Bitdefender ANTIVIRUS PLUS

MANUALE D'USO

Bitdefender Antivirus Plus
Manuale d'uso

Data di pubblicazione 20/07/2020

Avvertenze legali

Bitdefender

Indice

INSTALLAZIONE

1. PREPARARSI ALL'INSTALLAZIONE

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

- Assicurati che il dispositivo su cui desideri installare Bitdefender soddisfi i requisiti di sistema. Se il dispositivo non soddisfa tutti i requisiti di sistema, Bitdefender non sarà installato, o, nel caso venisse installato, non funzionerà correttamente e causerà rallentamenti e instabilità. Per un elenco completo dei requisiti di sistema, consultare la sezione «*Requisiti di sistema*» (p. 3).
- Accedere al dispositivo utilizzando un account Amministratore.
- Rimuovi qualsiasi altro programma simile dal dispositivo. Se dovesse rilevarne una durante l'installazione di Bitdefender, ti sarà chiesto di disinstallarla. L'esecuzione simultanea di due programmi di sicurezza può influenzarne il funzionamento e causare problemi seri al sistema. Durante l'installazione Windows Defender sarà disattivato.
- 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.

2. REQUISITI DI SISTEMA

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

- Windows 7 con Service Pack 1
- Windows 8
- 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 su **Computer** nel desktop e poi seleziona **Proprietà** nel menu.
- In **Windows 8**, dal menu Start di Windows, localizza l'opzione **Computer** (per esempio, puoi digitare direttamente "Computer" nella finestra di ricerca del menu Start) e poi clicca sulla sua icona con il pulsante destro. In **Windows 8.1**, localizza **Questo PC**.

  Seleziona **Proprietà** nel menu inferiore. Individua la sezione **Sistema** per trovare maggiori informazioni sul tuo sistema.
- In **Windows 10**, digita **Sistema** nella casella di ricerca della barra delle attività e clicca sulla sua icona. Individua la sezione **Sistema** per trovare maggiori informazioni sul tuo sistema.

2.1. Requisiti software

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

- Microsoft Edge 40 e superiore
- Internet Explorer 10 e superiore

- Mozilla Firefox 51 e superiore
- Google Chrome 34 e superiore

3. 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 vale per più di un dispositivo (per esempio hai acquistato Bitdefender Antivirus Plus per 3 PC), ripeti il processo d'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.

3.1. Installa 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 e poi il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, clicca sul pulsante corrispondente.
     b. Clicca su **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 email che hai digitato e poi clicca sul pulsante di download corrispondente.

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

Convalidare l'installazione

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

Se il tuo sistema non soddisfa i requisiti di sistema per installare Bitdefender, sarai informato delle aree da migliorare prima di poter procedere.

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

Il pacchetto d'installazione di Bitdefender Antivirus Plus è aggiornato costantemente.

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

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

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

In questa fase possono essere eseguite due attività aggiuntive:

- Mantieni attivata l'opzione **Invia rapporti sul prodotto**. Permettendo questa opzione, i rapporti contenenti informazioni su come il prodotto viene

utilizzato sono inviati ai server Bitdefender. Queste informazioni sono essenziali per migliorare il prodotto e possono aiutarci a offrire una migliore esperienza in futuro. I rapporti non conterranno dati confidenziali, come nome o indirizzo IP, e non saranno utilizzati per scopi commerciali.

- Seleziona la lingua con cui desideri installare il prodotto.

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

Fase 2 - Installazione in corso

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

Fase 3 - Fine dell'installazione

Il tuo prodotto Bitdefender è stato installato con successo.

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

Fase 4 - Analisi del dispositivo

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

Puoi nascondere l'interfaccia della scansione cliccando su **Esegui scansione in background**. Poi, scegliere se desideri essere informato oppure no del termine della scansione.

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

Nota

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

Fase 5 - Come iniziare

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

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

3.2. 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 controllerà il sistema per convalidare l'installazione.

Se il tuo sistema non soddisfa i requisiti di sistema per installare Bitdefender, sarai informato delle aree da migliorare prima di poter procedere.

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

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

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

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

In questa fase possono essere eseguite due attività aggiuntive:

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

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

Fase 2 - Installazione in corso

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

Fase 3 - Fine dell'installazione

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

Fase 4 - Analisi del dispositivo

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

Puoi nascondere l'interfaccia della scansione cliccando su **Esegui scansione in background**. Poi, scegliere se desideri essere informato oppure no del termine della scansione.

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

Nota

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

Fase 5 - Account Bitdefender

Dopo aver completato la configurazione iniziale, comparirà la finestra Account di Bitdefender. Per attivare il prodotto e utilizzare le sue funzioni online, è necessario avere un account Bitdefender. Per maggiori informazioni, fai riferimento a «*Bitdefender Central*» (p. 30).

Procedi in base alla tua situazione.

- **Voglio creare un account Bitdefender**

  1. Digita le informazioni richieste nei campi corrispondenti. I dati forniti resteranno riservati. La password deve essere lunga almeno 8 caratteri, includendo almeno un numero o un simbolo, una lettera minuscola e una maiuscola.
  2. Prima di procedere ulteriormente devi accettare i Termini di utilizzo. Accedi ai Termini di utilizzo e leggili attentamente, in quanto contengono i termini e le condizioni con cui puoi utilizzare Bitdefender.

     Inoltre, potrai accedere e leggere l'Informativa sulla privacy.
  3. Clicca su **CREA ACCOUNT**.

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

- **Ho già un account di Bitdefender**

  1. Fare clic su **Accedi**.
  2. Inserisci l'indirizzo e-mail nel campo corrispondente e clicca su **AVANTI**.
  3. Inserisci la tua password e clicca su **ACCEDI**.

     Se hai dimenticato la password per il tuo account o vuoi semplicemente modificare quella già impostata:

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

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

c. Controlla la tua casella di posta, inserisci il codice di sicurezza che hai ricevuto e clicca su **AVANTI**.

   In alternativa, puoi cliccare su **Cambia password** nella e-mail che ti abbiamo inviato.

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

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

- **Voglio accedere usando il mio account Microsoft, Facebook o Google**

  Per accedere con il tuo account Microsoft, Facebook o Google:

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

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

Fase 6 - Attiva il prodotto

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

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

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 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 e voglio provare il prodotto gratuitamente**, poi clicca su **CONTINUA**.

Fase 7 - Come iniziare

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

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

INIZIARE

4. 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).

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.

Connettersi a reti wireless pubbliche di aeroporti, centri commerciali, bar o alberghi senza protezione potrebbe essere pericoloso per il tuo dispositivo e i tuoi dati. Principalmente, perché eventuali impostori potrebbero osservare le tue attività e trovare il momento migliore per sottrarre dati personali, ma anche perché chiunque può vedere il tuo indirizzo IP, rendendo quindi il tuo dispositivo la probabile vittima di futuri attacchi informatici. Per evitare questo tipo di spiacevoli situazioni, installa e usa la app «*VPN*» (p. 123).

Puoi memorizzare le tue password e gli account online, salvandoli con «*Protezione di Password Manager per le tue credenziali*» (p. 113) in un Portafoglio. Con una sola password principale puoi proteggere la tua privacy da eventuali intrusi che potrebbero tentare di sottrarti del denaro.

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*» (p. 105).

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*» (p. 110).

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*» (p. 133).

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*» (p. 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*» (p. 30).

Nella sezione «Come fare» (p. 43) troverai una serie di istruzioni passo passo per eseguire le attività più comuni. Se dovessi riscontrare problemi nell'utilizzare Bitdefender, controlla la sezione «*Risolvere i problemi più comuni*» (p. 143) per alcune possibili soluzioni ai problemi più comuni.

4.1. Aprire la finestra di Bitdefender

Per accedere all'interfaccia principale di Bitdefender Antivirus Plus, clicca sull'icona sul desktop.

Se necessario, puoi anche seguire i passaggi sottostanti:

- In **Windows 7**:
  1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
  2. Clicca su **Bitdefender**.
  3. Clicca su **Bitdefender Antivirus Plus** o più rapidamente, clicca due volte sull'icona di Bitdefender nell'area di notifica.
- In **Windows 8 e Windows 8.1**:

  Dal menu Start di Windows, localizza Bitdefender (per esempio, puoi digitare direttamente "Bitdefender" nella finestra di ricerca del menu Start) e poi clicca sulla sua icona. In alternativa, apri l'applicazione sul desktop e poi clicca due volte sull'icona di Bitdefender nell'area di notifica.
- In **Windows 10**:

  Digita "Bitdefender" nella casella di ricerca della barra delle applicazioni e poi clicca sull'icona. In alternativa, clicca due volte sull'icona di Bitdefender nell'area di notifica.

Per maggiori informazioni sulla finestra di Bitdefender e l'icona nell'area di notifica, fai riferimento a «*Interfaccia di Bitdefender*» (p. 20).

4.2. Notifiche

Bitdefender conserva un registro dettagliato di eventi riguardanti la sua 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  compare un contatore.

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

- Gli eventi **critici** indicato problemi importanti. Dovresti controllarli subito.
- Gli **avvisi** indicano problemi non critici. Quando hai un po' di tempo, dovresti controllarli e risolverli.
- Gli eventi **informazione** indicano operazioni avvenute con successo.

Clicca su ogni scheda per scoprire maggiori dettagli sugli eventi generati. Cliccando una sola volta su ciascun titolo di un evento, vengono mostrati alcuni dettagli: una breve descrizione, l'azione intrapresa da Bitdefender quando è successo e la data e l'ora in cui si è verificato. Se necessario, possono essere fornite opzioni per intraprendere ulteriori azioni.

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

4.3. 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 laptop funziona a batterie, si consiglia che operazioni superflue, che consumano energia aggiuntiva, siano rimandate fino a quando il laptop è connesso all'alimentazione C/A.

I Profili di Bitdefender assegnano più risorse di sistema alle applicazioni 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 rete Wi-Fi pubblica
: 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.

4.3.1. 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 **Utilities** nel menu di navigazione dell'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*» (p. 133)

4.4. 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 dell'interfaccia di Bitdefender.
2. Nella finestra **Generale**, 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. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella finestra **Generale**, 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.

4.5. 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. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Avanzate**.
3. Disattiva **Rapporti sul prodotto**.

4.6. 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. Clicca su **Impostazioni** nel menu di navigazione dell'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.

5. 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.

5.1. Icona area di notifica

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

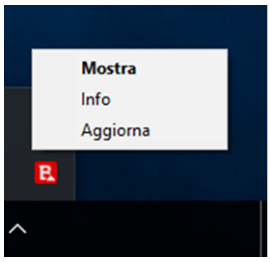
Nota
L'icona di Bitdefender potrebbe non essere sempre visibile. Per far apparire l'icona in modo permanente:

- In **Windows 7, Windows 8 e Windows 8.1**:
  1. Clicca sulla freccia nell'angolo in basso a destra dello schermo.
  2. Clicca su **Personalizza...** per aprire la finestra delle icone dell'area di Notifica.

3. Seleziona l'opzione **Mostra icone e notifiche** per l'**icona dell'agente di Bitdefender**.

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

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



Tray Icon

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

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

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

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

5.2. Menu di navigazione

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

- **Dashboard**. Da qui, puoi risolvere rapidamente eventuali problemi di sicurezza, visualizzare suggerimenti in base alle esigenze del tuo sistema e modalità d'uso, ed eseguire azioni rapide.
-
- **Protezione**. Da qui, potrai lanciare e configurare scansioni antivirus, ripristinare i dati nel caso venissero cifrati da un ransomware e configurare la protezione mentre si naviga su Internet.
- **Privacy**. Da qui, puoi creare gestori di password per i tuoi account online, effettuare pagamenti online in un ambiente sicuro e aprire la app VPN.
- **Utilities**. Da qui, puoi gestire i profili e accedere alla funzionalità Protezione dati.
- **Notifiche**. Da qui, puoi accedere alle notifiche già generate.
- **Impostazioni**. Da qui, puoi accedere alle impostazioni generali.

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

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

5.3. Dashboard

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

Tutto è a pochi clic di distanza.

La finestra è organizzata in tre sezioni principali:

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

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

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

5.3.1. Area stato di sicurezza

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

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

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

5.3.2. Autopilot

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

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

Disattivare le notifiche di Autopilot

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

Per disattivare le notifiche di Autopilot:

1. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella finestra **Generale**, disattiva **Notifiche suggerimenti**.

5.3.3. Azioni rapide

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

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

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

Le attività che puoi aggiungere all'interfaccia principale sono:

- **Scansione veloce**. Esegui una scansione veloce per rilevare prontamente possibili minacce eventualmente presenti sul tuo dispositivo.

- **Scansione di sistema**. Esegui una scansione di sistema per assicurarti che il tuo dispositivo sia privo di minacce.
- **Scansione vulnerabilità**. Esegui una scansione del dispositivo alla ricerca di vulnerabilità per assicurarti che tutte le applicazioni 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.
- **Portafogli**. Visualizza e gestisci i tuoi Portafogli.
- **Apri Safepay**. Apri Bitdefender Safepay™ per proteggere i tuoi dati sensibili durante l'elaborazione delle transazioni online.
- **Apri VPN**. Apri Bitdefender VPN per aggiungere un ulteriore livello di protezione mentre ti connetti a Internet.
- **Distruttore di file**. Esegui lo strumento Distruttore di file per rimuovere tracce di dati sensibili dal tuo dispositivo.

Per iniziare a proteggere altri dispositivi con Bitdefender:

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

   Sul tuo schermo comparirà una nuova finestra.

2. Clicca su **CONDIVIDI LINK DI DOWNLOAD**.

3. Segui i passaggi sullo schermo per installare Bitdefender.

In base alla scelta, saranno installati i seguenti prodotti di Bitdefender:

- Bitdefender Antivirus Plus su dispositivi Windows.
- Bitdefender Antivirus for Mac su dispositivi macOS.
- Bitdefender Mobile Security su dispositivi Android.
- Bitdefender Mobile Security su dispositivi iOS.

5.4. Le sezioni di Bitdefender

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

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

-  Protezione

-  Privacy
-  Utility

5.4.1. Protezione

Nella sezione Protezione puoi configurare le impostazioni avanzate di sicurezza, configurare le funzionalità di Protezione minacce online, verificare e risolvere eventuali 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*» (p. 74).

PREVENZIONE MINACCE ONLINE

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

Per maggiori informazioni su come configurare Bitdefender per proteggere le tue attività sul web, fai riferimento a «*Prevenzione minacce online*» (p. 98).

ADVANCED THREAT DEFENSE

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

Per maggiori informazioni su come tenere il sistema al sicuro dalle minacce, fai riferimento a «*Advanced Threat Defense*» (p. 95).

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*» (p. 101).

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*» (p. 110).

5.4.2. Privacy

Nella sezione Privacy, puoi aprire la app Bitdefender VPN, proteggere le tue transazioni online e mantenere sicura la tua navigazione.

Le funzionalità che puoi gestire nella sezione Privacy sono:

VPN

VPN protegge le tue attività online e nasconde il tuo indirizzo IP ogni volta che ti connetti a reti wireless non protette mentre sei in aeroporti, centri commerciali, bar o alberghi. Inoltre, puoi accedere a contenuti normalmente limitati a determinati territori.

Per maggiori informazioni su questa funzionalità, fai riferimento a «*VPN*» (p. 123).

PASSWORD MANAGER

Bitdefender Password Manager ti aiuta a memorizzare le tue password, proteggendo la tua privacy e garantendoti sempre una navigazione online sicura.

Per maggiori informazioni sulla configurazione del Password Manager, fai riferimento a «*Protezione di Password Manager per le tue credenziali*» (p. 113).

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*» (p. 126).

ANTI-TRACKER

La funzionalità Anti-Tracker ti aiuta a evitare il rilevamento, così che i tuoi dati restino privati mentre navighi online, riducendo anche il tempo necessario per caricare i siti web.

Per maggiori informazioni sulla funzionalità Anti-tracker, fai riferimento a «*Anti-tracker*» (p. 120).

5.4.3. Utility

Protezione dati

Il Distruttore di file di Bitdefender ti aiuterà a eliminare in modo permanente i dati, rimuovendoli fisicamente dal tuo disco fisso.

Per maggiori informazioni al riguardo, fai riferimento a «*Protezione dati*» (p. 140).

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 maggiori informazioni su questa funzionalità, fai riferimento a «*Profili*» (p. 133).

5.5. Modificare la lingua del prodotto

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

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

6. BITDEFENDER CENTRAL

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

Per installare la app Bitdefender Central sui tuoi dispositivi:

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

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

- Scarica e installa Bitdefender su sistemi operativi Windows, macOS, iOS e Android. I prodotti che è possibile scaricare sono:
  - Bitdefender Antivirus Plus
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security per Android
  - Bitdefender Mobile Security for iOS
- Gestisci e rinnova i tuoi abbonamenti di Bitdefender.
- Aggiungi nuovi dispositivi alla tua rete e gestiscili ovunque ti trovi.

6.1. Accedere a Bitdefender Central

Ci sono diversi modi per accedere a Bitdefender Central:

- Dall'interfaccia principale di Bitdefender:
  1. Clicca su **Il mio account** nel menu di navigazione nell'interfaccia di Bitdefender.
  2. Clicca su **Vai a Bitdefender Central**.
  3. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
- Dal tuo browser web:

1. Apri un browser web su un dispositivo con accesso a internet.
2. Vai a: https://central.bitdefender.com.
3. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.

- Dal tuo dispositivo Android o iOS:

  Apri la app Bitdefender Central che hai installato.

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

6.2. Autenticazione a due fattori

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

Attivare l'autenticazione a due fattori

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

Per attivare l'autenticazione a due fattori:

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

   Scegli uno dei seguenti metodi:

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

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

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

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

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

Clicca su **CONTINUA**.

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

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

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

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

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

c. Clicca su **ATTIVA**.

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

e. Clicca su **FINE**.

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

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

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

6.2.1. Aggiungere dispositivi affidabili

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

Per aggiungere dispositivi ai dispositivi affidabili:

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

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

6.3. I miei abbonamenti

La piattaforma Bitdefender Central ti dà la possibilità di gestire facilmente gli abbonamenti per tutti i tuoi dispositivi.

6.3.1. Controllare gli abbonamenti disponibili

Per controllare gli abbonamenti disponibili:

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

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

Puoi aggiungere un nuovo dispositivo a un abbonamento o rinnovarlo, selezionando una scheda d'abbonamento.

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

6.3.2. Aggiungi un nuovo dispositivo

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

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**

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

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

     Clicca su **INVIA LINK DI DOWNLOAD**. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA EMAIL**. Nota che il link di download generato è valido solo per le prossime 24 ore. Se il link dovesse scadere, dovrai generarne uno nuovo seguendo gli stessi passaggi.

     Sul dispositivo su cui vuoi installare il tuo prodotto Bitdefender, controlla l'account email che hai digitato e poi clicca sul pulsante di download corrispondente.
4. Attendi il completamento del download e poi esegui il programma d'installazione.

6.3.3. Rinnova abbonamento

Se hai disattivato il rinnovo automatico del tuo abbonamento a Bitdefender, puoi rinnovarlo manualmente seguendo questi passaggi:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **I miei abbonamenti**.
3. Seleziona la scheda di abbonamento desiderata.
4. Clicca su **RINNOVA** per continuare.

Si aprirà una pagina web nel tuo browser, da cui potrai rinnovare il tuo abbonamento a Bitdefender.

6.3.4. Attiva abbonamento

Un abbonamento può essere attivato durante la fase d'installazione, utilizzando il tuo account Bitdefender. Con il processo di attivazione, la sua validità inizia il conto alla rovescia.

Se hai acquistato un codice di attivazione da uno dei nostri rivenditori o l'hai ricevuto come omaggio, puoi aggiungere la sua disponibilità a qualsiasi abbonamento a Bitdefender esistente per l'account, a condizione che siano per lo stesso prodotto.

Per attivare un abbonamento utilizzando un codice di attivazione:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **I miei abbonamenti**.
3. Clicca sul pulsante **CODICE DI ATTIVAZIONE** e digita il codice nel campo corrispondente.
4. Clicca su **ATTIVA** per continuare.

Ora l'abbonamento è attivato. Vai al pannello **I miei dispositivi** e seleziona **INSTALLA PROTEZIONE** per installare il prodotto su uno dei tuoi dispositivi.

6.4. I miei dispositivi

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

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

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

1. Accedi a Bitdefender Central.
2. Seleziona la scheda **I miei dispositivi**.

3. Clicca sulla scheda del dispositivo desiderato e poi sull'icona nell'angolo in alto a destra dello schermo.
4. Seleziona **Impostazioni**.
5. Inserisci un nuovo nome nel campo **Nome dispositivo**, e clicca su **SALVA**.

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

1. Accedi a Bitdefender Central.
2. Seleziona la scheda **I miei dispositivi**.
3. Clicca sulla scheda del dispositivo desiderato e poi sull'icona nell'angolo in alto a destra dello schermo.
4. Seleziona **Profilo**.
5. Clicca su **Aggiungi proprietario**, poi compila i campi corrispondenti. Personalizza il profilo aggiungendo una foto e selezionando una data di nascita.
6. Clicca su **AGGIUNGI** per salvare il profilo.
7. Seleziona il proprietario desiderato dall'elenco **Proprietario dispositivo** e clicca su **ASSEGNA**.

Per aggiornare Bitdefender in remoto su un dispositivo Windows:

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

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

Una volta cliccato su una scheda di un dispositivo, saranno disponibili le seguenti schede:

- **Interfaccia**. In questa finestra puoi visualizzare maggiori dettagli sul dispositivo selezionato, oltre a controllare il suo stato di protezione, lo

stato di Bitdefender VPN e quante minacce sono state bloccate negli ultimi sette giorni. Lo stato di protezione può essere verde, quando nessun problema influenza il dispositivo, giallo quando il dispositivo richiede le tue attenzioni, e rosso, quando il dispositivo è a rischio. Quando ci sono eventuali problemi che influenzano il dispositivo, clicca sulla freccia a tendina nell'area di stato superiore per scoprire maggiori dettagli. Da qui puoi risolvere manualmente i problemi che influenzano la sicurezza del tuo dispositivo.

- **Protezione**. Da questa finestra, puoi eseguire in remoto una Scansione veloce o una Scansione di sistema sui tuoi dispositivi. Clicca sul pulsante **CONTROLLA** per avviare il processo. Puoi anche verificare quanto è stata eseguita l'ultima scansione sul dispositivo e visualizzare un rapporto della scansione più recente con tutte le informazioni più importanti.Per maggiori informazioni sui due processi di scansione, fai riferimento a Sezione 13.2.3, «*Eseguire una scansione del sistema*» e «*Eseguire una Scansione veloce*» (p. 80).
- **Vulnerabilità**. Per verificare le vulnerabilità di un dispositivo, come l'assenza di aggiornamenti di Windows, applicazioni datate o password poco sicure, clicca sul pulsante **CONTROLLA** nella scheda Vulnerabilità. Le vulnerabilità non possono essere corrette in remoto. Nel caso venisse rilevata una vulnerabilità, devi eseguire una nuova scansione del dispositivo e intraprendere le azioni consigliate. Clicca su **Maggiori dettagli** per accedere a un rapporto dettagliato sui problemi rilevati. Per maggiori dettagli su questa funzione, fai riferimento a «*Vulnerabilità*» (p. 101).

6.5. Attività

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

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

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

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

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

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

6.6. Notifiche

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

7. MANTENERE AGGIORNATO BITDEFENDER

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

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

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

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

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

- Se il tuo dispositivo si collega a Internet tramite un server proxy, devi configurare le impostazioni proxy come descritto nella sezione *«Come posso configurare Bitdefender per usare una connessione a Internet tramite proxy?»* (p. 67).
- Se sei connesso a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di Bitdefender su richiesta dell'utente. Per maggiori informazioni, fai riferimento a *«Eseguire un aggiornamento»* (p. 40).

7.1. Verificare se Bitdefender è aggiornato

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

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

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

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

7.2. Eseguire un aggiornamento

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

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

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

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

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

Per aggiornare Bitdefender in remoto su un dispositivo Windows:

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

7.3. Attivare o disattivare l'aggiornamento automatico

Per attivare o disattivare l'aggiornamento automatico:

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

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

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

7.4. Modificare le impostazioni di aggiornamento

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

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

Per regolare le impostazioni dell'aggiornamento:

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

Frequenza d'aggiornamento

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

Regole di esecuzione dell'aggiornamento

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

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

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

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

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

7.5. 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 con nuove funzionalità e miglioramenti saranno consegnati solo agli utenti che hanno installato Bitdefender 2020.

COME FARE

8. INSTALLAZIONE

8.1. Come installo 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.

   Sul tuo schermo comparirà una nuova finestra.

2. Clicca su **CONDIVIDI LINK DI DOWNLOAD**.
3. Segui le istruzioni sullo schermo per installare Bitdefender.

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

8.2. Come posso reinstallare Bitdefender?

Alcune tipiche situazioni in cui dovresti reinstallare Bitdefender sono:

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

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

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

- In **Windows 10**:

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

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

8.3. 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. 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**

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

- **Proteggi altri dispositivi**

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

  Clicca su **INVIA LINK DI DOWNLOAD**. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA EMAIL**. Nota che il link di download generato è valido solo per le prossime 24 ore. Se il link dovesse scadere, dovrai generarne uno nuovo seguendo gli stessi passaggi.

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

4. Esegui il prodotto Bitdefender che hai scaricato.

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

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

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

8.5. 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 passare gratuitamente all'ultima versione di Bitdefender, seguendo questi passaggi:

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

Può comparire in due occasioni:

- 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 **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
    2. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
    3. Clicca su **REINSTALLA** nella finestra che comparirà.
    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. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
    2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
    3. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
    4. Clicca su **REINSTALLA** nella finestra che comparirà.
    5. 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 10**:
  1. Clicca su **Start** e poi su Impostazioni.
  2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni**.
  3. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
  4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
  5. Clicca su **REINSTALLA** nella finestra che comparirà.
  6. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

     Apri l'interfaccia del tuo nuovo prodotto installato di Bitdefender per accedere alle sue funzionalità.

> **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.

- 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. Accedi a Bitdefender Central.
     b. Seleziona il pannello **I miei dispositivi** e clicca su **INSTALLA PROTEZIONE**.
     c. Seleziona una delle due opzioni disponibili:
        - **Proteggi questo dispositivo**

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

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

Clicca su **INVIA LINK DI DOWNLOAD**. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA EMAIL**. Nota che il link di download generato è valido solo per le prossime 24 ore. Se il link dovesse scadere, dovrai generarne uno nuovo seguendo gli stessi passaggi.

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

2. Esegui il prodotto Bitdefender che hai scaricato.

Per maggiori informazioni sull'installazione di Bitdefender, fai riferimento a «*Installare il tuo prodotto Bitdefender*» (p. 5).

8.6. 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: http://www.bitdefender.it/Downloads/. L'attivazione è possibile solo con un abbonamento valido.

9. BITDEFENDER CENTRAL

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

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

Per accedere con un altro account di Bitdefender:

1. Clicca sul nome del tuo account nella parte superiore dell'interfaccia di Bitdefender.
2. Clicca su **Cambia account** nell'angolo in alto a destra dello schermo per cambiare l'account collegato al dispositivo.
3. Inserisci l'indirizzo e-mail nel campo corrispondente e clicca su **AVANTI**.
4. Inserisci la tua password e clicca su **ACCEDI**.

Nota
Il prodotto Bitdefender dal tuo dispositivo cambia automaticamente in base all'abbonamento associato al nuovo account Bitdefender.
Se non ci fosse alcun abbonamento disponibile associato al nuovo account Bitdefender o si volesse trasferirlo dall'account precedente, contattare il supporto tecnico di Bitdefender, come descritto nella sezione *«Chiedere aiuto»* (p. 164).

9.2. Come posso disattivare i messaggi di aiuto di Bitdefender Central?

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

Se desideri disattivare questo tipo di messaggi:

1. Accedi a Bitdefender Central.
2. Clicca sull'icona nell'angolo in basso a destra dello schermo.
3. Clicca su **Il mio account** nel menu scorrevole.
4. Clicca su **Impostazioni** nel menu scorrevole.
5. Disattiva l'opzione **Attiva/disattiva i messaggi d'aiuto**.

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

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

- Dall'interfaccia di Bitdefender:
  1. Clicca su **Il mio account** nel menu di navigazione nell'interfaccia di Bitdefender.
  2. Clicca su **Cambia account** nell'angolo in alto a destra dello schermo.

     Comparirà una nuova finestra.
  3. Inserisci il tuo indirizzo e-mail e clicca su **AVANTI**.

     Comparirà una nuova finestra.
  4. Clicca su **Hai dimenticato la password?**.
  5. Clicca su **AVANTI**.
  6. Controlla la tua casella di posta, inserisci il codice di sicurezza che hai ricevuto e clicca su **AVANTI**.

     In alternativa, puoi cliccare su **Cambia password** nella e-mail che ti abbiamo inviato.
  7. Inserisci la nuova password che vuoi impostare e ridigitala ancora una volta. Clicca su **SALVA**.
- Dal tuo browser web:
  1. Vai a: https://central.bitdefender.com.
  2. Clicca su **ACCEDI**.
  3. Inserisci il tuo indirizzo e-mail e clicca su **AVANTI**.
  4. Clicca su **Hai dimenticato la password?**.
  5. Clicca su **AVANTI**.
  6. Verifica il tuo account e-mail e segui le istruzioni fornite per impostare una nuova password per il tuo account Bitdefender.

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

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

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

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

10. SCANSIONE CON BITDEFENDER

10.1. Come posso controllare un file o una cartella?

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

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

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

Tipiche situazioni in cui si userebbe questo metodo includono:

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

10.2. Come posso eseguire una scansione del mio sistema?

Per eseguire una scansione completa del sistema:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Clicca sul pulsante **Esegui scansione** accanto a **Scansione di sistema**.
4. Segui la procedura guidata della Scansione di sistema per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati.

   Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo. Per maggiori informazioni, fai riferimento a «*Procedura guidata scansione antivirus*» (p. 84).

10.3. Come posso programmare una scansione?

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

Per programmare una scansione:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Clicca su ••• accanto al tipo di scansione che vuoi programmare, Scansione di sistema o Scansione veloce, nella parte inferiore dell'interfaccia, poi seleziona **Modifica**.

   In alternativa, puoi creare un tipo di scansione che si adatti alle tue esigenze, cliccando su **+Crea scansione** accanto **Gestisci scansioni**.
4. Personalizza la scansione in base alle tue esigenze, poi clicca su **Avanti**.
5. Seleziona la casella accanto a **Scegli quando programmare questa attività**.

   Seleziona una delle opzioni corrispondenti per impostare un elenco:

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

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

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

10.4. Come posso creare un'attività di scansione personale?

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

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

1. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
2. Clicca su **+Crea scansione** accanto a **Gestisci scansioni**.
3. Nel campo del nome dell'attività, inserisci un nome per la scansione, seleziona i percorsi che vorresti esaminare e poi clicca su **AVANTI**.
4. Configura queste opzioni generali:
   - **Scansiona solo le applicazioni**. Puoi impostare Bitdefender per esaminare solo le app a cui si accede.
   - **Priorità attività scansione**. Puoi scegliere l'impatto che il processo di scansione dovrebbe avere sulle prestazioni del sistema.
     - Automatico - La priorità del processo di scansione dipenderà dalle attività del sistema. Per assicurarsi che la fase di scansione non influenzi le attività del sistema, Bitdefender deciderà se eseguire la scansione con una maggiore o minore priorità.
     - Alta - La priorità della fase di scansione sarà elevata. Scegliendo questa opzione, consentirai ad altri programmi di funzionare più lentamente, diminuendo il tempo necessario per completare la scansione.
     - Bassa - La priorità della fase di scansione sarà bassa. Scegliendo questa opzione, consentirai ad altri programmi di funzionare più velocemente, aumentando il tempo necessario per completare la scansione.
   - **Azioni di post scansione**. Seleziona quale azione Bitdefender dovrebbe intraprendere se non venisse rilevata alcuna minaccia:
     - Mostra la finestra del sommario
     - Spegni il dispositivo
     - Chiudi la finestra di scansione
5. Se vuoi configurare le opzioni di scansione nel dettaglio, clicca su **Mostra impostazioni avanzate**.

   Clicca su **Avanti**.
6. Se lo desideri, puoi attivare l'opzione **Programma attività di scansione** e poi scegli quando dovrebbe iniziare la scansione personalizzata che hai creato.

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

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

7. Clicca su **Salva** per salvare le impostazioni e chiudere la finestra di configurazione.

   In base ai percorsi da controllare, la scansione potrebbe richiedere un po' di tempo. Se durante la scansione venissero rilevate delle minacce, ti sarà chiesto di scegliere le azioni da intraprendere sui file rilevati.

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

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

3. Cliccare sul tasto **Impostazioni**.
4. Clicca su **Gestisci eccezioni**.
5. Clicca su **+Aggiungi un'eccezione**.
6. Inserisci il percorso della cartella che vuoi escludere dalla scansione nel campo corrispondente.

   In alternativa, puoi raggiungere la cartella cliccando sul pulsante Sfoglia nel lato destro dell'interfaccia, selezionala e clicca su **OK**.
7. Disattiva l'interruttore accanto alla funzionalità di protezione così da non esaminare la cartella. Ci sono tre opzioni:

   - Antivirus
   - Prevenzione minacce online
   - Advanced Threat Defense
8. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

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

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

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

      Comparirà una finestra di avviso. Devi confermare la tua scelta selezionando dal menu per quanto tempo desideri disattivare la protezione in tempo reale. Puoi disattivare la protezione in tempo reale per 5, 15 o 30 minuti, un'ora, in modo permanente o fino a un riavvio del sistema.
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a «*Come posso visualizzare gli elementi nascosti in Windows?*» (p. 69).

3. Ripristina il file dalla quarantena:
   a. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
   b. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
   c. Vai alla finestra **Impostazioni** e clicca su **Gestisci quarantena**.
   d. Seleziona il file e poi clicca su **Ripristina**.
4. Aggiungi il file all'elenco delle eccezioni. Per scoprire come fare, fai riferimento a «*Come posso escludere una cartella dalla scansione?*» (p. 57).

   Per impostazione predefinita, Bitdefender aggiunge automaticamente i file ripristinati nell'elenco delle eccezioni.
5. Attiva la protezione antivirus in tempo reale di Bitdefender.
6. Contatta gli operatori del nostro supporto in modo da poter rimuovere la rilevazione dell'aggiornamento delle informazioni sulle minacce. Per scoprire come fare, fai riferimento a «*Chiedere aiuto*» (p. 164).

10.7. Come posso verificare quali minacce sono state rilevate da Bitdefender?

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

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

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

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

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

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

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

11. PRIVACY PROTECTION

11.1. 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 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. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **SAFEPAY**, clicca su **Impostazioni**.
3. Nella finestra **Safepay**, clicca su **Esegui Safepay**.
4. Clicca sul pulsante  per accedere alla **tastiera virtuale**.

   Usa la **tastiera virtuale** ogni volta che devi digitare informazioni personali, come le password.

11.2. 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 dispositivo utilizzando il menu contestuale di Windows seguendo questi passaggi:

1. Clicca con il pulsante destro sul file o la cartella che vuoi eliminare in maniera definitiva, seleziona Bitdefender e poi **Distruttore di file**.
2. Clicca su **Elimina definitivamente** e conferma la tua volontà di continuare.

   Attendi che Bitdefender termini la distruzione dei file.
3. I risultati sono mostrati. Clicca su **FINE** per uscire dalla procedura guidata.

11.3. 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. Clicca su **Notifiche** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella scheda **Tutti**, seleziona la notifica sul più recente comportamento ransomware rilevato, e clicca su **File cifrati**.
3. Viene mostrato l'elenco con i file cifrati.

   Clicca su **Ripristina file** per continuare.
4. Nel caso l'intero processo di ripristino o una parte fallisse, dovrai scegliere il percorso in cui salvare i file decifrati. Clicca su **Ripristina l'ubicazione** e scegli un percorso sul tuo PC.
5. Apparirà una finestra di conferma.

   Clicca su **Fine** per terminare il processo di ripristino.

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

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

12. INFORMAZIONI UTILI

12.1. 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. Ora dalla tabella **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 «*Chiedere aiuto*» (p. 164).

12.2. Come posso rimuovere Bitdefender?

Se vuoi rimuovere il tuo Bitdefender Antivirus Plus:

- In **Windows 7**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
  2. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
  3. Clicca su **RIMUOVI** nella finestra che comparirà.

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

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

1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
3. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
4. Clicca su **RIMUOVI** nella finestra che comparirà.
5. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

- In **Windows 10**:

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

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

12.3. 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. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
2. Trova **Bitdefender VPN** e seleziona **Disinstalla**.

   Attendere che il processo di disinstallazione sia terminato.

- In **Windows 8 e Windows 8.1**:
  1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
  2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
  3. Trova **Bitdefender VPN** e seleziona **Disinstalla**.

     Attendere che il processo di disinstallazione sia terminato.
- In **Windows 10**:
  1. Clicca su **Start** e poi su Impostazioni.
  2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
  3. Trova **Bitdefender VPN** e seleziona **Disinstalla**.
  4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.

     Attendere che il processo di disinstallazione sia terminato.

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

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

- Internet Explorer
  1. Clicca su  accanto alla barra di ricerca e seleziona Gestisci add-on.

     Comparirà un elenco con le 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. Clicca su  accanto alla barra di ricerca.
2. Seleziona **Add-on** e poi **Estensioni**.

   Comparirà un elenco con le estensioni installate.

3. Clicca su ••• e seleziona **Rimuovi**.

12.5. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Scansioni**, clicca su ••• accanto a Scansione veloce o Scansione di sistema, e seleziona **Modifica**.
4. Personalizza la scansione in base alle tue esigenze e clicca su **Avanti**.
5. Seleziona la casella accanto a **Scegli quando programmare questa attività** e poi seleziona quando l'attività dovrà iniziare.

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

6. Clicca su **Salva**.

Per spegnere il dispositivo al termine di una scansione personalizzata:

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

Se non vengono rilevate minacce, il dispositivo si spegnerà.

Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo. Per maggiori informazioni, fai riferimento a «*Procedura guidata scansione antivirus*» (p. 84).

12.6. 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. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Avanzate**.

3. Attiva il **Server proxy**.
4. Clicca su **Modifica proxy**.
5. Ci sono due opzioni per determinare le impostazioni proxy:
   - **Importa le impostazioni del proxy dal browser predefinito** - le impostazioni del proxy dell'utente attuale, estratte dal browser predefinito. Se il server proxy richiede un nome utente e una password, devi indicarli nei rispettivi campi.

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

   - **Impostazioni proxy personalizzate** - le impostazioni proxy che puoi configurare direttamente. Le seguenti impostazioni devono essere specificate:
     - **Indirizzo** - inserisci l'indirizzo IP del server proxy.
     - **Porta** - inserisci la porta che Bitdefender utilizza per connettersi al server proxy.
     - **Nome utente** - inserisci un nome utente riconosciuto dal proxy.
     - **Password** - inserisci la password dell'utente già specificato in precedenza.
6. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

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

12.7. 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. Individua **Risorse del computer** nel menu **Start**.
  3. Clicca con il pulsante destro su **Computer** e seleziona **Proprietà**.
  4. Vai in **Sistema** per verificare le informazioni sul tuo sistema.

- Per **Windows 8**:

  1. Dal menu Start di Windows, localizza l'opzione **Computer** (puoi anche digitare direttamente "Computer" nella finestra di ricerca del menu Start) e poi clicca sulla sua icona con il pulsante destro.

     In **Windows 8.1**, localizza **Questo PC**.

  2. Seleziona **Proprietà** nel menu inferiore.
  3. Controlla in Sistema per verificare il tipo di sistema.

- In **Windows 10**:

  1. Digita "Sistema" nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona.
  2. Individua la sezione Sistema per trovare maggiori informazioni sul tuo sistema.

12.8. 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 poi seleziona **Pannello di controllo**.

   In **Windows 8 e Windows 8.1**: dal menu Start di Windows, localizza il **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella schermata Start) e poi clicca sulla sua icona.

2. Seleziona **Opzioni cartella**.
3. Vai alla scheda **Visualizza**.
4. Seleziona **Mostra file e cartelle nascoste**.
5. Deseleziona **Nascondi estensioni per i file conosciuti**.
6. Deseleziona **Nascondi file protetti del sistema operativo**.
7. Clicca su **Applica** e poi su **OK**.

In **Windows 10**:

1. Digita "Visualizza cartelle e file nascosti" nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona.

2. Seleziona **Visualizza cartelle, file e unità nascosti**.
3. Deseleziona **Nascondi estensioni per i file conosciuti**.
4. Deseleziona **Nascondi file protetti del sistema operativo**.
5. Clicca su **Applica** e poi su **OK**.

12.9. 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. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
  2. Attendi per qualche istante, finché non compare l'elenco del software installato.
  3. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
  4. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
- In **Windows 8 e Windows 8.1**:
  1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
  2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
  3. Attendi per qualche istante, finché non compare l'elenco del software installato.

4. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
5. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

- In **Windows 10**:

1. Clicca su **Start** e poi su Impostazioni.
2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni**.
3. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
5. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

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

12.10. 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 e Windows 10**:

1. Esegui **Configurazione di sistema** in Windows, premendo contemporaneamente i tasti **Windows + R** sulla tastiera.
2. Digita **msconfig** nella finestra di dialogo **aperta** e clicca su **OK**.
3. Seleziona la scheda **Avvio**.
4. Nella sezione **Opzioni di avvio**, seleziona la casella **Modalità provvisoria**.
5. Clicca su **Rete** e poi su **OK**.
6. Clicca su **OK** nella finestra **Configurazione di sistema**, che ti informerà della necessità di riavviare il sistema per effettuare le modifiche selezionate.

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

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

GESTIRE LA PROPRIA SICUREZZA

13. PROTEZIONE ANTIVIRUS

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

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

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

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

- Scansione su richiesta - Permette di rilevare e rimuovere minacce già residenti nel tuo sistema. Si tratta della classica scansione antivirus avviata dall'utente. Si sceglie quale unità, cartella o file Bitdefender deve controllare e Bitdefender li esamina, su richiesta.

Bitdefender controlla automaticamente ogni supporto rimovibile che è collegato al dispositivo per assicurarti di accedervi in sicurezza. Per maggiori informazioni, fai riferimento a «*Scansione automatica di supporti rimovibili*» (p. 88).

Gli utenti più esperti possono configurare le eccezioni della scansione, se non desiderano controllare determinati file o estensioni. Per maggiori informazioni, fai riferimento a «*Configurare le eccezioni della scansione*» (p. 90).

Quando rileva una minaccia, Bitdefender tenterà automaticamente di rimuovere il codice dannoso dal file infetto, ricostruendo il file originale. Questa operazione è denominata disinfezione. I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione. Per maggiori informazioni, fai riferimento a «*Gestire i file in quarantena*» (p. 93).

Se il tuo dispositivo è stato infettato da una minaccia, fai riferimento a «*Rimuovere le minacce dal sistema*» (p. 156). Per aiutarti a ripulire il tuo dispositivo dalle minacce che non possono essere rimosse dal sistema operativo Windows, Bitdefender ti offre una «*Ambiente di soccorso*» (p. 156).

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.

13.1. 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.

13.1.1. Attivare o disattivare la protezione in tempo reale

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

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

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

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

- **Scansiona solo le applicazioni.** Puoi impostare Bitdefender per esaminare solo le app a cui si accede.
- **Scansiona applicazioni potenzialmente indesiderate.** Seleziona questa opzione per esaminare le applicazioni indesiderate. Un'applicazione potenzialmente indesiderata (PUA) o un programma potenzialmente indesiderato (PUP) è un software, in genere fornito con un software freeware, che mostrerà pop-up o installerà una barra di strumenti nel browser predefinito. Alcuni modificheranno la homepage o il motore di ricerca, altri eseguiranno diversi processi in background rallentando il PC o mostreranno numerose pubblicità. Tali programmi possono essere installati senza il tuo consenso (vengono anche chiamati adware) o sono spesso inclusi in modo predefinito nei kit di installazione rapida (ad-supported).
- **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 archivi.** La scansione degli archivi è un processo lento e che richiede molte risorse, che quindi non è consigliato per la protezione in tempo reale. Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del sistema. La minaccia può colpire il sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la protezione in tempo reale.

  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.** È possibile impostare Bitdefender per controllare i settori di boot del disco rigido. Questo settore del disco rigido contiene il codice necessario per inizializzare il processo di avvio del computer. Quando una minaccia infetta il settore di boot, il disco potrebbe non essere accessibile e potrebbe non essere possibile avviare il sistema e accedere ai dati.
- **Esamina solo file nuovi e modificati.** Controllando solo i file modificati o nuovi, potresti migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.
- **Scansione keylogger.** Seleziona questa opzione per eseguire una scansione del sistema alla ricerca di applicazioni keylogger. I keylogger registrano ciò che digiti sulla tastiera per poi inviare queste informazioni tramite Internet a un hacker. L'hacker può trovare informazioni sensibili nei dati rubati, come numeri e password di un conto corrente, e usarle per ottenere benefici personali.
- **Scansione immediata all'avvio.** Seleziona l'opzione **Scansione immediata all'avvio** per eseguire la scansione all'avvio, quando vengono caricati tutti i servizi più importanti. Lo scopo di questa funzione è migliorare il rilevamento delle minacce all'avvio del sistema e il tempo necessario per avviare il sistema stesso.

Azioni intraprese sulle minacce rilevate

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

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Avanzate**, scorri verso il basso nella finestra finché non trovi l'opzione **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 database delle informazioni sulle minacce di Bitdefender. Bitdefender tenterà automaticamente di rimuovere il codice dannoso dal file infetto e di ricostruire il file originale. Questa operazione è denominata disinfezione.

  I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Per maggiori informazioni, fai riferimento a «*Gestire i file in quarantena*» (p. 93).

  > **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 sono stati 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 impedire una potenziale infezione.

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

- **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 file 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*» (p. 93).

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

13.1.3. Ripristinare le impostazioni predefinite

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

Per ripristinare le impostazioni predefinite della protezione in tempo reale:

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

13.2. 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.

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

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

13.2.2. Eseguire una Scansione veloce

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

Per eseguire una scansione veloce:

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

13.2.3. Eseguire una scansione del sistema

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

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

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

- Assicurati che Bitdefender sia aggiornato con il suo database delle informazioni delle minacce. Eseguire la scansione con un database delle informazioni delle minacce obsoleto può impedire a Bitdefender di rilevare nuove minacce, trovate dopo l'ultimo aggiornamento. Per maggiori informazioni, fai riferimento a «*Mantenere aggiornato Bitdefender*» (p. 39).
- Chiudere tutti i programmi aperti.

Se desideri controllare ubicazioni particolari sul tuo dispositivo o impostare le opzioni di scansione, configura ed esegui una scansione personale. Per maggiori informazioni, fai riferimento a «*Configurare una scansione personale*» (p. 81).

Per eseguire una scansione del sistema:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Scansioni**, clicca sul pulsante **Esegui scansione** accanto a **Scansione di sistema**.
4. La prima volta che esegui una Scansione di sistema, ti sarà presentata questa funzionalità. Clicca su **OK, ho capito** per continuare.
5. Segui la procedura guidata della scansione antivirus per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati. Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

13.2.4. Configurare una scansione personale

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

Per configurare una nuova scansione personalizzata nei dettagli:

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

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

   Clicca su **Avanti**.
7. Se lo desideri, puoi attivare **Programma attività di scansione** e poi scegli quando dovrebbe iniziare la scansione personalizzata che hai creato.
   - All'avvio del sistema
   - Giornalmente
   - Mensilmente

- Settimanalmente

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

8. Clicca su **Salva** per salvare le impostazioni e chiudere la finestra di configurazione.

   In base ai percorsi da controllare, la scansione potrebbe richiedere un po' di tempo. Se durante la scansione venissero rilevate delle minacce, ti sarà chiesto di scegliere le azioni da intraprendere sui file rilevati.

Informazioni sulle opzioni di scansione

Questa informazione potrebbe esserti utile:

- Se non conosci alcuni termini, verificali nel glossario. Puoi anche trovare informazioni utili cercando su Internet.
- **Scansiona applicazioni potenzialmente indesiderate.** Seleziona questa opzione per esaminare le applicazioni indesiderate. Un'applicazione potenzialmente indesiderata (PUA) o un programma potenzialmente indesiderato (PUP) è un software, in genere fornito con un software freeware, che mostrerà pop-up o installerà una barra di strumenti nel browser predefinito. Alcuni modificheranno la homepage o il motore di ricerca, altri eseguiranno diversi processi in background rallentando il PC o mostreranno numerose pubblicità. Tali programmi possono essere installati senza il tuo consenso (vengono anche chiamati adware) o sono spesso inclusi in modo predefinito nei kit di installazione rapida (ad-supported).
- **Scansiona archivi.** Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del sistema. La minaccia può colpire il sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la protezione in tempo reale. Tuttavia, si consiglia di usare questa opzione per rilevare e rimuovere ogni minaccia potenziale, anche se non è immediata.

  Trascina il cursore lungo la scala per escludere dalla scansione gli archivi superiori a un determinato valore di MB (Megabytes).

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

- **Esamina solo file nuovi e modificati.** Controllando solo i file modificati o nuovi, potresti migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.
- **Scansiona i settori di avvio.** È possibile impostare Bitdefender per controllare i settori di boot del disco rigido. Questo settore del disco rigido contiene il codice necessario per inizializzare il processo di avvio del computer. Quando una minaccia infetta il settore di boot, il disco potrebbe non essere accessibile e potrebbe non essere possibile avviare il sistema e accedere ai dati.
- **Scansiona memoria.** Seleziona questa opzione per controllare i programmi in esecuzione nella memoria di sistema.
- **Registro della scansione.** Seleziona questa opzione per controllare le chiavi del registro. Il registro di Windows è un database che memorizza le impostazioni e le opzioni di configurazione delle componenti del sistema operativo Windows, oltre a quelle delle applicazioni installate.
- **Scansiona i cookie.** Seleziona questa opzione per controllare i cookie memorizzati dai browser sul tuo dispositivo.
- **Scansione keylogger.** Seleziona questa opzione per eseguire una scansione del sistema alla ricerca di applicazioni keylogger. I keylogger registrano ciò che digiti sulla tastiera per poi inviare queste informazioni tramite Internet a un hacker. L'hacker può trovare informazioni sensibili nei dati rubati, come numeri e password di un conto corrente, e usarle per ottenere benefici personali.

13.2.5. Procedura guidata scansione antivirus

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

Nota
Se non compare la procedura guidata di scansione, potrebbe darsi che la procedura guidata sia configurata per un'esecuzione in background. Cerca

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

Fase 1 - Eseguire la scansione

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

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

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

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

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

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

Fase 2 - Scegliere le azioni

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

Nota

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

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

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

Esegui azioni appropriate

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

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

  I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Per maggiori informazioni, fai riferimento a «*Gestire i file in quarantena*» (p. 93).

  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 sono stati 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 impedire una potenziale infezione.

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

- **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.

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

Importante

Nella maggior parte dei casi Bitdefender disinfetta con successo i file infetti che rileva o isola l'infezione. Tuttavia, ci sono problemi che non possono essere risolti automaticamente. Se richiesto, riavvia il sistema per completare il processo di pulizia. Per maggiori informazioni e istruzioni su come rimuovere una minaccia manualmente, fai riferimento a «*Rimuovere le minacce dal sistema*» (p. 156).

13.2.6. Controllare i registri di scansione

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

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

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

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

   Qui puoi trovare tutti gli eventi della scansione anti-minacce, incluso le minacce rilevate dalla scansione all'accesso, le scansioni avviate dall'utente e le variazioni di stato per le scansioni automatiche.
3. Nell'elenco delle notifiche, puoi verificare quali scansioni sono state eseguite di recente. Clicca su una notifica per visualizzare maggiori dettagli al riguardo.
4. Per aprire il registro della scansione, clicca su **Guarda registro**.

13.3. Scansione automatica di supporti rimovibili

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

I dispositivi rilevati rientrano in una di queste categorie:

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

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

13.3.1. Come funziona?

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

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

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

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

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

Queste informazioni potrebbero esserti utili:

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

  Per scoprire come comportarsi con le minacce, fai riferimento a «*Rimuovere le minacce dal sistema*» (p. 156).

13.3.2. Gestire la scansione di supporti rimovibili

Per gestire la scansione automatica di supporti rimovibili:

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

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

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

13.4. 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. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Avanzate**.
3. Attiva o disattiva **Esamina file hosts**.

13.5. Configurare le eccezioni della scansione

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

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

Nota

Le eccezioni NON saranno applicate per la scansione contestuale. La scansione contestuale è un tipo di scansione su richiesta: clicca con il pulsante destro sul file o la cartella che desideri controllare e seleziona **Controlla con Bitdefender**.

13.5.1. Escludere file e cartelle dalla scansione

Per escludere determinati file e cartelle dalla scansione:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Impostazioni**, clicca su **Gestisci eccezioni**.
4. Clicca su **+Aggiungi un'eccezione**.
5. Inserisci il percorso della cartella che vuoi escludere dalla scansione nel campo corrispondente.

   In alternativa, puoi raggiungere la cartella cliccando sul pulsante Sfoglia nel lato destro dell'interfaccia, selezionala e clicca su **OK**.
6. Disattiva l'interruttore accanto alla funzionalità di protezione così da non esaminare la cartella. Ci sono tre opzioni:
   - Antivirus
   - Prevenzione minacce online
   - Advanced Threat Defense
7. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

13.5.2. Escludere estensioni di file dalla scansione

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

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

Per escludere estensioni di file dalla scansione:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Impostazioni**, clicca su **Gestisci eccezioni**.
4. Clicca su **+Aggiungi un'eccezione**.
5. Inserisci le estensioni che vuoi escludere dalla scansione con un punto prima di loro e separate da punto e virgola (;).

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

13.5.3. Gestire le eccezioni della scansione

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

Per gestire le eccezioni della scansione:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
3. Nella finestra **Impostazioni**, clicca su **Gestisci eccezioni**. Sarà visualizzato un elenco con tutte le tue eccezioni.
4. Per rimuovere o modificare le eccezioni della scansione, clicca su uno dei pulsanti disponibili. Procedi come segue:

   - Per rimuovere una voce dall'elenco, clicca sul pulsante accanto ad essa.
   - Per modificare una voce dalla tabella, clicca sul pulsante **Modifica** accanto ad essa. Apparirà una nuova finestra, dove potrai modificare l'estensione o il percorso da escludere e la funzionalità di sicurezza dal

quale escluderlo, a seconda delle necessità. Esegui i cambiamenti necessari, poi clicca su **MODIFICA**.

13.6. Gestire i file in quarantena

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

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

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

Per controllare e gestire i file in quarantena:

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

   Qui puoi visualizzare il nome dei file in quarantena, la loro posizione originale e il nome delle minacce rilevate.
4. I file in quarantena sono gestiti automaticamente da Bitdefender in base alle impostazioni di quarantena predefinite.

   Anche se non consigliato, puoi modificare le impostazioni della quarantena in base alle tue preferenze, cliccando su **Vedi impostazioni**.

   Clicca sugli interruttori per attivare o disattivare:

   Esamina di nuovo quarantena dopo agg. informazioni minacce
   Mantieni questa opzione attivata per eseguire automaticamente la scansione dei file in quarantena dopo ogni aggiornamento del database delle informazioni sulle minacce. I file puliti vengono spostati automaticamente alla loro ubicazione originale.

Elimina i contenuti più vecchi di 30 giorni
I file in quarantena più vecchi di 30 giorni sono eliminati automaticamente.

Crea eccezioni per i file ripristinati
I file ripristinati dalla quarantena vengono riportati alla loro posizione originale senza essere riparati e vengono esclusi automaticamente dalle scansioni future.

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

14. ADVANCED THREAT DEFENSE

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

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

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

14.1. Attivare o disattivare Advanced Threat Defense

Per attivare o disattivare Advanced Threat Defense:

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

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

14.2. Verificare gli attacchi dannosi rilevati

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

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ADVANCED THREAT DEFENSE**, clicca su **Apri**.
3. Vai alla finestra **Threat Defense**.

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

14.3. Aggiungere processi alle eccezioni

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

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

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ADVANCED THREAT DEFENSE**, clicca su **Apri**.
3. Nella finestra **Impostazioni**, clicca su **Gestisci eccezioni**.
4. Clicca su **+Aggiungi un'eccezione**.
5. Inserisci il percorso della cartella che vuoi escludere dalla scansione nel campo corrispondente.

   In alternativa, puoi raggiungere il file eseguibile cliccando sul pulsante Sfoglia nel lato destro dell'interfaccia, selezionalo e clicca su **OK**.
6. Attiva l'interruttore accanto a **Advanced Threat Defense**.
7. Clicca su **Salva**.

14.4. Rilevazioni exploit

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

Attivare o disattivare la rilevazione degli exploit

Per attivare o disattivare la rilevazione degli exploit:

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

- Vai alla finestra **Impostazioni** e clicca sull'interruttore accanto a **Rilevamento exploit** per attivare o disattivare la funzionalità.

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

15. PREVENZIONE MINACCE ONLINE

La Prevenzione minacce online di Bitdefender assicura una navigazione sicura, avvisandoti in caso di eventuali pagine web potenzialmente dannose.

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

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

Per configurare le impostazioni della Prevenzione minacce online:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **PREVENZIONE MINACCE ONLINE**, clicca su **Impostazioni**.

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

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

  Non dovresti visitare questa pagina web.

  Questa pagina web può contenere contenuti pericolosi. Se decidi di visitarlo, usa la massima cautela.

  Questa è una pagina sicura da visitare.

  Ricerca sicura valuta i risultati delle ricerche dei seguenti motori di ricerca via web:
  - Google
  - Yahoo!
  - Bing
  - Baidu

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

- Facebook
- 121

- Scansione web cifrata.

  Gli attacchi 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **PREVENZIONE MINACCE ONLINE**, clicca su **Impostazioni**.
3. Clicca su **Gestisci eccezioni**.
4. Clicca su **+Aggiungi un'eccezione**.
5. Inserisci nel campo corrispondente il nome del sito web, il nome del dominio o l'indirizzo IP che vuoi aggiungere alle eccezioni.
6. Clicca sull'interruttore accanto a **Prevenzione minacce di rete**.
7. Per rimuovere una voce dall'elenco, clicca sul pulsante accanto ad essa.

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

15.1. Avvisi di Bitdefender 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.

16. 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.

16.1. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **VULNERABILITÀ**, clicca su **Apri**.
3. Nella scheda **Scansione vulnerabilità**, clicca su **Avvia scansione** e attendi che Bitdefender esamini il tuo sistema alla ricerca di vulnerabilità. Le vulnerabilità rilevate sono raggruppate nelle 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 ruouter e la rete wireless a cui sei connesso, 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 poter restare connesso 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.

16.2. 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 Notifiche.

Per controllare e correggere i problemi rilevati:

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

   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.

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

   Aggiornamenti applicazioni
   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.

16.3. 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.

Per proteggerti dai pericoli degli hotspot pubblici non sicuri o cifrati, Bitdefender Wi-Fi Security Advisor analizza il livello di sicurezza di una rete wireless e, quando necessario, ti consiglia di utilizzare Bitdefender VPN.

Bitdefender Wi-Fi Security Advisor ti fornisce informazioni su:

- Reti Wi-Fi di casa

- Reti Wi-Fi ufficio
- Reti Wi-Fi pubbliche

16.3.1. Attivare o disattivare le notifiche di Wi-Fi Security Advisor

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

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **VULNERABILITÀ**, clicca su **Apri**.
3. Vai alla finestra **Impostazioni** e attiva o disattiva l'opzione **Wi-Fi Security Advisor**.

16.3.2. Configurare la rete Wi-Fi di casa

Per iniziare a configurare la tua rete di casa:

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

16.3.3. Configurare la rete Wi-Fi dell'ufficio

Per iniziare a configurare la tua rete dell'ufficio:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **VULNERABILITÀ**, clicca su **Apri**.
3. Vai alla finestra **Wi-Fi Security Advisor** e clicca su **Wi-Fi ufficio**.
4. Nella scheda **Wi-Fi ufficio**, clicca su **SELEZIONA WI-FI UFFICIO**.

   Viene mostrato un elenco con tutte le reti wireless a cui ti sei connesso finora.
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**.

16.3.4. 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 per aprire Bitdefender Safepay™. In questo caso, la Protezione hotspot per le reti non sicure viene attivata di default.

16.3.5. Controllare le informazioni sulle reti Wi-Fi

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

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

Rete Wi-Fi non sicura - Indica che il livello di sicurezza della rete è basso. Ciò significa che usarla comporta grossi rischi e non è consigliabile effettuare pagamenti o controllare il proprio conto bancario senza una protezione aggiuntiva. In situazioni simili, ti consigliamo di usare Bitdefender Safepay™ con l'opzione Protezione hotspot per reti non sicure attivata.

Rete Wi-Fi non sicura - Indica che il livello di sicurezza della rete è moderato. Ciò significa che potrebbe avere delle vulnerabilità e non è consigliabile effettuare pagamenti o controllare il proprio conto bancario senza una protezione aggiuntiva. In situazioni simili, ti consigliamo di usare Bitdefender Safepay™ con l'opzione Protezione hotspot per reti non sicure attivata.

Rete Wi-Fi sicura - Indica che la rete che stai utilizzando è sicura. In questo caso, puoi usare 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.

17. RISANAMENTO DA RANSOMWARE

Risanamento da ransomware di Bitdefender fa un backup dei tuoi file, come documenti, immagini, video o musica, per assicurarsi che non vengano danneggiati o vadano perduti in caso di cifratura ransomware. Ogni volta che viene rilevato un attacco ransomware, Bitdefender bloccherà tutti i processi coinvolti nell'attacco, avviando la fase di risanamento. In questo modo, potrai ripristinare i contenuti di tutti i tuoi file senza dover pagare alcun riscatto.

17.1. Attivare o disattivare il Risanamento da ransomware

Per attivare o disattivare il Risanamento da ransomware:

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.

17.2. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **RISANAMENTO DA RANSOMWARE**, clicca su **Gestisci**.
3. Nella finestra Impostazioni, attiva o disattiva l'interruttore **Ripristino automatico**.

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

17.4. Ripristinare file cifrati manualmente

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

1. Clicca su **Notifiche** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella scheda **Tutti**, seleziona la notifica sul più recente comportamento ransomware rilevato, e clicca su **File cifrati**.
3. Viene mostrato l'elenco con i file cifrati.

   Clicca su **Ripristina file** per continuare.
4. Nel caso l'intero processo di ripristino o una parte fallisse, dovrai scegliere il percorso in cui salvare i file decifrati. Clicca su **Ripristina l'ubicazione** e scegli un percorso sul tuo PC.
5. Apparirà una finestra di conferma.

   Clicca su **Fine** per terminare il processo di ripristino.

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

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png;

.pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

17.5. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **RISANAMENTO DA RANSOMWARE**, clicca su **Gestisci**.
3. Vai alla finestra **Eccezioni** e clicca su **+Aggiungi un'eccezione**.

18. PROTEZIONE DI PASSWORD MANAGER PER LE TUE CREDENZIALI

Oggi utilizziamo il dispositivo per fare acquisti o pagare le bollette online, ma anche per collegarsi ai social network o per chattare.

Ma come tutti sanno bene, non è sempre facile ricordarsi le password!

E se non si fa attenzione durante la navigazione online, le nostre informazioni personali, come l'indirizzo e-mail, le credenziali d'accesso alla chat o i dati della carta di credito possono essere compromesse.

Conservare le proprie password o informazioni personali nella propria agenda o nel computer può essere pericoloso, perché potrebbero essere consultate e utilizzate da persone che intendono rubarle e sfruttarle. Inoltre, ricordare tutte le password dei propri account online o dei propri siti web preferiti non è certo un compito facile.

Quindi, non c'è un modo per trovare subito tutte le password quando ci servono? E possiamo essere certi che le nostre password segrete siano sempre al sicuro?

Password Manager ti aiuta a memorizzare le tue password, proteggendo la tua privacy e garantendoti una navigazione online sempre sicura.

Utilizzando una sola password principale per accedere alle tue credenziali, Password Manager semplifica la protezione delle password in un Portafoglio.

Per offrire la migliore protezione per le tue attività online, Password Manager è integrato in Bitdefender Safepay™, garantendo così una soluzione unificata da tutti i metodi con cui i tuoi dati personali possono essere compromessi.

Password Manager protegge le seguenti informazioni private:

- Informazioni personali, come l'indirizzo e-mail o il numero di telefono
- Credenziali d'accesso per i siti web
- Informazioni per il conto corrente bancario o il numero della carta di credito
- Dati di accesso per gli account e-mail
- Password per le app
- Password per le reti Wi-Fi

18.1. Crea un nuovo database del Portafoglio

Il Portafoglio di Bitdefender è dove puoi archiviare i tuoi dati personali. Per un'esperienza di navigazione più semplice, devi creare un database del Portafoglio come segue:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **GESTORE PASSWORD**, clicca su **Impostazioni**.
3. Nella finestra **I miei Portafogli**, clicca su **Aggiungi Portafoglio**.
4. Clicca su **Crea nuovo**.
5. Digita le informazioni richieste nei campi corrispondenti.
   - Nome del Portafoglio - Inserisci un nome originale per il database del tuo Portafoglio.
   - Password principale - Inserisci una password per il tuo Portafoglio.
   - Suggerimento - Inserisci un suggerimento per ricordarti la password.
6. Clicca su **Continua**.
7. In questa fase, puoi scegliere di memorizzare le tue informazioni nel cloud, attivando l'interruttore accanto a **Sincronizza su tutti i miei dispositivi**. Scegli l'opzione che desideri e poi clicca su **Continua**.
8. Seleziona il browser web da cui vuoi importare le credenziali.
9. Clicca su **Termina**.

18.2. Importa un database esistente

Per importare un database del Portafoglio memorizzato in locale:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **GESTORE PASSWORD**, clicca su **Impostazioni**.
3. Nella finestra **I miei Portafogli**, clicca su **Aggiungi Portafoglio**.
4. Clicca su **Importa un database esistente**.
5. Raggiungi la posizione sul tuo dispositivo in cui hai salvato il database del Portafoglio e selezionalo.
6. Clicca su **Apri**.

7. Dai un nome al tuo Portafoglio e digita la password assegnata quando è stato creato.
8. Clicca su **Importa**.
9. Seleziona i programmi per cui vuoi importare le credenziali nel Portafoglio e poi il pulsante **Fine**.

18.3. Esporta il database del Portafoglio

Per esportare il database del tuo Portafoglio:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **GESTORE PASSWORD**, clicca su **Impostazioni**.
3. Vai alla finestra **I miei Portafogli**.
4. Clicca sull'icona ••• nel Portafoglio desiderato e seleziona **Esporta**.
5. Raggiungi la posizione sul tuo dispositivo in cui vuoi salvare il database del Portafoglio e poi scegli un nome da dargli.
6. Clicca su **Salva**.

Nota
Il Portafoglio deve essere aperto, affinché l'opzione **Esporta** sia disponibile. Se il Portafoglio che intendi esportare è bloccato, clicca su **Attiva Portafoglio** e digita la password assegnata quando è stato creato.

18.4. Sincronizzare i tuoi Portafogli nel cloud

Per attivare o disattivare la sincronizzazione dei Portafogli nel cloud:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **GESTORE PASSWORD**, clicca su **Impostazioni**.
3. Vai alla finestra **I miei Portafogli**.
4. Clicca sull'icona ••• nel Portafoglio desiderato e seleziona **Impostazioni**.
5. Scegli l'opzione che desideri nella finestra che comparirà e poi clicca su **Salva**.

Nota
Il Portafoglio deve essere aperto, affinché l'opzione **Esporta** sia disponibile. Se il Portafoglio che intendi sincronizzare è bloccato, clicca su **ATTIVA PORTAFOGLIO** e digita la password assegnata quando è stato creato.

18.5. Gestisci le tue credenziali del Portafoglio

Per gestire le tue password:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **GESTORE PASSWORD**, clicca su **Impostazioni**.
3. Vai alla finestra **I miei Portafogli**.
4. Seleziona il database del Portafoglio desiderato e clicca su **Attiva Portafoglio**.
5. Digita la password principale e clicca su **OK**.

Comparirà una nuova finestra. Seleziona la categoria desiderata dalla parte superiore della finestra:

- Identità
- Pagine web
- Online banking
- E-mail
- Applicazioni
- Reti Wi-Fi

Aggiungere/modificare le credenziali

- Per aggiungere una nuova password, seleziona la categoria desiderata in alto, clicca su **+ Aggiungi elemento**, inserisci le informazioni nei campi corrispondenti e clicca sul pulsante Salva.
- Per modificare una voce dalla tabella, selezionala e fai clic sul pulsante **Modifica** situato sulla destra.
- Per eliminare una voce, selezionala e clicca sul pulsante **Elimina**.

18.6. Attivare o disattivare la protezione del Password Manager

Per attivare o disattivare la protezione del Gestore Password:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **GESTORE PASSWORD**, attiva o disattiva l'interruttore.

18.7. Gestire le impostazioni del Password Manager

Per configurare la password principale in ogni dettaglio:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **GESTORE PASSWORD**, clicca su **Impostazioni**.
3. Vai alla finestra **Impostazioni**.

Nella sezione **Impostazioni di sicurezza**, sono disponibili le seguenti opzioni:

- **Chiedi la password principale quando accedo al dispositivo.** - Quando accedi al dispositivo, ti sarà chiesto di inserire la password principale.
- **Chiedi la password principale quando apro il browser e le applicazioni** - Quando accedi al browser o a un'applicazione, ti sarà chiesto di inserire la password principale.
- **Non chiedermi la password principale** - Quando accedi al dispositivo, un browser o una app, non ti sarà chiesto di inserire la tua password principale.
- **Blocca automaticamente il Portafoglio quando lascio il dispositivo incustodito** - Quando torni al tuo dispositivo dopo circa 15 minuti, ti sarà chiesto di inserire la password principale.

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

Migliora la tua esperienza

Per selezionare i browser o le applicazioni in cui desideri integrare il Gestore Password:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.

2. Nel pannello **GESTORE PASSWORD**, clicca su **Impostazioni**.
3. Seleziona la finestra **Impostazioni**.

   Attiva l'interruttore accanto a una app per utilizzare Gestore password e migliorare la tua esperienza:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Configurare l'opzione Compila automaticamente

La funzione Compila automaticamente semplifica la connessione con i tuoi siti web preferiti o l'accesso ai tuoi account online. La prima volta che inserisci le credenziali d'accesso ed eventuali informazioni personali nel browser web, vengono salvate e protette nel Portafoglio.

Per configurare le impostazioni di **compilazione automatica**:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **GESTORE PASSWORD**, clicca su **Impostazioni**.
3. Nella finestra **Impostazioni**, scorri fino alla scheda **Impostazioni comp. automatica**.
4. Puoi configurare le seguenti opzioni:
   - **Configura la protezione delle credenziali da parte del Password Manager**:
     - **Salva automaticamente le credenziali nel Portafoglio** - Le credenziali di accesso e altre informazioni identificabili, come dati personali o il numero della carta di credito, vengono salvati e aggiornati automaticamente nel Portafoglio.
     - **Chiedi sempre** - Ti sarà chiesto ogni volta se desideri aggiungere le credenziali al Portafoglio.
     - **Non salvare, aggiornerò le informazioni manualmente** - Le credenziali possono essere aggiunte nel Portafoglio solo manualmente.
   - **Compila automaticamente le credenziali di accesso**:
     - **Compila automaticamente le credenziali di accesso ogni volta** - Le credenziali vengono inserite automaticamente nel browser.

- **Comp. automaticamente moduli**:
  - **Inserisci direttamente i miei dati quando visito una pagina con dei moduli** - Ogni volta che Bitdefender rileva la tua intenzione di eseguire un pagamento o una registrazione online, comparirà una finestra di pop-up con le opzioni già compilate.

Gestisci le informazioni del Password Manager dal browser

Puoi facilmente gestire Password Manager direttamente dal browser, per avere a portata di mano tutti i tuoi dati più importanti. L'add-on del Portafoglio di Bitdefender è supportato dai seguenti browser: Google Chrome, Internet Explorer e Mozilla Firefox, ma è anche integrato in Safepay.

Per accedere all'estensione del Portafoglio di Bitdefender, apri il browser, consenti l'installazione dell'add-on e clicca sull'icona nella barra degli strumenti.

Il Portafoglio di Bitdefender include le seguenti opzioni:

- Apri Portafoglio - Apri il Portafoglio.
- Blocca Portafoglio - Blocca il portafoglio.
- Pagine web - Apri un sottomenu con tutti le credenziali d'accesso delle pagine web memorizzate nel Portafoglio. Clicca su **Aggiungi pagina web** per aggiungere nuove pagine web nell'elenco.
- Compila i moduli - Apri un sottomenu contenente tutte le informazioni aggiunte per una determinata categoria. Da qui puoi aggiungere nuovi dati al tuo Portafoglio.
- Generatore di password - Ti consente di generare password casuali da poter utilizzare per account esistenti o di nuova creazione. Clicca su **Mostra impostazioni avanzate** per personalizzare la complessità della password.
- Impostazioni - Apre la finestra delle impostazioni del Password Manager.
- Segnala problema - Segnala ogni problema che incontri con Bitdefender Password Manager.

19. 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 attivata nel tuo browser web, puoi evitare di essere monitorato 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.

19.1. Interfaccia anti-tracker

Quando viene attivata l'estensione anti-tracker di Bitdefender, nel tuo browser web comparirà l'icona  accanto alla barra di ricerca. Ogni volta che visiti un sito web, sull'icona è possibile rilevare un timer, che fa riferimento ai tracker rilevati e bloccati. Per visualizzare maggiori dettagli sui tracker bloccati, clicca sull'icona per aprire l'interfaccia. Oltre al numero dei tracker bloccati, puoi visualizzare il tempo richiesto dalla pagina per caricarsi e le

categorie a cui appartengono i tracker rilevati. Per visualizzare l'elenco dei siti web monitorati, 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.

19.2. Disattivare l'anti-tracker di Bitdefender

Per disattivare l'anti-tracker di Bitdefender:

- 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 di Bitdefender diventa grigia.
- Dall'interfaccia di Bitdefender:
  1. Clicca su **Privacy** nel menu di navigazione nell'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.

19.3. 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 tuo browser web.
2. Clicca sull'icona accanto alla barra di ricerca.

3. Clicca sull'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 .

20. VPN

La app VPN può essere installata dal tuo prodotto Bitdefender e utilizzata ogni volta che vuoi un livello aggiuntivo di protezione per la tua connessione. Il VPN opera come una sorta di tunnel tra il tuo dispositivo e la rete a cui ti connetti, proteggendo la tua connessione, cifrando i dati usando una cifratura di tipo bancario e nascondendo il tuo indirizzo IP, ovunque ti trovi. Il tuo traffico viene reindirizzato a un server indipendente, rendendo quindi il tuo dispositivo quasi impossibile da identificare tra la miriade di altri dispositivi che stanno usando i nostri servizi. Inoltre, mentre ti connetti a Internet tramite Bitdefender VPN, puoi accedere a contenuti che normalmente sono limitati ad alcuni paesi.

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

20.1. 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. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
  2. Nel pannello **VPN**, clicca su **Apri VPN**.

20.2. 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*» (p. 125).

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.

Mentre sei connesso, nella parte inferiore dell'interfaccia viene indicato il tempo trascorso e la banda utilizzata.

Per visualizzare interamente l'area del **Menu**, clicca sull'icona nel lato in alto a sinistra. Hai le seguenti opzioni:

- **Il mio account** - Mostra informazioni sull'account di Bitdefender e l'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:

  - **Generali**
    - 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
  - **Avanzato**
    - 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.

20.3. 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 Antivirus Plus, il che significa che potrai usarlo per la sua intera disponibilità, indipendentemente dallo stato dell'abbonamento della soluzione di sicurezza. Se l'abbonamento Bitdefender premium a VPN scadesse, ma quello a Bitdefender Antivirus Plus fosse ancora attivo, sarà riconvertito 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.

21. 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 sigillato, concepito per proteggere e mantenere private le operazioni bancarie, gli acquisti e qualsiasi altro tipo di transazione online.

Per assicurare una migliore protezione della privacy, Bitdefender Password Manager è stato integrato in Bitdefender Safepay™ per proteggere le proprie credenziali ogni volta che si desidera accedere a indirizzi privati online. Per maggiori informazioni, fai riferimento a «*Protezione di Password Manager per le tue credenziali*» (p. 113).

Bitdefender Safepay™ offre le seguenti funzioni:

- Blocca l'accesso al proprio desktop, impedendo qualsiasi tentativo di catturare delle immagini del proprio schermo.
- Protegge le tue password segrete mentre navighi online con Password Manager.
- 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 agli acquisti e alle transazioni bancarie online. Ma qualsiasi sito web può essere aperto in Bitdefender Safepay™.

21.1. Utilizzare Bitdefender Safepay™

Di norma, Bitdefender rileva l'accesso a un sito di online banking o a un negozio online in qualsiasi browser del dispositivo e ti indica di eseguirlo in Bitdefender Safepay™.

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

- Dall'interfaccia di Bitdefender:
  1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
  2. Nel pannello **SAFEPAY**, clicca su **Impostazioni**.
  3. Nella finestra **Safepay**, clicca su **Esegui Safepay**.
- Da Windows:
  - In **Windows 7**:
    1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
    2. Clicca su **Bitdefender**.
    3. Clicca su **Bitdefender Safepay™**.
  - In **Windows 8 e Windows 8.1**:

    Dal menu Start di Windows, localizza Bitdefender Safepay™ (puoi anche digitare direttamente "Bitdefender Safepay™" nella finestra di ricerca del menu Start) e poi clicca sulla sua icona.
  - In **Windows 10**:

    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  .

- Torna alla pagina precedente, vai alla successiva e aggiorna le pagine, utilizzando  rispettivamente.
- Accedi alle impostazioni di Bitdefender Safepay™, cliccando su e selezionando **Impostazioni**.
- proteggi le tue password con Password Manager cliccando su  .
- Gestisci i tuoi segnalibri cliccando su  accanto alla barra degli indirizzi.
- Apri la tastiera virtuale, cliccando su  .
- aumenta o riduci la dimensione del browser, premendo contemporaneamente **Ctrl** e i tasti **+/-** nel tastierino numerico.
- Visualizza maggiori informazioni sul tuo prodotto Bitdefender, cliccando su e selezionando **Informazioni**.
- Stampa informazioni importanti cliccando su e selezionando **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.

21.2. 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.

Manage Plugins

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

Gestisci i 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.

21.3. 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 **Segnalibri** per aprire la pagina dei Segnalibri.

> **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.

21.4. 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. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **SAFEPAY**, clicca su **Impostazioni**.
3. Nella finestra **Impostazioni**, disattiva l'interruttore accanto a **Notifiche di Safepay**.

21.5. Usare VPN con Safepay

Per effettuare pagamenti online in un ambiente sicuro mentre sei connesso a reti non affidabili, il prodotto Bitdefender può essere configurato automaticamente per lanciare la app VPN contemporaneamente a Safepay.

Per iniziare a usare la app VPN insieme a Safepay:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **SAFEPAY**, clicca su **Impostazioni**.
3. Nella finestra **Impostazioni**, attiva l'interruttore accanto a **Usa VPN con Safepay**.

22. 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, seleziona **Bitdefender** e poi l'opzione **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*» (p. 103).

UTILITY

23. 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 Lavoro
- Profilo Film
- Profilo Gioco
- Profilo rete Wi-Fi pubblica
- Profilo Modalità Batteria

Se decidi di non utilizzare i **Profili**, viene attivato un profilo **Standard**, che non offre particolari ottimizzazioni.

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.
- La Ricerca sicura è stata 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:

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

23.1. 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. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella scheda **Profili**. clicca su **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 lanciando una determinata applicazione lavorativa, Bitdefender non attiva automaticamente il profilo Lavoro, puoi aggiungere manualmente l'applicazione nell'**Elenco applicazioni lavoro**.

Per aggiungere manualmente le app all'Elenco applicazioni lavoro:

1. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella scheda **Profili**. clicca su **Impostazioni**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo 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.

23.2. 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. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella scheda **Profili**. clicca su **Impostazioni**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Film.
4. Seleziona le regolazioni del sistema da applicare, spuntando le seguenti opzioni:
   - Aumenta le prestazioni dei lettori multimediali
   - Ottimizza le impostazioni del prodotto per il profilo Film
   - Rimanda i programmi in background e le attività di manutenzione
   - Posticipa gli aggiornamenti automatici di Windows

- Modifica le impostazioni dei consumi energetici per i film

5. Clicca su **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. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella scheda **Profili**. clicca su **Impostazioni**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Film.
4. Nella finestra **Impostazioni profilo film**, clicca su **Elenco lettori**.
5. Clicca su **AGGIUNGI**.

   Comparirà una nuova finestra. Cerca il file eseguibile della app, selezionalo e clicca su **OK** per aggiungerlo all'elenco.

23.3. 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. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella scheda **Profili**. clicca su **Impostazioni**.
3. Clicca sul pulsante **Configura** nella sezione del Profilo gioco.
4. Seleziona le regolazioni del sistema da applicare, spuntando le seguenti opzioni:

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

5. Clicca su **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. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella scheda **Profili**. clicca su **Impostazioni**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Gioco.
4. Nella finestra **impostazioni profilo giochi**, clicca su **Elenco giochi**.
5. Clicca su **AGGIUNGI**.

   Comparirà una nuova finestra. Cerca il file eseguibile del gioco, selezionalo e clicca su **OK** per aggiungerlo all'elenco.

23.4. 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. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.

2. Nella scheda **Profili**. clicca su **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. Clicca su **Salva**.

23.5. 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. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella scheda **Profili**. clicca su **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. Clicca su **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 rinviato.
- Le scansioni programmate sono rinviate.

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.

23.6. Ottimizzazione in tempo reale

L'Ottimizzazione in tempo reale di Bitdefender è un plugin che migliora le prestazioni del sistema operando in background e assicurandosi di non interrompere le tue attività quando sei in una delle modalità profilo. In base al carico della CPU, il plugin monitora tutti i processi, concentrandosi su quelli che hanno un carico maggiore, per adeguarli alle tue esigenze.

Per attivare o disattivare l'Ottimizzazione in tempo reale:

1. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Nella scheda **Profili**. clicca su **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.

24. PROTEZIONE DATI

24.1. Eliminare i file in modo permanente

Quando elimini un file, non potrai più accedervi con i normali strumenti. Comunque, il file continuerà a essere archiviato sul disco rigido finché non sarà sovrascritto quando copierete nuovi file.

Il Distruttore di file di Bitdefender ti aiuterà a eliminare in modo permanente i dati, rimuovendoli fisicamente dal tuo disco fisso.

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. Clicca su **Utilities** nel menu di navigazione dell'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 termini la distruzione dei file.
   c. **Riepilogo risultati**

I risultati sono mostrati. Clicca su **Fine** per uscire dalla procedura guidata.

RISOLUZIONE DEI PROBLEMI

25. RISOLVERE I PROBLEMI PIÙ COMUNI

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

- «*Il mio sistema sembra lento*» (p. 143)
- «*La scansione non parte*» (p. 144)
- «*Non posso più usare una app*» (p. 147)
- «*Che cosa fare quando Bitdefender blocca un sito web, un dominio, un indirizzo IP o una app online che sono sicuri*» (p. 148)
- «*Come aggiornare Bitdefender con una connessione a Internet lenta*» (p. 149)
- «*I servizi Bitdefender non rispondono*» (p. 149)
- «*L'opzione Compila automaticamente nel mio Portafoglio non funziona*» (p. 150)
- «*Rimozione di Bitdefender non riuscita*» (p. 151)
- «*Il sistema non si riavvia dopo aver installato Bitdefender*» (p. 152)

Se non riesci a trovare il problema qui, o se la soluzione fornita non lo risolve, puoi contattare un operatore del supporto tecnico di Bitdefender come indicato nel capitolo «*Chiedere aiuto*» (p. 164).

25.1. Il mio sistema sembra lento

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

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

- **Bitdefender non è l'unico programma di sicurezza installato sul sistema.**

  Sebbene Bitdefender cerchi e rimuova i programmi di sicurezza trovati durante l'installazione, si consiglia di rimuovere ogni altra soluzione di sicurezza in uso prima dell'installazione di Bitdefender. Per maggiori informazioni, fai riferimento a «*Come posso rimuovere le altre soluzioni di sicurezza?*» (p. 70).

- **Non ci sono i requisiti di sistema per l'esecuzione di Bitdefender.**

  Se il tuo dispositivo non soddisfa i requisiti di sistema, il dispositivo diventerà lento, specialmente quando si eseguono più applicazioni contemporaneamente. Per maggiori informazioni, fai riferimento a «*Requisiti di sistema*» (p. 3).

- **Hai installato app che non utilizzi**.

  Ogni dispositivo ha programmi o app che non utilizzi. E molti programmi indesiderati sono eseguiti in background, occupando spazio su disco e memoria. Se non utilizzi un programma, disinstallalo. Ciò vale anche per qualsiasi altro programma pre-installato o di prova che ci si è dimenticati di rimuovere.

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

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

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

  Per avviare la scansione del sistema:

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

25.2. La scansione non parte

Questo tipo di problema può avere due cause principali:

- **Un'installazione precedente di Bitdefender che non è stata rimossa completamente o un'installazione difettosa di Bitdefender**.

  In questo caso, reinstalla Bitdefender:

  - In **Windows 7**:

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

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

    1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
    2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
    3. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
    4. Clicca su **REINSTALLA** nella finestra che comparirà.
    5. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.

  - In **Windows 10**:

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

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

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

  In questo caso:

  1. Rimuovi l'altra soluzione di sicurezza. Per maggiori informazioni, fai riferimento a «*Come posso rimuovere le altre soluzioni di sicurezza?*» (p. 70).
  2. Reinstalla Bitdefender:
     - In **Windows 7**:
       a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
       b. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
       c. Clicca su **REINSTALLA** nella finestra che comparirà.
       d. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.
     - In **Windows 8 e Windows 8.1**:
       a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
       b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
       c. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
       d. Clicca su **REINSTALLA** nella finestra che comparirà.
       e. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.
     - In **Windows 10**:
       a. Clicca su **Start** e poi su Impostazioni.
       b. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
       c. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.

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

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

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

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 164).

25.3. Non posso più usare una app

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

Dopo aver installato Bitdefender potrebbe verificarsi una di queste situazioni:

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

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

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

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

Per aggiungere il programma all'elenco delle eccezioni:

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

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

   In alternativa, puoi raggiungere il file eseguibile cliccando sul pulsante Sfoglia nel lato destro dell'interfaccia, selezionalo e clicca su **OK**.
6. Attiva l'interruttore accanto a **Advanced Threat Defense**.
7. Clicca su **Salva**.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 164).

25.4. Che cosa fare quando Bitdefender blocca un sito web, un dominio, un indirizzo IP o una app online che sono sicuri

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

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

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

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

6. Clicca sull'interruttore accanto a **Prevenzione minacce di rete**.
7. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 164).

25.5. Come aggiornare Bitdefender con una connessione a Internet lenta

Se hai una connessione a Internet lenta (ad esempio modem tramite linea telefonica), potrebbero verificarsi degli errori durante l'aggiornamento.

Per mantenere il tuo sistema aggiornato con il più recente database delle informazioni sulle minacce di Bitdefender:

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

25.6. I servizi Bitdefender non rispondono

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

- L'icona di Bitdefender nell'area di notifica è grigia e una finestra ti informa che i servizi di Bitdefender non rispondono.
- La finestra Bitdefender mostra che i servizi Bitdefender non stanno rispondendo.

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

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

Per risolvere questo errore, provare queste soluzioni:

1. Aspettare alcuni momenti e vedere se qualcosa cambia. L'errore potrebbe essere temporaneo.
2. Riavviare il dispositivo e aspettare alcuni attimi fino a quando Bitdefender è caricato. Aprire Bitdefender per vedere se l'errore persiste. Riavviare il dispositivo di solito risolve il problema.
3. Controllare che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di Bitdefender. Se è così si raccomanda di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente Bitdefender.

   Per maggiori informazioni, fai riferimento a *«Come posso rimuovere le altre soluzioni di sicurezza?»* (p. 70).

Se l'errore persiste, contatta i nostri operatori del supporto tecnico per ricevere assistenza, come indicato nella sezione *«Chiedere aiuto»* (p. 164).

25.7. L'opzione Compila automaticamente nel mio Portafoglio non funziona

Hai salvato le tue credenziali online nel Gestore Password di Bitdefender, notando così che l'opzione Compila automaticamente non sta funzionando. In genere, questo problema si verifica quando l'estensione del Portafoglio di Bitdefender non è installata nel tuo browser.

Per risolvere il problema, segui questi passaggi:

- In **Internet Explorer:**
  1. Apri Internet Explorer.
  2. Clicca su Strumenti.
  3. Clicca su Gestisci Add-on.
  4. Clicca su Barre degli strumenti ed Estensioni.
  5. Seleziona **Portafoglio di Bitdefender** e clicca su **Attiva**.

- In **Mozilla Firefox:**
  1. Apri Mozilla Firefox.
  2. Clicca sul pulsante **Apri menu** nell'angolo in alto a destra dello schermo.
  3. Clicca su Add-on.
  4. Clicca su Estensioni.
  5. Evidenzia **Portafoglio di Bitdefender** e clicca sull'interruttore accanto ad esso.
- In **Google Chrome:**
  1. Apri Google Chrome.
  2. Vai all'icona del menu.
  3. Clicca su Altri strumenti.
  4. Clicca su Estensioni.
  5. Evidenzia **Portafoglio di Bitdefender** e clicca sull'interruttore corrispondente.

> **Nota**
> L'add-on sarà disponibile una volta riavviato il browser.

Ora controlla se la funziona Completa automaticamente del Portafoglio funzioni per i tuoi account online.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 164).

25.8. Rimozione di Bitdefender non riuscita

Se desideri rimuovere il tuo prodotto Bitdefender ma il processo o il sistema si blocca, clicca su **Annulla** per interrompere l'operazione. Se questo non dovesse funzionare, riavviare il sistema.

Se la rimozione non riesce, alcuni file e alcune chiavi di registro di Bitdefender potrebbero rimanere sul sistema. Tali rimanenze potrebbero impedire una nuova installazione di Bitdefender. Potrebbero inoltre influenzare le prestazioni e la stabilità del sistema.

Per rimuovere completamente Bitdefender dal sistema:

- In **Windows 7**:

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

- In **Windows 8 e Windows 8.1**:
  1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
  2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
  3. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
  4. Clicca su **RIMUOVI** nella finestra che comparirà.
  5. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
- In **Windows 10**:
  1. Clicca su **Start** e poi su Impostazioni.
  2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
  3. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
  4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
  5. Clicca su **RIMUOVI** nella finestra che comparirà.
  6. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

25.9. Il sistema non si riavvia dopo aver installato Bitdefender

Se hai appena installato Bitdefender e non riesci più a riavviare il sistema in modalità normale potrebbero esserci varie cause per questo problema.

Molto probabilmente la causa è un'installazione precedente di Bitdefender che non è stata rimossa correttamente o un'altra soluzione di sicurezza ancora presente sul sistema.

Ecco come affrontare ogni situazione:

- **In precedenza avevi Bitdefender e non l'hai disinstallato correttamente.**

  Per risolvere:

  1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a «*Come posso riavviare in modalità provvisoria?*» (p. 71).
  2. Rimuovi Bitdefender dal tuo sistema:
     - In **Windows 7**:
       a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
       b. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
       c. Clicca su **RIMUOVI** nella finestra che comparirà.
       d. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
       e. Riavvia il sistema in modalità normale.
     - In **Windows 8 e Windows 8.1**:
       a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
       b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
       c. Trova **Bitdefender Antivirus Plus** e seleziona **Disinstalla**.
       d. Clicca su **RIMUOVI** nella finestra che comparirà.
       e. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
       f. Riavvia il sistema in modalità normale.
     - In **Windows 10**:
       a. Clicca su **Start** e poi su Impostazioni.

b. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.

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

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

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

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

g. Riavvia il sistema in modalità normale.

3. Reinstalla il tuo prodotto Bitdefender.

- **In precedenza avevi un'altra soluzione di sicurezza e non l'hai rimossa correttamente.**

  Per risolvere:

  1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a «*Come posso riavviare in modalità provvisoria?*» (p. 71).
  2. Rimuovi l'altra soluzione di sicurezza dal sistema:
     - In **Windows 7**:
       a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
       b. Trova il nome del programma che desideri rimuovere e seleziona **Rimuovi**.
       c. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
     - In **Windows 8 e Windows 8.1**:
       a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
       b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
       c. Trova il nome del programma che desideri rimuovere e seleziona **Rimuovi**.
       d. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

- In **Windows 10**:
  a. Clicca su **Start** e poi su Impostazioni.
  b. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
  c. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
  d. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

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

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

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

Per risolvere:

1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a «*Come posso riavviare in modalità provvisoria?*» (p. 71).
2. Usa l'opzione Ripristino configurazione di sistema di Windows per ripristinare il dispositivo a uno stato precedente all'installazione del prodotto Bitdefender.
3. Riavvia il sistema in modalità normale e contatta i nostri operatori del supporto per assistenza, come indicato nella sezione «*Chiedere aiuto*» (p. 164).

26. 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 soccorso*» (p. 156)
- «*Cosa fare quando Bitdefender trova delle minacce sul tuo dispositivo?*» (p. 157)
- «*Come posso rimuovere una minaccia in un archivio?*» (p. 159)
- «*Come posso rimuovere una minaccia in un archivio di e-mail?*» (p. 160)
- «*Cosa fare se sospetti che un file possa essere pericoloso?*» (p. 161)
- «*Quali sono i file protetti da password nel registro della scansione?*» (p. 161)
- «*Quali sono gli elementi ignorati nel registro della scansione?*» (p. 162)
- «*Quali sono i file supercompressi nel registro della scansione?*» (p. 162)
- «*Perché Bitdefender ha eliminato automaticamente un file infetto?*» (p. 162)

Se non riesci a trovare il problema qui, o se la soluzione fornita non lo risolve, puoi contattare un operatore del supporto tecnico di Bitdefender come indicato nel capitolo «*Chiedere aiuto*» (p. 164).

26.1. Ambiente di soccorso

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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
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 «Avviare il tuo sistema nell'Ambiente di soccorso» (p. 156).
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.

26.2. 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 il Servizio clienti di Bitdefender il prima possibile.

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

Il primo metodo può essere usato in modalità normale:

1. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
   b. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
   c. Nella finestra **Avanzate**, disattiva **Protezione di Bitdefender**.
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a «*Come posso visualizzare gli elementi nascosti in Windows?*» (p. 69).
3. Trova l'ubicazione del file infetto (controlla il registro della scansione) ed eliminalo.
4. Attiva la protezione antivirus in tempo reale di Bitdefender.

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

1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a «*Come posso riavviare in modalità provvisoria?*» (p. 71).
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a «*Come posso visualizzare gli elementi nascosti in Windows?*» (p. 69).
3. Trova l'ubicazione del file infetto (controlla il registro della scansione) ed eliminalo.
4. Riavvia il sistema ed entra in modalità normale.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 164).

26.3. 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. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
   b. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
   c. Nella finestra **Avanzate**, disattiva **Protezione di Bitdefender**.
3. Vai all'ubicazione dell'archivio e decomprimilo usando un programma di compressione, come WinZip.
4. Identifica il file infetto e lo elimina.
5. Elimina l'archivio originale per assicurarti che l'infezione sia stata rimossa completamente.
6. Ricomprimi i file in un nuovo archivio usando un'applicazione di archiviazione, come WinZip.
7. Attiva la protezione antivirus in tempo reale di Bitdefender ed esegui una scansione del sistema per assicurarti che non ci siano altre infezioni.

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 164).

26.4. 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. Controlla il database e-mail con Bitdefender.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
   b. Nel pannello **ANTIVIRUS**, clicca su **Apri**.
   c. Nella finestra **Avanzate**, disattiva **Protezione di Bitdefender**.
3. Apri il rapporto della scansione e usa le informazioni d'identificazione (oggetto, da, a) dei messaggi infettati per localizzarli nel client e-mail.
4. Elimina i messaggi infetti. La maggior parte dei client e-mail spostano il messaggio eliminato in una cartella di recupero, dalla quale può essere recuperato. Dovresti assicurarti che il messaggio sia eliminato anche da questa cartella di ripristino.
5. Compatta la cartella di memorizzazione del messaggio infetto.
   - Per Microsoft Outlook 2007: Nel menu File, clicca su Gestione file dati. Seleziona i file delle cartelle personali (.pst) che desideri compattare e clicca su Impostazioni. Clicca su Compatta.
   - Per Microsoft Outlook 2007 / 2013/ 2016: Nel menu File, clicca su Info e poi su Impostazioni account (Consente di aggiungere e rimuovere account o di modificare le impostazioni di connessione esistenti). Poi

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

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 164).

26.5. 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 del sistema** con Bitdefender. Per scoprire come fare, fai riferimento a «*Come posso eseguire una scansione del mio sistema?*» (p. 54).
2. Se il risultato della scansione non segnala nulla, ma hai ancora dubbi e vuoi essere certo che il file sia pulito, contatta gli operatori del nostro supporto tecnico per ricevere assistenza.

   Per scoprire come fare, fai riferimento a «*Chiedere aiuto*» (p. 164).

26.6. 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.

26.7. 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.

26.8. 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.

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

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

CONTACT US

27. CHIEDERE AIUTO

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

La sezione «*Risolvere i problemi più comuni*» (p. 143) fornisce le informazioni necessarie sui problemi più frequenti che potresti incontrare usando questo prodotto.

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

- «Contattaci direttamente da Bitdefender Antivirus Plus» (p. 164)
- «Contattaci tramite il nostro Centro di supporto online» (p. 165)

Contattaci direttamente da Bitdefender Antivirus Plus

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

Segui questi passaggi:

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

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

     Accedi ai nostri articoli e tutorial video online.
   - **CONTATTA IL SUPPORTO**

     Clicca su **CONTATTA SUPPORTO** per eseguire lo Strumento di supporto di Bitdefender e contattare il Supporto tecnico.

     a. Completa il modulo di invio con i dati richiesti:

i. Seleziona il tipo di problema che hai riscontrato.

ii. Inserisci una descrizione del problema riscontrato.

iii. Clicca su **PROVA A RIPRODURRE IL PROBLEMA** nel caso riscontrassi un problema con il prodotto. Riproduci il problema e poi clicca su **FINE** nel riquadro RIPRODUZIONE DEL PROBLEMA.

iv. Clicca su **CONFERMA TICKET**.

b. Continua a completare il modulo di invio con i dati necessari:

i. Inserisci il tuo nome completo.

ii. Inserisci il tuo indirizzo e-mail.

iii. Seleziona la casella di accettazione.

iv. Clicca su **CREA PACCHETTO DI DEBUG**.

Attendi qualche istante mentre Bitdefender raccoglie informazioni relative al prodotto. Queste informazioni aiuteranno i nostri ingegneri a trovare una soluzione al tuo problema.

c. Clicca su **CHIUDI** per uscire dalla procedura guidata. Uno dei nostri operatori ti contatterà il prima possibile.

Contattaci tramite il nostro Centro di supporto online

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

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

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

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

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

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

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

28. RISORSE ONLINE

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

- Centro di supporto di Bitdefender:

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

- Forum del supporto di Bitdefender:

  https://forum.bitdefender.com

- Il portale di sicurezza informatica HOTforSecurity:

  https://www.hotforsecurity.com

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

28.1. Centro di supporto di Bitdefender

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

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

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

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

28.2. Forum supporto di Bitdefender

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

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

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

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

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

28.3. Portale HOTforSecurity

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

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

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

29. CONTACT INFORMATION

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

29.1. Indirizzi web

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

29.2. Distributori locali

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

Per trovare un distributore di Bitdefender nel tuo paese:

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

29.3. Uffici di Bitdefender

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

USA

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

Regno Unito e Irlanda

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

Germania

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

Danimarca

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

Spagna

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

Romania

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

Emirati Arabi Uniti

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

Glossario

Abbonamento

Un accordo di acquisto che offre all'utente il diritto di utilizzare un particolare prodotto o servizio su un numero specifico di dispositivi e per un certo periodo di tempo. Un abbonamento scaduto può essere rinnovato automaticamente, utilizzando le informazioni fornite dall'utente con il primo acquisto.

ActiveX

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

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

Adware

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

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

Aggiornamento

Una nuova versione di un prodotto software o hardware creato per sostituire la versione precedente. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già

installata una versione precedente sul computer, diversamente non sarà possibile installare l'aggiornamento.

Bitdefender dispone della propria funzionalità di aggiornamento, che consente la verifica manuale degli aggiornamenti, oppure l'aggiornamento automatico del prodotto.

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

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

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

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

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

Area di notifica
Introdotta con Windows 95, l'area di notifica è situata nella barra delle applicazioni di Windows (in genere in basso vicino all'orologio) e contiene icone miniaturizzate per un accesso veloce a funzioni di sistema come fax, stampante, modem, volume e molto altro. Clicca due volte o clicca con il pulsante destro su un'icona per visualizzare e accedere ai dettagli e i controlli.

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

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

Attacco di forza bruta

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

Backdoor

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

Boot sector

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

Botnet

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

Browser

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

Client mail

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

Codice di attivazione

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

Cookie

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

Cyberbullismo

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

E-mail

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

Elementi di avvio

Qualsiasi file posizionato in questa cartella si aprirà all'avvio del computer. Ad esempio, una schermata di avvio, un file audio da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure app che possono essere elementi di avvio. Normalmente in questa cartella viene posizionato un alias di un file, al posto del file stesso.

Estensione del nome di un file

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

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

Euristico

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

Eventi

Un'azione oppure un evento segnalato da un programma. Gli eventi possono essere azioni dell'utente, come cliccare con il mouse o premere un tasto sulla tastiera, oppure del sistema, come l'esaurimento della memoria.

Exploit

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

Falso positivo

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

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

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

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

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

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

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

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

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

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

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

Minaccia

Un programma o parte di codice caricato sul computer a propria insaputa e che viene eseguito contro la propria volontà. La maggior parte delle minacce è anche in grado di auto replicarsi. Tutte le minacce informatiche sono state create dall'uomo. È relativamente facile produrre una semplice minaccia in grado di copiare sé stessa innumerevoli volte. Persino una minaccia così semplice è pericolosa in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di minaccia ancora più pericolosa è quella in grado di trasmettere sé stessa attraverso le reti superando i sistemi di sicurezza.

Minaccia avanzata persistente

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

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

Non euristico

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

Pacchetti di programmi

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

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

Percorso

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

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

Phishing

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

Photon

Photon è una tecnologia di Bitdefender innovativa e discreta, progettata per minimizzare l'impatto della tua soluzione di sicurezza sulle prestazioni del sistema. Monitorando in background l'attività del PC, crea degli schemi di utilizzo, per ottimizzare i processi di avvio e scansione.

Porta

Un'interfaccia su un computer dalla quale è possibile connettere un dispositivo. I personal computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, monitor e tastiere. Esternamente i personal computer hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

Nelle reti TCP/IP e UDP, un endpoint per una connessione logica. Il numero della porta ne identifica il tipo. Ad esempio, la porta 80 viene usata per il traffico HTTP.

Predatori online

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

Ransomware

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

L'infezione può partire, aprendo e-mail di spam, scaricando gli allegati di un messaggio o installando determinate applicazioni, il tutto lasciando l'utente ignaro di ciò che sta accadendo sul suo sistema. Gli autori di ransomware puntano a colpire soprattutto gli utenti normali e le aziende.

Rete privata virtuale (VPN)

È una tecnologia che consente una connessione diretta temporanea e cifrata a una determinata rete su una rete meno sicura. In questo modo, la ricezione e l'invio dei dati sono sempre sicuri e cifrati, ma soprattutto più difficili da intercettare dai pirati informatici. Una prova di sicurezza è l'autenticazione, che può essere fatta solo usando un nome utente e una password.

Rootkit

Un rootkit è una serie di strumenti software che consente di accedere a un sistema come amministratore. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la propria presenza, in modo da non essere visti dagli amministratori del sistema.

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

I rootkit non sono dannosi per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando i rootkit. Comunque, vengono principalmente utilizzati per nascondere minacce o per celare la presenza di un intruso nel sistema. Se combinati alle minacce, i rootkit rappresentano una grave minaccia per l'integrità e la

sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e registri, ed evitare il rilevamento.

Scarica

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

Script

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Spam

Messaggi di posta elettronica o newsgroup indesiderati. Generalmente conosciuto come e-mail non desiderate.

Spyware

Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessone a Internet, senza che questo se ne accorga, di solito per scopi pubblicitari. Le applicazioni spyware in genere sono incluse come componente nascosta di programmi freeware o shareware, che possono essere scaricati da Internet. Tuttavia, occorre segnalare che la maggioranza delle applicazioni shareware o freeware non includono alcun programma spyware. Una volta installato, uno spyware monitora le attività dell'utente su Internet e trasmette di nascosto tali informazioni a qualcun altro. Gli spyware possono anche raccogliere informazioni su indirizzi e-mail o addirittura password e numeri di carta di credito.

Gli spyware sono simili a un Trojan che gli utenti installano inconsapevolmente installando altre applicazioni. Un modo comune per diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli spyware utilizzano memoria e risorse del sistema,

le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di rete largamente utilizzati su Internet, che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il relativo traffico.

Trojan

Un programma distruttivo che si maschera da applicazione benevola. A differenza di programmi software dannosi e worm, i trojan non si replicano ma possono essere altrettanto distruttivi. Un tipo di minaccia Trojan particolarmente insidiosa è un programma che dichiara di pulire le minacce dal computer, ma al contrario le introduce.

Il termine deriva da una storia dell'Iliade di Omero, in cui i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

Unità disco

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

Un drive di disco rigido legge e scrive dischi rigidi.

Un drive di floppy accede i dischi floppy.

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

Virus di boot

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

Virus polimorfico

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

Worm

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