Mantieni questa opzione attivata per eseguire automaticamente la scansione dei file in quarantena dopo ogni aggiornamento del database delle informazioni sulle minacce. I file puliti vengono spostati automaticamente alla loro ubicazione originale.
   Elimina i contenuti più vecchi di 30 giorni
   I file in quarantena più vecchi di 30 giorni sono eliminati automaticamente.
   Crea eccezioni per i file ripristinati
   I file ripristinati dalla quarantena vengono riportati alla loro posizione originale senza essere riparati e vengono esclusi automaticamente dalle scansioni future.
5. Per eliminare un file in quarantena, selezionalo e clicca sul pulsante **Elimina**. Se desideri ripristinare un file in quarantena alla sua ubicazione originale, selezionalo e clicca su **Ripristina**.

3.2. Difesa avanzata dalle minacce

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

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

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

3.2.1. Attivare o disattivare Advanced Threat Defense

Per attivare o disattivare Advanced Threat Defense:

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

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

3.2.2. 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. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **DIFESA AVANZATA DALLE MINACCE** riquadro, fare clic **Aprire**.
3. Vai alla finestra **Threat Defense**.

Vengono mostrati gli attacchi rilevati negli ultimi 90 giorni. Per scoprire dettagli sul tipo di ransomware rilevato, il percorso del processo dannoso o se la disinfezione ha avuto successo, basta cliccarci sopra.

3.2.3. 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. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **DIFESA AVANZATA DALLE MINACCE** riquadro, fare clic **Aprire**.
3. Nel **Impostazioni** finestra, fare clic **Gestisci eccezioni**.
4. Clic **+ Aggiungi un'eccezione**.
5. Immettere il percorso della cartella che si desidera escludere dalla scansione nel campo corrispondente.
   In alternativa, puoi raggiungere il file eseguibile cliccando sul pulsante Sfoglia nel lato destro dell'interfaccia, selezionalo e clicca su **OK**.
6. Attiva l'interruttore accanto a **Advanced Threat Defense**.
7. Clic **Salva**.

3.2.4. 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.

3.2.5. Attivare o disattivare la rilevazione degli exploit

Per attivare o disattivare la rilevazione degli exploit:

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

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

3.3. Prevenzione delle minacce online

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

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

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

Per configurare le impostazioni della Prevenzione minacce online:

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

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

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

  Non dovresti visitare questa pagina web.

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

  Questa è pagina sicura da visitare.

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

- Google
- Yahoo!
- Bing
- Baidu

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

- Facebook
- 121

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

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

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

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

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **PREVENZIONE DELLE MINACCE ONLINE** riquadro, fare clic **Impostazioni**.
3. Clicca su **Gestisci eccezioni**.
4. Clic **+ Aggiungi un'eccezione**.
5. Inserisci nel campo corrispondente il nome del sito web, il nome del dominio o l'indirizzo IP che vuoi aggiungere alle eccezioni.

6. Clicca sull'interruttore accanto a **Prevenzione minacce di rete**.
7. Per rimuovere una voce dall'elenco, fare clic su pulsante accanto ad esso.
   Clic **Salva** per salvare le modifiche e chiudere la finestra.

3.3.1. Bitdefender ti avvisa nel browser

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

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

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

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

3.4. Vulnerabilità

Un passaggio importante nella protezione del dispositivo contro azioni e applicazioni dannose è mantenere aggiornato il sistema operativo e le applicazioni che usi regolarmente. Inoltre, per prevenire l'accesso fisico non autorizzato al tuo dispositivo, è necessario configurare password sicure (ovvero non facilmente indovinabili) per ogni account utente di Windows e per le reti Wi-Fi a cui ti connetti.

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

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

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

3.4.1. Controllare il sistema per rilevare vulnerabilità

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

Per esaminare il sistema alla ricerca di vulnerabilità:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel pannello **VULNERABILITÀ**, clicca su **Apri**.
3. Nella scheda **Scansione vulnerabilità**, clicca su **Avvia scansione**, poi attendi che Bitdefender controlli l'eventuale presenza di vulnerabilità nel tuo sistema. Le vulnerabilità rilevate sono raggruppate in tre categorie:
   - **SISTEMA OPERATIVO**
     - **Sicurezza del sistema operativo**
       Impostazioni di sistema modificate che possono compromettere il dispositivo e i dati, come la mancata visualizzazione di avvisi quando i file eseguiti effettuano modifiche sul sistema senza la tua autorizzazione o quando dispositivi MTP, come telefoni o fotocamere, si connettono ed eseguono operazioni diverse a tua insaputa.
     - **Aggiornamenti critici di Windows**
       Viene mostrato un elenco degli aggiornamenti critici di Windows che non sono stati installati sul computer. Per consentire a Bitdefender di completare l'installazione potrebbe essere necessario riavviare il sistema. Ricordati che potrebbe volerci un po' per installare gli aggiornamenti.
     - **Account Windows poco sicuri**
       Puoi visualizzare l'elenco degli account utente di Windows configurati sul tuo dispositivo e il livello di protezione che le loro password forniscono. Puoi scegliere tra chiedere di cambiare la password al prossimo accesso o cambiare subito la password direttamente. Per impostare una nuova password per il sistema, seleziona **Cambia la password ora**.
       Per creare una password sicura, ti consigliamo di usare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

- **APPLICAZIONI**
  - **Sicurezza browser**
    Modifica delle impostazioni del dispositivo che consente l'esecuzione di file e programmi scaricati tramite Internet Explorer senza una convalida dell'integrità, che potrebbe comportare la compromissione del dispositivo.
  - **Aggiornamenti applicazioni**
    Per visualizzare maggiori informazioni sulla app che necessita di essere aggiornata, clicca sul nome nell'elenco.
    Se un'applicazione non è aggiornata, clicca su **Scarica nuova versione** per scaricare la versione più recente.
- **RETE**
  - **Rete e credenziali**
    Impostazioni di sistema modificate come l'eventuale connessione automatica a reti di hotspot aperte a tua insaputa o la mancata applicazione della cifratura sul traffico di un canale sicuro in uscita.
  - **Reti Wi-Fi e router**
    Per avere maggiori informazioni sul router e la rete wireless a cui hai effettuato la connessione, clicca sul suo nome nell'elenco. Se ti venisse consigliato di impostare una password più sicura per la rete domestica, assicurati di seguire le nostre istruzioni, in modo da poterti connettere senza preoccuparti della privacy.
    Quando sono disponibili altri suggerimenti, segui le istruzioni fornite per assicurarti che la tua rete di casa sia sempre protetta dagli occhi indiscreti dei pirati informatici.

3.4.2. Usare il controllo automatico delle vulnerabilità

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

Per controllare e correggere i problemi rilevati:

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

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

Per configurare le impostazioni del monitoraggio vulnerabilità:

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

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

3. Vai alla scheda **Impostazioni**.

4. Seleziona le vulnerabilità del sistema che desideri siano controllate regolarmente usando gli interruttori corrispondenti.
   Aggiornamenti di Windows
   Verifica se il sistema operativo Windows ha gli ultimi aggiornamenti di sicurezza di Microsoft.
   Aggiornamenti dell'applicazione
   Verifica se le applicazioni installate sul sistema sono aggiornate. Applicazioni datate possono essere sfruttate da software dannosi, rendendo il tuo PC vulnerabile agli attacchi esterni.
   Password dell'utente
   Verifica se le password degli account Windows e dei router configurati sul sistema sono più o meno facili da indovinare. Impostare password difficili da indovinare (password sicure) ostacola l'accesso al tuo sistema da parte degli hacker. Una password sicura include una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).
   Esecuzione automatica
   Verifica lo stato della funzione di esecuzione automatica di Windows. Questa caratteristica consente alle applicazioni di essere avviate automaticamente da unità CD, DVD, USB o altri dispositivi esterni.
   Alcuni tipi di minacce usano l'esecuzione automatica per diffondersi automaticamente da supporti rimovibili al PC. Ecco perché si consiglia di disattivare questa funzione di Windows.
   Wi-Fi Security Advisor
   Verifica se la rete wireless di casa a cui sei connesso è sicura oppure no, e se ha eventuali vulnerabilità. Inoltre, verifica se la password del router domestico sia abbastanza sicura e ti consiglia come potenziarla.
   La maggior parte delle reti wireless non cifrate sono poco sicure, cosa che consente agli occhi indiscreti dei pirati informatici di accedere alle tue attività personali.

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

3.4.3. Wi-Fi Security Advisor

Mentre sei in viaggio, lavorando in un bar o aspettando all'aeroporto, connettersi a una rete wireless pubblica per effettuare pagamenti, controllare le e-mail o gli account dei social network può essere la

soluzione più rapida. Ma potrebbero esserci alcuni occhi indiscreti che cercheranno di ottenere i tuoi dati personali, sfruttando ogni falla nella rete per sottrarre informazioni.

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

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

Bitdefender Wi-Fi Security Advisor ti fornisce informazioni su:

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

Attivare o disattivare le notifiche di Wi-Fi Security Advisor

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

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

Configurare la rete Wi-Fi di casa

Per iniziare a configurare la tua rete di casa:

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

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

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

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

Configurare la rete Wi-Fi dell'ufficio

Per iniziare a configurare la tua rete dell'ufficio:

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

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

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

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

Wi-Fi pubblica

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

- Advanced Threat Defense è attivato
- Vengono attivate le seguenti impostazioni della Prevenzione minacce online:
  - Scansione web cifrata
  - Protezione dalle frodi

- Protezione da phishing

- È disponibile un pulsante che apre Bitdefender Safepay™. In questo caso, la protezione degli Hotspot per le reti non sicure viene attivata in maniera predefinita.

Controllare le informazioni sulle reti Wi-Fi

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

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

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

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

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

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

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

- **Protetto** - Qui puoi visualizzare se la rete selezionata è protetta oppure no. Reti non cifrate possono lasciare esposti i dati che utilizzi.

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

3.5. Risanamento da ransomware

Bitdefender Ransomware Remediation esegue un backup dei tuoi file, come documenti, immagini, video o musica per assicurarsi che siano protetti dall'essere danneggiati o persi in caso di cifratura di ransomware. Ogni volta che viene rilevato un attacco ransomware, Bitdefender bloccherà tutti i processi coinvolti nell'attacco e avvierà il processo di risanamento. In questo modo, potrai recuperare i contenuti dei tuoi interi file senza pagare alcun riscatto.

3.5.1. Attivare o disattivare il Risanamento da ransomware

Per attivare o disattivare il Risanamento da ransomware:

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

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

3.5.2. Attivare o disattivare il ripristino automatico

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

Per attivare o disattivare il ripristino automatico:

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

3.5.3. Visualizzare i file che sono stati ripristinati automaticamente

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

Per visualizzare i file che sono stati ripristinati automaticamente:

1. Clic **Notifiche** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nella scheda **Tutti**, seleziona la notifica sul più recente comportamento ransomware risanato, e clicca su **File ripristinati**.
   Viene mostrato l'elenco con i file ripristinati. Qui puoi anche visualizzare il percorso in cui i tuoi file sono stati memorizzati.

3.5.4. Ripristinare file cifrati manualmente

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

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

5. Apparirà una finestra di conferma.
   Clicca su **Fine** per terminare il processo di ripristino.

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

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

3.5.5. Aggiungere applicazioni alle eccezioni

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

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

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **RISOLUZIONE DEL RANSOMWARE** riquadro, fare clic **Maneggio**.
3. Vai alla finestra **Eccezioni** e clicca su **+Aggiungi un'eccezione**.

3.6. Anti-tracker

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

Con l'estensione anti-tracker di Bitdefender Anti-tracker attivata nel tuo browser web, puoi evitare la tracciatura così che i tuoi dati restino privati mentre navighi online, velocizzando il tempo necessario per caricare i siti web.

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

- Internet Explorer
- Google Chrome
- Mozilla Firefox

I tracker che rileviamo vengono raggruppati nelle seguenti categorie:

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

3.6.1. Interfaccia anti-tracker

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

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

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

3.6.2. Disattivare Bitdefender Anti-tracker off

Per disattivare Bitdefender Anti-tracker:

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

3.6.3. Consentire a un sito web di essere monitorato

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

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

3.7. VPN

La app VPN può essere installata dal tuo prodotto Bitdefender e usata ogni volta che vuoi aggiungere un ulteriore livello di protezione per la tua connessione. La VPN serve come una sorta di tunnel tra il tuo dispositivo e la rete a cui ti connetti per proteggere la tua connessione, cifrando i dati usando una cifratura di livello bancario e nascondendo il tuo indirizzo IP ovunque sei. Il tuo traffico viene reindirizzato attraverso un

server separato. Ciò rende il tuo dispositivo quasi impossibile da essere identificato attraverso la miriade di altri dispositivi che stanno usando i nostri servizi. Inoltre, connettendoti a Internet tramite Bitdefender VPN, potrai accedere a contenuti che normalmente sono vietati in determinate aree.

> **Nota**
> Alcuni paesi applicano una censura di Internet e quindi l'utilizzo delle VPN sul loro territorio è proibito per legge. Per evitare conseguenze legali, potrebbe comparire un messaggio di avviso quando cerchi di usare la app Bitdefender VPN per la prima volta. Continuando a utilizzare la app, confermi di essere consapevole dei regolamenti applicabili nel paese in cui ti trovi e dei rischi a cui potresti andare incontro.

3.7.1. Installare VPN

La app VPN può essere installata dalla tua interfaccia di Bitdefender come segue:

1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel pannello **VPN**, clicca su **Installa VPN**.
3. Nella finestra con la descrizione della app VPN, leggi l'**Accordo di abbonamento** e clicca su **INSTALLA BITDEFENDER VPN**.
   Attendi qualche istante per il download e l'installazione dei file.
   Se viene rilevata un'altra app VPN, ti consigliamo di disinstallarla. Con più soluzioni VPN installate, potresti riscontrare rallentamenti del sistema o altri problemi di funzionamento.
4. Clicca su **APRI BITDEFENDER VPN** per completare la fase di installazione.

> **Nota**
> Bitdefender VPN richiede .Net Framework 4.5.2 o superiore per essere installato. Nel caso non avessi installato questo pacchetto, comparirà una finestra di notifica. Clicca su **Installa .Net Framework** per andare a una pagina da cui potrai scaricare la versione più recente di questo software.

3.7.2. Aprire VPN

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

- Dall'area di notifica

  1. Clicca con il pulsante destro del mouse sull'icona nella barra delle applicazioni e poi clicca su **Mostra**.

- Dall'interfaccia di Bitdefender

  1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
  2. Nel pannello **VPN**, clicca su **Apri VPN**.

3.7.3. Interfaccia di VPN

L'interfaccia di VPN mostra lo stato della app, connessa o disconnessa. L'ubicazione del server per gli utenti con la versione gratuita viene impostata automaticamente da Bitdefender sul server più appropriato, mentre gli utenti premium hanno la possibilità di modificare la posizione del server a cui desiderano connettersi. Per maggiori informazioni sugli abbonamenti di VPN, fai riferimento a Abbonamenti (pagina 75).

Per connetterti o disconnetterti, clicca semplicemente sullo stato mostrato nella parte superiore della schermata, oppure clicca con il pulsante destro del mouse sull'icona nella barra delle applicazioni. L'icona nella barra delle applicazioni mostra un segno di spunta verde quando VPN è connesso e un segno di spunta rosso quando è disconnesso.

Durante la connessione, nella parte inferiore dell'interfaccia viene indicato il tempo speso e la banda utilizzata.

Per visualizzare interamente l'area del **Menu**, clicca sull'icona nel lato superiore a sinistra. Qui avrai le seguenti opzioni:

- **Il mio account** - Mostra informazioni sul tuo account Bitdefender e sull'abbonamento a VPN. Clicca su **Cambia account**, se vuoi accedere con un altro account.
  Clicca su **Aggiungilo qui** per aggiungere un codice di attivazione per Bitdefender Premium VPN.

- **Impostazioni** – In base alle tue necessità, puoi personalizzare il comportamento del tuo prodotto. Le impostazioni sono suddivise in due categorie:
  - **Generale**
    - Notifiche
    - Avvio - Scegli se eseguire Bitdefender VPN all'avvio oppure no
    - Rapporti del prodotto - invia rapporti del prodotto anonimi per aiutarci a migliorare la tua esperienza
    - Modalità scura
    - Lingua
  - **Avanzate**
    - Interruzione Internet - questa funzionalità interrompe temporaneamente tutto il traffico Internet se la connessione VPN dovesse cadere accidentalmente. Non appena ritorni online, viene ristabilita la connessione VPN.
    - Connettiti automaticamente - Connettiti automaticamente a Bitdefender VPN quando accedi a una rete Wi-Fi pubblica/non affidabile o quando viene avviata una app di condivisione file peer-to-peer.
- **Supporto** - Puoi accedere alla piattaforma del nostro Centro di supporto, da cui potrai leggere un articolo molto utile su come utilizzare Bitdefender VPN o inviarci un feedback.
- **Info** - Vengono mostrate alcune informazioni sulla versione installata.

3.7.4. Abbonamenti

Bitdefender VPN offre gratuitamente una quota di traffico giornaliera di 200 MB per proteggere la tua connessione ogni volta che ti serve, connettendoti automaticamente all'ubicazione del server ottimale.

Per ottenere traffico illimitato e accesso senza restrizioni a contenuti in tutto il mondo scegliendo l'ubicazione del server che preferisci, fai l'upgrade alla versione premium.

Puoi fare l'upgrade alla versione Bitdefender Premium VPN in qualsiasi momento cliccando sul pulsante **Fai l'upgrade** disponibile nell'interfaccia del prodotto.

L'abbonamento a Bitdefender Premium VPN è indipendente dall'abbonamento a Bitdefender VPN, ciò significa che potrai utilizzarlo per tutta la sua disponibilità, indipendentemente dallo stato dell'abbonamento della tua soluzione di sicurezza. Nel caso l'abbonamento a Bitdefender Premium VPN fosse scaduto, ma quello a Bitdefender VPN fosse ancora attivo, tornerai al piano gratuito.

Bitdefender VPN è un prodotto multipiattaforma, disponibile nei prodotti Bitdefender compatibili con Windows, macOS, Android e iOS. Una volta fatto l'upgrade al piano premium, potrai utilizzare il tuo abbonamento su tutti i prodotti, a patto di eseguire l'accesso allo stesso account di Bitdefender.

3.8. Safepay: sicurezza per le transazioni online

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

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

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

Bitdefender Safepay™ offre le seguenti funzioni:

- Blocca l'accesso al proprio desktop, impedendo qualsiasi tentativo di catturare delle immagini del proprio schermo.
- È dotato di una tastiera virtuale che, quando viene utilizzata, rende impossibile agli hacker rilevare la combinazione di tasti premuta.
- È completamente indipendente dagli altri browser.

- È dotato di una protezione integrata degli hotspot da utilizzare quando il dispositivo è connesso a reti Wi-Fi non protette.
- Supporta i segnalibri e consente di navigare nei propri siti bancari/commerciali preferiti.
- Non è limitato alle operazioni bancarie e lo shopping online. Infatti, è possibile aprire qualsiasi sito web in Bitdefender Safepay™.

3.8.1. Utilizzare Bitdefender Safepay™

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

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

- Dall'**interfaccia di Bitdefender**:
  1. Clic **Riservatezza** nel menu di navigazione sul Interfaccia di Bitdefender.
  2. Nel pannello **SAFEPAY**, clicca su **Impostazioni**.
  3. Nella finestra **Safepay**, clicca su **Lancia Safepay**.
- Da Windows:
  - In **Windows 7**:
    1. Clicca su **Avvia** e vai su **Tutti i programmi**.
    2. Clicca su **Bitdefender**.
    3. Clicca su **Bitdefender Safepay™**.
  - In **Windows 8** e **Windows 8.1**:
    Localizza Bitdefender Safepay™ nella schermata di Windows Start (per esempio, puoi iniziare digitando "Bitdefender Safepay™" direttamente nella schermata di Start) e poi clicca sulla relativa icona.
  - In **Windows 10** e **Windows 11**:
    Digita "Bitdefender Safepay™" nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona.

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

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

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

3.8.2. Configurare le impostazioni

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

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

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

Blocca pop-up

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

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

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

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

Gestisci plugin

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

Gestisci certificati

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

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

Usa tastiera virtuale

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

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

Conferma di stampa

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

3.8.3. Gestire i segnalibri

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

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

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

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

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

3.8.4. Disattivare le notifiche di Safepay

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

Per disattivare le notifiche di Safepay:

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

3.9. Bitdefender USB Immunizer

La funzione di esecuzione automatica inclusa nei sistemi operativi Windows è uno strumento molto utile che consente ai dispositivi di eseguire automaticamente un file da un qualsiasi supporto a esso collegato. Per esempio, l'installazione di un software si avvia automaticamente, inserendo un CD nel lettore ottico.

Sfortunatamente, questa funzione può essere utilizzata anche dalle minacce per avviarsi automaticamente e infiltrarsi nel tuo dispositivo da supporti riscrivibili, come unità USB e schede di memoria, collegate tramite lettori di schede. Negli ultimi anni, sono stati rilevati moltissimi attacchi basati sull'esecuzione automatica.

Con USB Immunizer puoi impedire a qualsiasi unità flash formattata in NTFS, FAT32 o FAT dall'eseguire automaticamente ogni minaccia. Una volta che un dispositivo USB è immunizzato, le minacce non possono

più configurarlo per eseguire una determinata applicazione quando il dispositivo viene collegato a un dispositivo con Windows.

Per immunizzare un dispositivo USB:

1. Collega l'unità flash al tuo dispositivo.
2. Esegui una ricerca nel dispositivo per localizzare il dispositivo di archiviazione rimovibile e clicca con il pulsante destro sulla sua icona.
3. Nel menu contestuale, punta su **Bitdefender** e seleziona **Immunizza questa unità**.

> **Nota**
> Se l'unità è già stata immunizzata, al posto dell'opzione Immunizza, comparirà il messaggio **L'unità USB è protetta da ogni minaccia basata sull'esecuzione automatica**.

Per impedire al dispositivo di eseguire minacce da dispositivi USB non immunizzati, disattiva la funzione di esecuzione automatica. Per maggiori informazioni, fai riferimento a Usare il controllo automatico delle vulnerabilità (pagina 62).

4. UTILITÀ

4.1. Profili

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

Bitdefender offre i seguenti profili:

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

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

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

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

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

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

- Le attività di manutenzione sono state ritardate.
- Le impostazioni di alimentazione sono state regolate.

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

- La protezione avanzata dalle minacce è attivata
- Le seguenti impostazioni di Prevenzione delle minacce online sono attivate:
  - Scansione Web crittografata
  - Protezione contro le frodi
  - Protezione contro il phishing

4.1.1. Profilo Lavoro

Eseguire più attività, come inviare e-mail, tenere una comunicazione video con alcuni colleghi in remoto o lavorare con applicazioni grafiche può influenzare notevolmente le prestazioni del sistema. Il profilo Lavoro è stato progettato per aiutarti a migliorare la tua efficienza lavorativa, disattivando alcuni servizi e attività di manutenzione in background.

Configurare il profilo Lavoro

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

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

Aggiungere manualmente le applicazioni all'elenco del profilo Lavoro

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

Per aggiungere manualmente le app all'Elenco applicazioni lavoro:

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

4.1.2. Profilo Film

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

Configurare il profilo Film

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

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

- Modifica le impostazioni dei consumi energetici per i film

5. Clic **SALVA** per salvare le modifiche e chiudere la finestra.

Aggiungere manualmente i lettori multimediali all'elenco del profilo Film

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

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

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Profili** scheda, fare clic **Impostazioni**.
3. Clicca il **CONFIGURA** pulsante dall'area Profilo film.
4. Nella finestra **Impostazioni Profilo Film**, clicca su **Elenco lettori**.
5. Clic **AGGIUNGERE**.
   Viene visualizzata una nuova finestra. Passare al file eseguibile dell'app, selezionarlo e fare clic **OK** per aggiungerlo all'elenco.

4.1.3. Profilo Gioco

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

Configurare il profilo Gioco

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

1. Clic **Utilità** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Profili** scheda, fare clic **Impostazioni**.
3. Clicca sul pulsante **Configura** nella sezione del Profilo gioco.
4. Scegli le regolazioni del sistema che desideri vengano applicate selezionando le seguenti opzioni:

- Aumenta le prestazioni con i giochi
- Ottimizza le impostazioni del prodotto per il profilo Gioco
- Rinvia i programmi in background e le attività di manutenzione
- Rinvia gli aggiornamenti automatici di Windows
- Modifica le impostazioni dei consumi energetici per i giochi

5. Clic **SALVA** per salvare le modifiche e chiudere la finestra.

Aggiungere manualmente giochi all'Elenco dei giochi

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

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

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

4.1.4. Profilo rete Wi-Fi pubblica

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

Configurare il profilo Rete Wi-Fi pubblica

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

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

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

4.1.5. Profilo Modalità Batteria

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

Configurare il profilo Modalità Batteria

Per configurare il profilo Modalità Batteria:

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

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

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

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

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

4.1.6. Ottimizzazione in tempo reale

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

Per attivare o disattivare l'Ottimizzazione in tempo reale:

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

4.2. Protezione dati

4.2.1. Eliminare i file in modo permanente

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

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

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

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

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

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

5. COME FARE

5.1. Installazione

5.1.1. Come posso installare Bitdefender su un secondo dispositivo?

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

Per installare Bitdefender su un secondo dispositivo:

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

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

5.1.2. 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.

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

- In **Windows 7**:
  1. Clic **Inizio** e vai a **Tutti i programmi**.
  2. Trova *Bitdefender Antivirus Plus* e seleziona **Disinstalla**.
  3. Clicca su **REINSTALLA** nella finestra che comparirà.
  4. Devi riavviare il dispositivo per completare il processo.
- In **Windows 8** E **Windows 8.1**:

1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
2. Clicca su **Disinstalla** un programma o **Programmi e funzionalità**.
3. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
4. Clic **REINSTALLARE** nella finestra che appare.
5. È necessario riavviare il dispositivo per completare il processo.

- In **Windows 10** E **Finestre 11**:
  1. Clicca su **Inizia** e poi su **Impostazioni**.
  2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **App e funzionalità**.
  3. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
  4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
  5. Clicca su **REINSTALLA**.
  6. È necessario riavviare il dispositivo per completare il processo.

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

5.1.3. Dove posso scaricare il mio prodotto Bitdefender?

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

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

Per installare Bitdefender da Bitdefender Central:

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

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

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

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

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

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

Potrebbero verificarsi due casi:

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

3. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
4. Clic **Disinstalla** di nuovo per confermare la tua scelta.
5. Clic **REINSTALLARE** nella finestra che appare.
6. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.
   Apri l'interfaccia del tuo nuovo prodotto Bitdefender installato per avere accesso alle sue funzionalità.

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

- Hai cambiato sistema e vuoi continuare a utilizzare la protezione di Bitdefender. In questo caso, devi installare nuovamente il prodotto utilizzando la versione più recente.
  Per risolvere questa situazione:
  1. Scarica il file di installazione:
     a. Accesso Bitdefender centrale.
     b. Seleziona il **I miei dispositivi** pannello, quindi fare clic su **INSTALLA LA PROTEZIONE**.
     c. Scegli una delle due opzioni disponibili:
        - **Proteggi questo dispositivo**
          Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.
        - **Proteggi un altro dispositivo**
          Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.
          Clic **INVIA IL LINK PER IL DOWNLOAD**. Digita un indirizzo email nel campo corrispondente e fai clic **INVIA UNA EMAIL**. Si noti che il collegamento per il download generato è valido solo per le prossime 24 ore. Se il link scade, dovrai generarne uno nuovo seguendo gli stessi passaggi.

Sul dispositivo su cui desideri installare il tuo prodotto Bitdefender, controlla l'account e-mail che hai digitato, quindi fai clic sul pulsante di download corrispondente.

2. Esegui il prodotto Bitdefender che hai scaricato.

Per maggiori informazioni sull'installazione di Bitdefender, fai riferimento a Installare il tuo prodotto Bitdefender (pagina 6).

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

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

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

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

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

5.2. Bitdefender centrale

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

Hai creato un nuovo account Bitdefender e ora vuoi utilizzarlo.

Per accedere con un altro account di Bitdefender:

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

> **Nota**
> Il prodotto Bitdefender del tuo dispositivo cambia automaticamente in base all'abbonamento associato al nuovo account Bitdefender. Se non vi è alcun abbonamento associato disponibile al nuovo account Bitdefender o desideri trasferirlo dall'account precedente, puoi contattare Bitdefender per ottenere assistenza come descritto nella sezione Richiesta d'aiuto (pagina 137).

5.2.2. Come disattivo i messaggi di aiuto di Bitdefender Central?

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

Se desideri disattivare questo tipo di messaggi:

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

5.2.3. 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:

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

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

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

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

5.3. Scansione con BitDefender

5.3.1. 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'elemento che desideri controllare, puntare Bitdefender e poi **Esamina con Bitdefender** dal menu.

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

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

Tipiche situazioni in cui si userebbe questo metodo includono:

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

5.3.2. Come posso eseguire una scansione del mio sistema

Per eseguire una scansione completa del sistema:

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

3. Clicca sul pulsante **Esegui scansione** accanto a **Scansione sistema**.
4. Segui la procedura guidata della Scansione di sistema per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati.
   Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo. Per maggiori informazioni, fai riferimento a Richiesta d'aiuto (pagina 137).

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

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

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

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

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

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

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

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

5.3.5. Come posso escludere una cartella dalla scansione?

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

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

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

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

Per aggiungere una cartella alla lista delle eccezioni:

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

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

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

1. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.

b. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.

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

2. Mostra gli oggetti nascosti in Windows. Per scoprire come fare, fai riferimento a Come posso visualizzare gli elementi nascosti in Windows? (pagina 114).
3. Ripristina il file dalla quarantena:
   a. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
   b. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
   c. Vai alla finestra **Impostazioni** e clicca su **Gestisci quarantena**.
   d. Seleziona il file e poi clicca su **Ripristina**.
4. Aggiungi il file all'elenco delle eccezioni. Per scoprire come fare, fai riferimento a Come posso escludere una cartella dalla scansione? (pagina 101).
5. Attiva la protezione antivirus in tempo reale di Bitdefender.
6. Contatta gli operatori del nostro supporto in modo da poter rimuovere la rilevazione dell'aggiornamento delle informazioni sulle minacce. Per scoprire come fare, fai riferimento a Richiesta d'aiuto (pagina 137).

5.3.7. 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.

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

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

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

5.4. Controllo privacy

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

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

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

Per mantenere le tue attività online sempre sicure e private:

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

5.4.2. Cosa posso fare in caso di furto del mio dispositivo?

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

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

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

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

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

5.4.3. Come posso eliminare un file in modo permanente con Bitdefender?

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

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

1. Clicca con il pulsante destro del mouse sul file o la cartella che vuoi eliminare in maniera definitiva, seleziona Bitdefender e poi **Distruttore di file**.
2. Clic **Elimina definitivamente**, quindi confermare che si desidera continuare con il processo.
   Attendi che Bitdefender finisca di distruggere i file.
3. I risultati sono mostrati. Clicca su **FINE** per uscire dalla procedura guidata.

5.4.4. Come posso proteggere la mia webcam da accessi non autorizzati?

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

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

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

- Da Windows Store
- Dalle tue app

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

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

1. Clic **Notifiche** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **Tutto** scheda, selezionare la notifica relativa all'ultimo comportamento ransomware rilevato, quindi fare clic su **File crittografati**.
3. Viene visualizzato l'elenco con i file crittografati.
   Clicca su **Ripristina file** per continuare.
4. Nel caso in cui l'intero o parte del processo di ripristino fallisca, è necessario scegliere la posizione in cui salvare i file decrittografati. Clic **Ripristina posizione**, quindi scegli una posizione sul tuo PC.
5. Viene visualizzata una finestra di conferma.
   Clic **Fine** per terminare il processo di ripristino.

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

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

5.5. Informazioni utili

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

Se non ricevi alcun avviso da parte di Bitdefender, ti consigliamo di contattare il supporto tecnico di Bitdefender come descritto nella sezione Richiesta d'aiuto (pagina 137).

5.5.2. Come posso rimuovere Bitdefender?

Se vuoi rimuovere Bitdefender Antivirus Plus:

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

- In **Windows 8** E **Windows 8.1**:
  1. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di

controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.

2. Clic **Disinstallare un programma** O **Programmi e caratteristiche**.
3. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
4. Clic **RIMUOVERE** nella finestra che appare.
5. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

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

1. Clicca su **Start** e poi su Impostazioni.
2. Clicca il **Sistema** nell'area Impostazioni, quindi selezionare **App**.
3. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
4. Clic **Disinstalla** di nuovo per confermare la tua scelta.
5. Clic **RIMUOVERE** nella finestra che appare.
6. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

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

5.5.3. Come posso rimuovere Bitdefender VPN?

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

- In **Windows 7**:

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

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

1. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di

controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.

2. Clic **Disinstalla** un programma o **Programmi e caratteristiche**.
3. Trovare **VPN di Bitdefender** e seleziona **Disinstalla**.
   Attendere il completamento del processo di disinstallazione.

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

5.5.4. Come posso rimuovere l'estensione Bitdefender Anti-tracker?

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

- Internet Explorer
  1. Clicca su  accanto alla barra di ricerca e seleziona Gestisci add-on. Comparirà un elenco delle estensioni installate.
  2. Clicca su Bitdefender Anti-tracker.
  3. Clicca su **Disattiva** nel lato inferiore destro.

- Google Chrome
  1. Clicca su accanto alla barra di ricerca.
  2. Seleziona **Altri strumenti** e poi **Estensioni**.
     Comparirà un elenco con le estensioni installate.
  3. Clicca su **Rimuovi** nella scheda Bitdefender Anti-tracker.
  4. Clicca su **Rimuovi** nella finestra che comparirà.

- Mozilla Firefox
  1. Clic  accanto alla barra di ricerca.

2. Seleziona **Add-on** e poi **Estensioni**.
   Viene visualizzato un elenco con le estensioni installate.
3. Clicca su ⋯ e seleziona **Rimuovi**.

5.5.5. Come posso spegnere automaticamente il dispositivo al termine della scansione?

Bitdefender offre diverse attività di scansione che puoi utilizzare per assicurarti che il tuo sistema sia privo di minacce. Eseguire una scansione dell'intero dispositivo potrebbe richiedere molto tempo in base alla propria configurazione hardware e software.

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

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

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

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

Per spegnere il dispositivo al termine di una scansione personalizzata:

1. Clicca su ⋯ accanto alla scansione personale che hai creato.
2. Clicca su **Avanti** e poi ancora su **Avanti**.

3. Seleziona la casella **Scegli quando programmare questa attività** e poi seleziona quando l'attività dovrà iniziare.
4. Clic **Salva**.

Se non vengono rilevate minacce, il dispositivo si spegnerà.

Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo. Per maggiori informazioni, fai riferimento a Procedura guidata scansione antivirus (pagina 46).

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

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

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

Per gestire le impostazioni del proxy:

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

Nota

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

- **Impostazioni proxy personalizzate** - Le impostazioni proxy che puoi configurare direttamente.
  Le seguenti impostazioni devono essere specificate:
  - **Indirizzo** - Inserisci l'indirizzo IP del server proxy.
  - **Porta** - Inserisci la porta che Bitdefender utilizza per connettersi al server proxy.
  - **Nome utente** - Inserisci un nome utente riconosciuto dal proxy.
  - **Password** - Inserisci la password valida dell'utente già specificato in precedenza.

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

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

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

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

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

- In **Windows 10** E **Finestre 11**:
  1. Digita "Sistema" nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona.
  2. Individua la sezione Sistema per trovare maggiori informazioni sul tuo sistema.

5.5.8. Come posso visualizzare gli elementi nascosti in Windows?

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

Segui questi passaggi per mostrare gli elementi nascosti in Windows:

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

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

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

5.5.9. 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 Plus rileva automaticamente altri programmi di sicurezza e ti offre la possibilità di disinstallarli.

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

- In **Windows 7**:
  1. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.
  2. Attendi per qualche istante, finché non compare l'elenco del software installato.
  3. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
  4. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

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

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

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

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

5.5.10. Come posso riavviare in modalità provvisoria?

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

Per avviare Windows in modalità provvisoria:

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

6. Per avviare Windows normalmente, riavvia semplicemente il sistema.

- In **Windows 8**, **Windows 8.1**, **Windows 10** e **Windows 11**:

  1. Lancia **Configurazione di sistema** in Windows, premendo contemporaneamente i tasti **Windows + R** sulla tastiera.
  2. Scrivi **msconfig** nella finestra di dialogo **Apri** e clicca su **OK**.
  3. Seleziona la scheda **Avvio**.
  4. Nella sezione **Opzioni di avvio**, seleziona la casella **Avvio in modalità provvisoria**.
  5. Clicca su **Rete** e poi su **OK**.
  6. Clicca su **OK** nella finestra **Configurazione di sistema**, che ti informa della necessità di riavviare il sistema per effettuare le modifiche selezionate.
     Il sistema sarà riavviato in modalità provvisoria con supporto di rete.

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

6. RISOLUZIONE DEI PROBLEMI

6.1. Risolvere i problemi più comuni

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

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

6.1.1. 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? (pagina 115).

- **Non ci sono i requisiti di sistema per l'esecuzione di Bitdefender.**
  Se il tuo dispositivo non soddisfa i requisiti di sistema, il dispositivo diventerà lento, specialmente quando si eseguono più applicazioni contemporaneamente. Per maggiori informazioni, fai riferimento a Requisiti di sistema (pagina 4).
- **Hai installato app che non utilizzi.**
  Ogni dispositivo ha programmi o app che non utilizzi. E molti programmi indesiderati sono eseguiti in background, occupando spazio su disco e memoria. Se non utilizzi un programma, disinstallalo. Ciò vale anche per qualsiasi altro programma pre-installato o di prova che ci si è dimenticati di rimuovere.

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

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

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

6.1.2. 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. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.
    2. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
    3. Clic **REINSTALLARE** nella finestra che appare.
    4. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.
  - In **Windows 8** E **Windows 8.1**:
    1. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.
    2. Clic **Disinstalla** un programma o **Programmi e caratteristiche**.
    3. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
    4. Clic **REINSTALLARE** nella finestra che appare.
    5. Attendere il completamento del processo di reinstallazione, quindi riavviare il sistema.
  - In **Windows 10** E **Finestre 11**:
    1. Clic **Inizio**, quindi fare clic su **Impostazioni**.
    2. Clicca il **Sistema** icona nell'area Impostazioni, quindi selezionare **App installate**.
    3. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
    4. Clic **Disinstalla** di nuovo per confermare la tua scelta.
    5. Clic **REINSTALLARE** nella finestra che appare.
    6. Attendere il completamento del processo di reinstallazione, quindi riavviare il sistema.

Nota

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

- **Bitdefender non è l'unica soluzione di sicurezza installata sul tuo sistema.**
  In questo caso:

  1. Rimuovi l'altra soluzione di sicurezza. Per maggiori informazioni, fai riferimento a Come posso rimuovere le altre soluzioni di sicurezza? (pagina 115).
  2. Reinstallare Bitdefender:
     - In **Windows 7**:
       a. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.
       b. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
       c. Clic **REINSTALLARE** nella finestra che appare.
       d. Attendere il completamento del processo di reinstallazione, quindi riavviare il sistema.
     - In **Windows 8** E **Windows 8.1**:
       a. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.
       b. Clic **Disinstalla** un programma o **Programmi e caratteristiche**.
       c. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
       d. Clic **REINSTALLARE** nella finestra che appare.
       e. Attendere il completamento del processo di reinstallazione, quindi riavviare il sistema.
     - In **Windows 10** E **Finestre 11**:
       a. Clic **Inizio**, quindi fare clic su **Impostazioni**.

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

c. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.

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

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

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

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

Se questa informazione non è stata utile, è possibile contattare BitDefender per avere assistenza, come descritto alla sezione Richiesta d'aiuto (pagina 137).

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

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 137).

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

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

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

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

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **PREVENZIONE DELLE MINACCE ONLINE** riquadro, fare clic **Impostazioni**.
3. Clic **Gestisci le eccezioni**.
4. Clic **+ Aggiungi un'eccezione**.

5. Digita nel campo corrispondente il nome del sito Web, il nome del dominio o l'indirizzo IP che desideri aggiungere alle eccezioni.
6. Fai clic sull'interruttore accanto a **Prevenzione delle minacce online**.
7. Clic **Salva** per salvare le modifiche e chiudere la finestra.

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

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 137).

6.1.5. 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. Clic **Impostazioni** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Seleziona il **Aggiornamento** scheda.
3. Disattiva l'interruttore **Aggiornamento silenzioso**.
4. La prossima volta che sarà disponibile un aggiornamento, ti sarà chiesto di selezionare quale aggiornamento vuoi scaricare. Seleziona solo **Aggiornamento delle firme**.
5. Bitdefender scaricherà e installerà solo il database delle informazioni sulle minacce.

6.1.6. I servizi di Bitdefender non rispondono

Questo articolo aiuta a risolvere i problemi nel caso in cui **I servizi BitDefender non funzionano**. Si potrebbe trovare questo errore:

- L'icona Bitdefender nella **barra delle applicazioni** è grigia e ti sarà comunicato che i servizi di Bitdefender non rispondono.

- La finestra BitDefender mostra che i servizi BitDefender non stanno rispondendo.

L'errore potrebbe essere causato da una delle seguenti condizioni:

- errori temporanei di comunicazione tra i servizi di BitDefender.
- alcuni servizi di BitDefender sono arrestati.
- altri programmi di sicurezza sono in esecuzione sul dispositivo contemporaneamente a Bitdefender.

Per risolvere questo errore, provare queste soluzioni:

1. Aspettare alcuni momenti e vedere se qualcosa cambia. L'errore potrebbe essere temporaneo.
2. Riavviare il dispositivo e aspettare alcuni attimi fino a quando Bitdefender è caricato. Aprire BitDefender per vedere se l'errore persiste. Riavviare il dispositivo di solito risolve il problema.
3. Controllare che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di BitDefender. Se è così si raccomanda di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente BitDefender.
   Per maggiori informazioni, fai riferimento a Come posso rimuovere le altre soluzioni di sicurezza? (pagina 115).

Se l'errore persiste, contatta i nostri operatori del supporto tecnico per ricevere assistenza, come indicato nella sezione Richiesta d'aiuto (pagina 137).

6.1.7. 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. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.
2. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
3. Clic **RIMUOVERE** nella finestra che appare.
4. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

- In **Windows 8** E **Windows 8.1**:
  1. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.
  2. Clic **Disinstallare un programma** O **Programmi e caratteristiche**.
  3. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
  4. Clic **RIMUOVERE** nella finestra che appare.
  5. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.

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

6.1.8. 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 hai avuto Bitdefender e non l'hai rimosso correttamente.**
  Per risolvere:

  1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a Come posso riavviare in modalità provvisoria? (pagina 116).
  2. Rimuovere Bitdefender dal tuo sistema:
     - In **Windows 7**:
       a. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.
       b. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
       c. Clic **RIMUOVERE** nella finestra che appare.
       d. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.
       e. Riavvia il sistema in modalità normale.
     - In **Windows 8** E **Windows 8.1**:
       a. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.
       b. Clic **Disinstallare un programma** O **Programmi e caratteristiche**.
       c. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
       d. Clic **RIMUOVERE** nella finestra che appare.
       e. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.
       f. Riavvia il sistema in modalità normale.

- In **Windows 10** E **Finestre 11**:
  a. Clic **Inizio**, quindi fai clic su Impostazioni.
  b. Clicca il **Sistema** icona nell'area Impostazioni, quindi selezionare **App installate**.
  c. Trovare **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
  d. Clic **Disinstalla** di nuovo per confermare la tua scelta.
  e. Clic **RIMUOVERE** nella finestra che appare.
  f. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.
  g. Riavvia il sistema in modalità normale.

3. Reinstalla il tuo prodotto Bitdefender.

- **In precedenza avevi un'altra soluzione di sicurezza e non l'hai rimossa correttamente.**
  Per risolvere questo:
  1. Riavvia il sistema ed entra in modalità provvisoria. Per sapere come fare, fare riferimento a Come posso riavviare in modalità provvisoria? (pagina 116).
  2. Rimuovi l'altra soluzione di sicurezza dal sistema:
     - In **Windows 7**:
       a. Clic **Inizio**, vai a **Pannello di controllo** e fare doppio clic **Programmi e caratteristiche**.
       b. Trova il nome del programma che desideri rimuovere e seleziona {1}Rimuovi{2}.
       c. Attendere il completamento del processo di disinstallazione, quindi riavviare il sistema.
     - In **Windows 8** E **Windows 8.1**:
       a. Dalla schermata Start di Windows, individuare **Pannello di controllo** (ad esempio, puoi iniziare a digitare "Pannello di controllo" direttamente nella schermata Start), quindi fare clic sulla sua icona.

b. Clic **Disinstallare un programma** O **Programmi e caratteristiche**.

c. Trova il nome del programma che desideri rimuovere e seleziona **Rimuovere**.

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

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

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

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

  c. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.

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

  Per disinstallare correttamente l'altro software, vai nel sito web del produttore ed esegui lo strumento di disinstallazione o contattalo direttamente per ricevere le istruzioni di disinstallazione.

3. Riavvia il sistema in modalità normale e reinstalla Bitdefender.

Hai già seguito i passaggi sopra indicati e la situazione non è cambiata.

Per risolvere questo:

1. Riavvia il sistema ed entra in modalità provvisoria. Per sapere come fare, fare riferimento a Come posso riavviare in modalità provvisoria? (pagina 116).
2. Usa l'opzione Ripristino configurazione di sistema di Windows per ripristinare il dispositivo a uno stato precedente all'installazione del prodotto Bitdefender.
3. Riavvia il sistema in modalità normale e contatta i nostri operatori del supporto per assistenza, come indicato nella sezione Richiesta d'aiuto (pagina 137).

6.2. Rimuovere le minacce dal sistema

Le minacce possono influenzare il sistema in molti modi diversi e l'approccio di Bitdefender dipende dal tipo di attacco della minaccia.

Poiché le minacce modificano spesso il loro comportamento, è difficile stabilire uno schema per il loro comportamento e le loro azioni.

Ci sono alcune circostanze in cui Bitdefender non può rimuovere automaticamente l'infezione della minaccia dal tuo sistema. In tali casi, è richiesto il tuo intervento.

- Ambiente di salvataggio (pagina 130)
- Cosa fare quando Bitdefender trova delle minacce sul tuo dispositivo? (pagina 131)
- Come posso rimuovere una minaccia in un archivio? (pagina 132)
- Come posso rimuovere una minaccia in un archivio di e-mail? (pagina 134)
- Cosa fare se sospetti che un file possa essere pericoloso? (pagina 135)
- Quali sono i file protetti da password nel registro della scansione? (pagina 135)
- Quali sono gli elementi ignorati nel registro della scansione? (pagina 136)
- Quali sono i file supercompressi nel registro della scansione? (pagina 136)
- Perché Bitdefender ha eliminato automaticamente un file infetto? (pagina 136)

Se non riesci a trovare il tuo problema qui, o se le soluzioni presentate non lo risolvono, puoi contattare i rappresentanti dell'assistenza tecnica di Bitdefender come presentato nel capitolo Richiesta d'aiuto (pagina 137).

6.2.1. Ambiente di salvataggio

L'**Ambiente di soccorso** è una funzionalità di Bitdefender che ti consente di controllare e disinfettare tutte le partizioni del disco rigido esistenti, interne ed esterne al tuo sistema operativo.

L'ambiente di soccorso di Bitdefender è integrato con Windows RE.

Avviare il tuo sistema nell'Ambiente di soccorso

Puoi accedere all'ambiente di soccorso solo dal tuo prodotto Bitdefender, come segue:

1. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
2. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
3. Clicca su **Apri** accanto ad **Ambiente di soccorso**.
4. Clicca su **RIAVVIA** nella finestra che comparirà.
   L'ambiente di soccorso di Bitdefender sarà pronto tra pochi istanti.

Controllare il sistema nell'Ambiente di soccorso

Per esaminare il tuo sistema nell'Ambiente di soccorso:

1. Accedi all'ambiente di soccorso, come descritto in .
2. Il processo di scansione di Bitdefender parte automaticamente non appena il sistema viene caricato nell'ambiente di soccorso.
3. Attendi il completamento della scansione. Se viene rilevata una minaccia, segui le istruzioni per rimuoverla.
4. Per uscire dall'Ambiente di soccorso, clicca sul pulsante Chiudi nella finestra dei risultati della scansione.

6.2.2. Cosa fare quando Bitdefender trova delle minacce sul tuo dispositivo?

Potresti scoprire che esiste una minaccia sul tuo dispositivo in uno dei seguenti modi:

- Hai controllato il tuo dispositivo e Bitdefender ha trovato alcuni elementi infetti.
- Un avviso di minaccia ti informa che Bitdefender ha bloccato una o più minacce sul tuo dispositivo.

In tali situazioni, aggiorna Bitdefender per assicurarti di avere il più recente database delle informazioni sulle minacce e avvia una Scansione del sistema per analizzarlo.

Al termine della scansione del sistema, seleziona l'azione desiderata per gli elementi infetti (Disinfetta, Elimina, Sposta in quarantena).

> **Avvertimento**
> Se sospetti che il file sia parte del sistema operativo Windows o che non sia un file infetto, non seguire questi passaggi e contatta l'assistenza clienti di Bitdefender il prima possibile.

Se l'azione selezionata non può essere eseguita e il registro della scansione rivela un'infezione non eliminabile, devi rimuovere manualmente i file:

Il primo metodo può essere usato in modalità normale:

1. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
   b. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
   c. Nel **Avanzate** finestra, spegnere **Scudo di Bitdefender**.
2. Visualizza gli oggetti nascosti in Windows. Per sapere come fare, fare riferimento a Come posso visualizzare gli elementi nascosti in Windows? (pagina 114).
3. Trova l'ubicazione del file infetto (controlla il registro della scansione) ed eliminalo.
4. Attiva la protezione antivirus in tempo reale di Bitdefender.

Se il primo metodo non riuscisse a rimuovere l'infezione:

1. Riavvia il sistema ed entra in modalità provvisoria. Per sapere come fare, fare riferimento a Come posso riavviare in modalità provvisoria? (pagina 116).
2. Visualizza gli oggetti nascosti in Windows. Per sapere come fare, fare riferimento a Come posso visualizzare gli elementi nascosti in Windows? (pagina 114).
3. Individuare la posizione del file infetto (controllare il registro della scansione) ed eliminarlo.
4. Riavvia il sistema ed entra in modalità normale.

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 137).

6.2.3. Come posso rimuovere una minaccia in un archivio?

Un archivio è un file o una raccolta di file compressi in un formato speciale per ridurre lo spazio su disco necessario alla loro archiviazione.

Alcuni di questi formati sono aperti, offrendo così a Bitdefender l'opportunità per controllarli all'interno e intraprendere le azioni adeguate per rimuoverli.

Altri formati dell'archivio sono chiusi parzialmente o interamente, e Bitdefender può solo rilevare la presenza di minacce al loro interno, senza poter intraprendere alcuna azione.

Se Bitdefender ti avvisa di aver rilevato una minaccia in un archivio e di non poter attuare alcuna azione, significa che non puoi rimuovere la minaccia a causa delle restrizioni sulle impostazioni di permesso dell'archivio.

Ecco come rimuovere una minaccia in un archivio:

1. Identifica l'archivio che include la minaccia, eseguendo una scansione del sistema.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
   b. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
   c. Nel **Avanzate** finestra, spegnere **Scudo di Bitdefender**.
3. Vai all'ubicazione dell'archivio e decomprimilo usando un programma di compressione, come WinZip.
4. Identifica il file infetto e lo elimina.
5. Elimina l'archivio originale per assicurarti che l'infezione sia stata rimossa completamente.
6. Ricomprimi i file in un nuovo archivio usando un'applicazione di archiviazione, come WinZip.
7. Attiva la protezione antivirus in tempo reale di Bitdefender ed esegui una scansione del sistema per assicurarti che non ci siano altre infezioni.

> **Nota**
> È importante notare che una minaccia in un archivio non è una minaccia immediata al sistema, poiché deve essere decompressa ed eseguita per infettarlo.

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 137).

6.2.4. Come posso rimuovere una minaccia in un archivio di e-mail?

Bitdefender può anche identificare le minacce nei database e-mail e negli archivi e-mail presenti sul disco rigido.

A volte devi identificare il messaggio infetto usando le informazioni fornite nel rapporto della scansione ed eliminarlo manualmente.

Ecco come rimuovere una minaccia presente in un archivio e-mail:

1. Esamina il database delle e-mail con Bitdefender.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clic **Protezione** nel menu di navigazione sul Interfaccia di Bitdefender.
   b. Nel **ANTIVIRUS** riquadro, fare clic **Aprire**.
   c. Nel **Avanzate** finestra, spegnere **Scudo di Bitdefender**.
3. Apri il rapporto della scansione e usa le informazioni d'identificazione (oggetto, da, a) dei messaggi infettati per localizzarli nel client e-mail.
4. Elimina i messaggi infetti. La maggior parte dei client e-mail spostano il messaggio eliminato in una cartella di recupero, dalla quale può essere recuperato. Dovresti assicurarti che il messaggio sia eliminato anche da questa cartella di ripristino.
5. Compatta la cartella di memorizzazione del messaggio infetto.
   - In Microsoft Outlook 2007: nel menu File, clicca su Gestione file dati. Seleziona i file delle cartelle personali (.pst) che intendi compattare e clicca su Impostazioni. Clicca su Compatta ora.
   - In Microsoft Outlook 2010 / 2013/ 2016: nel menu File, clicca su Info e poi su Impostazioni account (Aggiungi e rimuovi account o cambia le impostazioni di connessione attuali). Poi clicca su File di dati, seleziona i file delle cartelle personali (.pst) che intendi compattare e clicca su Impostazioni. Clicca su Compatta ora.

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

Se queste informazioni non sono state utili, puoi contattare Bitdefender per assistenza come descritto nella sezione Richiesta d'aiuto (pagina 137).

6.2.5. Cosa fare se sospetti che un file possa essere pericoloso?

Puoi sospettare che un file del tuo sistema sia pericoloso, anche se il prodotto Bitdefender non l'ha rilevato.

Per assicurarti che il tuo sistema sia protetto:

1. Esegui una **Scansione sistema** con Bitdefender. Per scoprire come fare, fai riferimento a {3}{4}.
2. Se il risultato della scansione non segnala nulla, ma hai ancora dubbi e vuoi essere certo che il file sia pulito, contatta gli operatori del nostro supporto tecnico per ricevere assistenza.
   Per scoprire come fare, fai riferimento a Richiesta d'aiuto (pagina 137).

6.2.6. 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.

6.2.7. 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.

6.2.8. 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.

6.2.9. Perché Bitdefender ha eliminato automaticamente un file infetto?

Se viene rilevato un file infetto, Bitdefender tenterà di disinfettarlo automaticamente. Se la disinfezione dovesse fallire, il file sarà messo in quarantena per contenere l'infezione.

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

Questo di solito è il caso di file di installazione che vengono scaricati da siti web non attendibili. Se dovessi trovarti in tale situazione, scarica il file d'installazione dal sito web del produttore o da un altro sito web affidabile.

7. OTTENERE AIUTO

7.1. Richiesta d'aiuto

Bitdefender offre ai suoi clienti un livello impareggiabile di supporto rapido e accurato. Se dovessi riscontrare un qualche problema o se avessi domande sul tuo prodotto Bitdefender, potrai usare diverse risorse online per trovare una soluzione o una risposta. Allo stesso tempo, potrai contattare il servizio clienti di Bitdefender. I nostri responsabili del supporto risponderanno alle tue domande in maniera tempestiva e ti forniranno tutto l'aiuto necessario.

7.2. Risorse online

Sono disponibili diverse risorse online per aiutarti a risolvere i tuoi problemi e le tue domande relative a Bitdefender.

- Centro di supporto di Bitdefender:
  https://www.bitdefender.it/consumer/support/
- La community di esperti di Bitdefender:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

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

7.2.1. Centro di supporto di Bitdefender

Il Centro di supporto di Bitdefender è un archivio online di informazioni sui prodotti Bitdefender. Conserva, in un formato facilmente accessibile, le notifiche sui risultati delle attività di risoluzioni bug e problemi del supporto tecnico di Bitdefender e dei team di sviluppo, oltre ad articoli più generali sulla prevenzione delle minacce, la gestione delle soluzioni di Bitdefender con spiegazioni dettagliate e molti altri articoli.

Il Centro di supporto di Bitdefender è aperto al pubblico e gratuitamente esplorabile. Le ricche informazioni che contiene sono un altro modo per fornire ai clienti di Bitdefender le conoscenze tecnologiche e le

informazioni necessarie. Tutte le richieste di informazioni o i rapporti sui difetti, provenienti dai clienti di Bitdefender, prima o poi arrivano al Centro di supporto di Bitdefender, come rapporti di disinfezione, metodi per aggirare le truffe, o articoli informativi, per integrare i file di aiuto dei prodotti.

Il Centro assistenza di Bitdefender è disponibile in qualsiasi momento al seguente indirizzo: https://www.bitdefender.it/consumer/support/.

7.2.2. La community di esperti di Bitdefender

La community di esperti è un ambiente in cui gli utenti di Bitdefender, oltre a fan e appassionati, possono interagire, scambiare idee, supportarsi a vicenda e condividere le proprie conoscenze e soluzioni. È anche un luogo creativo e fornisce feedback preziosi ai nostri team di sviluppo. I membri della community sono utenti esperti di Bitdefender, felici di aiutare altri utenti nel proprio tempo libero. Grazie al loro immenso contributo e sforzi volontari, abbiamo creato una knowledge base dove gli utenti possono trovare risposte e aiuto, ma con un tocco più umano di una semplice risposta automatizzata.

Qui potrai trovare molte conversazioni utili con utenti che utilizzano Bitdefender sui propri dispositivi. La community offre una vera connessione con i nostri membri e fa sentire la loro voce. Ti invitiamo a parteciparvi sapendo che la tua opinione e le tue informazioni saranno rispettate e apprezzate. In qualità di fornitore stimato, ci sforziamo di offrire un livello senza precedenti di supporto sempre rapido e preciso, sperando di avvicinare sempre più i nostri utenti. Abbiamo progettato la nostra community con questo obiettivo sempre in mente.

Puoi trovare la pagina web della nostra community di esperti qui:

https://community.bitdefender.com/en/

7.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia include tutte le informazioni necessarie sulle minacce informatiche più recenti. È anche dove gli esperti Bitdefender condividono trucchi e suggerimenti su come restare protetti da hacker, violazioni, furti d'identità e tentativi d'impersonificazione dei social.

La pagina web di Bitdefender Cyberpedia è disponibile qui:

https://www.bitdefender.com/cyberpedia/.

7.3. Informazioni di contatto

Una comunicazione efficiente è la chiave per un business di successo. Dal 2001 BITDEFENDER ha stabilito una reputazione indiscutibile impegnandosi costantemente per una migliore comunicazione in modo da superare le aspettative dei nostri clienti e partner. In caso di domande, non esitate a contattarci direttamente tramite il ns Centro di supporto di Bitdefender (pagina 137).

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

7.3.1. Distributori locali

I distributori locali di Bitdefender sono pronti a rispondere a ogni richiesta inerente le loro zone operative, sia in ambito commerciale sia generale.

Per trovare un distributore di Bitdefender nel tuo paese:

1. Vai a https://www.bitdefender.com/partners/partner-locator.html.
2. Seleziona il tuo paese e la tua città, utilizzando le opzioni corrispondenti.

GLOSSARIO

Codice di attivazione

È una chiave unica che può essere acquistata dal rivenditore e usata per attivare un servizio o un prodotto specifico. Un codice di attivazione consente l'attivazione di un abbonamento valido per un determinato periodo di tempo e un certo numero di dispositivi. Inoltre, può anche essere utilizzato per estendere un abbonamento, a condizione che venga generato per lo stesso prodotto o servizio.

ActiveX

ActiveX è un modello per la scrittura di programmi in modo che altri programmi e il sistema operativo possano chiamarli. La tecnologia ActiveX viene utilizzata con Microsoft Internet Explorer per creare pagine Web interattive che sembrano e si comportano come programmi per computer, piuttosto che come pagine statiche. Con ActiveX, gli utenti possono porre o rispondere a domande, utilizzare pulsanti e interagire in altri modi con la pagina web. I controlli ActiveX vengono spesso scritti utilizzando Visual Basic. Active X si distingue per una completa mancanza di controlli di sicurezza; gli esperti di sicurezza informatica ne scoraggiano l'uso su Internet.

Minaccia persistente avanzata

Advanced Persistent Threat (APT) sfrutta le vulnerabilità dei sistemi per rubare informazioni importanti per consegnarle alla fonte. Grandi gruppi come organizzazioni, aziende o governi sono presi di mira da questa minaccia. L'obiettivo di una minaccia persistente avanzata è rimanere inosservato per lungo tempo essendo in grado di monitorare e raccogliere informazioni importanti senza danneggiare le macchine mirate. Il metodo utilizzato per iniettare la minaccia nella rete è attraverso un file PDF o un documento di Office che sembra innocuo in modo che ogni utente possa eseguire i file.

Adware

L'adware è spesso combinato con un'app host fornita gratuitamente a condizione che l'utente accetti l'adware. Poiché le app adware vengono generalmente installate dopo che l'utente ha accettato un contratto di licenza che stabilisce lo scopo dell'app, non viene commesso alcun reato. Tuttavia, le pubblicità pop-up possono diventare fastidiose e in alcuni casi

degradare le prestazioni del sistema. Inoltre, le informazioni raccolte da alcune di queste app possono causare problemi di privacy per gli utenti che non erano pienamente a conoscenza dei termini del contratto di licenza.

Archivio

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

Un file che contiene uno o più file in un formato compresso.

Porta sul retro

Un buco nella sicurezza di un sistema deliberatamente lasciato in essere da progettisti o manutentori. La motivazione di tali buchi non è sempre sinistra; alcuni sistemi operativi, ad esempio, escono dalla confezione con account privilegiati destinati all'uso da parte dei tecnici dell'assistenza sul campo o dei programmatori di manutenzione del fornitore.

Settore di avvio

Un settore all'inizio di ogni disco che identifica l'architettura del disco (dimensione del settore, dimensione del cluster e così via). Per i dischi di avvio, il settore di avvio contiene anche un programma che carica il sistema operativo.

Avvio virus

Una minaccia che infetta il settore di avvio di un disco fisso o floppy. Un tentativo di avvio da un dischetto infettato da un virus del settore di avvio causerà l'attivazione della minaccia nella memoria. Ogni volta che avvierai il tuo sistema da quel momento in poi, avrai la minaccia attiva in memoria.

Botnet

Il termine “botnet” è composto dalle parole “robot” e “network”. Le botnet sono dispositivi connessi a Internet infettati da minacce e possono essere utilizzati per inviare e-mail di spam, rubare dati, controllare da remoto dispositivi vulnerabili o diffondere spyware, ransomware e altri tipi di minacce. Il loro obiettivo è quello di infettare il maggior numero possibile di dispositivi connessi, come PC, server, dispositivi mobili o IoT appartenenti a grandi aziende o industrie.

Navigatore

Abbreviazione di browser Web, un'app software utilizzata per individuare e visualizzare pagine Web. I browser più diffusi includono Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Questi sono browser

grafici, il che significa che possono visualizzare grafica e testo. Inoltre, la maggior parte dei browser moderni può presentare informazioni multimediali, inclusi audio e video, sebbene richiedano plug-in per alcuni formati.

Attacco di forza bruta

Attacco di indovinazione della password utilizzato per irrompere in un sistema informatico inserendo possibili combinazioni di password, per lo più a partire dalla password più facile da indovinare.

Riga di comando

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

Biscotti

Nell'industria di Internet, i cookie sono descritti come piccoli file contenenti informazioni su singoli computer che possono essere analizzati e utilizzati dagli inserzionisti per tenere traccia dei tuoi interessi e gusti online. In questo ambito, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di indirizzare gli annunci direttamente a ciò che hai dichiarato di essere i tuoi interessi. È un'arma a doppio taglio per molte persone perché, da un lato, è efficiente e pertinente in quanto si vedono solo annunci su ciò che ti interessa. cosa clicchi. Comprensibilmente, c'è un dibattito sulla privacy e molte persone si sentono offese dall'idea di essere viste come un "numero SKU" (sai, il codice a barre sul retro dei pacchi che viene scansionato alla cassa della drogheria) . Sebbene questo punto di vista possa essere estremo, in alcuni casi è accurato.

Cyber bullismo

Quando coetanei o estranei commettono atti violenti contro i bambini apposta per ferirli fisicamente. Per danneggiare emotivamente, gli aggressori inviano messaggi meschini o foto poco lusinghiere, isolando così le loro vittime dagli altri o sentendosi frustrate.

Dizionario Attacco

Attacchi di indovinazione della password utilizzati per irrompere in un sistema informatico inserendo una combinazione di parole comuni per generare potenziali password. Lo stesso metodo viene utilizzato per indovinare le chiavi di decrittazione di messaggi o documenti crittografati.

Gli attacchi con dizionario hanno successo perché molte persone tendono a scegliere password brevi e con parole singole facili da indovinare.

Unità disco

È una macchina che legge e scrive dati su un disco. Un disco rigido legge e scrive dischi rigidi. Un'unità floppy accede ai dischi floppy. Le unità disco possono essere interne (alloggiate all'interno di un computer) o esterne (alloggiate in una scatola separata che si collega al computer).

Scaricamento

Per copiare i dati (di solito un intero file) da una fonte principale a un dispositivo periferico. Il termine è spesso usato per descrivere il processo di copia di un file da un servizio online al proprio computer. Il download può anche riferirsi alla copia di un file da un file server di rete a un computer in rete.

E-mail

Mail elettronica. Un servizio che invia messaggi sui computer tramite reti locali o globali.

Eventi

Un'azione o un evento rilevato da un programma. Gli eventi possono essere azioni dell'utente, come fare clic su un pulsante del mouse o premere un tasto, o occorrenze di sistema, come l'esaurimento della memoria.

Exploit

Un modo per sfruttare diversi bug o vulnerabilità presenti in un computer (software o hardware). Pertanto, gli hacker possono ottenere il controllo di computer o reti.

Falso positivo

Si verifica quando uno scanner identifica un file come infetto quando in realtà non lo è.

Estensione del nome file

La parte di un nome di file, dopo il punto finale, che indica il tipo di dati memorizzati nel file. Molti sistemi operativi utilizzano estensioni di file, ad esempio Unix, VMS e MS-DOS. Di solito sono da una a tre lettere (alcuni tristi vecchi sistemi operativi non supportano più di tre). Gli esempi includono "c" per codice sorgente C, "ps" per PostScript, "txt" per testo arbitrario.

Euristico

Un metodo basato su regole per identificare nuove minacce. Questo metodo di scansione non si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione euristica è che non viene ingannata da una nuova variante di una minaccia esistente. Tuttavia, potrebbe occasionalmente segnalare codice sospetto nei normali programmi, generando il cosiddetto "falso positivo".

Vaso di miele

Un sistema informatico esca impostato per attirare gli hacker per studiare il modo in cui agiscono e identificare i metodi eretici che utilizzano per raccogliere informazioni di sistema. Le aziende e le aziende sono più interessate a implementare e utilizzare gli honeypot per migliorare il proprio stato di sicurezza generale.

IP

Protocollo Internet - Un protocollo instradabile nella suite di protocolli TCP/IP responsabile dell'indirizzamento IP, del routing e della frammentazione e riassemblaggio dei pacchetti IP.

Applet Java

Un programma Java progettato per essere eseguito solo su una pagina Web. Per utilizzare un'applet su una pagina Web, devi specificare il nome dell'applet e la dimensione (lunghezza e larghezza, in pixel) che l'applet può utilizzare. Quando si accede alla pagina Web, il browser scarica l'applet da un server e la esegue sulla macchina dell'utente (il client). Le applet differiscono dalle app in quanto sono governate da un rigido protocollo di sicurezza.

Ad esempio, anche se le applet vengono eseguite sul client, non possono leggere o scrivere dati sulla macchina del client. Inoltre, le applet sono ulteriormente limitate in modo che possano solo leggere e scrivere dati dallo stesso dominio da cui sono servite.

Registratore di tasti

Un keylogger è un'app che registra tutto ciò che digiti. I keylogger non sono di natura dannosa. Possono essere utilizzati per scopi legittimi, come il monitoraggio dell'attività dei dipendenti o dei bambini. Tuttavia, vengono sempre più utilizzati dai criminali informatici per scopi dannosi (ad esempio, per raccogliere dati privati, come credenziali di accesso e numeri di previdenza sociale).

Virus a macroistruzione

Un tipo di minaccia informatica codificata come macro incorporata in un documento. Molte app, come Microsoft Word ed Excel, supportano potenti linguaggi macro. Queste app ti consentono di incorporare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Cliente di posta

Un client di posta elettronica è un'app che consente di inviare e ricevere e-mail.

Memoria

Aree di archiviazione interne nel computer. Il termine memoria identifica l'archiviazione dei dati sotto forma di chip e la parola archiviazione viene utilizzata per la memoria che esiste su nastri o dischi. Ogni computer viene fornito con una certa quantità di memoria fisica, solitamente indicata come memoria principale o RAM.

Non euristico

Questo metodo di scansione si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione non euristica è che non si lascia ingannare da quella che potrebbe sembrare una minaccia e non genera falsi allarmi.

Predatori online

Individui che cercano di attirare minori o adolescenti in conversazioni apposta per coinvolgerli in attività sessuali illegali. I social network sono il luogo ideale in cui i bambini vulnerabili possono essere facilmente cacciati e indotti a commettere attività sessuali, online o faccia a faccia.

Programmi confezionati

Un file in un formato di compressione. Molti sistemi operativi e app contengono comandi che consentono di comprimere un file in modo che occupi meno memoria. Ad esempio, supponi di avere un file di testo contenente dieci caratteri spazio consecutivi. Normalmente, ciò richiederebbe dieci byte di archiviazione.

Tuttavia, un programma che comprime i file sostituirà i caratteri di spazio con uno speciale carattere di serie di spazi seguito dal numero di spazi da sostituire. In questo caso, i dieci spazi richiederebbero solo due byte. Questa è solo una delle tecniche di confezionamento, ce ne sono molte altre.

Sentiero

Le indicazioni esatte per un file su un computer. Queste direzioni sono solitamente descritte per mezzo del sistema di archiviazione gerarchico dall'alto verso il basso.

Il percorso tra due punti qualsiasi, ad esempio il canale di comunicazione tra due computer.

Phishing

L'atto di inviare un'e-mail a un utente che afferma falsamente di essere un'impresa legittima e consolidata nel tentativo di indurre l'utente a cedere informazioni private che verranno utilizzate per il furto di identità. L'e-mail indirizza l'utente a visitare un sito Web in cui viene chiesto di aggiornare le informazioni personali, come password e numeri di carta di credito, previdenza sociale e conto bancario, che l'organizzazione legittima già possiede. Il sito Web, tuttavia, è fasullo e impostato solo per rubare le informazioni dell'utente.

Fotone

Photon è una tecnologia di Bitdefender innovativa e discreta, progettata per minimizzare l'impatto della tua soluzione di sicurezza sulle prestazioni del sistema. Monitorando in background l'attività del PC, crea degli schemi di utilizzo, per ottimizzare i processi di avvio e scansione.

Virus polimorfo

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

Porta

Un'interfaccia su un computer alla quale puoi connettere un supporto. I PC hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, schermi e tastiere. Esternamente hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

Nelle reti TCP/IP e UDP, un endpoint per una connessione logica. Il numero della porta identifica di che tipo di porta si tratta. Ad esempio, la porta 80 viene usata per il traffico HTTP.

Ransomware

Un ransomware è un programma dannoso che prova a sottrarre illecitamente denaro agli utenti bloccando i loro sistemi vulnerabili.

CryptoLocker, CryptoWall e TeslaWall sono solo alcune delle varianti che cercano di bloccare i sistemi personali degli utenti.

L'infezione può partire, aprendo e-mail di spam, scaricando gli allegati di un messaggio o installando determinate applicazioni, il tutto lasciando l'utente ignaro di ciò che sta accadendo sul suo sistema. Gli autori di ransomware puntano a colpire soprattutto gli utenti normali e le aziende.

File di rapporto

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

Rootkit

Un rootkit è una serie di strumenti software che offre accesso a livello di amministratore a un sistema. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la propria presenza in modo da non dover essere visti dai veri amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, i login e i log. Possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche, se incorporano il software adeguato.

I rootkit non sono dannosi per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando i rootkit. Comunque, vengono principalmente utilizzati per nascondere minacce o per celare la presenza di un intruso nel sistema. Se combinati alle minacce, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e registri, ed evitare il rilevamento.

Script

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Spam

Messaggi di posta elettronica o newsgroup indesiderati. Generalmente conosciuti come e-mail non desiderate.

Spyware

Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessione a Internet, senza che questo se ne accorga, di solito per scopi pubblicitari. Le applicazioni spyware in genere sono incluse come componente nascosta di programmi freeware o shareware, che possono essere scaricati da Internet. Tuttavia, occorre segnalare che la maggioranza delle applicazioni shareware o freeware non includono alcun programma spyware. Una volta installato, uno spyware monitora le attività dell'utente su Internet e trasmette di nascosto tali informazioni a qualcun altro. Gli spyware possono anche raccogliere informazioni su indirizzi e-mail o addirittura password e numeri di carta di credito.

Gli spyware sono simili a un Trojan che gli utenti installano inconsapevolmente installando altre applicazioni. Un modo comune per diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli spyware utilizzano memoria e risorse del sistema, le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

Articoli di avvio

Qualsiasi file posizionato in questa cartella si aprirà all'avvio del computer. Ad esempio, una schermata di avvio, un file audio da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure app che possono essere elementi di avvio. Normalmente in questa cartella viene posizionato un alias di un file, al posto del file stesso.

Abbonamento

Un accordo di acquisto che offre all'utente il diritto di utilizzare un particolare prodotto o servizio su un numero specifico di dispositivi e per un certo periodo di tempo. Un abbonamento scaduto può essere rinnovato automaticamente, utilizzando le informazioni fornite dall'utente con il primo acquisto.

Area di notifica

Introdotta con Windows 95, la barra degli strumenti è situata nella barra delle applicazioni di Windows (in genere in basso vicino all'orologio) e contiene icone miniaturizzate per un accesso veloce a funzioni di sistema come fax, stampante, modem, volume e molto altro. Clicca due volte o

clicca con il pulsante destro su un'icona per visualizzare e accedere a dettagli e controlli.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di rete largamente utilizzati su Internet, che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il relativo traffico.

Minaccia

Un programma o parte di codice caricato sul computer a propria insaputa e che viene eseguito contro la propria volontà. La maggior parte delle minacce è anche in grado di auto replicarsi. Tutte le minacce informatiche sono state create dall'uomo. È relativamente facile produrre una semplice minaccia in grado di copiare sé stessa innumerevoli volte. Persino una minaccia così semplice è pericolosa in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di minaccia ancora più pericolosa è quella in grado di trasmettere sé stessa attraverso le reti superando i sistemi di sicurezza.

Aggiornamento delle informazioni sulle minacce

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

Troiano

Un programma distruttivo che si maschera da applicazione benevola. A differenza di programmi software dannosi e worm, i trojan non si replicano ma possono essere altrettanto distruttivi. Un tipo di minaccia Trojan particolarmente insidiosa è un programma che dichiara di pulire le minacce dal computer, ma al contrario le introduce.

Il termine deriva dalla storia dell'Iliade di Omero, dove i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, durante la notte, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

Aggiornamento

Una nuova versione di un prodotto software o hardware creato per sostituire una versione precedente dello stesso prodotto. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul computer; diversamente non sarà possibile installare l'aggiornamento.

Bitdefender dispone della propria funzionalità di aggiornamento, che consente la verifica manuale degli aggiornamenti, oppure l'aggiornamento automatico del prodotto.

Virtual Private Network (VPN)

È una tecnologia che consente una connessione diretta temporanea e cifrata a una determinata rete su una rete meno sicura. In questo modo, la ricezione e l'invio dei dati sono sempre sicuri e cifrati, ma soprattutto più difficili da intercettare dai pirati informatici. Una prova di sicurezza è l'autenticazione, che può essere fatta solo usando un nome utente e una password.

Verme

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