Bitdefender®
PREMIUM SECURITY

MANUALE D'USO

Mac iOS

Bitdefender Premium Security
Manuale d'uso

Data di pubblicazione 18/12/2019

Avvertenze legali

Bitdefender

Indice

Informazioni su questa guida

1. Finalità e destinatari

Il tuo abbonamento a Bitdefender Premium Security può proteggere fino a un massimo di 10 PC, Mac, iOS e smartphone e tablet Android diversi. La gestione dei dispositivi protetti può essere attuata tramite un account Bitdefender, che deve essere associato a un abbonamento attivo.

Con il tuo abbonamento a Bitdefender Premium Security, puoi usare la versione premium di Bitdefender VPN su tutti i dispositivi su cui installi Bitdefender. Ciò significa che otterrai traffico illimitato e accesso senza limitazioni a contenuti in tutto il mondo, scegliendo la posizione del server che desideri.

Questa guida fornisce assistenza con la configurazione e l'utilizzo dei prodotti inclusi in tuoi abbonamenti: Bitdefender Total Security (per Windows), Bitdefender Antivirus for Mac (per macOS), Bitdefender Mobile Security (per Android) e Bitdefender Mobile Security for iOS.

Puoi scoprire come configurare Bitdefender su diversi dispositivi per mantenerli sempre protetti da ogni tipo di minaccia.

2. Come usare questo manuale

Questa guida è basata essenzialmente su quattro prodotti inclusi in Bitdefender Premium Security:

- «Total Security per PC» (p. 1)

  Scopri come utilizzare il prodotto sui tuoi PC e portatili con Windows.

- «Antivirus per Mac» (p. 216)

  Scopri come utilizzare il prodotto sui tuoi Mac.

- «Mobile Security per iOS» (p. 261)

  Scopri come utilizzare il prodotto sui tuoi smartphone e tablet iOS.

- «Mobile Security per Android» (p. 278)

  Scopri come utilizzare il prodotto sui tuoi smartphone e tablet Android.

- «Contattaci» (p. 319)

  Scopri dove cercare aiuto se dovesse verificarsi qualcosa di inatteso.

TOTAL SECURITY PER PC

1. INSTALLAZIONE

1.1. Prepararsi all'installazione

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

- Assicurati che il computer su cui desideri installare Bitdefender soddisfi i requisiti di sistema. Se il computer non soffisfa 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. 2).
- Accedere al computer utilizzando un account Amministratore.
- Rimuovi qualsiasi altro programma simile dal computer. 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.
- Disabilita o rimuovi qualsiasi programma firewall che possa essere in esecuzione sul computer. L'esecuzione simultanea di due programmi firewall può influenzarne il funzionamento e causare problemi seri al sistema. Durante l'installazione il firewall di Windows sarà disattivato.
- Assicurati che il computer sia connesso a Internet durante l'installazione, anche se l'hai avviata da un CD/DVD. Se sono disponibili versioni più recenti dei file dell'applicazione inclusi nel pacchetto d'installazione, Bitdefender può scaricarli e installarli.

1.2. Requisiti di sistema

Puoi installare Bitdefender Total Security solo su computer 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)
- Intel CORE Duo (2 GHz) o processore equivalente
- 2 GB di memoria (RAM)

Nota

Per scoprire quale versione di Windows è attiva sul computer 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.

Requisiti software

Per poter usare Bitdefender e tutte le sue funzioni, il tuo computer 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

1.3. Installare il tuo prodotto Bitdefender

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

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

1.3.1. 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 Total Security viene attivato.

Per scaricare Bitdefender Total Security da Bitdefender Central:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **I miei dispositivi** e clicca su **INSTALLA PROTEZIONE**.
3. Seleziona una delle due opzioni disponibili:
   - **Proteggi questo dispositivo**
     a. Seleziona questa opzione e poi il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, clicca sul pulsante corrispondente.
     b. Salva il file di installazione.
   - **Proteggi altri dispositivi**
     a. Seleziona questa opzione 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 computer per completare la rimozione delle soluzioni di sicurezza rilevate.

Il pacchetto d'installazione di Bitdefender Total Security 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 Total Security.

Fase 1 - Installazione di Bitdefender

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

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. Clicca su **INIZIA A USARE Bitdefender** per continuare.

Fase 4 - Come iniziare

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

Clicca su **FINE** per accedere all'interfaccia di Bitdefender Total Security.

2. INIZIARE

2.1. Le basi

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

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

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. 146).

Puoi memorizzare le tue password e gli account online, salvandoli con «*Protezione di Password Manager per le tue credenziali*» (p. 137) in un Portafoglio. Con una sola password principale puoi proteggere la tua privacy da eventuali intrusi che potrebbero tentare di sottrarti del denaro.

«*Protezione webcam*» (p. 124)Impedisce alle app non affidabili di accedere alla tua videocamera, bloccando così ogni tentativo di prenderne il controllo. In base alle scelte degli utenti di Bitdefender, l'accesso delle app più popolari alla tua webcam sarà consentito o bloccato.

Per proteggerti da potenziali occhi indiscreti, quando il dispositivo è connesso a una rete wireless non protetta, Bitdefender analizza il suo livello di sicurezza e, se necessario, fornisce suggerimenti per aumentare la sicurezza delle tue attività online. Per maggiori istruzioni su come proteggere i tuoi dati personali, fai riferimento al «*Wi-Fi Security Advisor*» (p. 120).

I tuoi file personali salvati in locale, come documenti, fotografie o filmati, e anche quelli memorizzati nel cloud, ora possono restare sempre al sicuro dalle minacce moderne e più pericolose, meglio conosciute come ransomware. Per informazioni su come proteggere i file personali, fai riferimento a «*Safe files*» (p. 127).

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. 130).

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. 177).

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. 9).

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 computer e i tuoi dati.

Per utilizzare le funzioni online di Bitdefender Total Security e gestire i tuoi abbonamenti e dispositivi, accedi al tuo account Bitdefender. Per maggiori informazioni, fai riferimento a «*Bitdefender Central*» (p. 26).

Nella sezione «*Come fare*» (p. 39) 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. 185) per alcune possibili soluzioni ai problemi più comuni.

Aprire la finestra di Bitdefender

Per accedere all'interfaccia principale di Bitdefender Total Security, segui questi passaggi:

- In **Windows 7**:
  1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
  2. Clicca su **Bitdefender**.
  3. Clicca su **Bitdefender Total Security** 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. 13).

2.1.1. Notifiche

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

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

Per accedere al 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.

2.1.2. Profili

Alcune attività del computer, come giochi online o presentazioni video, richiedono una maggiore prontezza del sistema, prestazioni più elevate e nessuna interruzione. Quando il 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.

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.

Per consentire a Bitdefender di attivare i profili:

1. Clicca su **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Profili**.
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. 177)

2.1.3. Impostazioni protette da password di Bitdefender

Se non sei l'unica persona a utilizzare questo computer, 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.

2.1.4. Rapporti prodotto

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

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

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

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

2.1.5. Notifiche offerte speciali

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

Per attivare o disattivare le notifiche sulle offerte speciali:

1. 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.

2.2. Interfaccia di Bitdefender

Bitdefender Total Security 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 al tuo account Bitdefender, l'area delle impostazioni, le notifiche e le sezioni di Bitdefender per una configurazione dettagliata e attività amministrative avanzate. Inoltre, puoi contattarci per richiedere supporto nel caso avessi domande o si verificasse qualcosa di inatteso.

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

2.2.1. Icona area di notifica

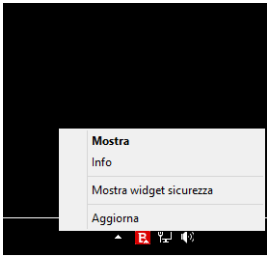
Per gestire tutto il prodotto più velocemente, puoi utilizzare l'icona di Bitdefender nell'area di notifica.

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 compaoano 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.

- **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.



Icona della barra delle applicazioni

- **Nascondi / Mostra widget sicurezza** - Attiva / disattiva il widget sicurezza.
- **Aggiorna ora** - Inizia un aggiornamento immediato. Puoi seguire lo stato di aggiornamento nel pannello Aggiornamento della finestra principale di Bitdefender.

L'icona di Bitdefender nell'area di notifica fornisce informazioni relative ai problemi del computer 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.

2.2.2. Menu di navigazione

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

- **Dashboard**. Da qui, puoi risolvere rapidamente eventuali problemi di sicurezza, visualizzare suggerimenti in base alle esigenze del tuo sistema e modalità d'uso, eseguire azioni rapide e installare Bitdefender su altri dispositivi.
- **Protezione**. Da qui, puoi lanciare e configurare le scansioni antivirus, accedere alle impostazioni del firewall, proteggere i file e le app da attacchi ransomware, ripristinare i dati nel caso venissero cifrati da un ransomware e configurare la protezione mentre navighi in Internet.
- **Privacy**. Da qui, puoi creare gestori di password per i tuoi account online, proteggere l'accesso alla tua webcam da occhi indiscreti, effettuare pagamenti online in un ambiente sicuro, aprire la app VPN e proteggere i tuoi bambini visualizzando e limitando le loro attività online.
- **Utilities**. Da qui, puoi migliorare la velocità del sistema e configurare la funzionalità Anti-Theft per i tuoi dispositivi.
- **Notifiche**. Da qui, puoi accedere alle notifiche già generate.
- **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.

- **Impostazioni**. Da qui, puoi accedere alle impostazioni generali.
- **Supporto**. Da qui, se hai bisogno di assistenza per risolvere un determinato problema con Bitdefender Total Security, puoi contattare l'assistenza tecnica di Bitdefender.

2.2.3. Dashboard

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

Tutto è a pochi clic di distanza.

La finestra è organizzata in tre sezioni principali:

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

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

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

Area stato di sicurezza

Bitdefender utilizza un sistema di identificazione dei problemi per rilevare e fornire informazioni relative ai problemi che potrebbero avere effetto sulla sicurezza del computer 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 computer, 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.

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**.

Azioni rapide

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

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

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

Le attività che puoi aggiungere all'interfaccia principale sono:

- **Scansione veloce**. Esegui una scansione veloce per rilevare prontamente possibili minacce eventualmente presenti sul tuo computer.
- **Scansione di sistema**. Esegui una scansione di sistema per assicurarti che il tuo computer sia privo di minacce.
- **Scansione vulnerabilità**. Esegui una scansione del computer alla ricerca di vulnerabilità per assicurarti che tutte le applicazioni installate, incluso il sistema operativo, siano aggiornate e funzionino correttamente.
- **Controlla la sicurezza del Wi-Fi**. Apri Wi-Fi Security Advisor per verificare se la rete wireless di casa a cui ti connetti è sicura oppure no, e se ha eventuali 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 computer.
- **File Vault**. Crea Vault in cui memorizzare i tuoi documenti confidenziali e sensibili.
- **Apri Ottimizzatore immediato**. Libera spazio su disco, ripara gli errori del registro e proteggi la tua privacy, eliminando i file che non usi più con il semplice clic di un pulsante.
- **Apri Ottimizzatore avvio**. Riduci il tempo di avvio del sistema, escludendo applicazioni non necessarie all'avvio.
- **Libera il mio dispositivo**. Fai spazio per nuovi dati eliminando i file non necessari.

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 Total Security su dispositivi Windows.
- Bitdefender Antivirus for Mac su dispositivi macOS.

- Bitdefender Mobile Security su dispositivi Android.
- Bitdefender Mobile Security su dispositivi iOS.

2.2.4. 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

Protezione

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

Le funzionalità che puoi gestire nella sezione Protezione sono:

ANTIVIRUS

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

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

- Scans. veloce
- Scansione sistema
- Gestisci scansioni
- Modalità di soccorso (Ambiente di soccorso in Windows 10)

Per maggiori informazioni sulle attività di scansione e su come configurare la protezione antivirus, fai riferimento a «*Protezione antivirus*» (p. 76).

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. 99).

FIREWALL

Il firewall ti protegge mentre sei connesso alle reti e a Internet filtrando tutti i tentativi di connessione.

Per maggiori informazioni sulla configurazione del firewall, fai riferimento a «*Firewall*» (p. 110).

ADVANCED THREAT DEFENSE

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

Per maggiori informazioni su come tenere il sistema al sicuro dalle minacce, fai riferimento a «*Difesa da minacce avanzate*» (p. 97).

ANTISPAM

La funzionalità antispam di Bitdefender protegge la tua casella di posta da messaggi indesiderati, filtrando tutto il traffico POP3.

Per maggiori informazioni sulla protezione antispam, fai riferimento a «*Antispam*» (p. 101).

VULNERABILITÀ

La funzionalità 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 **Scansione vulnerabilità** nella funzionalità Vulnerabilità per iniziare a 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 **Wi-Fi security** 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. 116).

SAFE FILES

La funzionalità Safe files garantisce che i tuoi file personali siano sempre protetti dagli attacchi ransomware.

Per maggiori informazioni su come configurare Safe files per proteggere i tuoi file personali dagli attacchi ransomware, fai riferimento a «*Safe files*» (p. 127).

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. 130).

Privacy

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

Le funzionalità che puoi gestire nella sezione Privacy sono:

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. 146).

CRITTOGRAFIA FILE

Ti consente di creare unità logiche (o vault) criptate e protette da password sul computer, dove puoi conservare i documenti confidenziali e sensibili in modo sicuro.

Per trovare maggiori informazioni su come creare unità logiche (o vault) crittografate e protette da password sul computer, fai riferimento a «*Crittografia file*» (p. 133).

PROTEZIONE AUDIO E VIDEO

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

Per maggiori informazioni su come mantenere la tua webcam protetta da accessi indesiderati e come impostare Bitdefender per avvisarti sulle attività del microfono, fai riferimento a «*Protezione audio e video*» (p. 123).

GESTORE PASSWORD

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. 137).

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. 147).

CONTROLLO GENITORI

Il Controllo genitori di Bitdefender ti consente di monitorare ciò che i bambini fanno sul proprio computer. In caso di contenuti inappropriati, puoi decidere di limitare l'accesso a Internet o a determinate applicazioni.

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

Per maggiori informazioni sulla configurazione del Controllo genitori, fai riferimento a «*Controllo Genitori*» (p. 153).

PROTEZIONE DATI

La funzionalità Protezione dati ti consente di eliminare i file in modo permanente.

Clicca su **Distruttore di file** nel pannello di Protezione dei dati per avviare una procedura guidata che ti consentirà di eliminare completamente i file dal sistema.

Per maggiori informazioni sulla configurazione della Protezione dati, fai riferimento a «*Protezione dati*» (p. 152).

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. 143).

Utility

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

Strumenti di ottimizzazione

Bitdefender Total Security non solo offre sicurezza, ma ti aiuta anche a ottimizzare le prestazioni del computer.

Gli strumenti di ottimizzazione disponibili sono:

- Ottimizzatore immediato
- Ottimizzatore avvio
- Pulizia disco

Per maggiori informazioni sugli strumenti di ottimizzazione delle prestazioni, fai riferimento a «*Utility*» (p. 173).

Antifurto

La funzione Anti-Theft di Bitdefender protegge il computer e i dati da furti e perdite. In caso di un tale evento, ti consente di localizzare o bloccare in remoto il tuo computer. Puoi anche eliminare tutti i dati presenti nel tuo sistema.

La funzione Anti-Theft di Bitdefender offre le seguenti funzionalità:

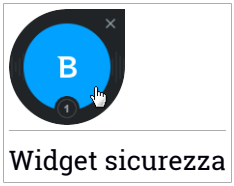
- Localizzazione remota
- Blocco remoto
- Cancellazione remota
- Avviso in remoto

Per maggiori informazioni su come tenere il sistema al sicuro da mani sbagliate, fai riferimento a «*Funzione antifurto (Anti-Theft)*» (p. 169).

2.2.5. Widget sicurezza

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

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



Widget sicurezza

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


Alcuni problemi critici influenzano la sicurezza del tuo sistema.

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

 Alcuni problemi non critici influenzano la sicurezza del tuo sistema. Quando hai un po' di tempo, dovresti controllarli e risolverli. Clicca sull'icona di stato per iniziare a risolvere i problemi segnalati.

 Il tuo sistema è protetto.

 Quando è in corso una scansione su richiesta, viene mostrata questa icona.

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

Il lato inferiore del widget mostra il contatore degli eventi non letti (il numero di eventi rilevanti segnalati da Bitdefender, in caso ve ne fossero). Clicca sul contatore degli eventi, per esempio 1, nel caso di un evento non letto, per aprire la finestra delle Notifiche. Per maggiori informazioni, fai riferimento a «*Notifiche*» (p. 9).

Eseguire la scansione di file e cartelle

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

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

Nascondi / mostra widget sicurezza

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

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

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

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

Di norma, il widget sicurezza di Bitdefender è disattivato.

2.2.6. Modificare la lingua del prodotto

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

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

2.3. 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 computer 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 Total Security
  - Bitdefender Antivirus for Mac

- Bitdefender Mobile Security per Android
- Bitdefender Mobile Security for iOS
- Controllo genitori di Bitdefender

- Gestisci e rinnova i tuoi abbonamenti di Bitdefender.
- Aggiungi nuovi dispositivi alla tua rete e gestiscili ovunque ti trovi.
- Proteggi i dispositivi nella rete e i loro dati da perdite o furti con la funzione Anti-Theft.
- Configura le impostazioni del Controllo genitori per i dispositivi dei bambini e monitora le loro attività ovunque ti trovi.

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.

2.3.1. 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 computer, 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.

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.

2.3.2. I miei abbonamenti

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

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).

Aggiungi un nuovo dispositivo

Se l'abbonamento copre più di un dispositivo, è possibile aggiungerne un altro e installare Bitdefender Total Security 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.

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.

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.

2.3.3. 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 «*Eseguire una scansione del sistema*» (p. 83) e «*Eseguire una Scansione veloce*» (p. 83).

- **Ottimizzatore**. Qui puoi migliorare in remoto le prestazioni di un dispositivo, esaminando, rilevando e pulendo rapidamente eventuali file non necessari. Clicca sul pulsante **AVVIO** e poi seleziona le aree che vuoi ottimizzare. Clicca di nuovo sul pulsante **AVVIO** per avviare il processo di ottimizzazione. Clicca su **Maggiori dettagli** per accedere a un rapporto dettagliato sui problemi risolti.

  Inoltre, puoi migliorare l'avvio del dispositivo identificando le applicazioni che consumano molte risorse del sistema. Clicca su **MAGGIORI DETTAGLI** e seleziona cosa intendi fare con le applicazioni rilevate. Per maggiori dettagli su queste funzionalità, fai riferimento a «*Ottimizzare la velocità del sistema con un semplice clic*» (p. 173) e «*Ottimizzare il tempo di avvio del PC*» (p. 174).

- **Anti-Theft**. In caso di dimenticanza, smarrimento o furto, con la funzione Anti-Theft puoi localizzare il tuo dispositivo ed eseguire alcune azioni in remoto. Clicca su **LOCALIZZA** per rilevare la posizione del dispositivo. Sarà mostrata l'ultima posizione nota, accompagnata da ora e data. Per maggiori dettagli su questa funzione, fai riferimento a «*Funzione antifurto (Anti-Theft)*» (p. 169).

- **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. 116).

2.3.4. 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.

2.3.5. 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.

2.4. 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 computer e in seguito ad ogni **ora**. Se vi è un aggiornamento disponibile, viene scaricato e installato automaticamente sul computer.

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 computer 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. 70).
- 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. 36).

2.4.1. 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.

2.4.2. 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 computer, 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**.

2.4.3. 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.

2.4.4. 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 computer. Questo per impedire che il processo di aggiornamento di Bitdefender interferisca con il lavoro dell'utente.

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

2.4.5. 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 2019.

3. COME FARE

3.1. Installazione

3.1.1. Come faccio a installare Bitdefender su un secondo computer?

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

Per installare Bitdefender su un secondo computer:

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.

3.1.2. Come posso reinstallare Bitdefender?

Alcune tipiche situazioni in cui dovresti reinstallare Bitdefender sono:

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

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 Total Security** e seleziona **Disinstalla**.
  3. Clicca su **REINSTALLA** nella finestra che comparirà.
  4. Devi riavviare il computer 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 Total Security** e seleziona **Disinstalla**.
4. Clicca su **REINSTALLA** nella finestra che comparirà.
5. Devi riavviare il computer 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 Total Security** e seleziona **Disinstalla**.
4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
5. Clicca su **REINSTALLA**.
6. Devi riavviare il computer 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.

3.1.3. Dove posso scaricare il mio prodotto Bitdefender?

Puoi installare Bitdefender dal disco di installazione oppure utilizzare il programma d'installazione che puoi scaricare sul tuo computer 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 computer, 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.

3.1.4. 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.

3.1.5. 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 Total Security** 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 Total Security** 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 Total Security** 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. 3).

3.1.6. 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 2019, 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 che il computer venga riavviato.

   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.

3.2. Bitdefender Central

3.2.1. 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 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 per cambiare l'account collegato al computer.
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. 320).

3.2.2. 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**.

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

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

- 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. Clicca su **Hai dimenticato la password?**.
  4. Inserisci l'indirizzo e-mail del tuo account e clicca su **AVANTI**.
  5. 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.
  6. 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. 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.

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

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

1. 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 **Gestione sessione** nel menu scorrevole.
5. Nella sezione **Sessioni attive**, seleziona l'opzione **ESCI** accanto al dispositivo in cui vuoi terminare la sessione di accesso.

3.3. Scansione con Bitdefender

3.3.1. Come posso controllare un file o una cartella?

Il modo più semplice di controllare un file o una cartella è cliccare con il pulsante destro sull'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 computer.

3.3.2. 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 **Scansione sistema**.
3. 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. 87).

3.3.3. Come posso programmare una scansione?

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

Per programmare una scansione:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Gestisci scansioni**.
3. Clicca su  accanto al tipo di scansione che vuoi programmare, Scansione del sistema o Scansione veloce.

   In alternativa, puoi creare un tipo di scansione che si adatti alle tue necessità, cliccando su **Crea una nuova attività di scansione**.
4. Attiva l'opzione **Programma attività di scansione**.

   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.

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

Se desideri controllare percorsi particolari sul tuo computer 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 **Gestisci scansioni**.
2. Clicca su **Crea una nuova attività di scansione**.
3. Nel campo **Nome attività**, inserisci un nome per la scansione, seleziona i percorsi che vorresti esaminare e 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. Attiva **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.

3.3.5. Come posso escludere una cartella dalla scansione?

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

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

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

Per aggiungere una cartella alla lista delle eccezioni:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Impostazioni**.
3. Clicca sulla scheda **Eccezioni**.
4. Clicca sul menu a fisarmonica **Elenco di file e cartelle escluse dalla scansione** e poi su **Aggiungi**.
5. Clicca su **ESPLORA**, seleziona la cartella che desideri escludere dalla scansione e quindi scegli il tipo di scansione da cui escluderla.
6. Clicca su **AGGIUNGI** per salvare le modifiche e chiudere la finestra.

3.3.6. 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 **Impostazioni**.
   c. Nella finestra **Protezione**, 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. 72).
3. Ripristina il file dalla quarantena:
   a. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.

b. Nel pannello **ANTIVIRUS**, clicca su **Quarantena**.

c. Seleziona il file e 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. 50).
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. 320).

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

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

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

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**.

3.4. Controllo Genitori

3.4.1. Come posso proteggere i bambini dalle minacce online?

Il Controllo genitori di Bitdefender ti consente di limitare l'accesso a Internet e a particolari applicazioni, impedendo ai bambini di visualizzare contenuti inappropriati quando non ci sei.

Per configurare il Controllo genitori:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **CONTROLLO GENITORI**, clicca su **Configura**.

   Sarai reindirizzato alla pagina web account Bitdefender. Assicurati di aver eseguito l'accesso con le tue credenziali.
3. Si aprirà la dashboard del Controllo genitori. Qui è dove puoi verificare e configurare le impostazioni del Controllo genitori.
4. Clicca su **CREA UN PROFILO DEL BAMBINO** nella finestra **I miei bambini**.
5. Imposta determinate informazioni, come nome, data di nascita o sesso. Per aggiungere un'immagine al profilo del tuo bambino, clicca sull'icona nell'angolo in basso a destra dell'opzione **Immagine del profilo**. Clicca su **SALVA** per continuare.

   In base agli standard di sviluppo, impostando la data di nascita del bambino, il programma carica automaticamente alcune impostazioni di ricerca del web considerate appropriate per quella categoria d'età.
6. Clicca su **AGGIUNGIAMO UN DISPOSITIVO**.
7. Se sul dispositivo del bambino è già stato installato un prodotto Bitdefender, seleziona il suo dispositivo nell'elenco disponibile e l'account che vuoi monitorare. Clicca su **ASSEGNA**.

   Se il bambino non ha alcun prodotto di Bitdefender installato sul dispositivo che utilizza, clicca su **Installa su un nuovo dispositivo** e 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 Bitdefender, controlla l'account e-mail che hai digitato e poi clicca sul pulsante di download corrispondente.

Importante
Sui dispositivi Windows e macOS che non hanno un prodotto di Bitdefender installato, sarà installato il Parental Control di Bitdefender che monitora i tracker, così potrai monitorare le attività online dei bambini.
Sui dispositivi Android e iOS, sarà scaricata e installata la app Parental Control di Bitdefender.

3.4.2. Come posso impedire che i bambini accedano a un sito web?

Il Controllo genitori di Bitdefender ti consente di controllare i contenuti a cui il bambino accede tramite il proprio dispositivo e di bloccare eventualmente l'accesso a una pagina web.

Per bloccare l'accesso a una pagina web, devi aggiungerla all'elenco delle eccezioni, in questo modo:

1. Vai a: https://central.bitdefender.com.
2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
3. Clicca su **Controllo genitori** per accedere alla dashboard.
4. Seleziona il profilo del bambino dalla finestra **Bambini**.
5. Seleziona la scheda **Siti web** e clicca su **GESTISCI**.
6. Inserisci il sito web che vuoi bloccare nel campo corrispondente.
7. Seleziona **Consenti** o **Blocca**.
8. Clicca su **FINISH** per salvare le modifiche.

Nota
Le restrizioni possono essere impostate solo per i dispositivi Android, macOS e Windows.

3.4.3. Come posso impedire a mio figlio di usare determinate app?

Il Parental Control di Bitdefender ti consente di controllare i contenuti a cui i bambini accedono mentre usano i dispositivi.

Per bloccare l'accesso a una app:

1. Vai a: https://central.bitdefender.com.
2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
3. Clicca su **Controllo genitori** per accedere alla dashboard.
4. Seleziona un profilo del bambino dalla finestra **I miei bambini**.
5. Seleziona la scheda **Applicazioni**.
6. Viene mostrato un elenco con i dispositivi assegnati.

   Seleziona la scheda con il dispositivo in cui vuoi limitare l'accesso alle app.
7. Clicca su **Gestisci le app usate da...**

   Viene mostrato un elenco con le app installate.
8. Seleziona **Bloccato** accanto alle app di cui vuoi bloccare l'utilizzo da parte del bambino.
9. Clicca su **SALVA** per applicare le nuove impostazioni.

Nota
Le restrizioni possono essere impostate solo per i dispositivi Android, macOS e Windows.

3.4.4. Come posso impedire che il bambino entri in contatto con persone sconosciute?

Il Parental Control di Bitdefender ti dà la possibilità di bloccare le chiamate dall'elenco telefonico del tuo bambino. Le limitazioni alle chiamate telefoniche possono essere impostate solo per i dispositivi iOS aggiungi al profilo del tuo bambino, e applicate solo alle chiamate in entrata.

Per bloccare un determinato contatto su un dispositivo che ha la app Parental Control di Bitdefender installata:

1. Vai a: https://central.bitdefender.com.
2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
3. Clicca su **Controllo genitori** per accedere alla dashboard.

4. Seleziona il profilo del bambino per cui vuoi impostare le limitazioni.

   Assicurati che il profilo selezionato utilizzi il dispositivo Android assegnato.

5. Seleziona la scheda **Contatti telefonici**.

   Verrà mostrato un elenco di carte. Le carte rappresentano i contatti del telefono del bambino.

6. Seleziona la carta con il numero di telefono che vuoi bloccare.

   L'icona  che compare indica che il bambino non potrà più essere raggiunto dal numero di telefono selezionato.

3.4.5. Come posso impostare un luogo come sicuro o vietato per il bambino?

Il Controllo genitori di Bitdefender ti consente di impostare un determinato luogo come sicuro o vietato per il bambino.

Per impostare un luogo:

1. Vai a: https://central.bitdefender.com.
2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
3. Clicca su **Controllo genitori** per accedere alla dashboard.
4. Seleziona il profilo del bambino dalla finestra **Bambini**.
5. Seleziona la scheda **Posizione bambino**.
6. Clicca su **Dispositivi** nella sezione della finestra **Posizione bambino**.
7. Clicca su **SCEGLI DISPOSITIVI** e seleziona il dispositivo che vuoi configurare.
8. Nella finestra **Area**, clicca sul pulsante **AGGIUNGI AREA**.
9. Seleziona il tipo di luogo, **SICURO** o **VIETATO**.
10. Inserisci un nome valido per l'area dove il bambino ha il permesso di andare oppure no.
11. Imposta la distanza da applicare per il monitoraggio dal cursore scorrevole **Raggio**.
12. Clicca su **AGGIUNGI AREA** per salvare le tue impostazioni.

Ogni volta che vuoi impostare un luogo vietato come sicuro o viceversa, cliccaci sopra e seleziona il pulsante **MODIFICA AREA**. In base al cambiamento che vuoi fare, seleziona l'opzione **SICURO** o **VIETATO** e clicca su **AGGIORNA AREA**.

3.4.6. Come posso impedire al bambino di accedere ai dispositivi assegnati durante le attività giornaliere?

Controllo genitori di Bitdefender ti consente di limitare l'accesso ai dispositivi assegnati da parte del bambino durante le attività giornaliere, come le ore di scuola e quando dovrebbe fare i compiti, oppure quando dovrebbe andare a dormire.

Per impostare limiti temporali:

1. Vai a: https://central.bitdefender.com.
2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
3. Clicca su **Controllo genitori** per accedere alla dashboard.
4. Dalla finestra **Il mio bambino**, seleziona il profilo del bambino per cui vuoi impostare le limitazioni.
5. Seleziona la scheda **Tempo speso**.
6. Clicca su **Rivedi limitazioni temporali**.
7. Nell'area **Imposta limitazioni temporali**, clicca su **Aggiungi nuova limitazione**.
8. Dai un nome alla limitazione che vuoi impostare (per esempio, ora di dormire, compiti, lezioni di tennis, ecc.).
9. Imposta l'intervallo di tempo e i giorni in cui le limitazioni dovranno essere applicate e poi clicca su **AGGIUNGI** per salvare le impostazioni.

3.4.7. Come posso impedire al bambino di accedere ai dispositivi assegnati durante il giorno o la notte?

Controllo genitori di Bitdefender ti consente di limitare l'accesso ai dispositivi assegnati da parte del bambino in diversi momenti durante una giornata.

Per impostare un limite giornaliero di utilizzo:

1. Vai a: https://central.bitdefender.com.

2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
3. Clicca su **Controllo genitori** per accedere alla dashboard.
4. Dalla finestra **Il mio bambino**, seleziona il profilo del bambino per cui vuoi impostare le limitazioni.
5. Seleziona la scheda **Tempo speso**.
6. Clicca su **Rivedi limitazioni temporali**.
7. Nell'area **Imposta un limite per l'utilizzo giornaliero**, clicca su **Aggiungi un nuovo limite giornaliero**.
8. Imposta l'intervallo di tempo e i giorni in cui le limitazioni dovranno essere applicate e poi clicca su **SALVA** per salvare le impostazioni.

3.4.8. Come rimuovere un profilo di un bambino

Se vuoi rimuovere un profilo di un bambino esistente:

1. Vai a: https://central.bitdefender.com.
2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
3. Clicca su **Controllo genitori** per accedere alla dashboard.
4. Clicca sull'icona ⋮ dal profilo del bambino che vuoi eliminare e poi seleziona **Rimuovi**.
5. Conferma la tua scelta.

3.4.9. Come posso fare l'upgrade a Bitdefender Parental Control Premium?

Con l'abbonamento a Bitdefender Parental Control Premium, puoi restare informato in tempo reale sulle minacce a cui è esposto il bambino mentre utilizza i social network, come WhatsApp, Facebook Messenger o Instagram. In particolare, ogni volta che vengono rilevati i seguenti comportamenti nelle conversazioni online:

- Fotografie che contengono nudità.
- Messaggi di testo perfidi.

- Divulgazione di informazioni personali (indirizzo di casa, password, numeri di carta di credito, codici fiscali, ecc.).
- Richieste di incontro da estranei.

Un abbonamento a Bitdefender Parental Control Premium include un numero illimitato di dispositivi dei bambini su dispositivi Windows, macOS, Android e iOS.

Per fare l'upgrade a Bitdefender Parental Control Premium:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **Controllo genitori**.
3. Clicca su **ALTRE INFO** nel banner in alto che compare sopra ai profili dei bambini.
4. Clicca su **ACQUISTA PREMIUM**.

   Sarai reindirizzato al sito web di Bitdefender, da dove potrai procedere con l'acquisto.

Nota
Puoi fare l'upgrade a Bitdefender Parental Control Premium solo se ti trovi nei seguenti paesi: Stati Uniti, Canada, Regno Unito, Irlanda, Sud Africa, Australia o Nuova Zelanda. L'elenco sarà aggiornato presto con ulteriori paesi, non appena il prodotto sarà disponibile in nuove aree.

3.5. Protezione della Privacy

3.5.1. 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 **Apri Safepay**.

3. Clicca sul pulsante  per accedere alla **tastiera virtuale**.

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

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

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

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

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

1. Accedi a Bitdefender Central.
2. Seleziona la scheda **I miei dispositivi**.
3. Clicca sulla scheda del dispositivo desiderato e seleziona **Anti-Theft**.
4. Seleziona la funzione che vuoi utilizzare:
   - **LOCALIZZA** - Mostra la posizione del dispositivo su Google Maps.
   -  **Avviso** - Invia un avviso al dispositivo.
   -  **Blocca** - Blocca il computer e imposta un codice PIN numerico per sbloccarlo. In alternativa, attiva l'opzione corrispondente per consentire a Bitdefender di scattare delle fotografie a chiunque provi ad accedere al tuo dispositivo.
   -  **Cancella** - Elimina tutti i dati dal dispositivo.

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

   - **Mostra IP** - Mostra l'ultimo indirizzo IP per il dispositivo selezionato.

3.5.3. Come posso usare i File Vault?

Il File Vault di Bitdefender permette di creare drive logici (o vault) criptati e protetti da password sul computer, dove puoi archiviare i documenti confidenziali e sensibili in modo sicuro. Fisicamente, il Vault è un file archiviato su un disco fisso locale con estensione .bvd.

Quando crei un File Vault, due aspetti sono molto importanti: la dimensione e la password. Lo spazio standard di 100 MB dovrebbe essere sufficiente per i tuoi documenti privati, file di Excel e altri dati simili. Tuttavia, per video o altri file, potresti aver bisogno di più spazio.

Per archiviare in sicurezza i tuoi file o le tue cartelle confidenziali e importanti nei File Vault di Bitdefender:

- **Crea un File Vault e imposta una password sicura per usarlo.**

  Per creare un Vault, clicca con il pulsante destro su un'area vuota del desktop o in una cartella del tuo computer, vai a **Bitdefender** e **CIFRATURA FILE di Bitdefender** e seleziona **Crea file Vault**.

  Comparirà una nuova finestra. Procedi come segue:

  1. Clicca su **Sfoglia**, seleziona la posizione del vault e salva il file sotto il nome desiderato.
  2. Scegliere una lettera dal menu per il drive. Aprendo il Vault, un disco virtuale con la lettera selezionata comparirà su **Risorse del computer**.
  3. Digita la password del vault nei campi **Password** e **Conferma**.
  4. Se desideri cambiare la dimensione predefinita del Vault (100 MB), usa i tasti freccia su e giù nella casella numerica **Dimensione Vault (MB)**.
  5. Clicca su **Crea**.

  > **Nota**
  > Aprendo il Vault, comparirà un disco virtuale in **Risorse del computer**. Il drive avrà la lettera di disco assegnata al vault.

- **Aggiungi i file o le cartelle che desideri tenere al sicuro nel vault.**

  Per aggiungere un file a un vault, devi prima aprire il vault.

  1. Sfoglia per trovare il File Vault .bvd.

2. Clicca con il pulsante destro sul File Vault, vai a File Vault di Bitdefender e seleziona **Apri**.
3. Nella finestra che comparirà, inserisci la password, seleziona una lettera dell'unità da assegnare al Vault e clicca su **OK**.

Ora puoi eseguire operazioni sull'unità che corrisponde al File Vault desiderato usando Windows Explorer, proprio come se fosse una normale unità. Per aggiungere un file a un File Vault aperto, puoi anche cliccare con il pulsante destro sul file, andare a File Vault di Bitdefender e selezionare **Aggiungi a File Vault**.

- **Mantieni il vault sempre bloccato.**

  Apri i vault solo in caso di necessità o quando devi gestirne i contenuti. Per bloccare un Vault, clicca con il pulsante destro sull'unità disco virtuale corrispondente da **Risorse del computer**, vai a **File Vault di Bitdefender** e seleziona **Blocca**.

- **Assicurati di non eliminare il File Vault .bvd.**

  Eliminando il file, saranno eliminati anche i contenuti del Vault.

Per maggiori informazioni su come usare i File Vault, fai riferimento a «*Crittografia file*» (p. 133).

3.5.4. 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 computer 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.

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

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

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **PROTEZIONE AUDIO E VIDEO**, clicca su **Accesso a webcam**.

   Comparirà l'elenco delle app che hanno richiesto di accedere alla tua videocamera.
3. Trova l'applicazione a cui vuoi permettere o proibire l'accesso e clicca sull'interruttore corrispondente.

   Per scoprire ciò che gli altri utenti di Bitdefender hanno scelto di fare con la app selezionata, clicca sull'icona . Sarai informato ogni volta che una delle app indicate viene bloccata dagli utenti di Bitdefender.

Per aggiungere manualmente le app a questo elenco, clicca sul link **Aggiungi una nuova applicazione all'elenco**.

3.5.6. 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;

3.6. Strumenti di ottimizzazione

3.6.1. Come posso migliorare le prestazioni del sistema?

Le prestazioni del sistema non dipendono solo dalla configurazione hardware, ma anche dal carico della CPU, dall'uso della memoria e dallo spazio su disco fisso. È anche direttamente collegata alla tua configurazione software e gestione dei dati.

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

- «*Ottimizza le prestazioni del sistema con un semplice clic*» (p. 64)
- «*Controlla periodicamente il sistema*» (p. 65)

Ottimizza le prestazioni del sistema con un semplice clic

L'Ottimizzatore immediato ti consente di risparmiare tempo prezioso quando cerchi un modo rapido per migliorare le prestazioni del sistema, esaminando, rilevando ed eliminando velocemente ogni file inutile.

Per avviare l'Ottimizzatore immediato:

1. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Clicca su **OTTIMIZZA IL MIO DISPOSITIVO**.
3. Consenti a Bitdefender di cercare i file che possono essere eliminati, poi clicca sul pulsante **OTTIMIZZA** per completare il processo.

Per maggiori informazioni su come migliorare la velocità del computer con un semplice clic, fai riferimento a «*Ottimizzare la velocità del sistema con un semplice clic*» (p. 173).

Controlla periodicamente il sistema

La velocità del tuo sistema e le sue prestazioni generali possono essere anche influenzate dalle minacce.

Assicurati di controllare periodicamente il tuo sistema, almeno una volta alla settimana.

Si consiglia di usare la Scansione di sistema perché controlla tutti i tipi di minacce che mettono in pericolo la sicurezza del tuo sistema, oltre a eseguire una scansione degli archivi.

Per avviare la scansione del sistema:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Scansione sistema**.
3. Segui i passaggi della procedura guidata.

3.6.2. Come posso migliorare il tempo di avvio del sistema?

Le applicazioni non necessarie che rallentano fastidiosamente il tempo di avvio del sistema all'apertura del PC, possono essere disattivate o ritardate con l'Ottimizzatore avvio, così da risparmiare tempo prezioso.

Per usare l'Ottimizzatore avvio:

1. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Clicca su **OTTIMIZZA AVVIO DISPOSITIVO**.
3. Seleziona le applicazioni che vuoi ritardare all'avvio del sistema.

Per maggiori informazioni su come ottimizzare il tempo di avvio del PC, fai riferimento a «*Ottimizzare il tempo di avvio del PC*» (p. 174).

3.7. Informazioni utili

3.7.1. 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. 320).

3.7.2. Come posso rimuovere Bitdefender?

Se vuoi rimuovere il tuo Bitdefender Total Security:

- In **Windows 7**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
  2. Trova **Bitdefender Total Security** 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 Total Security** 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 Total Security** 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.

3.7.3. Come posso rimuovere Bitdefender VPN?

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

- 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.

3.7.4. 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 **Rimuovi** nella scheda Bitdefender Anti-tracker.

3.7.5. Come posso spegnere automaticamente il computer 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 sistema 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 finito di lavorare al computer e vuoi andare a riposare. Ti piacerebbe che Bitdefender eseguisse una scansione per rilevare eventuali minacce sull'intero sistema.

Per spegnere il computer 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 **Gestisci scansioni**.
3. Clicca su accanto a Scansione veloce o Scansione del sistema.
4. Nell'elenco **Azioni di post scansione**, seleziona **Spegni il dispositivo** e poi clicca su **AVANTI**.
5. Attiva **Programma attività di scansione** e scegli quando far partire tale attività.

   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.

Per spegnere il computer al termine di una scansione personalizzata:

1. Clicca su accanto alla scansione personalizzata che hai creato.
2. Nella finestra **Atttività scansione**, clicca su **AVANTI**.
3. Nell'elenco **Azioni di post scansione**, seleziona **Spegni il dispositivo**.
4. Clicca su **AVANTI** e clicca su **SALVA**.

Se non vengono rilevate minacce, il computer 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. 87).

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

Se il tuo computer 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.

3.7.7. 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.

3.7.8. 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**.

3.7.9. 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 computer, il sistema diventa instabile. Il programma d'installazione di Bitdefender Total Security rileva automaticamente altri programmi di sicurezza e ti offre la possibilità di disinstallarli.

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

- In **Windows 7**:
  1. 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.

3.7.10. 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 computer.
  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.

4. GESTIRE LA PROPRIA SICUREZZA

4.1. Protezione antivirus

Bitdefender protegge il tuo computer 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 computer, 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 computer per assicurarti di accedervi in sicurezza. Per maggiori informazioni, fai riferimento a «*Scansione automatica di supporti rimovibili*» (p. 91).

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. 93).

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. 96).

Se il tuo computer è stato infettato da una minaccia, fai riferimento a «*Rimuovere le minacce dal sistema*» (p. 206). Per aiutarti a ripulire il tuo computer dalle minacce che non possono essere rimosse dal sistema operativo Windows, Bitdefender ti offre una «*Bitdefender Modalità di soccorso (Ambiente di soccorso in Windows 10)*» (p. 207). Si tratta di un ambiente sicuro, realizzato specificatamente per la rimozione delle minacce, che ti consente di avviare il tuo computer in modo indipendente da Windows. Quando il computer parte in Modalità soccorso (Ambiente di soccorso in Windows 10), le minacce di Windows non sono attive, semplificando così la loro rimozione.

4.1.1. Scansione all'accesso (protezione in tempo reale)

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

Attivare o disattivare la protezione in tempo reale

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

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

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 **Impostazioni**.
3. Nella finestra **Protezione**, clicca sul menu a fisarmonica **Mostra impostazioni avanzate**.

   Verrà mostrata una finestra a pannelli.
4. Scorri in basso sulla finestra per 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 computer, 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).
- **Esaminare email.** Per impedire il download di minacce sul tuo computer, Bitdefender esamina automaticamente le e-mail in entrata e uscita.

  Sebbene non consigliabile, per aumentare le prestazioni del sistema, puoi disattivare la scansione di minacce per le e-mail. Disattivando le opzioni di scansione corrispondenti, le e-mail e i file ricevuti non saranno esaminati, consentendo ai file infetti di essere salvati sul computer. Questa non è una minaccia particolarmente importante, perché la protezione in tempo reale bloccherà le minacce quando si accede ai file infetti (apertura, spostamento, copiatura o esecuzione).
- **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 **Impostazioni**.
3. Nella finestra **Protezione**, clicca sul menu a fisarmonica **Mostra impostazioni avanzate**.

   Verrà mostrata una finestra a pannelli.
4. Scorri in basso nella finestra finché non trovi l'opzione **Azioni minaccia**.
5. 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. 96).

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. 96).

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

Ripristinare le impostazioni predefinite

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

Per ripristinare le impostazioni predefinite della protezione in tempo reale:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Impostazioni**.
3. Nella finestra **Protezione**, clicca sul menu a fisarmonica **Mostra impostazioni avanzate**.

   Verrà mostrata una finestra a pannelli.
4. Scorri in basso nella finestra finché non trovi l'opzione **Azzera impostazioni**. Seleziona questa opzione per riportare le impostazioni dell'antivirus ai valori predefiniti.

4.1.2. Scansione a richiesta

L'obiettivo principale di Bitdefender è di mantenere il proprio computer privo di minacce. Ciò avviene tenendo lontani le nuove minacce dal computer 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 computer alla ricerca di minacce residenti dopo aver installato Bitdefender. Inoltre, è una buona idea effettuare frequentemente una scansione del computer, 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 computer ogni volta che vuoi, avviando le attività predefinite o una tua scansione (attività definite dall'utente). Se desideri controllare ubicazioni particolari sul tuo computer o impostare le opzioni di scansione, configura ed esegui una scansione personale.

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.

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 **Scansione veloce**.
3. Segui la procedura guidata della scansione antivirus per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati. Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

Eseguire una scansione del sistema

La Scansione del sistema esamina l'intero computer 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 computer.

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. 35).
- Chiudere tutti i programmi aperti.

Se desideri controllare ubicazioni particolari sul tuo computer o impostare le opzioni di scansione, configura ed esegui una scansione personale. Per maggiori informazioni, fai riferimento a «*Configurare una scansione personale*» (p. 84).

Per eseguire una scansione del sistema:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Scansione sistema**.
3. La prima volta che esegui una Scansione di sistema, ti sarà presentata questa funzionalità. Clicca su **OK, HO CAPITO** per continuare.
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.

Configurare una scansione personale

Nella finestra **Gestisci scansioni**, puoi impostare Bitdefender per eseguire le scansioni ogni volta che ritieni che il tuo computer 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.

Accedendo alla finestra, saranno disponibili le seguenti icone:

L'attività di scansione programmata viene disattivata.

L'attività di scansione programmata viene attivata.

Qui è possibile eseguire la configurazione nei dettagli.

Elimina la scansione selezionata. Questa opzione è disponibile solo per le nuove scansioni personalizzate.

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 **Gestisci scansioni**.
3. Clicca su **Crea una nuova attività di 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. Attiva **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 computer.
- **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.

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 ignorare questo oggetto 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. 96).

  > **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. 206).

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**.

4.1.3. Scansione automatica di supporti rimovibili

Bitdefender rileva automaticamente quando si collega un dispositivo di archiviazione rimovibile al computer 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 computer.

I dispositivi rilevati rientrano in una di queste categorie:

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

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

Come funziona?

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

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. 206).

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 **Impostazioni**.
3. Seleziona la scheda **Unità e dispositivi**.

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.

4.1.4. 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**.

4.1.5. 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**.

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 **Impostazioni**.
3. Seleziona la scheda **Eccezioni**.
4. Clicca sul menu a fisarmonica **Elenco di file e cartelle escluse dalla scansione**. Nella finestra che compare, puoi gestire i file e le cartelle esclusi dalla scansione.
5. Aggiungi eccezioni seguendo questi passaggi:
   a. Clicca su **Add** (Aggiungi).
   b. Clicca su **SFOGLIA**, seleziona il file o la cartella che desideri escludere dalla scansione e quindi clicca su **Aggiungi**. In alternativa, puoi digitare (o copiare e incollare) il percorso del file o della cartella nello spazio apposito.
   c. Di norma, il file o la cartella selezionati sono esclusi dalla scansione all'accesso e da quella su richiesta. Per cambiare quando applicare l'eccezione, seleziona una delle altre opzioni.
   d. Clicca su **Add** (Aggiungi).

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 computer. 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 computer 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 **Impostazioni**.
3. Seleziona la scheda **Eccezioni**.
4. Clicca sul menu a fisarmonica **Elenco delle estensioni escluse dalla scansione**. Nella finestra che compare, puoi gestire le estensioni dei file escluse dalla scansione.
5. Aggiungi eccezioni seguendo questi passaggi:
   a. Clicca su **Add** (Aggiungi).
   b. Inserisci le estensioni che vuoi escludere dalla scansione, separate da punto e virgola (;). Ecco un esempio:

      txt;avi;jpg

   c. Di norma, tutti i file con le estensioni indicate sono esclusi dalla scansione all'accesso e da quella su richiesta. Per cambiare quando applicare l'eccezione, seleziona una delle altre opzioni.
   d. Clicca su **AGGIUNGI**.

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 **Impostazioni**.
3. Seleziona la scheda **Eccezioni**.
4. Usa le opzioni nel menu a fisarmonica **Elenco di file e cartelle escluse dalla scansione** per gestire le eccezioni della scansione.
5. Per rimuovere o modificare le eccezioni della scansione, clicca su uno dei collegamenti disponibili. Procedi come segue:
   - Per rimuovere una voce dall'elenco, selezionala e clicca su **Rimuovi**.
   - Per modificare una voce dalla tabella, cliccaci sopra due volte (o selezionala e clicca su **Modifica**). Apparirà una nuova finestra, dove

potrai modificare l'estensione o il percorso da escludere e il tipo di scansione dal quale escluderlo, a seconda delle necessità. Esegui i cambiamenti necessari, poi clicca su **MODIFICA**.

4.1.6. 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 **Quarantena**.

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

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

   Clicca sugli interruttori per attivare o disattivare:

   Esamina nuovamente la quarantena dopo l'aggiornamento delle informazioni delle minacce

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

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

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

4. 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**.

4.2. Difesa da minacce avanzate

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 computer, cercando eventuali minacce. A ognuna viene assegnato un punteggio e per ogni processo viene poi assegnato un punteggio totale.

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

Attivare o disattivare Advanced Threat Defense

Per attivare o disattivare Advanced Threat Defense:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ADVANCED THREAT DEFENSE**, attiva o disattiva l'interruttore.

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

Verificare gli attacchi dannosi rilevati

Ogni volta che vengono rilevate minacce o processi potenzialmente dannosi, Bitdefender li bloccherà per impedire l'infezione del tuo computer 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 **Difesa minacce**.
3. La prima volta che accedi alla Protezione da ransomware, ti sarà presentata questa funzionalità. Clicca su **OK, HO CAPITO** per continuare.

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

Aggiungere processi alle eccezioni

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

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

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ADVANCED THREAT DEFENSE**, clicca su **Impostazioni**.
3. Nell'area **Eccezioni**, clicca su **Aggiungi applicazioni alle eccezioni**.
4. Trova e seleziona l'applicazione che vuoi escludere, e clicca su **OK**.

   Per rimuovere una voce dall'elenco, clicca sull'opzione **Rimuovi** accanto ad essa.

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 computer 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 **Impostazioni**.
- Clicca sull'interruttore corrispondente per attivarla o disattivarla.

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

4.3. 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**.

Nella finestra **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 dalle frodi.

- Protezione da phishing.

Nella finestra **Prevenzione minacce rete**, hai l'opzione **Prevenzione minacce rete**. Per mantenere il tuo computer 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 **Eccezioni**.
3. Inserisci nel campo corrispondente il nome del sito web, il nome del dominio o l'indirizzo IP che vuoi aggiungere alle eccezioni, e clicca su **AGGIUNGI**.

   Per rimuovere una voce dall'elenco, selezionala e clicca su **Rimuovi**.

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

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.

4.4. Antispam

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

L'antispam di Bitdefender impiega notevoli innovazioni tecnologiche e filtri standard dell'industria antispam per eliminare lo spam prima che raggiunga la Posta in arrivo dell'utente. Per maggiori informazioni, fai riferimento a «*Approfondimenti antispam*» (p. 102).

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

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

I messaggi spam rilevati da Bitdefender sono segnati con il prefisso [spam] nell'oggetto. Bitdefender sposta automaticamente i messaggi spam a una cartella specifica, come segue:

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

Se si utilizza un altro client di posta, è necessario creare una regola per spostare i messaggi e-mail segnati come [spam] da Bitdefender in una cartella personalizzata di quarantena. Se le cartelle Posta eliminata o Cestino vengono eliminate, sarà eliminata anche la cartella Spam. Tuttavia, sarà creata una nuova cartella Spam non appena un'e-mail sarà indicata come spam.

4.4.1. Approfondimenti antispam

Filtri Antispam

Il motore antispam Bitdefender include una protezione cloud e altri filtri, che proteggono la tua casella di posta in arrivo da ogni SPAM, come Elenco Amici, Elenco Spammer e Filtro Caratteri..

Elenco amici / Elenco spammer

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

Nota

Raccomandiamo di aggiungere i nomi e gli indirizzi e-mail dei propri amici all'**elenco Amici**. Bitdefender non blocca i messaggi dai mittenti inclusi nell'elenco; perciò, aggiungendo gli amici i loro messaggi legittimi arriveranno.

Filtro caratteri

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

Operazione antispam

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

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

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

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

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

Programmi e protocolli di posta elettronica supportati

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

- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 e superiore

4.4.2. Attivare o disattivare la protezione antispam

Di norma la protezione antispam è attivata.

Per attivare o disattivare la funzionalità Antispam:

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

2. Nel pannello **ANTISPAM**, attiva o disattiva l'interruttore.

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

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

Importante

Bitdefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo. Per un elenco completo delle applicazioni di posta supportate, fai riferimento a «*Programmi e protocolli di posta elettronica supportati*» (p. 103).

Qui di seguito la spiegazione di ogni pulsante della barra degli strumenti di Bitdefender:

Impostazioni - Apre una finestra dove puoi configurare i filtri antispam e le impostazioni della barra degli strumenti.
È spam - Indica che l'e-mail selezionata è spam. L'e-mail sarà spostata immediatamente alla cartella **Spam**. Se i servizi cloud antispam sono attivati, il messaggio è inviato al cloud di Bitdefender per ulteriori analisi.
Non è spam - Indica che l'e-mail selezionata non è spam e Bitdefender non deve marcarla. L'e-mail sarà spostata dalla cartella **Spam** alla **Posta in arrivo**. Se i servizi cloud antispam sono attivati, il messaggio è inviato al cloud di Bitdefender per ulteriori analisi.

Importante

Il pulsante **Non è spam** si attiva quando si seleziona un messaggio marcato come SPAM da Bitdefender (normalmente questi messaggi sono situati nella cartella **Spam**).

Aggiungi Spammer - aggiunge il mittente dell'e-mail selezionata all'elenco degli Spammer. Può essere necessario premere **OK** per confermare. I messaggi e-mail ricevuti dagli indirizzi nell'elenco Spammer sono contrassegnati automaticamente come [spam].
Aggiungi amico - aggiunge il mittente dell'e-mail selezionata all'elenco Amici. Può essere necessario premere **OK** per confermare. Riceverai sempre

e-mail provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

Spammer - Apre l'**elenco Spammer**, che contiene tutti gli indirizzi e-mail dai quali non vuoi ricevere messaggi, indipendentemente dal loro contenuto. Per maggiori informazioni, fai riferimento a «*Configurazione dell'elenco Spammer*» (p. 107).

Amici - Apre l'**elenco Amici** che contiene tutti gli indirizzi e-mail dai quali desideri ricevere sempre i messaggi, indipendentemente dal loro contenuto. Per maggiori informazioni, fai riferimento a «*Configurazione dell'elenco Amici*» (p. 106).

Indicare gli errori di rilevazione

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

1. Apri il tuo client e-mail.
2. Vai alla cartella posta indesiderata, dove vengono spostati i messaggi spam.
3. Seleziona il messaggio legittimo scorrettamente contrassegnato come [spam] da Bitdefender.
4. Clicca sul pulsante **Aggiungi amico** sulla barra degli strumenti antispam di Bitdefender per aggiungere il mittente all'elenco Amici. Può essere necessario premere **OK** per confermare. Riceverai sempre e-mail provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.
5. Clicca sul pulsante **Non è Spam** sulla barra degli strumenti antispam di Bitdefender (in genere localizzata nella parte superiore della finestra del client di posta). L'e-mail sarà spostata nella cartella Posta in arrivo.

Indicare messaggi spam non rilevati

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

1. Apri il tuo client e-mail.

2. Vai alla cartella Posta in arrivo.
3. Seleziona i messaggi di spam non rilevati.
4. Clicca sul pulsante **È Spam** sulla barra degli strumenti antispam di Bitdefender (in genere localizzata nella parte superiore della finestra del client di posta). Vengono immediatamente contrassegnati come [spam] e verranno spostati alla cartella posta indesiderata.

Configurare le impostazioni della barra degli strumenti

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

Hai le seguenti opzioni:

- **Etichetta i messaggi di spam come "letti"** - Etichetta i messaggi di spam come letti in modo automatico, in modo tale da non disturbare quando questi vengono ricevuti.
- Puoi scegliere se visualizzare o no le finestre di conferma quando clicchi sui pulsanti **Aggiungi Spammer** e **Aggiungi Amico** nella barra degli strumenti antispam.

  Le finestre di conferma possono impedire di aggiungere accidentalmente i mittenti all'elenco Amici / Spammer.

4.4.4. Configurazione dell'elenco Amici

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

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

Per configurare e gestire l'elenco Amici:

- Se stai usando Microsoft Outlook, clicca sul pulsante **Amici** nella barra degli strumenti antispam di Bitdefender.
- In alternativa:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTISPAM**, clicca su **Gestisci amici**.

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

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

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

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

Per eliminare un elemento dall'elenco, clicca sul collegamento **Rimuovi** corrispondente. Per eliminare tutti i dati dall'elenco, cliccare su **CANCELLA LISTA**.

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

Per caricare un elenco Amici salvato in precedenza, clicca sul pulsante **CARICA** e apri il corrispondente file .bwl. Per ripristinare il contenuto dell'elenco esistente quando si carica un elenco salvato in precedenza, seleziona **Sovrascrivi elenco attuale**.

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

4.4.5. Configurazione dell'elenco Spammer

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

Per configurare e gestire l'elenco Spammer:

- Se stai usando Microsoft Outlook o Thunderbird, clicca sul pulsante **Spammer** nella barra degli strumenti antispam di Bitdefender integrata nel tuo client e-mail.
- In alternativa:
  1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
  2. Nel pannello **ANTISPAM**, clicca su **Gestisci spammer**.

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

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

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

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

Avvertimento

Non aggiungere domini di servizi e-mail legittimi (ad esempio Yahoo, Gmail, Hotmail o altri) all'elenco Spammer. In caso contrario gli indirizzi e-mail ricevuti dagli utenti registrati di tali servizi verranno identificati come spam. Se, ad esempio, aggiungi yahoo.com all'elenco Spammer, tutti i messaggi e-mail provenienti da indirizzi yahoo.com saranno contrassegnati come [spam].

Per eliminare un elemento dall'elenco, clicca sul collegamento **Rimuovi** corrispondente. Per eliminare tutti i dati dall'elenco, cliccare su **CANCELLA LISTA**.

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

Per caricare un elenco Spammer salvato in precedenza, clicca sul pulsante **CARICA** e apri il corrispondente file .bwl. Per ripristinare il contenuto dell'elenco esistente quando si carica un elenco salvato in precedenza, seleziona **Sovrascrivi elenco attuale**.

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

4.4.6. Configurare i filtri locali antispam

Come descritto in «*Approfondimenti antispam*» (p. 102), Bitdefender usa una combinazione di diversi filtri antispam per identificare lo spam. I filtri antispam sono pre-configurati per una protezione ottimale.

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

Per configurare i filtri locali antispam:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTISPAM**, clicca su **Impostazioni**.
3. Clicca sui corrispondenti interruttori di attivazione o disattivazione.

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

4.4.7. Configurare le impostazioni cloud

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

La protezione cloud funziona finché si tiene attivo l'antispam di Bitdefender.

Campioni di e-mail legittime o spam possono essere inviati al cloud di Bitdefender, indicando errori di rilevazione o messaggi spam non rilevati. Ciò contribuisce a migliorare la rilevazione antispam di Bitdefender.

Configura l'invio di un'e-mail campione al cloud di Bitdefender e seleziona le opzioni desiderate seguendo questi passaggi:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTISPAM**, clicca su **Impostazioni**.
3. Clicca sui corrispondenti interruttori di attivazione o disattivazione.

Se stai usando Microsoft Outlook o Thunderbird, puoi configurare la rilevazione cloud direttamente dal tuo client di posta. Clicca sul pulsante ⚙ **Impostazioni** sulla barra degli strumenti antispam di Bitdefender (in genere localizzata nella parte superiore della finestra del client di posta) e poi sulla scheda **Impostazioni cloud**.

4.5. Firewall

Il firewall protegge il computer da tentativi di connessione in entrata e in uscita non autorizzati, su reti locali e Internet. È abbastanza simile a una guardia a un cancello: tiene traccia dei tentativi di connessione e decide chi far entrare e chi bloccare.

Il firewall di Bitdefender utilizza un set di regole per filtrare i dati trasmessi al e dal sistema.

In condizioni normali, Bitdefender crea automaticamente una regola ogni volta che un'applicazione cerca di accedere a Internet. Puoi anche aggiungere o modificare manualmente le regole per le applicazioni.

Come misura di sicurezza sarai avvisato ogni volta che a una app potenzialmente dannosa viene impedito di accedere a Internet.

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

Per scoprire altre informazioni sulle impostazioni del firewall per ogni tipo di rete e come modificare le impostazioni della rete, fai riferimento a «*Gestire le impostazioni di connessione*» (p. 114).

Attivare o disattivare la protezione del firewall

Per attivare o disattivare la protezione del firewall:

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

> **Avvertimento**
>
> Poiché espone il computer a connessioni non autorizzate, la disattivazione del firewall dovrebbe essere solo una misura temporanea. Riattiva il firewall il prima possibile.

4.5.1. Gestire le regole delle app

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

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **FIREWALL**, clicca su **Accesso applicazione**.
3. La prima volta che accedi al Firewall, ti sarà presentata questa funzionalità. Clicca su **OK, HO CAPITO** per continuare.

Puoi vedere gli ultimi 15 programmi (processi) che sono passati tramite Bitdefender e la rete Internet a cui sei connesso. Per visualizzare le regole create per un'applicazione specifica, cliccaci semplicemente sopra, e poi clicca sul link **Vedi regole applicazione**. Si aprirà la finestra **Regole**.

Per ogni regola sono visualizzate le seguenti informazioni:

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

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

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

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

Aggiungere regole per le app

Per aggiungere una regola per una app:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **FIREWALL**, clicca su **Impostazioni**.
3. Nella finestra **Regole**, clicca su **Aggiungi regola**.

Nella finestra **Impostazioni**, puoi applicare le seguenti modifiche:

- **Applica questa regola a tutte le applicazioni.** Attiva questo interruttore per applicare la regola creata a tutte le applicazioni.
- **Percorso del Programma.** Clicca su **SFOGLIA** e seleziona la app sulla quale applicare la regola.
- **Autorizzazione.** Seleziona uno dei permessi disponibili:

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

- **Tipo di rete.** Seleziona il tipo di rete a cui si applica la regola. Puoi cambiare il tipo, aprendo il menu a tendina **Tipo di rete** e selezionare uno dei tipi disponibili dall'elenco.

Tipo di rete	Descrizione
Ogni rete	Consenti tutto il traffico tra il tuo computer e gli altri computer, indipendentemente dal tipo di rete.
Casa/Ufficio	Consente tutto il traffico tra il tuo computer e quelli nella rete locale.
Pubblica	Tutto il traffico viene filtrato.

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

    Nota

    I numeri dei protocolli IP vengono assegnati dalla Internet Assigned Numbers Authority (IANA). Puoi trovare l'elenco completo dei numeri di protocolli IP assegnati su http://www.iana.org/assignments/protocol-numbers.

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

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

Nella finestra **Avanzate**, puoi personalizzare le seguenti impostazioni:

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

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

4.5.2. Gestire le impostazioni di connessione

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

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

Per configurare i tuoi adattatori di rete:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **FIREWALL**, clicca su **Impostazioni**.
3. Seleziona la scheda **Adattatori di rete**.
4. Seleziona le impostazioni che desideri applicare quando ti connetti ai seguenti adattatori:
   - Wi-Fi
   - Ethernet

4.5.3. Configurare le impostazioni avanzate

Per configurare le impostazioni avanzate del firewall:

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

Possono essere configurate le seguenti funzionalità:

- **Protezione da port scan** - rileva e blocca i tentativi di scoprire quali porte sono aperte.

  Le scansioni delle porte vengono comunemente usate dagli hacker per scoprire quali porte sono aperte sul tuo computer. Potrebbero quindi introdursi nel computer, se trovassero una porta meno sicura o vulnerabile.

- **Modalità allerta** - Gli avvisi vengono mostrati ogni volta che un'applicazione tenta di connettersi a Internet. Seleziona **Consenti** o **Blocca**. Quando viene attivata la modalità allerta, la funzionalità Profili viene disattivata automaticamente. La modalità allerta può essere utilizzata simultaneamente con la **Modalità Batteria**.

- **Consenti accesso al dominio di rete** - Consente o nega l'accesso a risorse e condivisioni definite dai controller di dominio.

- **Modalità invisibile** - Possibilità di essere rilevati da altri computer. Clicca su **Modifica impostazioni modalità invisibile** per scegliere quando il dispositivo deve o non deve essere visibile agli altri computer.

- **Comportamento applicazione predefinito** - Consente a Bitdefender di applicare impostazioni automatiche alle applicazioni senza regole definite. Clicca su **Modifica regole predefinite** per scegliere se applicare o no le impostazioni automatiche.

  - Automatico - L'accesso alle applicazioni sarà autorizzato o negato in base al Firewall automatico e alle regole utente.
  - Consenti - Le applicazioni che non hanno una regola del Firewall definita saranno autorizzate automaticamente.
  - Blocca - Le applicazioni che non hanno una regola del Firewall definita saranno bloccate automaticamente.

4.6. Vulnerabilità

Un passaggio importante nella protezione del computer 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 computer, 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 controlla automaticamente il sistema alla ricerca di vulnerabilità e fornisce avvisi al riguardo. Esamina quanto segue:

- app datate sul tuo computer.
- aggiornamenti di Windows mancanti.
- password deboli per gli account utente di Windows.
- Reti e router wireless non sicuri.

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.

4.6.1. 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 **Scansione vulnerabilità**.
3. La prima volta che accedi alla Scansione vulnerabilità, ti viene introdotta tale funzionalità. Clicca su **AVVIA SCANSIONE** per continuare e attendi che Bitdefender controlli il sistema alla ricerca di vulnerabilità.

- **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.

- **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.

- **Account Windows poco sicuri**

  Puoi visualizzare l'elenco degli account di Windows configurati sul tuo computer 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 @).

- **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.

4.6.2. 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 **Impostazioni**.

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

3. Seleziona le vulnerabilità del sistema che desideri siano controllate regolarmente usando gli interruttori corrispondenti.

Agg. Windows
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.

4.6.3. 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

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 **Impostazioni**.
3. Nella finestra **Impostazioni**, attiva o disattiva l'opzione **Wi-Fi Security Advisor**.

Configurare la rete Wi-Fi di casa

Per iniziare a configurare la tua rete di casa:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **VULNERABILITÀ**, clicca su **Sicurezza Wi-Fi**.
3. 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.
4. Individua la tua rete di casa e clicca su **SELEZIONA**.

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

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

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

Configurare la rete Wi-Fi dell'ufficio

Per iniziare a configurare la tua rete dell'ufficio:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **VULNERABILITÀ**, clicca su **Sicurezza Wi-Fi**.
3. 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.
4. Individua la tua rete dell'ufficio e clicca su **SELEZIONA**.

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

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

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

Wi-Fi pubblica

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

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

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 **Sicurezza Wi-Fi**.
3. In base alle informazioni che ti servono, seleziona una delle tre schede, **Wi-Fi di casa**, **Wi-Fi ufficio** o **Wi-Fi pubblica**.
4. 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.

4.7. Protezione audio e video

Sempre più minacce sono progettate per accedere a webcam e microfoni integrati. Per impedire l'accesso non autorizzato alla tua webcam e informarti su quali app non affidabili cerchino di accedere al microfono del tuo dispositivo e quando, Bitdefender audio e video ha incluso:

- Protezione webcam

- Controllo microfono

4.7.1. Protezione webcam

Hacker che potrebbero prendere il controllo della tua webcam per spirati non sono più una fantasia e le soluzioni per proteggerla, come revocare i privilegi dell'applicazione e disattivare o coprire la videocamera integrata non sono molto pratiche. Per prevenire ulteriori tentativi di ottenere l'accesso alla tua privacy, la Protezione webcam di Bitdefender monitora continuamente le app che tentano di accedere alla videocamera, bloccando quelle non indicate come affidabili.

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

Attivare o disattivare la Protezione webcam

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

Configurare la Protezione webcam

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

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **PROTEZIONE AUDIO E VIDEO**, clicca su **Impostazioni**.
3. Seleziona la scheda **Webcam**.

Sono disponibili le seguenti opzioni:

Regole di blocco delle applicazioni

- **Blocca ogni accesso alla webcam** - Nessuna applicazione potrà accedere alla tua webcam.
- **Blocca l'accesso dei browser alla webcam** - A nessun browser web, tranne Internet Explorer e Microsoft Edge, sarà consentito di accedere alla tua webcam. Siccome le app di Windows Store vengono eseguite in un singolo processo, Internet Explorer e Microsoft Edge non possono essere rilevati da Bitdefender come browser web e quindi sono esclusi da questa impostazione.

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

  Sarai informato ogni volta che una delle tue app installate sarà indicata come bloccata dalla maggior parte degli utenti di Bitdefender.

Notifiche

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

Aggiungere app all'elenco della Protezione webcam

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

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **PROTEZIONE AUDIO E VIDEO**, clicca su **Accesso a webcam**.
3. La prima volta che accedi alla Protezione webcam, ti sarà presentata questa funzionalità.
4. Clicca sul link desiderato:
   - **Seleziona le app di Windows Store da aggiungere all'elenco di quelle autorizzate** - Viene mostrato un elenco con le app di Windows Store rilevate. Attiva gli interruttori accanto alle app che vuoi aggiungere all'elenco.
   - **Inizia ad aggiungere applicazioni all'elenco di accesso alla webcam** - Vai al file .exe che desideri aggiungere all'elenco e clicca su **OK**.

     Per aggiungere altre app, clicca su **Aggiungi una nuova applicazione all'elenco**.

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

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

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

Per bloccare l'accesso alla tua webcam di una app aggiunta, clicca sull'icona  . L'icona diventa  , indicando che la app selezionata non avrà alcun accesso alla tua webcam.

4.7.2. Controllo microfono

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

Attivare o disattivare Controllo microfono

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **PROTEZIONE AUDIO E VIDEO**, clicca su **Impostazioni**.
3. Seleziona la scheda **Microfono**.
4. Nella finestra **Microfono**, attiva o disattiva l'interruttore corrispondente.

Configurare le notifiche per Controllo microfono

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

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **PROTEZIONE AUDIO E VIDEO**, clicca su **Impostazioni**.
3. Seleziona la scheda **Microfono**.

Notifiche

- **Informa quando un'applicazione prova ad accedere al microfono**
- **Ti informa quando i browser accedono al microfono**
- **Ti informa quando app non affidabili accedono al microfono**

- **Mostra una notifica in base alle scelte degli utenti di Bitdefender**

Aggiungere app all'elenco di Controllo microfono

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

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **PROTEZIONE AUDIO E VIDEO**, clicca su **Controllo microfono**.
3. La prima volta che accedi a Controllo microfono, ti sarà presentata questa funzionalità.
4. Clicca sul link desiderato:
   - **Seleziona le app di Windows Store da aggiungere all'elenco** - Viene mostrato un elenco con le app di Windows Store rilevate. Attiva gli interruttori accanto alle app che vuoi aggiungere all'elenco.
   - **Inizia ad aggiungere applicazioni all'elenco** - Vai al file .exe che desideri aggiungere all'elenco e clicca su **OK**.

     Per aggiungere altre app, clicca su **Aggiungi una nuova applicazione all'elenco**.

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

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

Per non ricevere più notifiche relative alle attività di una app aggiunta, clicca sull'icona  . L'icona diventa  , indicando che nessuna notifica di Bitdefender sarà mostrata quando la app selezionata cercherà di accedere al tuo microfono.

4.8. Safe files

Un Ransomware è un programma dannoso che colpisce i sistemi vulnerabili bloccandoli e chiedendo denaro agli utenti per riavere il controllo dei propri sistemi. Questo programma dannoso agisce in maniera molto scaltra,

mostrando falsi messaggi per allarmare l'utente, spingendoli al pagamento delle cifre richieste.

L'infezione può diffondersi tramite le e-mail spam, scaricando allegati o visitando siti web infetti e installando app dannose, tutto senza che l'utente si renda conto di ciò che sta accadendo al suo sistema.

Un Ransomware può utilizzare uno dei seguenti comportamenti per impedire all'utente di accedere al suo sistema:

- Crittografare file personali e sensibili senza dare la possibilità di decrittarli fino al pagamento di un riscatto da parte della vittima.
- Bloccare lo schermo di un computer e visualizzare una richiesta di denaro. In questo caso, non viene cifrato alcun file, ma l'utente è comunque costretto a pagare.
- Impedisce l'esecuzione delle app.

Con Safe files di Bitdefender, puoi mantenere protetti dagli attacchi ransomware i tuoi file personali, come documenti, fotografie o film.

Nota
Advanced Threat Defense e Safe files sono due livelli di protezione dai ransomware. Advanced Threat Defense è una funzionalità che blocca immediatamente gli attacchi ransomware alle zone critiche del tuo sistema, mentre Safe files si assicura che nessun file importante sul computer venga cifrato.

4.8.1. Attivare o disattivare Safe files

Per attivare o disattivare la funzionalità Safe files:

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

Ogni volta che un'applicazione tenterà di accedere a un file protetto, comparirà una finestra pop-up di Bitdefender. Puoi autorizzare o bloccare l'accesso.

Nota
La funzionalità Safe files non viene attivata automaticamente.

4.8.2. Proteggi i tuoi file personali dagli attacchi dei Ransomware.

Se vuoi inserire i tuoi file personali in un'area protetta:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **SAFE FILES**, clicca su **Cartelle protette**.
3. La prima volta che accedi a Cartelle protette, ti sarà presentata questa funzionalità. Clicca su **PROTEGGI ALTRE CARTELLE** per continuare.
4. Seleziona la cartella che vuoi proteggere e clicca su **OK**.

   Per aggiungere altre cartelle, clicca sul link **Proteggi altre cartelle**. In alternativa, trascina le cartelle in questa finestra.

Di norma, le cartelle Immagini, Video, Documenti e Musica sono protette dagli attacchi di ogni minaccia. I dati personali memorizzati in servizi online di file hosting come Box, Dropbox, Google Drive e OneDrive sono inclusi nell'ambiente di protezione, a condizione che le loro applicazioni siano installate sul sistema.

Per evitare rallentamenti al sistema, ti consigliamo di aggiungere un massimo di 30 cartelle, o salvare più file in una sola cartella.

> **Nota**
> Le cartelle personali possono essere protette solo per gli utenti attuali. I file di sistema e delle applicazioni non possono essere aggiunti alle eccezioni.

4.8.3. Configurare l'accesso alle app

Le applicazioni che cercano di modificare o eliminare file protetti potrebbero essere segnalate come potenzialmente pericolose e aggiunte all'elenco delle "applicazioni bloccate". Se un'applicazione venisse bloccata ma hai la certezza che il suo comportamento sia assolutamente normale, puoi autorizzarla seguendo questi passaggi:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **SAFE FILES**, clicca su **Accesso applicazioni**.

3. Verranno elencate le app che hanno richiesto di modificare i file nelle tue cartelle protette. Attiva l'interruttore accanto alla app che ritieni essere sicura.

Nella stessa finestra, puoi disattivare la protezione dai ransomware per determinate app, disattivando l'interruttore corrispondente.

Se vuoi aggiungere nuove applicazioni all'elenco, clicca sul link **Aggiungi una nuova applicazione all'elenco**.

4.8.4. Protezione all'avvio

È risaputo che molte app dannose sono impostate per essere eseguite all'avvio del sistema, cosa che può danneggiare seriamente un computer. La Protezione avvio di Bitdefender esamina tutte le aree critiche del sistema prima che i file vengano caricate, non influenzandone le prestazioni.

Per disattivare la protezione all'avvio:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **SAFE FILES**, clicca su **Impostazioni**.
3. Disattiva **Protezione all'avvio**.

> **Nota**
> Le applicazioni aggiunte alle eccezioni saranno esaminate e trattate di conseguenza.

4.9. 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.

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.

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 **Impostazioni**.
3. Attiva o disattiva l'interruttore **Ripristino automatico**.

Visualizzare i file che sono stati ripristinati automaticamente

Quando l'opzione **Ripristino automatico** è attiva, Bitdefender ripristinerà automaticamente i file che sono stati cifrati da un ransomware. Quindi potrai usare il computer 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.

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;

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 **Eccezioni**.
3. Per iniziare ad aggiungere app all'elenco, clicca sul link **Aggiungi una nuova applicazione all'elenco**.

4.10. Crittografia file

La Crittografia file di Bitdefender permette di creare drive logici (o vault) criptati e protetti da password sul computer, dove puoi archiviare i documenti confidenziali e sensibili in modo sicuro. L'accesso ai dati immagazzinati in questi vault è consentito solo agli utenti che conoscono la password.

La password ti consente di aprire, archiviare dati e chiudere un vault, mantenendo la sua sicurezza. Mentre un vault è aperto, puoi aggiungere nuovi file, accedere ai file correnti o modificarli.

Fisicamente, il Vault è un file immagazzinato nel disco fisso locale, con l'estensione .bvd. Anche se l'accesso ai file fisici che rappresentano i drive protetti è possibile da diversi sistemi operativi (come Linux), le informazioni immagazzinate in essi non possono essere lette perché criptate.

I File Vault possono essere gestiti dalla finestra di Bitdefender o usando il menu contestuale di Windows e l'unità logica associata con il Vault.

Gestire i File Vault

Per gestire i tuoi File Vault da Bitdefender:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **CIFRATURA FILE**, clicca su **Impostazioni**.

   I File Vault esistenti compaiono in questa finestra.

Creare i File Vault

Per creare un nuovo Vault:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **CRITTOGRAFIA FILE**, clicca su **Crea nuovo File Vault**.
3. Specifica il nome e la posizione del File Vault.
   - Inserisci il nome del File Vault nel campo corrispondente.
   - Clicca su **SFOGLIA**, seleziona la posizione del Vault e salva il File Vault sotto il nome desiderato.
4. Scegli una lettera dell'unità dal menu corrispondente. Aprendo il Vault, un disco virtuale con la lettera selezionata comparirà su Risorse del Computer.

5. Se desideri cambiare la dimensione predefinita del Vault (100 MB), usa i tasti freccia su e giù nella casella numerica **Dimensione Vault (MB)**.
6. Digita la password desiderata per il Vault nei campi **Password** e **Conferma password**. La password deve essere composta da almeno 8 caratteri. Qualsiasi persona che tenti di aprire il vault e accedere ai suoi file, dovrà fornire la password.
7. Clicca su **CREA**.

Bitdefender informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizza il relativo messaggio per risolverlo.

Per creare un nuovo Vault più rapidamente, clicca con il pulsante destro su un'area vuota del desktop o in una cartella del tuo computer, vai a **Bitdefender** e **CIFRATURA FILE di Bitdefender** e seleziona **Crea file Vault**.

Nota
Potrebbe essere conveniente salvare tutti i file vault nella stessa posizione. In questo modo, è possibile trovarli più velocemente.

Importare un File Vault

Per importare un File Vault memorizzato in locale:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **CRITTOGRAFIA FILE**, clicca su **Importa Vault**.
3. Cerca il percorso del tuo Vault e selezionalo (il file .bvd).
4. Clicca su **Apri**.

Aprire i File Vault

Per accedere e lavorare sui file immagazzinati in un vault, dovrai aprire il vault. Aprendo un Vault, comparirà un disco virtuale nelle Risorse del Computer. Il drive avrà la lettera di disco assegnata al vault.

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **CIFRATURA FILE**, clicca su **Impostazioni**.
3. Seleziona il Vault che vuoi aprire e clicca su **SBLOCCA**.
4. Digita la password richiesta e clicca su **OK**.
5. Clicca su **APRI** per aprire il tuo Vault.

Bitdefender informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizza il relativo messaggio per risolverlo.

Per aprire più rapidamente un Vault, individua sul computer il file .bvd che rappresenta il Vault che vuoi aprire. Clicca con il pulsante destro sul file, trova **Bitdefender** > **Bitdefender File Vault** e seleziona **Sblocca**. Digita la password richiesta e clicca su **OK**.

Aggiungere file ai Vault

Prima di poter aggiungere file o cartelle a un vault, devi aprire il vault.

Per aggiungere nuovi file al tuo Vault:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **CIFRATURA FILE**, clicca su **Impostazioni**.
3. Seleziona il Vault a cui vuoi aggiungere file e poi clicca su **SBLOCCA**.
4. Digita la password richiesta e clicca su **OK**.
5. Clicca su **APRI** per aprire il tuo Vault.
6. Aggiungi file o cartelle come faresti normalmente in Windows (per esempio, puoi utilizzare il classico metodo "copia e incolla").

Per aggiungere più rapidamente file al tuo Vault, clicca con il pulsante destro del mouse sul file o la cartella che vuoi copiare nel Vault, vai a **Bitdefender** > **Bitdefender File Vault** e seleziona **Aggiungi al File Vault**.

- Se solo un vault è aperto, il file o la cartella è copiata direttamente a quel vault.
- Se diversi vault sono aperti, verrà chiesto di scegliere il vault in cui copiare l'elemento. Seleziona dal menu la lettera dell'unità corrispondente al Vault desiderato e clicca su **OK** per copiare l'elemento.

Bloccare i Vault

Quando hai finito di lavorare in un Vault, dovrai bloccarlo per proteggere i tuoi dati. Bloccando la vault, l'unità disco virtuale corrispondente sparisce da Risorse del Computer. Di conseguenza l'accesso ai dati archiviati nel vault è completamente bloccato.

Per bloccare un Vault:

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

2. Nel pannello **CIFRATURA FILE**, clicca su **Impostazioni**.
3. Seleziona il Vault che vuoi bloccare e poi clicca su **BLOCCA**.

Bitdefender informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizza il relativo messaggio per risolverlo.

Per bloccare più rapidamente un vault, clicca con il pulsante destro del mouse sul file .bvd che rappresenta il Vault, vai a **Bitdefender** > **Bitdefender File Vault** e clicca su **Blocca**.

Rimuovere file dai Vault

Per rimuovere i file o cartelle da un vault, il vault deve essere aperto. Per rimuovere file o cartelle da un Vault:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **CIFRATURA FILE**, clicca su **Impostazioni**.
3. Seleziona il vault da cui vuoi rimuovere i file e clicca su **SBLOCCA** nel caso fosse bloccato.
4. Clicca su **APRI**.

   Rimuovi file o cartelle come si fa normalmente in Windows (ad esempio, clicca con il pulsante destro su un file che desideri eliminare e seleziona **Elimina**).

Cambiare la password del Vault

La password protegge il contenuto di un vault da accessi non autorizzati. Solo utenti che conoscono la password possono aprire il vault e accedere a documenti e dati in esso archiviati.

Il vault deve essere bloccato prima che si possa cambiare la sua password. Per cambiare la password di un Vault:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **CIFRATURA FILE**, clicca su **Impostazioni**.
3. Seleziona il Vault per cui vuoi modificare la password e clicca su **IMPOSTAZIONI**.
4. Digita la password corrente del vault nel campo **Vecchia password**.
5. Digita la nuova password del vault nei campi **Nuova password** e **Conferma nuova password**.

> **Nota**
> La password deve essere composta da almeno 8 caratteri. Per avere una password sicura, utilizza una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

Bitdefender informerà immediatamente sul risultato dell'operazione. Se si verifica un errore, utilizza il relativo messaggio per risolverlo.

Per cambiare più rapidamente la password di un vault, localizza sul computer il file .bvd che rappresenta il Vault. Clicca con il pulsante destro sul file, vai a **Bitdefender** > **Bitdefender File Vault** e seleziona **Modifica Password Vault**.

4.11. Protezione di Password Manager per le tue credenziali

Oggi utilizziamo il computer 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

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 **Crea nuovo Portafoglio**.
3. Clicca su **Crea nuovo**.
4. Digita le informazioni richieste nei campi corrispondenti.
   - Etichetta Portafoglio - Imposta un nome unico per il database del tuo Portafoglio.
   - Password principale - Inserisci una password per il tuo Portafoglio.
   - Ridigita la password - Ridigita la password impostata.
   - Suggerimento - Inserisci un suggerimento per ricordarti la password.
5. Clicca su **CONTINUA**.
6. In questa fase, puoi scegliere di archiviare i tuoi dati nel cloud. Selezionando Sì, le informazioni bancarie resteranno comunque memorizzate a livello locale sul tuo dispositivo. Scegli l'opzione desiderata e clicca su **CONTINUA**.
7. Seleziona il browser web da cui vuoi importare le credenziali.
8. Clicca su **FINE**.

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 **Crea nuovo Portafoglio**.
3. Clicca su **PERCORSO**.
4. Raggiungi la posizione sul tuo dispositivo in cui vuoi salvare il database del Portafoglio e poi scegli un nome da dargli.
5. Clicca su **Apri**.
6. Dai un nome al tuo Portafoglio e digita la password assegnata quando è stato creato.
7. Clicca su **IMPORTA**.
8. Seleziona i programmi per cui vuoi importare le credenziali nel Portafoglio e poi il pulsante **FINE**.

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 **I miei portafogli**.
3. Clicca sull'icona ⋮ nel Portafoglio desiderato e seleziona **Esporta**.
4. Cerca il percorso del tuo database del Portafoglio e selezionalo (il file .db).
5. 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.

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 **I miei portafogli**.
3. Clicca sull'icona ⋮ nel Portafoglio desiderato e seleziona **Impostazioni**.

4. 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.

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 **I miei portafogli**.
3. Seleziona il database del Portafoglio desiderato e clicca su **ATTIVA PORTAFOGLIO**.
4. Digita la password principale e clicca su **OK**.

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

- Identità
- Siti web
- Online banking
- E-mail
- App
- 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, selezionarla e fare clic sul pulsante **Modifica**.
- Per eliminare una voce, selezionala e clicca sul pulsante **Elimina**.

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.

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. Seleziona la scheda **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 computer, 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 scheda **Plugin**.

   Controlla se un'applicazione utilizza Password Manager e migliora 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. Seleziona la scheda **Imp. 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.

4.12. 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.

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.

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.

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 .

4.13. VPN

Puoi accedere alla app VPN dal tuo prodotto Bitdefender e usarla 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.

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**.

Interfaccia di VPN

L'interfaccia di VPN mostra lo stato della app, connessa o disconnessa. Qui avrai la possibilità di cambiare la posizione del server a cui vuoi connetterti.

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 avere più opzioni, accedi all'area **Menu**, cliccando sull'icona nel lato superiore 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.
- **Impostazioni** – In base alle tue necessità, puoi personalizzare il comportamento del tuo prodotto:
  - Ricevi notifiche quando VPN si connette o disconnette automaticamente
  - Esegui automaticamente la app VPN all'avvio di Windows
  - Lancia automaticamente la app VPN quando il dispositivo si connette a reti wireless non sicure
- **Supporto** - Sarai reindirizzato alla piattaforma del nostro Centro di supporto, da cui potrai leggere un articolo molto utile su come utilizzare Bitdefender VPN.
- **Info** - Vengono mostrate alcune informazioni sulla versione installata.

4.14. 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. 137).

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 computer 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™.

Utilizzare Bitdefender Safepay™

Di norma, Bitdefender rileva l'accesso a un sito di online banking o a un negozio online in qualsiasi browser del computer 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 **Apri 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.

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.

Gestione Plug-in
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 I CERTIFICATI** e segui la procedura guidata per utilizzare i certificati in Bitdefender Safepay™.

Usa tastiera virtuale

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

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

Conferma di stampa

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

Gestire i segnalibri

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

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

1. Clicca sull'icona ☆ accanto alla barra degli indirizzi 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.

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. Disattiva **Notifiche di Safepay**.

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. Attiva **Usa VPN con Safepay**.

4.15. Protezione dati

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 computer 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 conferma la tua volontà di continuare.

   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 **Privacy** nel menu di navigazione nell'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 file o cartelle che vuoi rimuovere in modo permanente.

      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.

4.16. Controllo Genitori

Bitdefender Parental Control ti consente di gestire e proteggere le attività online dei bambini. Una volta configurato Bitdefender Parental Control, puoi scoprire facilmente cosa stanno facendo i bambini sui dispositivi che usano e dove sono stati nelle ultime 24 ore. Inoltre, per aiutarti a sapere meglio cosa stanno facendo i bambini, la funzionalità ti fornisce alcune statistiche sulle sue attività e i suoi interessi.

Nel tuo abbonamento a Bitdefender hai incluso le seguenti funzionalità:

- Su dispositivi Windows, macOS e Android:
  - Bloccare pagine web inappropriate.
  - Bloccare app come giochi, chat, programmi di condivisione file o altri.
  - Bloccare l'uso del dispositivo monitorato.
  - Bloccare l'accesso a Internet durante specifici periodi di tempo (come durante le lezioni).
  - Impostare restrizioni temporali per l'uso dei dispositivi.
  - Vedi il tempo medio trascorso dai tuoi bambini su un dispositivo.

- Vedi un rapporto con le app usate sul dispositivo monitorato negli ultimi 30 giorni.
- Impostare zone vietate.
- Trovare la posizione del dispositivo Android del bambino.

- Sui dispositivi iOS:
  - Bloccare le chiamate in arrivo dall'elenco dei contatti.
  - Impostare zone vietate.
  - Trovare la posizione del dispositivo iOS del bambino.

Se vuoi accedere a maggiori funzionalità, puoi fare l'upgrade alla versione Bitdefender Parental Control Premium. Le funzionalità incluse nella versione Premium sono:

- Scoprire se il bambino è stato vittima di un comportamento predatorio.
- Scoprire se si sono verificati tentantivi di cyberbullismo da parte di compagni o estranei durantela sua presenza online.

Le funzionalità incluse nella versione Premium sono disponibili per dispositivi Windows, macOS, Android e iOS.

Per controllare le attività online dei bambini, gestire i dispositivi che i bambini possono usare o modificare le impostazioni di Parental Control, devi accedere al tuo account Bitdefender.

Ci sono due possibilità per accedere al tuo account Bitdefender, o tramite un browser web visitando https://central.bitdefender.com o dalla app Bitdefender Central, che può essere installata su 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.

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

4.16.1. Accedere Controllo genitori - I miei bambini

Una volta eseguito l'accesso alla sezione Controllo genitori, la finestra **I miei bambini** sarà disponibile. Qui puoi iniziare a creare profili per i bambini, che successivamente potrai rivedere e modificare. Una volta creati, i profili vengono mostrati come schede, consentendoti di gestirli rapidamente e verificare subito il proprio stato.

Non appena crei un profilo, puoi iniziare a personalizzare le impostazioni più dettagliate per monitorare e controllare l'accesso a Internet e a determinate applicazioni del bambino.

Puoi accedere alle impostazioni del Controllo genitori da Bitdefender Central su qualsiasi computer o dispositivo mobile connesso a Internet.

Accedi al tuo account Bitdefender:

- Da qualsiasi dispositivo con accesso a Internet:
  1. Accedi a Bitdefender Central.
  2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
  3. Seleziona il pannello **Controllo genitori**.
  4. Nella finestra **I miei bambini** che comparirà, potrai gestire e configurare i profili del Controllo genitori per ogni dispositivo.
- Dall'interfaccia di Bitdefender:
  1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
  2. Nel pannello **CONTROLLO GENITORI**, clicca su **Configura**.

     Sarai reindirizzato alla pagina web account Bitdefender. Assicurati di aver eseguito l'accesso con le tue credenziali.
  3. Seleziona la funzionalità **Controllo genitori**.
  4. Nella finestra **I miei bambini** che comparirà, potrai gestire e configurare i profili del Controllo genitori per ogni dispositivo.

> **Nota**
> Assicurati di aver avviato il computer con un account amministratore. Solo gli utenti con diritti di amministrazione (amministratori del sistema) possono accedere e configurare il Controllo genitori.

4.16.2. Creare profili per i bambini

Per iniziare a monitorare le attività dei bambini, devi configurare i profili e installare la app Parental Control di Bitdefender sui dispositivi che usano.

Per creare un profilo bambino:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello Controllo genitori.
3. Clicca su **CREA UN PROFILO DEL BAMBINO** nella finestra **I miei bambini**.
4. Imposta determinate informazioni, come nome, data di nascita o sesso. Per aggiungere un'immagine al profilo del tuo bambino, clicca sull'icona nell'angolo in basso a destra dell'opzione **Immagine del profilo**. Clicca su **SALVA** per continuare.

   In base agli standard di sviluppo, impostando la data di nascita del bambino, il programma carica automaticamente alcune impostazioni di ricerca del web considerate appropriate per quella categoria d'età.
5. Clicca su **AGGIUNGIAMO UN DISPOSITIVO**.
6. Se sul dispositivo del bambino è già stato installato un prodotto Bitdefender, seleziona il suo dispositivo nell'elenco disponibile e l'account che vuoi monitorare. Clicca su **ASSEGNA**.

   Se il bambino non ha alcun prodotto di Bitdefender installato sul dispositivo che utilizza, clicca su **Installa su un nuovo dispositivo** e 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 Bitdefender, controlla l'account e-mail che hai digitato e poi clicca sul pulsante di download corrispondente.

Importante

Sui dispositivi Windows e macOS che non hanno un prodotto di Bitdefender installato, sarà installato il Parental Control di Bitdefender che monitora i tracker, così potrai monitorare le attività online dei bambini.
Sui dispositivi Android e iOS, sarà scaricata e installata la app Parental Control di Bitdefender.

Per assegnare altri dispositivi, clicca sull'icona ⋮ nel profilo del bambino e scegli **Dispositivi**. Segui le istruzioni dal passaggio 6 fornite in questo capitolo.

Installare la app Bitdefender Parental Control su dispositivi Android e iOS

Per monitorare le attività online dei bambini sui dispositivi Android e iOS, devi installare la app Parental Control dedicata e collegare i loro dispositivi al tuo account Bitdefender. In base ai dispositivi usati dai bambini, segui questi passaggi:

- Su **Android**:

  1. Vai nel Google Play Store, cerca Bitdefender Parental Control e tocca l'opzione Installa.
  2. Tocca **ACCETTA** quando ti saranno chiesti i permessi. Bitdefender richiede i permessi per tenerti informato sulle attività del bambino. Se non vengono accettati, la app non sarà installata.
  3. Apri la app Controllo genitori.
  4. La prima volta che apri la app, viene visualizzata una procedura guidata di introduzione contenente maggiori dettagli sulle funzionalità del prodotto. Seleziona **AVANTI** per continuare con la guida, o **SALTA** per chiudere la procedura guidata.
  5. Per continuare l'installazione, Bitdefender richiede la tua approvazione per ottenere i dati personali che appartengono a tuo figlio, che saranno usati solo per fornirti informazioni sulle attività del bambino. Per maggiori dettagli, tocca **Informativa sulla privacy**. Toccando **CONTINUA** acconsenti alla raccolta dei dati personali dal dispositivo.
  6. Accedi al tuo account di Bitdefender esistente. Se non hai un account Bitdefender, puoi scegliere di crearne uno utilizzando l'opzione corrispondente. In alternativa, puoi accedere a un account Facebook, Google o Microsoft.
  7. Tocca **ATTIVA** per essere reindirizzato alla schermata da cui potrai attivare l'opzione Accessibilità per la app. Segui le istruzioni sullo schermo per configurare correttamente la app.

8. Tocca **CONSENTI** per essere reindirizzato alla schermata da cui potrai attivare l'opzione Attiva accesso utilizzo per la app. Segui le istruzioni sullo schermo per configurare correttamente la app.
9. Tocca **ATTIVA** per essere reindirizzato alla schermata da cui potrai attivare l'opzione Attiva diritti amministratore dispositivo per la app. Segui le istruzioni sullo schermo per configurare correttamente la app.

   Ciò impedirà al bambino di disinstallare la app Controllo genitori.
10. Assegna il dispositivo al profilo del bambino.

- Su **iOS**:

1. Vai in App Store, cerca cerca Bitdefender Parental Control e tocca l'opzione di installazione.
2. Per continuare l'installazione, Bitdefender richiede la tua approvazione per ottenere i dati personali che appartengono a tuo figlio, che saranno usati solo per fornirti informazioni sulle attività del bambino. Per maggiori dettagli, tocca **Informativa sulla privacy**. Toccando **Continua**, acconsenti alla raccolta dei dati personali del dispositivo.
3. Accedi al tuo account di Bitdefender esistente. Se non hai un account Bitdefender, puoi scegliere di crearne uno utilizzando l'opzione corrispondente. In alternativa, puoi accedere a un account Facebook, Google o Microsoft.
4. Ti sarà chiesto di concedere l'accesso a tutte le autorizzazioni richieste per la app. Tocca **Consenti**.
5. Consenti l'accesso alla posizione del dispositivo in modo che Bitdefender possa localizzarlo.
6. Consenti alla app di inviare delle notifiche. Per gestire le notifiche Bitdefender, vai in Impostazioni > Notifiche > Parental.
7. Per poter monitorare i contatti del bambino, devi attivare **Blocco chiamata & Identificazione**. Segui i passaggi necessari così potrai usare Bitdefender Parental Control per limitare le chiamate telefoniche in arrivo.
8. Assegna il dispositivo al profilo del bambino.

Monitorare le attività online dei bambini

Bitdefender Parental Control ti aiuta a monitorare ciò che i bambini fanno online. In questo modo, puoi sempre scoprire esattamente in quali attività siano stati coinvolti mentre usano i propri dispositivi.

In base alle impostazioni scelte, i rapporti di Bitdefender possono includere informazioni dettagliate su ogni evento, come:

- Lo stato dell'evento.
- L'intensità delle notifiche.
- Il nome del dispositivo.
- La data e l'ora in cui si è verificato l'evento.

Per monitorare il traffico Internet, le applicazioni utilizzate o le attività online del bambino:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello Controllo genitori.
3. Seleziona la scheda del dispositivo desiderato.

   Nella finestra **Attività**, puoi visualizzare le informazioni che ti interessano. In alternativa, seleziona il link **Vedi le attività odierne** nella scheda del dispositivo monitorato per essere reindirizzato alla finestra **Attività**.

> **Nota**
> La sezione Attività includerà solo dettagli da dispositivi Windows, macOS e Android.

Configurare le impostazioni dei rapporti

Di norma, quando il Parental Control è attivato, le attività dei bambini vengono registrate.

Per ricevere notifiche via e-mail sulle attività online dei bambini:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello Controllo genitori.
3. Seleziona la scheda **Impostazioni rapporti**.
4. Attiva l'opzione corrispondente per ricevere rapporti sulle attività.
5. Inserisci l'indirizzo e-mail in cui vuoi ricevere le notifiche e-mail.

6. Imposta la frequenza selezionando: settimanalmente o mensilmente, e poi clicca su **SALVA**.

Puoi anche scegliere di ricevere notifiche nel tuo account Bitdefender nelle seguenti situazioni:

- Ogni volta che i bambini cercano di accedere alle app bloccate (su Windows, macOS e Android).
- Ogni volta che i bambini ricevono chiamate da numeri di telefono bloccati/sconosciuti (su iOS).
- Ogni volta che i bambini lasciano le aree sicure o entrano in aree vietate.
- Ogni volta che i bambini segnalano di essere arrivati.

Modificare un profilo

Per modificare un profilo esistente:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **Controllo genitori**.
3. Clicca sull'icona ⋮ sulla scheda del profilo desiderato e seleziona **Modifica**.
4. Dopo aver personalizzato le impostazioni desiderate, seleziona **SALVA**.

Rimuovere un profilo

Per rimuovere un profilo esistente:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **Controllo genitori**.
3. Clicca sull'icona ⋮ sulla scheda del profilo desiderato e seleziona **Rimuovi**.
4. Conferma la tua scelta.

4.16.3. Configurare i profili del Controllo genitori

Per iniziare a monitorare i bambini, un profilo deve essere assegnato ai dispositivi su cui hanno installato la funzionalità o app Bitdefender Parental Control.

Dopo aver creato un profilo, puoi personalizzare più impostazioni dettagliate per monitorare e controllare l'accesso a Internet e a determinate applicazioni.

Per avviare la configurazione di un profilo, seleziona la scheda del profilo desiderato dalla finestra **Bambini**.

Clicca su una scheda per configurare la funzionalità corrispondente del Controllo genitori per il dispositivo:

- Attività - Qui puoi visualizzare tutte le attività, gli interessi, i luoghi e le interazioni con gli amici, dal giorno attuale.
- Applicazioni - Qui puoi bloccare l'accesso a determinate applicazioni, come giochi, programmi di chat, film, ecc.
- Siti web - Qui puoi filtrare filtrare la navigazione web.
- Contatti telefonici - Qui puoi indicare quali contatti nella rubrica dei bambini possono contattarli tramite il telefono.
- Posizione del bambino - Qui puoi impostare i luoghi che sono sicuri o vietati per i bambini.
- Social - Qui puoi visualizzare le attività dei bambini negli ultimi 30 giorni sulle piattaforme dei social network. Queste informazioni sono disponibili solo agli utenti che sono passati a Bitdefender Parental Control Premium.
- Tempo speso - Qui puoi bloccare l'accesso ai dispositivi indicati nei profili dei bambini. L'accesso può essere limitato sia per un certo intervallo di tempo che per limiti giornalieri cumulativi.
- Dispositivi - Qui puoi visualizzare lo stato dei dispositivi monitorati, assegnare un nuovo dispositivo al profilo del bambino o rimuovere un dispositivo associato.

Attività

La finestra delle Attività ti dà informazioni dettagliate sulle attività online dei bambini nelle ultime 24 ore, sia dentro che fuori casa. Per visualizzare le attività dei giorni precedenti, clicca sull'icona del calendario nell'angolo in alto a sinistra della finestra.

In base all'attività, la finestra potrebbe includere informazioni circa:

- **Luoghi** - Qui puoi visualizzare i luoghi in cui i bambini sono stati durante la giornata.

- **Interessi** - Qui puoi visualizzare informazioni sulle categorie dei siti web visitati dai bambini. Clicca sul link **Verifica contenuto inappropriato** per consentire o negare l'accesso a determinati interessi.
- **Interazioni sociali** - Qui puoi controllare i contatti con cui i bambini interagiscono. Clicca sul link **Gestisci i contatti** per selezionare i contatti con cui i bambini possono o meno interagire.
- **Applicazioni** - Qui puoi visualizzare le app usate dai bambini. Clicca sul link **Rivedi limitazioni app** per bloccare o consentire l'accesso a determinate applicazioni.
- **Attività quotidiane** - Qui puoi visualizzare il tempo trascorso online su tutti i dispositivi assegnati ai bambini, oltre ai luoghi in cui si sono recati. Le informazioni raccolte sono della giornata odierna.

Applicazioni

La finestra Applicazioni ti consente di bloccare l'esecuzione delle app su dispositivi Windows, macOS e Android. In questo modo è possibile bloccare giochi, altri media, programmi di chat e altre categorie di applicazioni.

Qui puoi anche visualizzare le app più usate in 30 giorni, oltre al tempo trascorso dai bambini con esse. Le informazioni sul tempo trascorso usando le app possono essere recuperate solo da dispositivi Windows, macOS e Android.

Per configurare il controllo applicazioni per un account utente specifico:

1. Viene mostrato un elenco con i dispositivi assegnati.

   Seleziona la scheda con il dispositivo in cui vuoi limitare l'accesso alle app.

2. Clicca su **Gestisci le app usate da...**

   Viene mostrato un elenco con le app installate.

3. Seleziona **Bloccato** accanto alle app di cui vuoi bloccare l'utilizzo da parte del bambino.

4. Clicca su **SALVA** per applicare le nuove impostazioni.

Puoi smettere di monitorare le app installate disattivando l'opzione **Monitora app usate** nell'angolo in alto a destra della finestra.

Siti web

La finestra Siti web ti aiuta a bloccare i siti web con contenuti inappropriati su dispositivi Windows, macOS e Android. In questo modo è possibile bloccare siti web che contengono video, giochi, altri media e programmi di chat, oltre ad altre categorie di contenuti negativi.

La funzionalità può essere attivata o disattivata utilizzando l'interruttore corrispondente.

In base all'età impostata per i bambini, di norma, l'elenco degli Interessi include una selezione di categorie attivate. Per consentire o negare l'accesso a una determinata categoria, cliccaci sopra.

L'icona  che comparirà indica che il bambino non potrà accedere ai contenuti di quella determinata categoria.

Consentire o bloccare un sito web

Per consentire o limitare l'accesso a determinate pagine web, devi aggiungerle all'elenco delle eccezioni, in questo modo:

1. Clicca sul pulsante **GESTISCI**.
2. Inserisci la pagina web che vuoi consentire o bloccare nel campo corrispondente.
3. Seleziona **Consenti** o **Blocca**.
4. Clicca su **FINISH** per salvare le modifiche.

Nota
Le restrizioni di accesso ai siti web possono essere impostate solo per dispositivi Windows, Android e macOS aggiunti al profilo del tuo bambino.

Contatti telefono

La finestra Contatti telefonici ti consente di specificare quali amici nella rubrica del bambino possano o non possano contattarlo tramite il telefono. Sui dispositivi iOS puoi bloccare le chiamate in arrivo, mentre sui dispositivi Android puoi visualizzare l'elenco dei contatti.

Per limitare le chiamate in arrivo da un determinato numero di telefono di un contatto, per iniziare devi aggiungere il dispositivo iOS del bambino a questo profilo:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **Controllo genitori**.
3. Clicca sull'icona ⋮ nel profilo del bambino e poi scegli **Dispositivi**.
4. Seleziona il dispositivo iOS che vuoi assegnare e clicca su **ASSEGNA**. Se il dispositivo iOS che vuoi assegnare la profilo del bambino non è disponibile nell'elenco, clicca su **Installa su un nuovo dispositivo** e 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 Bitdefender, controlla l'account e-mail che hai digitato e poi clicca sul pulsante di download corrispondente.
5. Seleziona la scheda **Contatti telefonici** in Bitdefender Central.

   Verrà mostrato un elenco di carte. Le tessere rappresentano i contatti dello smartphone Android del bambino.
6. Seleziona la carta con il numero di telefono che vuoi bloccare.

   L'icona ⊘ che compare indica che il bambino non potrà più essere raggiunto dal numero di telefono selezionato.

Nota
Non sarà bloccata alcuna chiamata in uscita, oltre agli SMS in arrivo e in uscita.

Posizione bambino

Scopri la posizione attuale del dispositivo su Google Maps. La posizione è aggiornata ogni 5 secondi, in modo da poterlo rintracciare, se è in movimento.

L'accuratezza della posizione dipende da come Bitdefender può rilevarla:

- Se nel dispositivo il GPS è attivato, la sua posizione può essere determinata con un'accuratezza di un paio di metri, finché resta nel raggio dei satelliti GPS (ad esempio, non dentro a un edificio).
- Se il dispositivo è in un edificio, la sua posizione può essere determinata entro decine di metri, se il Wi-Fi è attivato e ci sono reti wireless disponibili nel suo raggio d'azione.

- Diversamente, la posizione sarà determinata usando solo le informazioni dalla rete mobile, che offrono un'accuratezza non superiore a diverse centinaia di metri.

Configurare la posizione del controllo

Per essere sicuri che il bambino vada in determinati luoghi, puoi creare un elenco di luoghi sicuri e non. Ogni volta che accede da solo in una determinata area, una notifica comparirà nella app Controllo genitori chiedendo di confermare che va tutto bene. Toccando **SONO ARRIVATO SENZA PROBLEMI**, sarai informato tramite una notifica nel tuo account di Bitdefender che la destinazione finale è stata ricevuta.

Nel caso in cui non si ricevesse alcuna notifica da parte del bambino, è possibile visualizzare la sua posizione nel corso della giornata, consultando il suo profilo nel proprio account di Bitdefender.

Per configurare un luogo:

1. Clicca su **Dispositivi** nella sezione della finestra **Posizione bambino**.
2. Clicca su **SCEGLI DISPOSITIVI** e seleziona il dispositivo che vuoi configurare.
3. Nella finestra **Area**, clicca sul pulsante **AGGIUNGI AREA**.
4. Seleziona il tipo di luogo, **SICURO** o **VIETATO**.
5. Inserisci un nome valido per l'area dove il bambino ha il permesso di andare oppure no.
6. Imposta la distanza da applicare per il monitoraggio dal cursore scorrevole **Raggio**.
7. Clicca su **AGGIUNGI AREA** per salvare le tue impostazioni. Ti sarà chiesto se i bambini stanno viaggiando da soli oppure no. Conferma con Sì o No.

Nota
Il localizzatore può essere usato per monitorare i dispositivi Android e iOS su cui è stata installata la app Controllo genitori di Bitdefender.

Social - Cyberbullismo e predatori online

La finestra Social ti dà informazioni sulle attività online dei bambini negli ultimi 30 giorni sulle app dei social network, come WhatsApp, Facebook Messenger o Instagram. Per guidarti verso possibili trappole online in cui i

tuoi bambini potrebbero cadere, i tentativi di comportamenti di cyberbullismo e predazione vengono rilevati e mostrati in questa zona. Ciò è possibile grazie alle tecnologie di intelligenza artificiale che usiamo per rilevare i pericoli, come:

- Fotografie che contengono nudità.
- Messaggi di testo perfidi.
- Divulgazione di informazioni personali (indirizzo di casa, password, numeri di carta di credito, codici fiscali, ecc.).
- Richieste di incontro da estranei.

In particolare, Bitdefender Parental Control Premium analizza:

- Messaggi di testo inviati solo in inglese su WhatsApp (Android, Windows e macOS), Messenger Facebook (Windows e Mac) e Instagram (Android).
- Immagini inviate o ricevute in WhatsApp (Android, Windows e macOS), Messenger Facebook (Android, Windows e macOS) e Instagram (Android).
- Immagini inviati o ricevute da qualsiasi app (iOS).

Nota
I messaggi che analizziamo su WhatsApp provengono sia dalla app che dalla versione web da Google Chrome. Per poter analizzare i messaggi su WhatsApp Web da Google Chrome sui dispositivi Android, l'opzione Accessibilità deve essere attivata per Bitdefender Parental Control. Per attivare l'Accessibilità: vai in Impostazioni > Accessibilità > Parental Control.
I messaggi che analizziamo su Messenger Facebook provengono dalla app, da https://www.facebook.com/ e da https://www.messenger.com/ su Google Chrome, Mozilla Firefox e Microsoft Edge.

Importante
La scheda Social diventa disponibile solo agli utenti che hanno fatto l'upgrade alla versione Premium. Per fare l'upgrade a Bitdefender Parental Control Premium, fai riferimento a «*Abbonamenti a Bitdefender Parental Control*» (p. 168).

Per poter rilevare comportamenti di cyberbullismo e predazione, devi:

1. Creare un profilo bambino e assegnare i dispositivi al profilo del bambino, come descritto in «*Creare profili per i bambini*» (p. 156).
2. Consenti le autorizzazioni richieste durante l'installazione della app Bitdefender Parental Control su dispositivin Android e iOS.

3. Attiva l'opzione **Bullismo & Predatori**, come segue:
   a. Accedi a Bitdefender Central.
   b. Seleziona il pannello Controllo genitori.
   c. Clicca su **Impostazioni rapporti**.
   d. Attiva l'interruttore corrispondente.

Una volta configurate, le informazioni vengono raccolte automaticamente dai dispositivi Windows, macOS e iOS. Per consentire a Bitdefender di raccogliere informazioni dalle app Messenger Facebook e Instragram dai dispositivi Android, devi attivare alcune impostazioni, come segue:

- App Messenger Facebook:
  1. Tocca l'immagine del profilo
  2. Tocca **Fotografie & Media**.
  3. Attiva **Salva fotografie** e **Salva alla cattura**.
- App Instagram:
  1. Tocca l'immagine del profilo.
  2. Tocca **Fotografie & Media**.
  3. Tocca ⋯, e poi tocca **Fotografie originali**
  4. Attiva **Salva alla cattura**.
  5. Attiva **Salva fotografie originali** e **Salva fotografie postate**.

Tempo speso

In Tempo speso trovi informazioni sul tempo speso sui dispositivi assegnati nella giornata attuale, oltre a quanto tempo resta del limite giornaliero impostato, e lo stato del profilo selezionato, attivo o in pausa. Da questa finestra puoi anche impostare le limitazioni di tempo per diversi momenti della giornata, come l'ora di dormire, per i compiti o lezioni private.

Limitazioni temporali

Per iniziare a configurare le limitazioni:

1. Clicca su **Rivedi limitazioni temporali**.
2. Nell'area **Imposta limitazioni temporali**, clicca su **Aggiungi nuova limitazione**.

3. Dai un nome alla limitazione che vuoi impostare (per esempio, ora di dormire, compiti, lezioni di tennis, ecc.).
4. Imposta l'intervallo di tempo e i giorni in cui le limitazioni dovranno essere applicate e poi clicca su **AGGIUNGI** per salvare le impostazioni.

Per modificare una limitazione impostata, vai nella finestra Tempo speso, individua la limitazione che vuoi modificare e clicca sull'icona che vuoi modificare.

Per eliminare una limitazione, vai nella finestra Tempo speso, individua la limitazione che vuoi modificare e clicca sull'icona che vuoi modificare.

Limite giornaliero

Il limite giornaliero di utilizzo può essere applicato a dispositivi Windows, macOS e Android. Se hai impostato un profilo per entrare in pausa una volta raggiunto il limite, tale impostazione si applicherà a tutti i dispositivi assegnati, indipendentemente che abbiano Windows, macOS, Android o iOS.

Per impostare un limite giornaliero di utilizzo:

1. Clicca su **Rivedi limitazioni temporali**.
2. Nell'area **Imposta un limite per l'utilizzo giornaliero**, clicca su **Aggiungi un nuovo limite giornaliero**.
3. Imposta l'intervallo di tempo e i giorni in cui le limitazioni dovranno essere applicate e poi clicca su **SALVA** per salvare le impostazioni.

4.16.4. Abbonamenti a Bitdefender Parental Control

Oltre alle funzionalità di Parental Control incluse nel tuo abbonamento Bitdefender (Applicazioni, Siti web, Contatti telefonici, Posizione bambino, e Tempo speso), hai la possibilità di essere informato in tempo reale sulle minacce a cui i bambini sono esposti mentre usano i social network. Pertanto, puoi agire e iniziare a proteggere i bambini dall'essere molestati da compagni o estranei. Per ricevere informazioni sulle attività dei bambini mentre usano i social network, puoi fare l'upgrade alla versione Premium.

Per fare l'upgrade a Bitdefender Parental Control Premium:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **Controllo genitori**.
3. Clicca su **ALTRE INFO** nel banner in alto.

4. Clicca su **ACQUISTA PREMIUM**.

   Sarai reindirizzato al nostro sito web da cui potrai effettuare l'acquisizione.

L'abbonamento a Bitdefender Parental Control Premium è indipendente dall'abbonamento a Bitdefender Premium Security, il che significa che potrai usarlo per la sua intera disponibilità, indipendentemente dallo stato dell'abbonamento della soluzione di sicurezza. Nel caso in cui l'abbonamento a Bitdefender Parental Control Premium scadesse, ma quello per Bitdefender Premium Security fosse ancora attivo, avrai comunque accesso alle funzionalità del prodotto tranne il monitoraggio di cyberbulli e predatori online, che sono incluse nella funzionalità Social. Una volta fatto l'upgrade al piano Premium, potrai utilizzare il tuo abbonamento su tutti i dispositivi dei bambini, a patto di eseguire l'accesso allo stesso account Bitdefender.

Nota

Puoi fare l'upgrade a Bitdefender Parental Control Premium solo se ti trovi nei seguenti paesi: Stati Uniti, Canada, Regno Unito, Irlanda, Sud Africa, Australia o Nuova Zelanda. L'elenco sarà aggiornato presto con ulteriori paesi, non appena il prodotto sarà disponibile in nuove aree.

4.17. Funzione antifurto (Anti-Theft)

Il furto di un computer portatile è un problema molto serio sia per i privati che per le aziende. Più che la perdita dell'hardware in quanto tale, la perdita di dati può causare danni molto seri, sia a livello finanziario che personale.

Tuttavia, pochi prendono le giuste precauzioni per proteggere i propri dati personali, finanziari e aziendali in caso di furto o smarrimento.

Bitdefender Anti-Theft ti aiuta a essere più preparato a una tale possibilità, consentendoti di localizzare o bloccare il tuo portatile in remoto o persino cancellare tutti i suoi dati, qualora ti fosse stato sottratto contro la tua volontà.

Per utilizzare le funzioni Anti-Theft, occorre soddisfare i seguenti requisiti:

- I comandi possono essere inviati solo dall'account Bitdefender.
- Per ricevere i comandi il portatile deve essere connesso a Internet.

Le funzioni Anti-Theft operano in questo modo:

Trova

Visualizza la posizione del dispositivo su Google Maps.

L'accuratezza della posizione dipende da come Bitdefender può rilevarla. Se nel portatile è attivo il Wi-Fi e nel suo raggio d'azione ci sono reti wireless, la posizione viene determinata con una precisione di decine di metri.

Se il portatile è connesso a una rete LAN e non ci sono connessioni Wi-Fi disponibili, la posizione sarà determinata in base all'indirizzo IP, che è decisamente meno accurato.

Avviso

Invia un avviso in remoto al dispositivo.

La funzione è disponibile solo sui dispositivi mobile.

Blocca

Blocca il portatile e imposta un PIN di 4 cifre per sbloccarlo. Una volta inviato il comando **Blocco**, il portatile si riavvia e sarà possibile accedere a Windows solo dopo aver inserito il codice PIN stabilito.

Se vuoi che Bitdefender scatti delle fotografie a chiunque cerchi di accedere al tuo portatile, spunta la casella corrispondente. Le fotografie vengono scattate utilizzando la fotocamera frontale e mostrate insieme alla data nell'interfaccia di Anti-Theft. Verranno salvate solo le due foto più recenti.

Questa azione è disponibile solo per portatili dotati di una fotocamera frontale.

Cancella

Rimuovi tutti i dati dal sistema. Inviando il comando **Cancellazione**, il portatile si riavvia e i dati su tutte le partizioni del disco rigido vengono eliminati.

Mostra IP

Mostra l'ultimo indirizzo IP per il dispositivo selezionato. Clicca su **MOSTRA IP** per renderlo visibile.

Il servizio Anti-Theft viene attivato dopo l'installazione e può essere utilizzato ovunque da qualsiasi dispositivo connesso a Internet, ma solo attraverso il proprio account Bitdefender.

Usare le funzioni Antifurto

Per accedere alle caratteristiche di Anti-Theft, utilizza una delle seguenti possibilità:

- Dall'interfaccia principale di Bitdefender:
  1. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
  2. Clicca su **VAI A CENTRAL**.

     Sarai reindirizzato alla pagina di Bitdefender Central. Assicurati di aver eseguito l'accesso con le tue credenziali.
  3. Nella finestra di Bitdefender Central che si aprirà, clicca sulla scheda del dispositivo desiderato e seleziona **Anti-Theft**.
- Da qualsiasi dispositivo con accesso a Internet:
  1. Apri un browser web e vai a: https://central.bitdefender.com.
  2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
  3. Seleziona la scheda **I miei dispositivi**.
  4. Clicca sulla scheda del dispositivo desiderato e seleziona **Anti-Theft**.
  5. Seleziona la funzione che vuoi utilizzare:

     Mostra IP - Mostra l'ultimo indirizzo IP del tuo dispositivo.
     Localizza - Mostra la posizione del dispositivo su Google Maps.

     Avviso - Invia un avviso al dispositivo.

     Blocca - Blocca il portatile e imposta un PIN per sbloccarlo.

     Cancella - Elimina tutti i dati dal portatile.

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

4.18. Bitdefender USB Immunizer

La funzione di esecuzione automatica inclusa nei sistemi operativi Windows è uno strumento molto utile che consente ai computer 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 computer 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 computer con Windows.

Per immunizzare un dispositivo USB:

1. Collega l'unità flash al tuo computer.
2. Esegui una ricerca nel computer 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 computer 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. 117).

5. OTTIMIZZAZIONE SISTEMA

5.1. Utility

Bitdefender è dotato di una sezione Utilities, che ti aiuta a mantenere l'integrità del sistema. Gli strumenti di manutenzione offerti sono importanti per migliorare la reattività del sistema e la gestione efficace dello spazio sul disco rigido.

Bitdefender fornisce i seguenti strumenti di ottimizzazione del PC:

- L'Ottimizzatore immediato analizza e migliora la velocità del sistema eseguendo più attività con un semplice clic su un pulsante.
- L'Ottimizzatore avvio riduce il tempo di avvio del sistema bloccando l'esecuzione di applicazioni non necessarie quando il PC viene riavviato.
- Pulizia disco identifica i file che potrebbero essere responsabili del poco spazio sul disco, dandoti la possibilità di decidere se mantenerli oppure no.

5.1.1. Ottimizzare la velocità del sistema con un semplice clic

Problemi come guasti al disco rigido, file di registro rimasti e cronologia del browser, possono rallentare il funzionamento del computer, diventando fastidiosi. Ora tutti questi problemi possono essere risolti con un semplice clic su un pulsante.

L'Ottimizzatore immediato ti consente d'identificare e rimuovere i file inutili eseguendo più attività di pulizia contemporaneamente.

Per avviare l'Ottimizzatore immediato:

1. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Clicca su **OTTIMIZZA IL MIO DISPOSITIVO**.
   a. **Analisi in corso**

      Attendi che Bitdefender termini la ricerca dei problemi al sistema.

      - Pulizia disco - Identifica le cartelle e i file non necessari.
      - Pulizia registro - Identifica le referenze non valide o aggiornate nel registro di Windows.

- Pulizia privacy - Identifica i file temporanei di Internet e i cookie, la cache del browser e la cronologia.

Viene visualizzato il numero di problemi rilevati. Clicca sul link **Mostra dettagli** per rivederli prima di procedere con il processo di pulizia. Clicca su **OTTIMIZZA** per continuare.

b. **Ottimizzare**

Attendi che Bitdefender termini l'ottimizzazione del sistema.

c. **Problemi**

Qui puoi visualizzare il risultato dell'operazione.

Se desideri avere ulteriori informazioni sul processo di ottimizzazione, clicca sul pulsante **GUARDA RAPPORTO DETTAGLIATO**.

5.1.2. Ottimizzare il tempo di avvio del PC

Un tempo di avvio del sistema troppo lungo, spesso indica la presenza di alcune applicazioni non necessarie che si avviano automaticamente. Attendere diversi minuti per l'avvio di un sistema può costare molto in termini di tempo e produttività.

La finestra dell'Ottimizzatore avvio mostra quali applicazioni vengono eseguite durante l'avvio del sistema, consentendoti di gestire il loro comportamento in tale fase.

Per avviare l'Ottimizzatore avvio:

1. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Clicca su **OTTIMIZZA AVVIO DISPOSITIVO**.

a. **Seleziona le applicazioni**

Puoi vedere un elenco di applicazioni che vengono eseguite all'avvio del sistema. Seleziona quelle che vuoi disattivare o almeno togliere dall'avvio.

b. **Scelta della community**

Visualizza ciò che gli altri utenti di Bitdefender hanno deciso di fare con l'applicazione che hai selezionato.

c. **Tempo di avvio del sistema**

Controlla il cursore scorrevole nella parte superiore della finestra per visualizzare il tempo richiesto dal tuo sistema e dalle applicazioni selezionate per essere eseguite all'avvio.

Per recuperare le informazioni sul tempo di avvio del sistema e delle applicazioni è necessario riavviare.

d. **Stato dell'avvio**

- **Attiva.** Seleziona questa opzione quando desideri che un'applicazione venga eseguita all'avvio del sistema. Di norma, questa opzione è attivata.
- **Ritarda.** Seleziona questa opzione per ritardare un programma e non eseguirlo all'avvio del sistema. Ciò significa che le applicazioni selezionate inizieranno con un ritardo di cinque minuti dopo l'accesso dell'utente nel sistema. La funzione **Ritarda** è predefinita e non può essere configurata dall'utente.
- **Disattiva.** Seleziona questa opzione per disattivare un programma e non eseguirlo all'avvio del sistema.

e. **Risultati**

Vengono mostrate alcune informazioni, come il tempo di avvio stimato dopo aver disattivato o ritardato i programmi.

Per visualizzare tutte le informazioni, potrebbe essere necessario riavviare il sistema.

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

Nota
Nel caso l'abbonamento scadesse o se decidessi di disinstallare Bitdefender, i programmi che hai tolto dall'esecuzione automatica all'avvio saranno ripristinati alle loro impostazioni originali.

5.1.3. Ottimizzare il tuo disco

Le cartelle e i file non più necessari che consumano spazio sul tuo disco potrebbero causare rallentamenti al sistema. Inoltre, si consiglia di migliorare la velocità del sistema, pulendolo a intervalli regolari.

Pulizia disco di Bitdefender ti aiuta a ottimizzare lo spazio sul disco con facilità, identificando i file che potrebbero essere responsabili del poco spazio libero. Inoltre, hai la possibilità di decidere cosa fare con i file individuati.

Per iniziare a pulire il tuo sistema:

1. Clicca su **Utilities** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Clicca su **LIBERA IL MIO DISPOSITIVO**.
3. La prima volta che accedi a Pulizia disco, ti sarà presentata questa funzionalità. Clicca su **OK, HO CAPITO** per continuare.
   a. **Unità e dispositivi**

      Puoi vedere un elenco dei dischi disponibili. Oltre a quelli utilizzati da Windows, nell'elenco vengono esaminati e mostrati anche dischi rigidi esterni e unità USB. Clicca su **ANALIZZA UNITÀ** nell'area del disco che vuoi pulire.

   b. **Analisi unità**

      L'unità selezionata viene analizzata. Attendi che Bitdefender termini la ricerca di cartelle e grandi file.

   c. **Problemi**

      Qui è dove puoi visualizzare i risultati dell'operazione. Per selezionare in quale ordine devono essere mostrati i risultati, usa la freccia a cascata **ORDINA PER** nel lato sinistro della finestra. Puoi ordinare i risultati in base alla dimensione (da 10 MB a oltre 5 GB) o al tipo (i file vengono ordinati in cartelle separate in base alle proprie estensioni).

      Seleziona i file che vuoi eliminare e clicca su **CONFERMA LA SELEZIONE** per avviare il processo di eliminazione.

      Anche i file protetti e importanti, responsabili per il funzionamento del tuo sistema, vengono identificati ma non è possibile selezionarli o eliminarli.

      Clicca sull'icona per accedere alle cartelle che appartengono ai file selezionati.

   d. **Conferma la tua selezione**

      Viene mostrato l'elenco con i file selezionati. Controlla nuovamente e assicurati di non aver davvero più bisogno di questi file, in quanto non appena proseguirai, non potrai più recuperarli dal Cestino. Conferma la tua scelta cliccando su **ELIMINA**.

   e. **Riepilogo risultati**

      Viene mostrato lo stato del processo, come segue:

Tutti i file selezionati vengono eliminati.
Uno o più dei file selezionati potrebbero non essere eliminati **o** nessuno dei file selezionati potrebbe essere eliminato.

Clicca su **FINE** per chiudere la finestra.

5.2. 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 Total Security viene impostato automaticamente per applicare le seguenti impostazioni del programma:

- Advanced Threat Defense è attivato
- Il Firewall di Bitdefender è stato attivato e al tuo adattatore wireless verranno applicate le seguenti impostazioni:
  - Modalità invisibile - ATTIVATA
  - Tipo di rete - Pubblica
- Vengono attivate le seguenti impostazioni della Prevenzione minacce online:
  - Scansione web cifrata
  - Protezione dalle frodi
  - Protezione da phishing

5.2.1. 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 **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Profili**.
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 **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Profili**.
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.

5.2.2. 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 **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Profili**.
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 **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Profili**.
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.

5.2.3. 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 **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Profili**.
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 **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Profili**.
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.

5.2.4. 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 **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Profili**.
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**.

5.2.5. 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 **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Profili**.

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.
- Il Widget sicurezza è disattivato.

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.

5.2.6. 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 **Impostazioni** nel menu di navigazione dell'interfaccia di Bitdefender.

2. Seleziona la scheda **Profili**.
3. Scorri verso il basso finché non trovi l'opzione dell'ottimizzazione in tempo reale e usa l'interruttore corrispondente per attivarla o disattivarla.

6. RISOLUZIONE DEI PROBLEMI

6.1. 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. 185)
- «*La scansione non parte*» (p. 187)
- «*Non posso più usare una app*» (p. 189)
- «*Che cosa fare quando Bitdefender blocca un sito web, un dominio, un indirizzo IP o una app online che sono sicuri*» (p. 190)
- «*Cosa fare se Bitdefender rilevasse un'applicazione sicura come ransomware*» (p. 190)
- «*Come aggiornare Bitdefender con una connessione a Internet lenta*» (p. 195)
- «*I servizi Bitdefender non rispondono*» (p. 195)
- «*Il filtro antispam non funziona correttamente*» (p. 196)
- «*L'opzione Compila automaticamente nel mio Portafoglio non funziona*» (p. 201)
- «*Rimozione di Bitdefender non riuscita*» (p. 202)
- «*Il sistema non si riavvia dopo aver installato Bitdefender*» (p. 203)

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. 320).

6.1.1. Il mio sistema sembra lento

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

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

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

Sebbene Bitdefender cerchi e rimuova i programmi di sicurezza trovati durante l'installazione, si consiglia di rimuovere ogni altra soluzione di sicurezza in uso prima dell'installazione di Bitdefender. Per maggiori informazioni, fai riferimento a «*Come posso rimuovere le altre soluzioni di sicurezza?*» (p. 72).

- **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. 2).

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

  Qualsiasi computer ha programmi o app che non si usano. 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 computer. 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 **Scansione sistema**.
  3. Segui i passaggi della procedura guidata.

6.1.2. La scansione non parte

Questo tipo di problema può avere due cause principali:

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

  In questo caso, reinstalla Bitdefender:

  - In **Windows 7**:
    1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
    2. Trova **Bitdefender Total Security** 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 Total Security** 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 Total Security** 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. 72).
  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 Total Security** 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 Total Security** 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 Total Security** 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. 320).

6.1.3. Non posso più usare una app

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

Dopo aver installato Bitdefender potrebbe verificarsi una di queste situazioni:

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

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

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

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

Per aggiungere il programma all'elenco delle eccezioni:

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

3. Nell'area **Eccezioni**, clicca su **Aggiungi applicazioni alle eccezioni**.
4. Trova e seleziona l'applicazione che vuoi escludere, e clicca su **OK**.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 320).

6.1.4. 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 **Eccezioni**.
3. Inserisci l'indirizzo del sito web bloccato, il nome del dominio, l'indirizzo IP o l'applicazione online nel campo corrispondente e clicca su **AGGIUNGI**.
4. 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. 320).

6.1.5. Cosa fare se Bitdefender rilevasse un'applicazione sicura come ransomware

Un Ransomware è un programma dannoso che cerca di sottrarre denaro agli utenti, bloccando i loro sistemi vulnerabili. Per mantenere sempre sicuro il

sistema da ogni situazione spiacevole, Bitdefender ti dà la possibilità di proteggere i file personali.

Quando un'applicazione cerca di cambiare o eliminare uno dei tuoi file protetti, verrà considerata pericolosa e Bitdefender ne bloccherà il funzionamento.

Nel caso in cui una tale app venga aggiunta all'elenco delle app non affidabili, ma si ha la certezza che sia sicura, segui questi passaggi:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **SAFE FILES**, clicca su **Accesso applicazioni**.
3. Verranno elencate le app che hanno richiesto di modificare i file nelle tue cartelle protette. Clicca sull'interruttore **Consenti** accanto alla app che ritieni sicura.

6.1.6. Non riesco a connettermi a Internet

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

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

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **FIREWALL**, clicca su **Impostazioni**.
3. Nella finestra **Regole**, clicca su **Aggiungi regola**.
4. Apparirà una nuova finestra, dove potrai aggiungere i dettagli. Assicurati di selezionare tutti i tipi di rete disponibili e nella sezione **Autorizzazione** seleziona **Consenti**.

Chiudi Bitdefender, apri l'applicazione e riprova a connetterti a Internet.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 320).

6.1.7. Non riesco ad accedere a un dispositivo nella mia rete

In base alla rete a cui sei connesso, il firewall di Bitdefender potrebbe bloccare la connessione tra il sistema e un altro dispositivo (come un altro computer o stampante). Di conseguenza, non potresti più condividere o stampare file.

In questo caso, la migliore soluzione è configurare Bitdefender per consentire automaticamente le connessioni da e per il rispettivo dispositivo, come segue:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **FIREWALL**, clicca su **Impostazioni**.
3. Nella finestra **Regole**, clicca su **Aggiungi regola**.
4. Nella finestra **Impostazioni**, attiva l'opzione **Applica questa regola a tutte le applicazioni**.
5. Clicca sulla scheda **Avanzate**.
6. Nella casella **Indirizzo remoto personale**, digita l'indirizzo IP del computer o della stampante a cui vuoi accedere senza restrizioni.

Se non riesci ancora a collegarti al dispositivo, il problema potrebbe non essere causato da Bitdefender.

Controllare altre potenziali cause, ad esempio le seguenti:

- Il firewall su un altro computer potrebbe bloccare la condivisione di file e stampante con il tuo computer.
  - Se viene utilizzato il firewall di Windows, è possibile configurarlo per permettere la condivisione di file e stampanti nel modo seguente:
    - In **Windows 7**:
      1. Clicca su **Start**, vai al **Pannello di controllo** e seleziona **Sistema e sicurezza**.
      2. Vai a **Windows Firewall** e clicca su **Consenti un programma con Windows Firewall**.
      3. Seleziona la casella **Condivisione file e stampanti**.
    - In **Windows 8 e Windows 8.1**:

1. 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 **Sistema e sicurezza**, vai a **Windows Firewall** e seleziona **Consenti una app con Windows Firewall**.
3. Seleziona la casella **Condivisione file e stampanti** e clicca su **OK**.

- In **Windows 10**:
  1. Digita "Consenti app attraverso Windows Firewall" nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona.
  2. Clicca su **Cambia impostazioni**.
  3. Nell'elenco **App e funzionalità consentite**, metti la spunta a **Condivisione file e stampanti** e clicca su **OK**.
- Se viene utilizzato un altro programma firewall, fai riferimento alla sua documentazione o al file della guida.

- Condizioni generiche che possono impedire l'utilizzo o la connessione a una stampante condivisa:
  - Potrebbe essere necessario accedere a un account di amministratore di Windows per poter accedere alla stampante condivisa.
  - Potrebbero essere state impostate delle autorizzazioni per la stampante condivisa che permettono l'accesso solo a specifici computer e utenti. Se stai condividendo la tua stampante, controlla le autorizzazioni impostate per la stampante per verificare che l'utente dell'altro computer sia autorizzato ad accedervi. Se stai provando a collegarti a una stampante condivisa, controlla insieme all'utente dell'altro computer di disporre delle autorizzazioni al collegamento alla stampante.
  - La stampante collegata al proprio computer o all'altro computer non è condivisa.
  - La stampante condivisa non è stata aggiunta al computer.

> **Nota**
> Per apprendere come gestire la condivisione di stampanti (condividere una stampante, impostare o rimuovere autorizzazioni per una stampante, collegarsi a una stampante di rete o a una stampante condivisa) vai alla Guida in Linea e Supporto Tecnico di Windows (nel menu Start, clicca su **Guida in Linea e Supporto Tecnico**).

- L'accesso a una stampante di rete potrebbe essere ristretto a specifici computer o utenti. Controlla con l'amministratore della rete, se disponi delle autorizzazioni al collegamento con tale stampante.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 320).

6.1.8. Internet è lento

Questa situazione potrebbe verificarsi dopo aver installato Bitdefender. Il problema potrebbe essere causato da errori nella configurazione del firewall di Bitdefender.

Per risolvere questa situazione:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **FIREWALL**, disattiva l'interruttore per disattivare la funzionalità.
3. Verifica se la tua connessione a Internet è migliorata con il firewall di Bitdefender disattivato.
   - Se hai ancora una connessione a Internet lenta, il problema potrebbe non essere causato da Bitdefender. Contatta il tuo fornitore di servizi Internet per verificare se la connessione è attiva.

     Se ricevi conferma dal tuo fornitore di servizi Internet che la connessione è operativa e il problema persiste, contatta Bitdefender come descritto nella sezione «*Chiedere aiuto*» (p. 320).
   - Se la connessione a Internet è migliorata dopo aver disattivato il firewall di Bitdefender:
     a. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
     b. Nel pannello **FIREWALL**, clicca su **Impostazioni**.
     c. Vai alla scheda **Adattatori di rete** e imposta la tua connessione a Internet come **Casa/Ufficio**.
     d. Nella scheda **Impostazioni**, disattiva **Protezione da port scan**.

        Nell'area **Modalità invisibile**, clicca su **Modifica impostazioni furtive**. Attiva la modalità invisibile per l'adattatore di rete a cui sei connesso.

e. Chiudi Bitdefender, riavvia il sistema e verifica la velocità della connessione a Internet.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 320).

6.1.9. 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.

6.1.10. 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 computer 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 computer e aspettare alcuni attimi fino a quando Bitdefender è caricato. Aprire Bitdefender per vedere se l'errore persiste. Riavviare il computer 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. 72).

Se l'errore persiste, contatta i nostri operatori del supporto tecnico per ricevere assistenza, come indicato nella sezione «*Chiedere aiuto*» (p. 320).

6.1.11. Il filtro antispam non funziona correttamente

Questo articolo permette di risolvere i seguenti problemi delle operazioni di filtro Antispam di Bitdefender:

- Un numero di messaggi e-mail legittimi sono contrassegnati come [spam].
- Molti messaggi spam non sono contrassegnati come tali dal filtro antispam.
- Il filtro antispam non rileva nessun messaggio spam.

I messaggi legittimi sono contrassegnati come [spam]

I messaggi legittimi vengono contrassegnati come [spam] semplicemente perché appaiono come tali al filtro antispam di Bitdefender. Normalmente puoi risolvere questo problema configurando adeguatamente il filtro antispam.

Bitdefender aggiunge automaticamente i destinatari dei messaggi e-mail inviati all'elenco Amici. I messaggi e-mail ricevuti dai contatti nell'elenco degli Amici sono considerati legittimi. Non vengono verificati dal filtro antispam e di conseguenza non vengono mai contrassegnati come [spam].

La configurazione automatica dell'elenco Amici non impedisce gli errori di rilevamento che possono accadere in queste situazioni:

- Si ricevono molte e-mail commerciali richieste come risultato della sottoscrizione a vari siti web. In questo caso la soluzione è di aggiungere gli indirizzi e-mail da cui ricevi tali messaggi all'elenco amici.
- Una parte significativa delle tue e-mail legittime proviene da individui a cui non hai mai inviato e-mail in precedenza, ad esempio clienti, potenziali partner d'affari o altri. In questo caso sono richieste altre soluzioni.

  Se stai utilizzando uno dei programmi di posta elettronica con cui Bitdefender si integra, indica gli errori di rilevazione.

  Nota
  Bitdefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo. Per un elenco completo delle applicazioni di posta supportate, fai riferimento a «*Programmi e protocolli di posta elettronica supportati*» (p. 103).

Aggiungi contatti all'elenco Amici

Se stai utilizzando un'applicazione di posta supportata, puoi facilmente aggiungere i mittenti dei messaggi legittimi all'elenco amici. Segui questi passaggi:

1. Nell'applicazione di posta seleziona un messaggio e-mail inviato dal mittente che desideri aggiungere all'elenco Amici.
2. Clicca sul pulsante **Aggiungi Amico** sulla barra degli strumenti antispam di Bitdefender.
3. Può essere richiesto di accettare gli indirizzi aggiunti all'elenco Amici. Seleziona **Non mostrare di nuovo questo messaggio** e clicca su **OK**.

Riceverai sempre e-mail provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

Se utilizzi un'applicazione di posta differente, puoi aggiungere i contatti all'elenco Amici dall'interfaccia di Bitdefender. Segui questi passaggi:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTISPAM**, clicca su **Gestisci amici**.

   Apparirà una finestra di configurazione.

3. Digita l'indirizzo e-mail da cui vuoi sempre ricevere i messaggi e clicca su **AGGIUNGI**. Puoi aggiungere quanti indirizzi e-mail desideri.
4. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

Indica errori di rilevamento

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

1. Apri il tuo client e-mail.
2. Vai alla cartella posta indesiderata, dove vengono spostati i messaggi spam.
3. Seleziona il messaggio legittimo scorrettamente contrassegnato come [spam] da Bitdefender.
4. Clicca sul pulsante **Aggiungi amico** sulla barra degli strumenti antispam di Bitdefender per aggiungere il mittente all'elenco Amici. Può essere necessario premere **OK** per confermare. Riceverai sempre e-mail provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.
5. Clicca sul pulsante **Non è Spam** sulla barra degli strumenti antispam di Bitdefender (in genere localizzata nella parte superiore della finestra del client di posta). L'e-mail sarà spostata nella cartella Posta in arrivo.

Molti messaggi spam non vengono rilevati

Se ricevi molti messaggi spam che non vengono contrassegnati come [spam], devi configurare il filtro antispam di Bitdefender in modo da migliorarne l'efficienza.

Prova le seguenti soluzioni:

1. Se stai utilizzando uno dei programmi di posta elettronica con cui Bitdefender si integra, indica i messaggi spam non rilevati.

> **Nota**
>
> Bitdefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo. Per un elenco completo delle applicazioni di

posta supportate, fai riferimento a «*Programmi e protocolli di posta elettronica supportati*» (p. 103).

2. Aggiungi spammer all'elenco Spammer. I messaggi e-mail ricevuti dagli indirizzi nell'elenco Spammer sono contrassegnati automaticamente come [spam].

Indica messaggi spam non rilevati

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

1. Apri il tuo client e-mail.
2. Vai alla cartella Posta in arrivo.
3. Seleziona i messaggi di spam non rilevati.
4. Clicca sul pulsante **È Spam** sulla barra degli strumenti antispam di Bitdefender (in genere localizzata nella parte superiore della finestra del client di posta). Vengono immediatamente contrassegnati come [spam] e verranno spostati alla cartella posta indesiderata.

Aggiungi spammer a elenco Spammer

Se stai utilizzando un'applicazione di posta supportata, puoi facilmente aggiungere i mittenti dei messaggi di spam all'elenco Spammer. Segui questi passaggi:

1. Apri il tuo client e-mail.
2. Vai alla cartella posta indesiderata, dove vengono spostati i messaggi spam.
3. Seleziona i messaggi contrassegnati come [spam] da Bitdefender.
4. Clicca sul pulsante **Aggiungi Spammer** sulla barra degli strumenti antispam di Bitdefender.
5. Può essere richiesto di accettare gli indirizzi aggiunti all'elenco degli Spammer. Seleziona **Non mostrare di nuovo questo messaggio** e clicca su **OK**.

Se utilizzi un client di posta diverso, puoi aggiungere manualmente nuovi contatti all'elenco Spammer dall'interfaccia di Bitdefender. Si tratta di un

metodo conveniente solo quando si ricevono diversi messaggi spam dallo stesso indirizzo e-mail. Segui questi passaggi:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTISPAM**, clicca su **Gestisci spammer**.

   Apparirà una finestra di configurazione.
3. Digita l'indirizzo e-mail dello spammer e poi clicca su **AGGIUNGI**. Puoi aggiungere quanti indirizzi e-mail desideri.
4. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

Il Filtro antispam non rileva alcun messaggio spam

Se nessun messaggio spam viene contrassegnato come [spam], potrebbe esserci un problema relativo al filtro antispam di Bitdefender. Prima di risolvere questo problema, assicurati che non sia causato da una delle seguenti condizioni:

- La protezione antispam potrebbe essere disattivata. Per verificare lo stato della protezione antispam, clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender. Guarda nel pannello **Antispam** per controllare se la funzionalità è attivata.

  Se l'antispam è disattivato, questa è la causa dei problemi. Clicca sull'interruttore corrispondente per attivare la protezione antispam.
- La protezione antispam di Bitdefender è disponibile solo per client e-mail configurati per ricevere messaggi e-mail tramite il protocollo POP3. Questo vuol dire che:
  - I messaggi e-mail ricevuti tramite servizi e-mail web (ad esempio Yahoo, Gmail, Hotmail o altri) non sono filtrati per spam da Bitdefender.
  - Se il tuo client e-mail è configurato per ricevere messaggi e-mail usando un protocollo diverso da POP3 (per esempio, IMAP4), il filtro antispam di Bitdefender non verifica se siano spam.

  Nota

  POP3 è uno dei protocolli più usati per scaricare messaggi e-mail da un server di posta. Se non si conosce il protocollo usato dal proprio client e-mail per scaricare messaggi e-mail, chiedere alla persona che ha configurato il proprio client e-mail.

- Bitdefender Total Security non esegue la scansione del traffico POP3 di Lotus Notes.

Una possibile soluzione consiste nel riparare o reinstallare il prodotto. Tuttavia puoi contattare Bitdefender per ricevere supporto, come descritto nella sezione «*Chiedere aiuto*» (p. 320).

6.1.12. 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 su Strumenti.
  3. Clicca su Add-on.
  4. Clicca su Estensioni.
  5. Seleziona **Portafoglio di Bitdefender** e clicca su **Attiva**.
- In **Google Chrome:**
  1. Apri Google Chrome.
  2. Vai all'icona del menu.
  3. Clicca su Altri strumenti.
  4. Clicca su Estensioni.

5. Seleziona **Portafoglio di Bitdefender** e clicca su **Attiva**.

> **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. 320).

6.1.13. 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 Total Security** 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 Total Security** 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 Total Security** 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.

6.1.14. 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. 74).
  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 Total Security** 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 Total Security** 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 Total Security** 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. 74).
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. 74).
2. Usa l'opzione Ripristino configurazione di sistema di Windows per ripristinare il computer 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. 320).

6.2. Rimuovere le minacce dal sistema

Le minacce possono influenzare il sistema in molti modi diversi e l'approccio di Bitdefender dipende dal tipo di attacco della minaccia. Poiché le minacce modificano spesso il loro comportamento, è difficile stabilire uno schema per il loro comportamento e le loro azioni.

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

- «*Bitdefender Modalità di soccorso (Ambiente di soccorso in Windows 10)*» (p. 207)
- «*Cosa fare quando Bitdefender trova delle minacce sul computer?*» (p. 210)
- «*Come posso rimuovere una minaccia in un archivio?*» (p. 211)
- «*Come posso rimuovere una minaccia in un archivio di e-mail?*» (p. 213)
- «*Cosa fare se sospetti che un file possa essere pericoloso?*» (p. 214)
- «*Quali sono i file protetti da password nel registro della scansione?*» (p. 214)
- «*Quali sono gli elementi ignorati nel registro della scansione?*» (p. 214)
- «*Quali sono i file supercompressi nel registro della scansione?*» (p. 215)
- «*Perché Bitdefender ha eliminato automaticamente un file infetto?*» (p. 215)

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. 320).

6.2.1. Bitdefender Modalità di soccorso (Ambiente di soccorso in Windows 10)

La **Modalità soccorso** è una funzione di Bitdefender che ti consente di controllare e disinfettare tutte le partizioni del disco esistenti, interne ed esterne al tuo sistema operativo.

Una volta installato Bitdefender Total Security s **Windows 7, Windows 8 e Windows 8.1** e scaricato il file dell'immagine della modalità Soccorso di Bitdefender, la modalità Soccorso può essere utilizzata anche se non sei più in grado di avviare Windows.

In Windows 10, l'ambiente di Soccorso di Bitdefender è integrato con Windows RE, il che significa che non sarà necessario scaricare alcuna immagine della modalità Soccorso in questo sistema operativo.

Scaricare l'immagine della modalità di Soccorso di Bitdefender

Per poter utilizzare la modalità Soccorso in **Windows 7, Windows 8 e Windows 8.1**, per iniziare devi scaricare il file della sua immagine, come segue:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Modalità Soccorso**.
3. Clicca su **Sì** nella finestra di conferma che compare per riavviare il computer.

   Attendi che il file dell'immagine della modalità Soccorso di Bitdefender sia stato scaricato dai server di Bitdefender. Non appena termina il processo di download, il computer sarà riavviato.

   Comparirà un menu per avvisarti di selezionare un sistema operativo. In questo passaggio, puoi scegliere di avviare il tuo sistema in modalità soccorso o normale.

> **Nota**
> A causa dell'integrazione con l'ambiente di ripristino di Windows in **Windows 10**, non è necessario scaricare alcuna immagine della modalità di soccorso su questo sistema operativo.

Avviare il sistema in modalità soccorso in Windows 7, Windows 8 e Windows 8.1

Puoi accedere alla Modalità soccorso in uno dei due modi:

Dall'interfaccia di Bitdefender

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Nel pannello **ANTIVIRUS**, clicca su **Modalità Soccorso**.
3. Clicca su **Sì** nella finestra di conferma che compare per riavviare il computer.
4. Dopo il riavvio del computer, compare un menu che ti avvisa di selezionare un sistema operativo. Seleziona **Modalità soccorso di Bitdefender** per avviare un ambiente di Bitdefender da cui poter pulire la tua partizione Windows.
5. Se richiesto, premi **Invio** e seleziona la risoluzione dello schermo più vicina a quella che usi normalmente. Poi premi di nuovo **Invio**.

   La modalità soccorso di Bitdefender sarà pronta tra pochi istanti.

Avvia il computer direttamente in Modalità soccorso

Se Windows non parte più, puoi avviare il tuo computer direttamente nella Modalità soccorso di Bitdefender seguendo i passaggi sottostanti:

- In **Windows 7**:
  1. Premi il tasto **F8** finché non compaiono sullo schermo le **Opzioni avanzate di avvio**.
  2. Usa i tasti freccia per selezionare la modalità di soccorso di Bitdefender e premi **Invio**.

     Tra pochi istanti la Modalità soccorso di Bitdefender si caricherà.
- In **Windows 8 e Windows 8.1**:
  1. Premi il tasto **Shift** finché non compaiono sullo schermo le **Opzioni avanzate di avvio**.
  2. Seleziona l'opzione **Usa un altro sistema operativo** e poi Modalità soccorso di Bitdefender.

     Tra pochi istanti la Modalità soccorso di Bitdefender si caricherà.

Nota
È possibile caricare il tuo computer in modalità soccorso solo se il file dell'immagine della modalità soccorso in precedenza è stato scaricat, come descritto in «Scaricare l'immagine della modalità di Soccorso di Bitdefender» (p. 207).

Avviare il tuo sistema con l'ambiente di soccorso in Windows 10

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 **Ambiente di soccorso**.
3. Clicca su **Riavvia** nella finestra che comparirà.

   L'ambiente di soccorso di Bitdefender sarà pronto tra pochi istanti.

Esaminare il tuo sistema nella modalità di soccorso (Ambiente di soccorso in Windows 10)

Per esaminare il tuo sistema nella modalità di soccorso (Ambiente di soccorso):

- In **Windows 7, Windows 8 e Windows 8.1**:
  1. Entra in Modalità soccorso, come descritto in «Avviare il sistema in modalità soccorso in Windows 7, Windows 8 e Windows 8.1» (p. 208).
  2. Comparirà il logo di Bitdefender e i motori della soluzione di sicurezza inizieranno a essere copiati.
  3. Comparirà una finestra di benvenuto. Clicca su **Continua**.
  4. Viene avviato un aggiornamento del database delle informazioni sulle minacce.
  5. Una volta completato l'aggiornamento, compare la finestra della scansione antivirus su richiesta di Bitdefender.
  6. Clicca su **Controlla ora**, seleziona l'obiettivo della scansione nella finestra che compare e clicca su **Apri** per avviare la scansione.

     Si consiglia di controllare la tua intera partizione di Windows.

> **Nota**
> Quando si lavora in Modalità soccorso, avrai a che fare con nomi di partizioni tipo Linux. Le partizioni del disco compariranno come sda1 che corrisponde alla partizione di Windows (C:), sda2 che corrisponde a (D:) e così via.

7. Attendi il completamento della scansione. Se viene rilevata una minaccia, segui le istruzioni per rimuoverla.
8. Per uscire dalla modalità soccorso, clicca con il pulsante destro in un'area libera del desktop, seleziona **Esci** nel menu che comparirà e poi seleziona se riavviare o spegnere il computer.

- In **Windows 10**:
  1. Accedi all'ambiente di soccorso, come descritto in «Avviare il tuo sistema con l'ambiente di soccorso in Windows 10» (p. 209).
  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 con i risultati della scansione.

6.2.2. Cosa fare quando Bitdefender trova delle minacce sul computer?

Puoi scoprire la presenza di una minaccia sul computer in uno dei seguenti modi:

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

In tali situazioni, aggiorna Bitdefender per assicurarti di avere il più recente database dele 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 **Impostazioni**.
   c. Nella finestra **Protezione**, 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. 72).
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. 74).
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a «*Come posso visualizzare gli elementi nascosti in Windows?*» (p. 72).
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. 320).

6.2.3. Come posso rimuovere una minaccia in un archivio?

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

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

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

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

Ecco come rimuovere una minaccia in un archivio:

1. Identifica l'archivio che include la minaccia, eseguendo una scansione del sistema.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
   b. Nel pannello **ANTIVIRUS**, clicca su **Impostazioni**.
   c. Nella finestra **Protezione**, 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. 320).

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

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

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

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

1. 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 **Impostazioni**.
   c. Nella finestra **Protezione**, 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. 320).

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

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

Per assicurarti che il tuo sistema sia protetto:

1. Esegui una **Scansione del sistema** con Bitdefender. Per scoprire come fare, fai riferimento a «*Come posso eseguire una scansione del mio sistema?*» (p. 47).
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. 320).

6.2.6. Quali sono i file protetti da password nel registro della scansione?

Questa è solo una notifica per indicare che Bitdefender ha rilevato che questi file sono protetti da una password o da una qualche forma di crittografia.

In genere gli elementi protetti da password sono:

- File che appartengono a un'altra soluzione di sicurezza.
- File che appartengono al sistema operativo.

Per poter controllare i contenuti, devi estrarre o quantomeno decriptare questi file.

Qualora tali contenuti venissero estratti, la scansione in tempo reale di Bitdefender li controllerebbe automaticamente per proteggere il tuo computer. Se desideri controllare quei file con Bitdefender, devi contattare il produttore per ottenere maggiori informazioni sui file.

Ti consigliamo di ignorare quei file perché non sono una minaccia per il sistema.

6.2.7. Quali sono gli elementi ignorati nel registro della scansione?

Tutti i file che compaiono come Ignorati nel rapporto della scansione sono puliti.

Per prestazioni superiori, Bitdefender non controlla file che non sono stati modificati dall'ultima scansione.

6.2.8. Quali sono i file supercompressi nel registro della scansione?

Gli oggetti supercompressi sono elementi che non possono essere estratti dal motore di scansione o elementi per i quali la crittografia avrebbe impiegato troppo tempo, rendendo il sistema instabile.

Supercompresso significa che Bitdefender ha saltato la scansione di quell'archivio perché scompattarlo avrebbe richiesto troppe risorse di sistema. Se necessario, il contenuto sarà controllato solo durante l'accesso in tempo reale.

6.2.9. Perché Bitdefender ha eliminato automaticamente un file infetto?

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

Per 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.

ANTIVIRUS PER MAC

7. INSTALLAZIONE E RIMOZIONE

Questo capitolo include i seguenti argomenti:

- «*Requisiti di sistema*» (p. 217)
- «*Installazione di Bitdefender Antivirus for Mac*» (p. 217)
- «*Rimuovere Bitdefender Antivirus for Mac*» (p. 222)

7.1. Requisiti di sistema

Puoi installare Bitdefender Antivirus for Mac su computer Macintosh con OS X Yosemite (10.10.5), OS X El Capitan (10.11.6), macOS Sierra (10.12.6), macOS High Sierra (10.13.6), o macOS Mojave (10.14 o successivo).

Il tuo Mac deve avere un minimo di 1 GB di spazio disponibile sul disco rigido.

Per registrare e aggiornare Bitdefender Antivirus for Mac è richiesta una connessione a Internet.

Come scoprire la versione del tuo macOS X e le informazioni hardware sul tuo Mac

Clicca sull'icona Apple nell'angolo in alto a sinistra dello schermo e seleziona **Informazioni su questo Mac**. Nella finestra che compare, puoi vedere la versione del sistema operativo e altre informazioni utili. Clicca su **Rapporto di sistema** per informazioni dettagliate sull'hardware.

7.2. Installazione di Bitdefender Antivirus for Mac

La app Bitdefender Antivirus for Mac può essere installata dal tuo account di Bitdefender nel seguente modo:

1. Accedi come amministratore.
2. Vai a: https://central.bitdefender.com.
3. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
4. Seleziona il pannello **I miei dispositivi** e clicca su **INSTALLA PROTEZIONE**.
5. Seleziona una delle due opzioni disponibili:
   - **Proteggi questo dispositivo**

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

b. Salva il file di installazione.

- **Proteggi altri dispositivi**

a. Seleziona questa opzione 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.

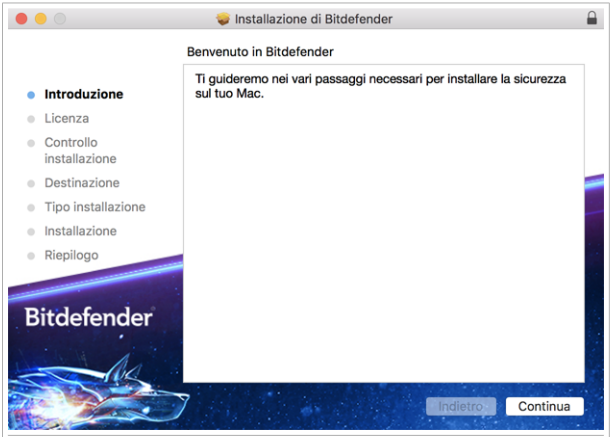
6. Esegui il prodotto Bitdefender che hai scaricato.
7. Completa tutti i passaggi dell'installazione.

7.2.1. Fase di installazione

Per installare Bitdefender Antivirus for Mac:

1. Clicca sul file scaricato. Sarà lanciato l'installer, che ti guiderà attraverso il processo d'installazione.
2. Segui la procedura guidata dell'installazione.

Passo 1 - Finestra di benvenuto



Finestra di benvenuto

Clicca su **Continua**.

Passo 2 - Leggi l'Accordo di Abbonamento

Leggi l'Accordo di Abbonamento

Prima di continuare con l'installazione, devi accettare l'Accordo di abbonamento. Prenditi qualche istante per leggere l'Accordo di abbonamento

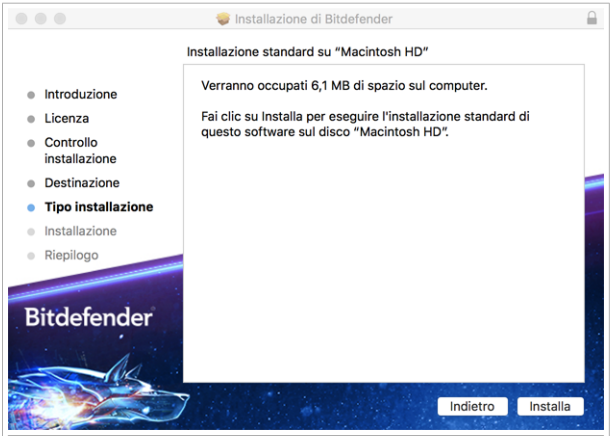
in quanto contiene i termini e le condizioni con cui è possibile utilizzare Bitdefender Antivirus for Mac.

Da questa finestra puoi anche selezionare la lingua con cui vuoi installare il prodotto.

Clicca su **Continua** e poi su **Accetta**.

Importante
Se non accetti questi termini, clicca su **Continua** e poi su **Rifiuta** per annullare l'installazione e uscire dal relativo programma.

Passo 3 - Inizia l'installazione

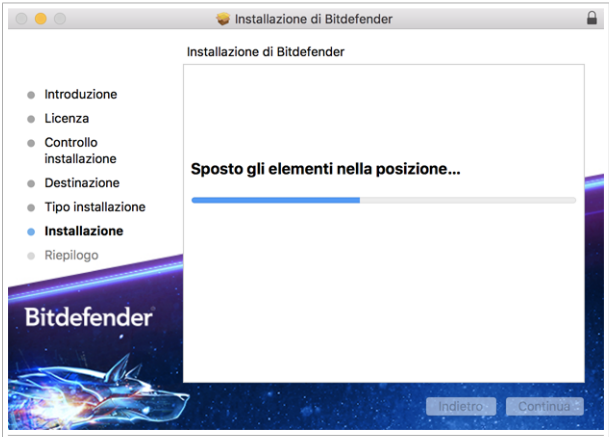


Inizia l'installazione

Bitdefender Antivirus for Mac sarà installato in Macintosh HD/Library/Bitdefender. Il percorso d'installazione non può essere modificato.

Clicca su **Installa** per avviare l'installazione.

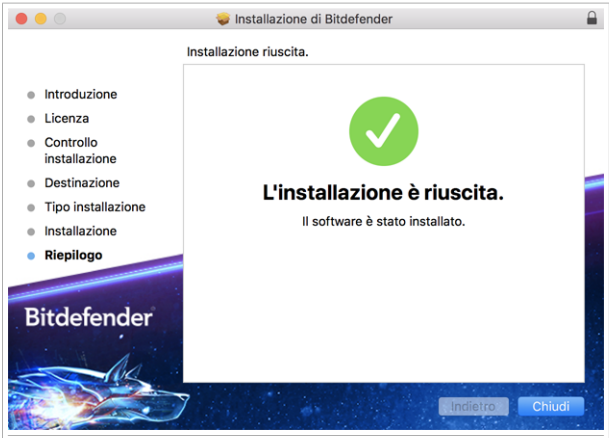
Passo 4 - Installare Bitdefender Antivirus for Mac



Installazione di Bitdefender Antivirus for Mac

Attendi la fine dell'installazione e clicca su **Continua**.

Passaggio 5 - Fine



Fine

Clicca su **Chiudi** per chiudere la finestra del programma d'installazione.

Ora la fase d'installazione è stata completata.

Importante

- Se stai installando Bitdefender Antivirus for Mac su macOS High Sierra 10.13.0 o una versione più recente, comparirà la notifica **Estensione di sistema bloccata**. Tale notifica ti informa che le estensioni firmate da Bitdefender sono state bloccate e devono essere consentite manualmente. Clicca su **OK** per continuare. Nella finestra Bitdefender Antivirus for Mac che comparirà, clicca sul link **Sicurezza e Privacy**. Clicca su **Consenti** nella parte inferiore della finestra o seleziona Bitdefender SRL dall'elenco, e poi clicca su **OK**.
- Se stai installando Bitdefender Antivirus for Mac su macOS Mojave 10.14 o una versione superiore, comparirà una notifica, che ti informa di dover autorizzare manualmente Bitdefender Antivirus for Mac a caricare i suoi file sul sistema. Per continuare, clicca sul link **Sicurezza e Privacy** e poi su **OK**. Clicca **Consenti** accanto a Bitdefender SRL.

7.3. Rimuovere Bitdefender Antivirus for Mac

Essendo un'applicazione complessa, Bitdefender Antivirus for Mac non può essere rimossa in modo tradizionale, semplicemente trascinando l'icona dell'applicazione dalla cartella Applicazioni al Cestino.

Per rimuovere Bitdefender Antivirus for Mac, segui questi passaggi:

1. Apri una finestra di **Finder** e vai alla cartella Applicazioni.
2. Apri la cartella Bitdefender e poi clicca due volte su BitdefenderUninstaller.
3. Clica su **Disinstalla** e attendi il completamento del processo.
4. Clicca su **Chiudi** per finire.

Importante

In caso di errore, puoi contattare il Servizio clienti di Bitdefender come descritto in «*Chiedere aiuto*» (p. 320).

8. COME INIZIARE

Questo capitolo include i seguenti argomenti:

8.1. Informazioni su Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac è un potente scanner antivirus, che può rilevare e rimuovere ogni tipo di software dannoso ("minacce"), tra cui:

- ransomware
- adware
- virus
- spyware
- Trojan
- keylogger
- worm

Questa applicazione non solo rileva e rimuove le minacce per Mac, ma anche quelle per Windows, impedendo quindi di inviare accidentalmente file infetti a familiari, amici e colleghi che utilizzano un PC.

8.2. Avviare Bitdefender Antivirus for Mac

Hai diversi modi a disposizione per aprire Bitdefender Antivirus for Mac.

- Clicca sull'icona di Bitdefender Antivirus for Mac nel Launchpad.
- Clicca sull'icona nella barra dei menu e seleziona **Apri finestra principale**.
- Apri una finestra di Finder, vai in Applicazioni e clicca due volte sull'icona di Bitdefender Antivirus for Mac.

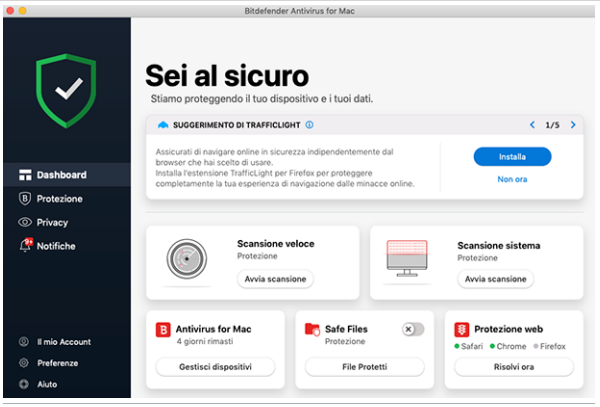
Importante

La prima volta che si apre Bitdefender Antivirus for Mac su macOS Mojave 10.14 o una versione più recente, comparirà un suggerimento di protezione. Tali suggerimenti compaiono perché ci servono i permessi per esaminare l'intero sistema alla ricerca di minacce. Per darci i permessi, devi accedere come amministratore e seguire questi passaggi:

1. Clicca sul link **Preferenze di sistema**.
2. Clicca sull'icona e poi inserisci le tue credenziali di amministratore.
3. Si aprirà una nuova finestra. Trascina il file **BDLDaemon** nell'elenco delle app autorizzate.

8.3. Finestra principale della app

Bitdefender Antivirus for Mac 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.



Finestra principale della app

Per apprendere l'interfaccia di Bitdefender, in alto a sinistra comparirà una procedura guidata introduttiva contenente maggiori dettagli su come interagire con il prodotto e configurarlo correttamente. Scegli la giusta parentesi angolare per continuare con la guida, o **Salta il tour** per chiudere la procedura guidata.

La barra di stato nella parte superiore della finestra ti informa sullo stato di sicurezza del sistema utilizzando messaggi chiari e colori indicativi. Se

Bitdefender Antivirus for Mac non ha alcun avviso, la barra di stato è verde. Quando viene rilevato un problema di sicurezza, la barra di stato cambia il suo colore, diventando rossa. Per informazioni dettagliate sui problemi o su come risolverli, fai riferimento a «*Risoluzione problemi*» (p. 238).

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, sia che tu stia lavorando o effettuando pagamenti online, Bitdefender Autopilot ti fornirà suggerimenti contestuali basati sull'uso e le esigenze del tuo dispositivo. Ciò ti aiuterà a scoprire e usufruire dei vantaggi offerti dalle funzionalità incluse nella app Bitdefender Antivirus for Mac.

Dal menu di navigazione sul lato sinistro puoi accedere alle sezioni di Bitdefender per una configurazione dettagliata e attività amministrative avanzate (schede **Protezione** e **Privacy**), le notifiche, il tuo account Bitdefender e l'area delle Preferenze. Inoltre, puoi anche contattarci (scheda **Aiuto**) per ricevere supporto nel caso avessi delle domande o comparisse un qualche elemento inatteso.

8.4. Icona app nel Dock

L'icona di Bitdefender Antivirus for Mac può essere notata nel Dock non appena apri l'applicazione. L'icona nel Dock ti fornisce un modo semplice e immediato per controllare file e cartelle alla ricerca di minacce. Basta trascinare e rilasciare il file o la cartella sull'icona del Dock e la scansione inizierà immediatamente.

Icona nel Dock

8.5. Menu di navigazione

Sul lato sinistro dell'interfaccia di Bitdefender si trova il menu di navigazione, che ti consente di accedere rapidamente alle funzionalità di Bitdefender necessarie per la gestione del prodotto. 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 l'utilizzo del prodotto, eseguire azioni rapide e andare al tuo account Bitdefender per gestire i dispositivi che hai aggiunto al tuo abbonamento Bitdefender.
- **Protezione**. Da qui, puoi eseguire attività di scansione antivirus, aggiungere file all'elenco delle eccezioni, proteggere file e app da attacchi ransomware, proteggere i tuoi backup Time Machine, e configurare la protezione durante la navigazione su Internet.
- **Privacy**. Da qui, puoi aprire la app Bitdefender VPN e installare l'estensione Anti-tracker nel tuo browser web.
- **Notifiche**. Da qui puoi visualizzare maggiori dettagli sulle azioni intraprese sui file esaminati.
- **Il mio account**. Da qui, puoi 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.
- **Preferenze**. Da qui, puoi configurare le impostazioni di Bitdefender.
- **Aiuto**. a qui, ogni volta che ti serve assistenza nel risolvere una situazione con il tuo prodotto Bitdefender, puoi contattare il Supporto tecnico. Puoi anche lasciarci un tuo feedback pre aiutarci a migliorare il prodotto.

8.6. Modalità scura

Per proteggere gli occhi da bagliori e luci mentre si lavora di notte o in condizioni di scarsa luminosità, Bitdefender Antivirus for Mac supporta la modalità scura per Mojave 10.14 e versioni successive. I colori dell'interfaccia sono stati ottimizzati per poter usare il Mac senza sforzare gli occhi. L'interfaccia di Bitdefender Antivirus for Mac si regola automaticamente in base alle impostazioni video del tuo dispositivo.

9. PROTEGGERSI DA SOFTWARE DANNOSO

Questo capitolo include i seguenti argomenti:

9.1. Consigli

Per tenere il tuo sistema sempre privo di minacce e impedire un'infezione accidentale di altri sistemi, segui questi consigli:

- Mantieni **Bitdefender Shield** attivato, così da consentire ai file di sistema di essere esaminati automaticamente da Bitdefender Antivirus for Mac.
- Mantieni il tuo prodotto Bitdefender Antivirus for Mac aggiornato con gli ultimi aggiornamenti del prodotto e delle informazioni delle minacce.
- Controlla e risolvi i problemi segnalati regolarmente da Bitdefender Antivirus for Mac. Per informazioni dettagliate, fai riferimento a «*Risoluzione problemi*» (p. 238).
- Controlla il registro degli eventi riguardanti le attività di Bitdefender Antivirus for Mac sul tuo computer. Ogni volta che accade qualcosa di rilevante per la sicurezza del sistema o dei dati, viene aggiunto un nuovo

messaggio all'area delle notifiche di Bitdefender. Per maggiori dettagli, accedi a «*Notifiche*» (p. 240).

- Dovresti seguire questi consigli:
  - Prendi l'abitudine di controllare i file che scarichi da periferiche di memorizzazione esterne (come una chiavetta USB o un CD), specialmente se non ne conosci l'origine.
  - Se hai un file DMG, montalo e poi controllane il contenuto (i file all'interno del volume/immagine montata).

  Il modo più semplice per controllare un file, una cartella o un volume è di trascinarli e lasciarli sulla finestra di Bitdefender Antivirus for Mac o nell'icona sul Dock.

Non è necessaria nessun'altra configurazione o azione. Tuttavia, se lo desideri, puoi modificare le impostazioni e le preferenze dell'applicazione in base alle tue esigenze. Per maggiori informazioni, fai riferimento a «*Configurare le preferenze*» (p. 243).

9.2. Eseguire una scansione sul Mac

Oltre alla funzione **Bitdefender Shield**, che monitora regolarmente le app installate, cercando azioni simili a minacce e impedendo a nuove minacce di accedere al sistema, puoi eseguire una scansione sul tuo Mac o esaminare determinati file in qualsiasi momento.

Il modo più semplice per controllare un file, una cartella o un volume è di trascinarli e lasciarli sulla finestra di Bitdefender Antivirus for Mac o nell'icona sul Dock. Comparirà la procedura guidata della scansione, che ti guiderà attraverso il processo di scansione.

Puoi avviare una scansione anche in questo modo:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Seleziona la scheda **Antivirus**.
3. Clicca su uno dei tre pulsanti di scansione per avviare la scansione desiderata.
   - **Scansione veloce** - Cerca eventuali minacce nei punti più vulnerabili del sistema (per esempio nelle cartelle contenenti documenti, file scaricati, messaggi di posta e altri file temporanei di ciascun utente).

- **Scansione completa** - Esegue un controllo dell'intero sistema alla ricerca di eventuali minacce. Saranno controllati anche tutti i mount connessi.

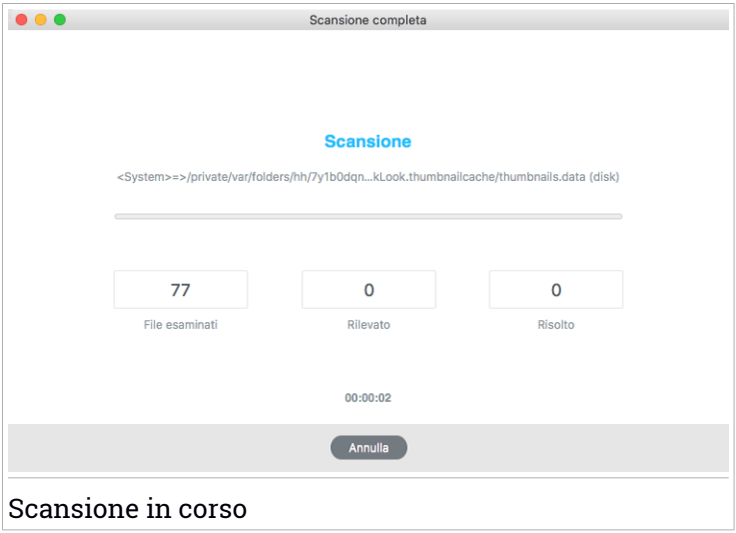
  > **Nota**
  >
  > In base alla misura del disco fisso, controllare l'intero sistema potrebbe richiedere un po' di tempo (fino a un'ora o persino di più). Per ottenere prestazioni migliori, si consiglia di non avviare questa attività mentre se ne eseguono altre piuttosto esigenti in termini di risorse di sistema (come ad esempio una sessione di editing video).
  > Se preferisci, puoi scegliere di non controllare determinati volumi montati, aggiungendoli all'elenco delle Eccezioni dalla finestra Protezione.

- **Scansione personalizzata** - Ti aiuta a controllare file, cartelle o volumi particolari in cerca di eventuali minacce.

Puoi anche avviare una Scansione veloce o di sistema dalla Dashboard.

9.3. Procedura guidata per la scansione

Ogni volta che avvii una scansione, comparirà la relativa procedura guidata di Bitdefender Antivirus for Mac.



Scansione in corso

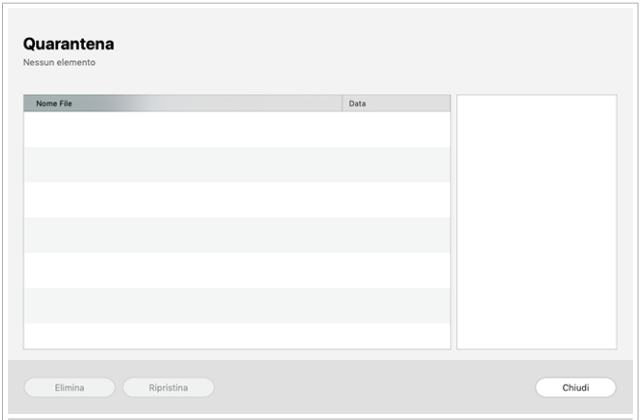
Durante ogni scansione, vengono mostrate informazioni in tempo reale sulle minacce eventualmente rilevate e risolte.

Attendi che Bitdefender Antivirus for Mac termini la scansione.

Nota
La durata del processo dipende dalla complessità della scansione.

9.4. Quarantena

Bitdefender Antivirus for Mac consente di isolare i file infetti o sospetti in un'area sicura, chiamata quarantena. Quando una minaccia è in quarantena, non può più arrecare alcun danno, in quanto non può essere eseguita o letta.



File in quarantena

La sezione Quarantena mostra tutti i file attualmente isolati nella cartella Quarantena.

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

Per visualizzare un elenco con tutti gli elementi aggiunti alla quarantena:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Si apre la finestra **Antivirus**.

   Clicca su **Apri** nel pannello **Quarantena**.

9.5. Bitdefender Shield (protezione in tempo reale)

Bitdefender fornisce una protezione in tempo reale da una vasta gamma di minacce esaminando tutte le app installate, le loro versioni aggiornate e i file nuovi e modificati.

Per disattivare la protezione in tempo reale:

1. Clicca su **Preferenze** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Disattiva **Bitdefender Shield** nella finestra **Protezione**.

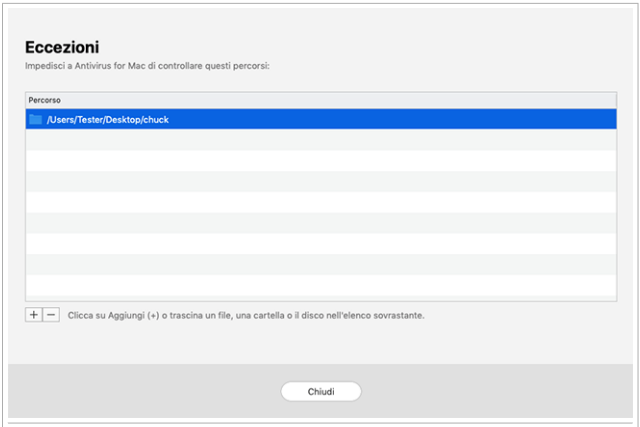
Avvertimento

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

9.6. Scansione eccezioni

Se lo desideri, puoi configurare Bitdefender Antivirus for Mac per non controllare determinati file e cartelle o anche interi volumi. Per esempio, potresti voler escludere dalla scansione:

- File che sono stati identificati per errore come infetti (conosciuti come falsi positivi)
- File che causano errori di scansione
- Backup dei volumi



Scansione eccezioni

L'elenco delle eccezioni contiene i percorsi che sono stati esclusi dalla scansione.

Per accedere all'elenco delle eccezioni:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Si apre la finestra **Antivirus**.

   Clicca su **Apri** nel pannello **Eccezioni**.

Ci sono due modi per impostare un'eccezione di scansione:

- Trascina e rilascia un file, una cartella o un volume sull'elenco delle eccezioni.
- Clicca sul pulsante con il segno più (+), posizionato sotto l'elenco delle eccezioni. Poi, seleziona il file, la cartella o il volume da escludere dalla scansione.

Per rimuovere un'eccezione, selezionala dall'elenco e clicca sul pulsante con il segno meno (-), posizionato sotto l'elenco delle eccezioni.

9.7. Protezione web

Bitdefender Antivirus for Mac utilizza le estensioni di TrafficLight per proteggere completamente la tua navigazione web. Le estensioni di

TrafficLight intercettano, elaborano e filtrano tutto il traffico web, bloccando eventuali contenuti dannosi.

Le estensioni funzionano e si integrano con i seguenti browser: Mozilla Firefox, Google Chrome e Safari.

Attivare le estensioni di TrafficLight

Per attivare le estensioni di TrafficLight:

1. Clicca su **Risolvi ora** nella scheda **Protezione web** sulla Dashboard.
2. Si apre la finestra **Protezione web**.

   Comparirà il browser web rilevato che hai installato sul tuo sistema. Per installare l'estensione di TrafficLight sul tuo browser, clicca su **Ottieni estensione**.
3. Sarai reindirizzato a:

   https://bitdefender.com/solutions/trafficlight.html
4. Seleziona **Download gratuito**.
5. Segui i passaggi per installare l'estensione di TrafficLight corrispondente al tuo browser.

Gestire le impostazioni delle estensioni

Per proteggerti da ogni tipo di minaccia che potresti incontrare durante la tua navigazione web, è disponibile una vasta gamma di funzioni. Per accedervi, clicca sull'icona di TrafficLight accanto alle impostazioni del browser e poi clicca su **Impostazioni**:

- **Impostazioni di Bitdefender TrafficLight**
  - Filtro Minacce avanzate - Ti impedisce di accedere a siti web utilizzati per attacchi malware, tentativi di phishing e frodi.
  - Rilevatore di tracker - Rileva eventuali tracker nelle pagine web visitate, mantenendoti informato sulla loro presenza.
  - Analisi risultati della ricerca - Segnala eventuali siti web rischiosi tra i risultati della tua ricerca.

    Se tutte le impostazioni sono disattivate, non sarà esaminato alcun sito web,
- **Whitelist**

È possibile escludere dalla scansione dei motori di Bitdefender alcuni siti web. Nel campo corrispondente, inserisci il nome del sito web che vuoi aggiungere all'elenco delle eccezioni e poi clicca su **AGGIUNGI**.

Non comparirà alcun avviso in caso di minacce presenti sulle pagine escluse. Ecco perché in questa lista devi indicare siti web affidabili.

Valutazione delle pagine e avvisi

In base a come TrafficLight classifica la pagina web che stai visualizzando, in quest'area sarà mostrata una delle seguenti icone:

Questa è una pagina sicura da visitare. Puoi continuare il tuo lavoro.
Questa pagina web può contenere contenuti pericolosi. Se decidi di visitarlo, usa la massima cautela.
Devi lasciare la pagina web immediatamente poiché contiene malware o altre minacce.

In Safari, lo sfondo delle icone di TrafficLight è nero.

9.8. Anti-tracker

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

Con l'estensione 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:

- Google Chrome
- Mozilla Firefox
- Safari

I tracker che rileviamo vengono raggruppati nelle seguenti categorie:

- **Pubblicità** - Usati per analizzare il traffico del sito web, il comportamento dell'utente o gli schemi di traffico dei visitatori.

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

Attivare Bitdefender Anti-tracker

Per attivare l'estensione Bitdefender Anti-tracker nel tuo browser web:

1. Clicca su **Privacy** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Seleziona la scheda **Anti-tracker**.
3. Clicca su **Attiva estensione** accanto al browser web per cui vuoi attivare l'estensione.

9.8.1. 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.

9.8.2. Disattivare l'anti-tracker di Bitdefender

Per disattivare Bitdefender Anti-tracker dal tuo browser web:

1. Apri il tuo browser web.

2. Clicca sull'icona accanto alla barra dell'indirizzo nel tuo browser web.
3. Clicca sull'icona nell'angolo in alto a destra.
4. Usa l'interruttore corrispondente per disattivarlo.

   L'icona di Bitdefender diventa grigia.

9.8.3. 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 .

9.9. Safe files

Un Ransomware è un programma dannoso che colpisce i sistemi vulnerabili bloccandoli e chiedendo denaro agli utenti per riavere il controllo dei propri sistemi. Questo programma dannoso agisce in maniera molto scaltra, mostrando falsi messaggi per allarmare l'utente, spingendoli al pagamento delle cifre richieste.

Utilizzando le tecnologie più moderne, Bitdefender assicura l'integrità del sistema proteggendone le aree critiche da attacchi ransomware senza influenzarne le prestazioni. Tuttavia, potresti voler proteggere anche i tuoi file personali, come documenti, fotografie o filmati, impedendone l'accesso ad applicazioni non affidabili. Con Safe files di Bitdefender, puoi proteggere i tuoi personali e configurare le app autorizzate a effettuare modifiche nei tuoi file protetti, bloccando tutte le altre.

Per aggiungere successivamente file all'ambiente protetto:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Seleziona la scheda **Anti-Ransomware**.
3. Clicca su **File protetti** nell'area Safe files.
4. Clicca sul pulsante con il segno più (+), posizionato sotto l'elenco dei file protetti. Poi, seleziona un file, una cartella o un volume da proteggere da eventuali attacchi ransomware.

Per evitare rallentamenti al sistema, ti consigliamo di aggiungere un massimo di 30 cartelle, o salvare più file in una sola cartella.

Di norma, le cartelle Immagini, Documenti, Desktop e Download sono protette dagli attacchi di ogni minaccia.

Nota
Le cartelle personali possono essere protette solo per gli utenti attuali. Unità esterne, oltre a file di sistema e delle applicazioni, non possono essere aggiunti all'ambiente protetto.

Sarai informato ogni volta che una app sconosciuta con un comportamento anomalo cercherà di modificare i file che hai aggiunto. Clicca su **Consenti** o **Blocca** per aggiungerla all'elenco delle Applicazioni gestite.

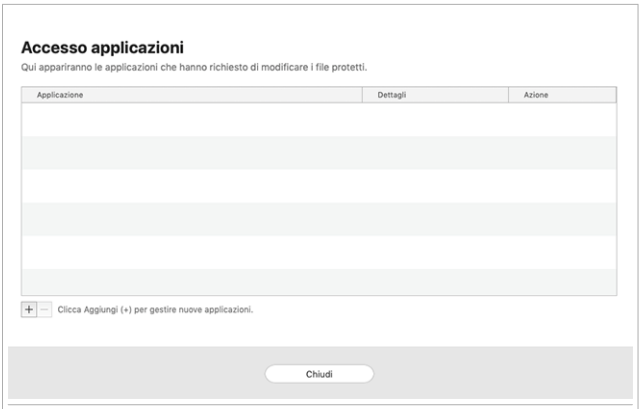
9.9.1. Applicazioni gestite

Le applicazioni che cercano di modificare o eliminare file protetti potrebbero essere segnalate come potenzialmente pericolose e aggiunte all'elenco delle "applicazioni bloccate". Se un'applicazione venisse bloccata ma hai la certezza che il suo comportamento sia assolutamente normale, puoi autorizzarla seguendo questi passaggi:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Seleziona la scheda **Anti-Ransomware**.
3. Clicca su **Accesso applicazione** nell'area Safe files.
4. Cambia lo stato in Consenti accanto alla app bloccata.

Anche le app impostate su Consenti possono essere bloccate.

Usa il metodo trascina e rilascia o clicca sul segno più (+) per aggiungere altre app all'elenco.



Safe files

9.10. Protezione Time Machine

Bitdefender Time Machine Protection serve come ulteriore strato di sicurezza per l'unità di backup, incluso tutti i file che hai deciso di archiviarci, bloccando l'accesso a qualsiasi fonte esterna. Nel caso in cui i file nella tua unità Time Machine venissero cifrati da un ransomware, potrai recuperarli senza dover cedere al ricatto.

Nel caso dovessi ripristinare degli elementi da un backup di Time Machine, controlla la pagina del supporto Apple per le istruzioni.

Attivare o disattivare la Protezione Time Machine

Per attivare o disattivare la Protezione Time Machine:

1. Clicca su **Protezione** nel menu di navigazione nell'**interfaccia di Bitdefender**.
2. Seleziona la scheda **Anti-Ransomware**.
3. Attiva o disattiva l'interruttore **Protezione Time Machine**.

9.11. Risoluzione problemi

Bitdefender Antivirus for Mac rileva automaticamente e ti informa sui problemi che possono influenzare la sicurezza del sistema e dei dati. In

questo modo, puoi risolvere facilmente e in maniera tempestiva ogni rischio per la sicurezza.

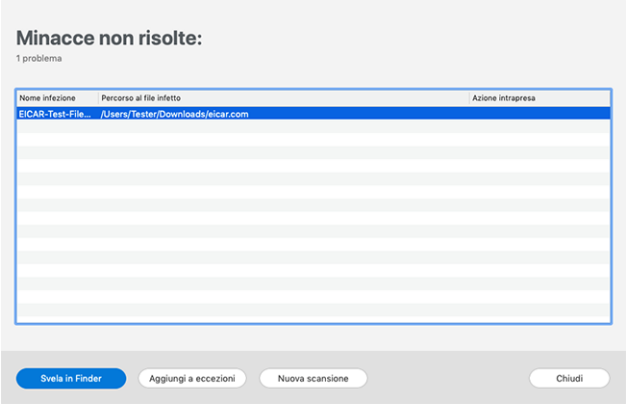
Risolvere i problemi indicati da Bitdefender Antivirus for Mac è un modo rapido e semplice per assicurare una protezione ottimale al tuo sistema e ai tuoi dati.

I problemi rilevati includono:

- Il nuovo aggiornamento sulle informazioni delle minacce non è stato scaricato dai nostri server.
- Sul tuo sistema sono state rilevate delle minacce e il prodotto non ha potuto disinfettarle automaticamente.
- La protezione in tempo reale è stata disattivata.

Per controllare e correggere problemi rilevati:

1. Se Bitdefender non ha alcun avviso, la barra di stato è verde. Quando viene rilevato un problema di sicurezza, la barra di stato cambia il suo colore, diventando rossa.
2. Verifica la descrizione per maggiori informazioni.
3. Quando viene rilevato un problema, clicca sul pulsante corrispondente per intervenire.



Finestra minacce non risolte

L'elenco delle minacce non risolte viene aggiornato dopo ogni scansione del sistema, indipendentemente se la scansione è stata eseguita automaticamente in background o avviata da te.

Puoi scegliere di intraprendere le seguenti azioni sulle minacce non risolte:

- Elimina manualmente. Intraprendi questa azione per rimuovere manualmente le infezioni.
- Aggiungi a eccezioni. Questa azione non è disponibile per le minacce presenti negli archivi.

9.12. Notifiche

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

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

Per accedere al 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.

9.13. Aggiornamenti

Tutti giorni vengono trovate e identificate nuove minacce. Ecco perché è molto importante mantenere Bitdefender Antivirus for Mac sempre aggiornato con i nuovi aggiornamenti delle informazioni delle minacce.

Gli aggiornamenti delle informazioni delle minacce sono eseguiti al volo, ciò significa che i file da aggiornare sono sostituiti progressivamente. In questo modo, l'aggiornamento non interesserà l'operatività del prodotto, e, allo stesso tempo, ogni vulnerabilità sarà esclusa.

- Se Bitdefender Antivirus for Mac è aggiornato, può rilevare tutte le ultime minacce scoperte e pulire i file infetti.
- Se Bitdefender Antivirus for Mac non è aggiornato, non potrà rilevare e rimuovere le nuove minacce scoperte dai laboratori di Bitdefender.

9.13.1. Richiedere un aggiornamento

Puoi richiedere un aggiornamento manualmente in qualsiasi momento.

Per controllare la disponibilità di aggiornamenti e scaricarli, è richiesta una connessione a Internet attiva.

Per richiedere un aggiornamento manualmente:

1. Clicca sul pulsante **Azioni** nella barra dei menu.
2. Seleziona **Aggiornamento database informazioni minacce**.

In alternativa, puoi richiedere un aggiornamento manuale, premendo CMD + U.

Puoi visualizzare l'avanzamento dell'aggiornamento e i file scaricati.

9.13.2. Ottenere gli aggiornamenti tramite server proxy

Bitdefender Antivirus for Mac può essere aggiornato solo tramite server proxy che non richiedono l'autenticazione. Non devi configurare alcuna impostazione del programma.

Se ti connetti a Internet attraverso un server proxy che richiede l'autenticazione, devi passare a una normale connessione Internet diretta per ottenere gli aggiornamenti delle informazioni delle minacce.

9.13.3. Aggiornare a una nuova versione

Occasionalmente, rendiamo disponibili aggiornamenti del prodotto per aggiungere nuove funzioni e miglioramenti, o per risolvere eventuali problemi. Tali aggiornamenti potrebbero richiedere un riavvio del sistema per avviare l'installazione dei nuovi file. Di norma, se un aggiornamento richiede un riavvio del computer, Bitdefender Antivirus for Mac continuerà a funzionare con i file precedenti fin quando il sistema non sarà riavviato. In questo caso, il processo di aggiornamento non interferirà con le attività dell'utente.

Quando l'aggiornamento di un prodotto viene completato, una finestra di pop-up ti informerà di riavviare il sistema. Se hai saltato questa notifica, puoi cliccare su **Riavvia per aggiornare** dalla barra dei menu oppure riavviare il sistema manualmente.

9.13.4. Trovare informazioni su Bitdefender Antivirus for Mac

Per trovare informazioni sulla versione di Bitdefender Antivirus for Mac che hai installato, accedi alla finestra **Info**. Nella stessa finestra puoi accedere e visualizzare l'Accordo di abbonamento, l'Informativa sulla privacy e le licenze open source.

Per accedere alla finestra Info:

1. Apri Bitdefender Antivirus for Mac.
2. Clicca su Bitdefender Antivirus for Mac nella barra dei menu e seleziona **Info su Antivirus for Mac**.

10. CONFIGURARE LE PREFERENZE

Questo capitolo include i seguenti argomenti:

10.1. Accedere alle preferenze

Per aprire la finestra delle preferenze di Bitdefender Antivirus for Mac:

1. Esegui una delle seguenti azioni:
   - Clicca su **Preferenze** nel menu di navigazione nell'interfaccia di Bitdefender.
   - Clicca su Bitdefender Antivirus for Mac nella barra del menu e seleziona **Preferenze**.
   - Premi Comando-Virgola(,).

10.2. Preferenze protezione

La finestra delle preferenze di protezione ti consente di configurare l'approccio generale alla scansione. Puoi configurare le azioni intraprese sui file infetti o sospetti, e altre impostazioni generali.

- **Protezione di Bitdefender.** Bitdefender Shield fornisce una protezione in tempo reale da una vasta gamma di minacce esaminando tutte le app installate, le loro versioni aggiornate e i file nuovi e modificati. Non ti consigliamo di disattivare Bitdefender Shield, ma se dovessi farlo, fallo per il minor tempo possibile. Se Bitdefender Shield viene disattivato, non sarai protetto dalle minacce.
- **Scansiona solo file nuovi e modificati.** Seleziona questa casella per fare in modo che Bitdefender Antivirus for Mac controlli solo i file che non sono già stati controllati o che sono stati modificati dall'ultima scansione.

  Puoi scegliere di non applicare questa impostazione per la scansione trascina e rilascia personalizzata, deselezionando la casella corrispondente.
- **Non esaminare i contenuti nei backup.** Seleziona questa casella per escludere i file di backup dalla scansione. Se i file infetti venissero

ripristinati in un secondo momento, Bitdefender Antivirus for Mac li rileverà automaticamente, adottando tutti i provvedimenti necessari.

10.3. Preferenze avanzate

Puoi scegliere quale azione generale intraprendere per tutti i problemi ed elementi sospetti trovati durante un processo di scansione.

Azione per elementi infetti

Prova a disinfettare o spostare in quarantena - Se vengono rilevati file infetti, Bitdefender tenterà di disinfettarli (rimuovendo il codice dannoso) o spostarli in quarantena.

Non fare nulla - Nessuna azione verrà intrapresa sui file rilevati.

Azione per elementi sospetti

Sposta i file in quarantena - Se vengono rilevati file sospetti, Bitdefender li sposterà in quarantena.

Non fare nulla - Nessuna azione verrà intrapresa sui file rilevati.

10.4. Offerte speciali

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

Per attivare o disattivare le notifiche sulle offerte speciali:

1. Clicca su **Preferenze** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Seleziona la scheda **Altro**.
3. Attiva o disattiva l'interruttore **Le mie offerte**.

Di norma, l'opzione **Le mie offerte** è attivata.

11. VPN

Questo capitolo include i seguenti argomenti:

11.1. Informazioni su VPN

Con Bitdefender VPN puoi mantenere privati i tuoi dati ogni volta che ti connetti a reti wireless non protette mentre sei in aeroporti, centri commerciali, bar o alberghi. In questo modo, è possibile evitare situazioni spiacevoli, come furti di dati personali o tentativi di rendere accessibile il tuo indirizzo IP a pirati informatici.

Il VPN opera come una sorta di tunnel tra il tuo dispositivo e la rete a cui ti connetti, proteggendo la tua connessione, cifrando i dati usando una cifratura di tipo bancario e nascondendo il tuo indirizzo IP, ovunque ti trovi. Il tuo traffico viene reindirizzato a un server indipendente, rendendo quindi il tuo dispositivo quasi impossibile da identificare tra la miriade di altri dispositivi che stanno usando i nostri servizi. Inoltre, mentre ti connetti a Internet tramite 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.

11.2. Aprire VPN

Ci sono tre metodi per aprire la app Bitdefender VPN:

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

  Clicca su **Apri** nella scheda Bitdefender VPN.

- Clicca sull'icona nella barra dei menu.

- Vai alla cartella Applicazioni, apri la cartella Bitdefender e poi clicca due volte sull'icona Bitdefender VPN.

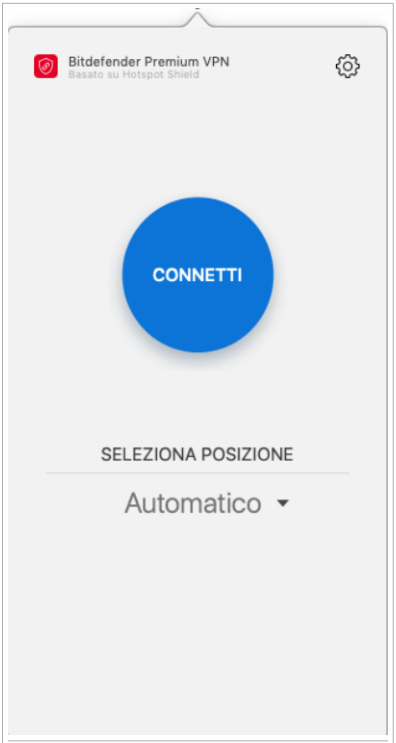
La prima volta che apri la app, ti sarà chiesto di consentire a Bitdefender di aggiungere configurazioni. Consentendo a Bitdefender di aggiungere configurazioni, accetti che tutte le attività di rete del tuo dispositivo possano essere filtrate o monitorate quando si usa la app VPN.

Nota
La app Bitdefender VPN può essere installata solo su macOS Sierra (10.12.6), macOS High Sierra (10.13.6), o macOS Mojave (10.14 o successivo).

11.3. Interfaccia

L'interfaccia di VPN mostra lo stato della app, connessa o disconnessa. Qui avrai la possibilità di cambiare la posizione del server a cui vuoi connetterti.

Per connetterti o disconnetterti, clicca semplicemente sullo stato mostrato nella parte superiore della schermata. L'icona della barra dei menu diventa nera quando VPN è connesso e bianca quando VPN è disconnesso.



Interfaccia di VPN

Mentre sei connesso, nella parte inferiore dell'interfaccia viene indicato il tempo trascorso. Per accedere a più opzioni, clicca sull'icona ⚙ nella parte in alto a destra:

- **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.
- **Impostazioni** - In base alle tue necessità, puoi personalizzare il comportamento del tuo prodotto:
  - Imposta l'esecuzione di VPN all'avvio del sistema
  - Ricevi notifiche quando VPN si connette o disconnette automaticamente

- **Supporto** - Sarai reindirizzato alla piattaforma del nostro Centro di supporto, da cui potrai leggere un articolo molto utile su come utilizzare Bitdefender VPN.
- **Info** - Vengono mostrate alcune informazioni sulla versione installata.
- **Esci** - Esci dalla app.

12. BITDEFENDER CENTRAL

Questo capitolo include i seguenti argomenti:

- «*Informazioni su Bitdefender Central*» (p. 249)
- «*I miei abbonamenti*» (p. 252)
- «*I miei dispositivi*» (p. 253)

12.1. Informazioni su 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 computer o dispositivo mobile connesso a internet, andando su https://central.bitdefender.com o direttamente dalla app Bitdefender Central sui dispositivi iOS e Android.

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 for Mac
  - Linea di prodotti Bitdefender per Windows
  - 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.

12.2. Accedere a Bitdefender Central

Ci sono diversi modi per accedere a Bitdefender Central. In base all'attività che intendi eseguire, puoi utilizzare una delle seguenti possibilità:

- Dall'interfaccia principale di Bitdefender Antivirus for Mac:
  1. Clicca sul link **Vai al tuo account** nel lato in basso a destra della schermata.
- 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 usando il tuo indirizzo e-mail e la tua password.
- Dal tuo dispositivo Android o iOS:

  Apri la app Bitdefender Central che hai installato.

Nota
In questo materiale abbiamo incluso le opzioni che puoi trovare nell'interfaccia web.

12.3. 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 **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 computer, 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.

  c. Clicca su **ATTIVA**.

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.
3. Conferma la tua scelta.

12.4. 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.

12.5. I miei abbonamenti

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

12.5.1. Attiva abbonamento

Un abbonamento può essere attivato durante la fase d'installazione, utilizzando il tuo account Bitdefender. Con il processo di attivazione, il periodo di validità dell'abbonamento inizia a scalare.

Se hai acquistato un codice di attivazione da uno dei nostri rivenditori o l'hai ricevuto come omaggio, puoi aggiungere la sua disponibilità al tuo abbonamento a Bitdefender.

Per attivare un abbonamento utilizzando un codice di attivazione, segui questi passaggi:

1. Accedi a Bitdefender Central.
2. Clicca sull'icona nell'angolo in alto a sinistra della finestra e poi 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.

Per avviare l'installazione del prodotto sui tuoi dispositivi, fai riferimento a «*Installazione di Bitdefender Antivirus for Mac*» (p. 217).

12.5.2. Acquista abbonamento

Puoi acquistare un abbonamento direttamente dal tuo account Bitdefender, seguendo questi passaggi:

1. Accedi a Bitdefender Central.
2. Clicca sull'icona nell'angolo in alto a sinistra della finestra e poi seleziona il pannello **I miei abbonamenti**.
3. Clicca sul link **Acquista ora**. Verrai reindirizzato a una pagina web da cui potrai effettuare l'acquisto.

Una volta completato il processo, la disponibilità dell'abbonamento sarà visibile nell'angolo in basso a destra dell'interfaccia principale del prodotto.

12.6. I miei dispositivi

L'area **I miei dispositivi** nel tuo account Bitdefender 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.

12.6.1. Personalizza il tuo dispositivo

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, selezionando una data di nascita e inserendo un indirizzo e-mail e un numero di telefono.
6. Clicca su **AGGIUNGI** per salvare il profilo.
7. Seleziona il proprietario desiderato dall'elenco **Proprietario dispositivo** e clicca su **ASSEGNA**.

12.6.2. Azioni in remoto

Per aggiornare Bitdefender in remoto su un dispositivo:

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**.

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 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 completa 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 «*Eseguire una scansione sul Mac*» (p. 228).

13. DOMANDE FREQUENTI

Come posso provare Bitdefender Antivirus for Mac prima di sottoscrivere un abbonamento?

Sei un nuovo cliente di Bitdefender e vorresti provare il nostro prodotto prima di acquistarlo? Il periodo di prova dura 30 giorni ed è possibile continuare a utilizzare il prodotto installato, solo se acquisti un abbonamento a Bitdefender. Per provare Bitdefender Antivirus for Mac, devi:

1. Crea un account Bitdefender, seguendo questi passaggi:
   a. Vai a: https://central.bitdefender.com.
   b. Digita le informazioni richieste nei campi corrispondenti. I dati forniti resteranno riservati.
   c. Prima di procedere ulteriormente devi accettare i Termini di utilizzo. Accedi ai Termini di utilizzo e leggili attentamente, in quanto contengono i termini e le condizioni con cui puoi utilizzare Bitdefender.

      Inoltre, potrai accedere e leggere l'Informativa sulla privacy.
   d. Clicca su **CREA ACCOUNT**.
2. Scarica Bitdefender Antivirus for Mac nel seguente modo:
   a. Seleziona il pannello **I miei dispositivi** e clicca su **INSTALLA PROTEZIONE**.
   b. Seleziona una delle due opzioni disponibili:
      - **Proteggi questo dispositivo**
        i. Seleziona questa opzione e poi il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, clicca sul pulsante corrispondente.
        ii. Salva il file di installazione.
      - **Proteggi altri dispositivi**
        i. Seleziona questa opzione e poi il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, clicca sul pulsante corrispondente.
        ii. Clicca su **INVIA LINK DI DOWNLOAD**.

iii. 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.

iv. 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.

c. Esegui il prodotto Bitdefender che hai scaricato.

Il registro della scansione indica che ci sono ancora alcuni elementi non risolti. Come posso rimuoverli?

Gli elementi non risolti nel registro della scansione possono essere:

- archivi ad accesso limitato (xar, rar, ecc.)

  Soluzione: Usa l'opzione **Rivela in Finder** per trovare il file ed eliminarlo manualmente. Assicurati di svuotare il Cestino.

- caselle di posta ad accesso limitato (Thunderbird, ecc.)

  Soluzione: usa l'applicazione per rimuovere l'elemento contenente il file infetto.

- Contenuti nei backup

  Soluzione: attiva l'opzione **Non esaminare i contenuti nei backup** nelle preferenze della Protezione o **Aggiungi a eccezioni** i file rilevati.

  Se i file infetti venissero ripristinati in un secondo momento, Bitdefender Antivirus for Mac li rileverà automaticamente, adottando tutti i provvedimenti necessari.

> **Nota**
> I file ad accesso limitato sono file che solo Bitdefender Antivirus for Mac può aprire, ma non può comunque modificarli.

Dove posso visualizzare maggiori dettagli sulle attività del prodotto?

Bitdefender salva un registro di tutte le azioni importanti, i cambiamenti di stato e gli altri messaggi critici relativi alle sue attività. Per accedere a tali informazioni, clicca su **Notifiche** nel menu di navigazione nell'interfaccia di Bitdefender.

Posso aggiornare Bitdefender Antivirus for Mac attraverso un server proxy?

Bitdefender Antivirus for Mac può essere aggiornato solo tramite server proxy che non richiedono l'autenticazione. Non devi configurare alcuna impostazione del programma.

Se ti connetti a Internet attraverso un server proxy che richiede l'autenticazione, devi passare a una normale connessione Internet diretta per ottenere gli aggiornamenti delle informazioni delle minacce.

Come posso rimuovere Bitdefender Antivirus for Mac?

Per rimuovere Bitdefender Antivirus for Mac, segui questi passaggi:

1. Apri una finestra di **Finder** e vai alla cartella Applicazioni.
2. Apri la cartella Bitdefender e poi clicca due volte su BitdefenderUninstaller.
3. Clica su **Disinstalla** e attendi il completamento del processo.
4. Clicca su **Chiudi** per finire.

> **Importante**
> In caso di errore, puoi contattare il Servizio clienti di Bitdefender come descritto in «*Chiedere aiuto*» (p. 320).

Come posso rimuovere le estensioni di TrafficLight dal mio browser web?

- Per rimuovere le estensioni di TrafficLight da Mozilla Firefox, segui questi passaggi:
  1. Vai a **Strumenti** e seleziona **Add-on**.
  2. Seleziona **Estensioni** sulla colonna a sinistra.
  3. Seleziona l'estensione e clicca su **Rimuovi**.
  4. Riavvia il browser per completare il processo di rimozione.
- Per rimuovere le estensioni di TrafficLight da Google Chrome, segui questi passaggi:
  1. In alto a destra, clicca su **Altro** .
  2. Vai ad **Altri strumenti** e seleziona **Estensioni**.
  3. Clicca sull'icona **Rimuovi...** accanto all'estensione che vuoi rimuovere.

4. Clicca su **Rimuovi** per confermare il processo di rimozione.

- Per rimuovere Bitdefender TrafficLight da Safari, segui questi passaggi:

  1. Andare in **Preferenze** o premere **Command-Comma(,)**.
  2. Seleziona **Estensioni**.

     Comparirà un elenco con le estensioni installate.
  3. Seleziona l'estensione Bitdefender TrafficLight e poi clicca su **Disinstalla**.
  4. Clicca nuovamente su **Disinstalla** per confermare il processo di rimozione.

Quando dovrei utilizzare Bitdefender VPN?

Devi fare sempre attenzione quando accedi, scarichi o invii contenuti su internet. Per assicurarti di essere sempre al sicuro mentre navighi sul web, ti consigliamo di utilizzare Bitdefender VPN quando:

- vuoi connetterti a reti wireless pubbliche
- vuoi accedere a contenuti che normalmente sono riservati a determinate aree, indipendentemente dal fatto che ti trovi a casa o all'estero
- vuoi mantenere i tuoi dati personali privati (nomi utente, password, informazioni della carta di credito, ecc.)
- vuoi nascondere il tuo indirizzo IP

Bitdefender VPN avrà un impatto negativo sulla durata della batteria del mio dispositivo?

Bitdefender VPN è progettato per proteggere i tuoi dati personali, nascondere il tuo indirizzo IP mentre sei connesso a reti wireless non sicure e accedere a contenuti inaccessibili in determinati paesi. Per evitare un consumo non necessario della batteria del tuo dispositivo, ti consigliamo di utilizzare VPN solo quando ne hai bisogno e disconnetterti quando sei offline.

Perché riscontro rallentamenti in Internet mentre sono connesso con Bitdefender VPN?

Bitdefender VPN è stato progettato per offrirti un'esperienza di navigazione sul web leggera; tuttavia, la tua connettività a Internet o la distanza del server a cui ti connetti potrebbero causare dei rallentamenti. In questo caso, se non è obbligatorio connetterti a un server ospitato

molto distante (ad esempio negli Stati Uniti o in Cina), ti consigliamo di consentire a Bitdefender VPN di connettersi automaticamente al server più vicino o trovarne uno più vicino alla tua ubicazione attuale.

MOBILE SECURITY PER IOS

14. CHE COS'È BITDEFENDER MOBILE SECURITY FOR IOS

Attività online come pagare le bollette, prenotare le vacanze o acquistare beni o servizi, sono molto comode e pratiche. Ma come molte attività che si sono sviluppate su Internet, possono comportare dei rischi, se si ignorano alcune norme di sicurezza, che potrebbero condurre alla compromissione dei propri dati personali. E cosa c'è di più importante del proteggere i dati memorizzati negli account online e nel proprio smartphone?

Bitdefender Mobile Security for iOS ti consente di:

- Proteggi i tuoi dati mentre utilizzi reti wireless non affidabili.
- Quando sei online, fai attenzione a siti web e domini potenzialmente dannosi.
- Verifica l'eventuale presenza di una violazione negli account online usati quotidianamente.

Bitdefender Mobile Security for iOS viene offerto gratuitamente e richiede l'attivazione con un account di Bitdefender.

15. COME INIZIARE

Requisiti dispositivo

Bitdefender Mobile Security for iOS funziona su qualsiasi dispositivo con iOS 11.2 o superiore, e richiede una connessione a Internet per essere attivato e rilevare l'eventuale presenza di violazioni nei tuoi account online.

Installazione di Bitdefender Mobile Security for iOS

- **Da Bitdefender Central**
  - Su iOS
    1. Accedi a Bitdefender Central.
    2. Tocca l'icona nell'angolo in alto a sinistra dello schermo e seleziona **I miei dispositivi**.
    3. Tocca **INSTALLA PROTEZIONE**, e poi tocca **Proteggi questo dispositivo**.
    4. Seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, tocca il pulsante corrispondente.
    5. Sarai reindirizzato all'applicazione di **App Store**. Nella schermata di App Store, tocca l'opzione di installazione.
  - Su Windows, macOS, Android
    1. Accedi a Bitdefender Central.
    2. Premi l'icona nell'angolo in alto a sinistra dello schermo e seleziona **I miei dispositivi**.
    3. Premi **INSTALLA PROTEZIONE** e poi premi **Proteggi altri dispositivi**.
    4. Seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, premi il pulsante corrispondente.
    5. Premi **INVIA LINK DI DOWNLOAD**.
    6. Inserisci l'indirizzo email nel campo corrispondente e premi **INVIA EMAIL**. Nota che il link di download generato è valido solo per le prossime 24 ore. Se il link dovesse scadere, dovrai generarne uno nuovo seguendo gli stessi passaggi.

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

- **Da App Store**

  Cerca Bitdefender Mobile Security for iOS per trovare e installare la app.

La prima volta che apri la app, viene visualizzata una finestra di introduzione contenente maggiori dettagli sulle funzionalità del prodotto. Tocca **Iniziare** per passare alla finestra successiva.

Prima di passare alle diverse fasi per la convalida, devi accettare l'Accordo di abbonamento. Prenditi qualche istante per leggere l'Accordo di abbonamento in quanto contiene i termini e le condizioni con cui è possibile utilizzare Bitdefender Mobile Security for iOS.

Tocca **Continua** per passare alla finestra successiva.

Accedi al tuo account di Bitdefender

Per usare Bitdefender Mobile Security for iOS, devi collegare il tuo dispositivo a un account di Bitdefender o Facebook, Google o Microsoft, accedendo all'account direttamente dalla app. La prima volta che apri l'applicazione, ti sarà chiesto di accedere a un account.

Per collegare il tuo dispositivo a un account di Bitdefender:

1. Inserisci l'indirizzo e-mail del tuo account Bitdefender nel campo corrispondente e tocca **AVANTI**. Se non hai un account Bitdefender e vuoi crearne uno, seleziona il link corrispondente e segui le istruzioni sullo schermo fino all'attivazione dell'account.

   Per accedere utilizzando un account Facebook, Google o Microsoft, tocca il servizio che vuoi utilizzare dall'area **O ACCEDI CON**. Sarai reindirizzato alla pagina di accesso del servizio selezionato. Segui le istruzioni per collegare il tuo account a Bitdefender Mobile Security for iOS.

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

2. Inserisci la tua password e tocca **ACCEDI**.

Da qui puoi anche accedere all'Informativa sulla privacy di Bitdefender.

Dashboard

Tocca l'icona di Bitdefender Mobile Security for iOS nell'app drawer del dispositivo per aprire l'interfaccia dell'applicazione.

La prima volta che accedi alla app, ti sarà chiesto di consentire a Bitdefender di inviarti delle notifiche. Tocca **Consenti** per restare informato ogni volta che Bitdefender ha qualcosa da comunicarti di importante sulla app. Per gestire le notifiche Bitdefender, vai in Impostazioni > Notifiche > Mobile Security.

Per ottenere le informazioni necessarie, tocca l'icona corrispondente nella parte inferiore della schermata.

VPN

Ottieni sempre la massima privacy indipendentemente dalla rete a cui ti connetti, mantenendo la tua comunicazione Internet cifrata. Per maggiori informazioni, fai riferimento a «*VPN*» (p. 267).

Protezione web

Resta al sicuro mentre navighi sul web e ogni volta che app meno sicure cercheranno di accedere a domini non affidabili. Per maggiori informazioni, fai riferimento a «*Protezione web*» (p. 269).

Privacy dell'account

Scopri se i tuoi account e-mail sono stati violati oppure no. Per maggiori informazioni, fai riferimento a «*Privacy dell'account*» (p. 271).

Per vedere opzioni aggiuntive, tocca l'icona ••• sul tuo dispositivo nella schermata principale dell'applicazione. Compariranno le seguenti opzioni:

- **Ripristina acquisti** - Qui puoi ripristinare l'abbonamento premium a VPN che hai acquistato tramite il tuo account iTunes.
- **Impostazioni** - Qui puoi accedere alle impostazioni VPN, come segue:
  - **Accordo** - Puoi leggere i termini che regolano l'utilizzo del servizio Bitdefender VPN. Toccando l'opzione **Non sono più d'accordo**, non potrai utilizzare Bitdefender VPN almeno finché non toccherai **Accetto**.
  - **Avviso Wi-Fi pubblico** - Puoi attivare o disattivare la notifica del prodotto che compare ogni volta che ti connetti a una rete Wi-Fi non sicura. Lo

scopo di questa notifica è aiutarti a mantenere i tuoi dati sempre privati e protetti usando Bitdefender VPN.

- **Feedback** - Da qui puoi lanciare il client email predefinito per inviarci un tuo feedback sulla app.
- **Info app** - Da qui, puoi accedere a varie informazioni sulla versione installata e l'Accordo di abbonamento, l'Informativa sulla privacy e gli accordi per le licenze open-source.

16. VPN

Con Bitdefender VPN puoi mantenere privati i tuoi dati ogni volta che ti connetti a reti wireless non protette mentre sei in aeroporti, centri commerciali, bar o alberghi. In questo modo, è possibile evitare situazioni spiacevoli, come furti di dati personali o tentativi di rendere accessibile il tuo indirizzo IP a pirati informatici.

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

Nota
La Cina, l'Iraq, gli Emirati Arabi Uniti, la Turchia, la Bielorussia, l'Oman, l'Iran e la Russia praticano la censura di Internet e quindi l'uso delle VPN sul loro territorio è stato vietato dalla legge. Di conseguenza, la funzionalità di Bitdefender VPN non sarà disponibile sul loro territorio.

Per attivare Bitdefender VPN:

1. Tocca l'icona nella parte inferiore della schermata.
2. Tocca **Connetti** ogni volta che vuoi restare protetto mentre sei conesso a reti wireless non affidabili.

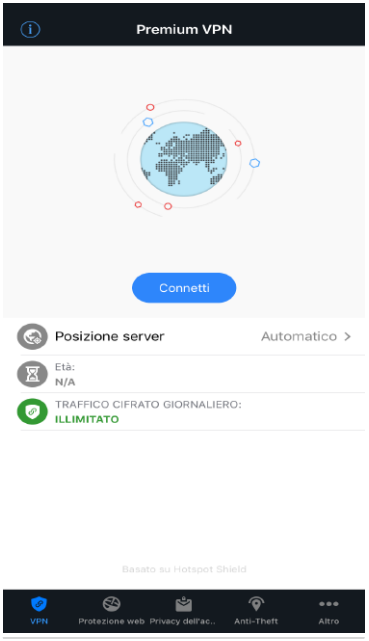
   Tocca **Disconnetti** ogni volta che vuoi disattivare la connessione.

Nota
La prima volta che attivi VPN, ti viene chiesto di consentire a Bitdefender di impostare le configurazioni VPN che monitoreranno il traffico di rete. Tocca **Consenti** per continuare. Se per proteggere il tuo smartphone è stato impostato un metodo di autenticazione (come impronta digitale o codice PIN), dovrai utilizzarlo.

L'icona VPN compare nella barra di stato quando VPN è attivo.

Per risparmiare la batteria, ti consigliamo di disattivare VPN quando non ti serve.

Se vuoi connetterti a un server a tua scelta, tocca **Posizione server** nell'interfaccia di VPN e seleziona la posizione desiderata.



VPN

17. PROTEZIONE WEB

Protezione web di Bitdefender assicura un'esperienza di navigazione sicura avvisandoti di pagine web potenzialmente dannose e quando app installate meno sicure cercheranno di accedere a domini non affidabili.

Quando un URL porta a un sito web noto per essere fraudolento o phishing, o a contenuti dannosi come spyware o virus, la pagina web viene bloccata, mostrando un avviso. La stessa cosa accade quando le app installate cercano di accedere a domini dannosi.

Per attivare Protezione web:

1. Tocca l'icona nella parte inferiore della schermata.
2. Tocca **PROVA LA PROTEZIONE WEB**.
3. Scegli uno dei tre periodi di prova gratuita e conferma i dettagli del pagamento.
4. Attiva l'interruttore della Protezione web.

Nota
La prima volta che attivi Protezione web, ti viene chiesto di consentire a Bitdefender di impostare le configurazioni VPN che monitoreranno il traffico di rete. Tocca **Consenti** per continuare. Se per proteggere il tuo smartphone è stato impostato un metodo di autenticazione (come impronta digitale o codice PIN), dovrai utilizzarlo. Per rilevare l'accesso a domini non affidabili, Protezione web collabora con i servizi VPN.

Importante
Se ti trovi in un'area in cui l'uso di un servizio VPN è vietato per legge, la funzionalità Protezione web non sarà disponibile.

17.1. Avvisi di Bitdefender

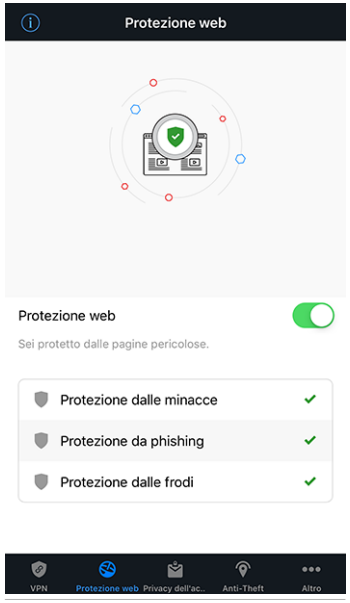
Ogni volta che visiti un sito web classificato come non sicuro, questo viene bloccato. Per informarti dell'evento, vieni avvisato da Bitdefender nel Centro notifiche e nel tuo browser. La pagina di avviso contiene informazioni come l'URL del sito web e la minaccia rilevata. Devi decidere la tua prossima azione.

Inoltre, nel Centro notifiche sarai avvisato ogni volta che una app meno sicura prova ad accedere a domini non affidabili. Tocca la notifica mostrata per essere reindirizzato alla finestra dove potrai decidere cosa fare.

Le seguenti opzioni sono disponibili per entrambi i casi:

- Allontanati dal sito web toccando **RIPORTAMI ALLA PROTEZIONE**.
- Procedi al sito web, malgrado l'avviso, toccando la notifica mostrata e poi su **Voglio accedere alla pagina**.

  Conferma la tua scelta.



Protezione web

17.2. Abbonamenti

Protezione web è una funzionalità su abbonamento con una possibilità di prova gratuita, così da decidere se soddisfa le proprie esigenze. Puoi scegliere fra due tipi di abbonamento: annuale e mensile.

Nel caso in cui l'abbonamento a Protezione web di Bitdefender fosse scaduto, non riceverai alcun avviso accedendo a contenuti dannosi.

Se hai acquistato uno dei pacchetti di Bitdefender, come Bitdefender Total Security, allora avrai accesso illimitato a Protezione web.

18. PRIVACY DELL'ACCOUNT

Privacy dell'account di Bitdefender rileva se si sono verificate perdite di dati negli account che utilizzi per fare pagamenti e acquisti online, o per accedere a diversi siti web e app online. I dati che potrebbero essere stati memorizzati in un account possono essere password, dati della carta di credito o informazioni bancarie, e, se non protetti correttamente, potrebbero verificarsi furti d'identità o invasioni alla privacy.

Lo stato della privacy di un account viene mostrato subito dopo la conferma.

Per verificare se un account è stato violato, tocca **Scansione per violazioni**.

Per iniziare a proteggere le informazioni personali:

1. Tocca l'icona nella parte inferiore della schermata.
2. Tocca **Aggiungi** nell'angolo in alto a destra della schermata.
3. Inserisci il tuo indirizzo e-mail nel campo corrispondente e tocca **Avanti**.

   Bitdefender deve confermare questo account prima di mostrare informazioni private. Inoltre, viene inviata un'e-mail con un codice di conferma all'indirizzo fornito.
4. Controlla la tua casella di posta e inserisci il codice che hai ricevuto nella sezione **Privacy dell'account** della tua app. Se non riesci a trovare l'e-mail di conferma nei tuoi messaggi in arrivo, controlla anche la cartella dello Spam.

   Viene mostrato lo stato della privacy dell'account confermato.

Se in uno degli account viene rilevata una violazione, ti consigliamo di modificarne la password il prima possibile. Per creare una password sicura, segui questi suggerimenti:

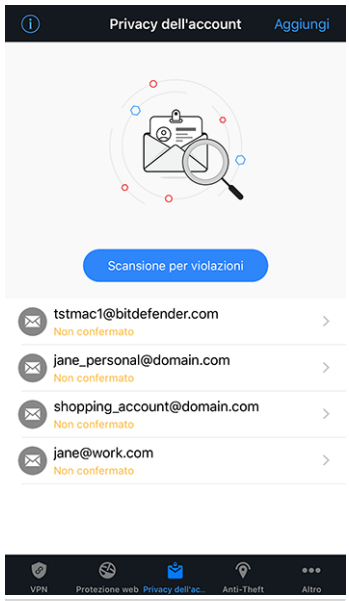
- Deve contenere almeno otto caratteri.
- Includi sia caratteri minuscoli che maiuscoli.
- Aggiungi almeno un numero o simbolo, come #, @, % or !.

Una volta protetto un account coinvolto in una violazione della privacy, puoi confermare le modifiche spuntando le fughe rilevate come **Risolto**. Per farlo:

1. Tocca ··· accanto all'account che hai appena protetto.
2. Tocca **Segna come risolto**.

L'account comparirà nell'elenco **RISOLTO**.

Quando tutte le violazioni rilevate sono state segnate come **Risolte**, l'account non apparirà più come violato, almeno fino al rilevamento di una nuova violazione.



Privacy dell'account

19. BITDEFENDER CENTRAL

Bitdefender Central è la piattaforma web 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 computer o dispositivo mobile connesso a internet, andando su https://central.bitdefender.com o direttamente dalla app Bitdefender Central sui dispositivi iOS e Android.

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 Mobile Security per Android
  - Bitdefender Mobile Security for iOS
  - Bitdefender Antivirus for Mac
  - Linea di prodotti Bitdefender per Windows
- Gestisci e rinnova i tuoi abbonamenti di Bitdefender.
- Aggiungi nuovi dispositivi alla tua rete e gestiscili ovunque ti trovi.

Accedere al tuo account Bitdefender

Ci sono due modi per accedere a Bitdefender Central

- 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 usando il tuo indirizzo e-mail e la tua 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.

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. Tocca l'icona nel lato destro superiore della schermata.
3. Tocca **account di Bitdefender** nel menu scorrevole.
4. Seleziona la scheda **Password e sicurezza**.
5. Tocca **Autenticazione a due fattori**.
6. Tocca **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. Tocca **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 computer, puoi aggiungere manualmente il codice mostrato.

Tocca **CONTINUA**.

c. Inserisci il codice fornito dalla app o quello mostrato nel passaggio precedente e poi tocca **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. Tocca **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. Tocca **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. Tocca **FATTO**.

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

1. Tocca **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.

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. Tocca l'icona nel lato destro superiore della schermata.
3. Tocca **account di Bitdefender** nel menu scorrevole.
4. Seleziona la scheda **Password e sicurezza**.
5. Tocca **Dispositivi affidabili**.
6. Viene mostrato l'elenco con i dispositivi su cui è stato installato Bitdefender. Tocca il dispositivo desiderato.

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

I miei dispositivi

L'area **I miei dispositivi** nel tuo account Bitdefender 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 identificare e gestire i tuoi dispositivi, puoi personalizzare il nome del dispositivo e creare o assegnare un proprietario a ciascuno di esso:

1. Tocca l'icona nell'angolo in alto a sinistra dello schermo e seleziona **I miei dispositivi**.
2. Tocca la scheda del dispositivo desiderato e poi l'icona nell'angolo in alto a destra dello schermo. Sono disponibili le seguenti opzioni:
   - **Impostazioni** - Qui puoi modificare il nome del dispositivo selezionato.
   - **Profilo** - Da qui è possibile assegnare un profilo al dispositivo selezionato. Tocca **Aggiungi proprietario** e poi compila i campi corrispondenti, impostando nome, indirizzo e-mail, numero di telefono, data di nascita e nel caso, aggiungendo un'immagine del profilo.
   - **Rimuovi** - Qui è possibile rimuovere un profilo con il relativo dispositivo assegnato dal tuo account di Bitdefender.

Accedere con un altro account di Bitdefender

Per accedere con un altro account di Bitdefender:

1. Tocca l'icona nella parte inferiore della schermata.

2. Tocca **Esci**.
3. Inserisci l'indirizzo e-mail e la password del tuo account di Bitdefender nei campi corrispondenti.
4. Tocca **ACCEDI**.

MOBILE SECURITY PER ANDROID

20. FUNZIONI DI PROTEZIONE

Bitdefender Mobile Security protegge il tuo dispositivo Android con le seguenti funzioni:

- Scansione malware
- Protezione web
- VPN
- Antifurto, incluso:
  - Localizzazione remota
  - Blocco remoto
  - Cancellazione remota
  - Avvisi in remoto
- Privacy dell'account
- Blocco App
- Rapporti
- WearON

Puoi usare gratuitamente le funzioni del prodotto per 14 giorni. Alla scadenza di tale periodo, devi acquistare la versione completa per proteggere il tuo dispositivo mobile.

21. COME INIZIARE

Requisiti dispositivo

Bitdefender Mobile Security funziona su qualsiasi dispositivo con Android 4.1 o superiore. Per la scansione minaccia nel cloud serve una connessione a internet attiva.

Installazione di Bitdefender Mobile Security

- **Da Bitdefender Central**
  - su Android
    1. Vai a: https://central.bitdefender.com.
    2. Accedi al tuo account di Bitdefender.
    3. Tocca ☰ nell'angolo in alto a sinistra della schermata e seleziona **I miei dispositivi**.
    4. Tocca **INSTALLA PROTEZIONE**, e poi tocca **Proteggi questo dispositivo**.
    5. Seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, tocca il pulsante corrispondente.
    6. Sarai reindirizzato all'applicazione **Google Play**. Nella schermata di Google Play, tocca l'opzione di installazione.
  - In Windows, macOS, iOS
    1. Vai a: https://central.bitdefender.com.
    2. Accedi al tuo account di Bitdefender.
    3. Premi ☰ nell'angolo in alto a sinistra dello schermo e seleziona **I miei dispositivi**.
    4. Premi **INSTALLA PROTEZIONE** e poi premi **Proteggi altri dispositivi**.
    5. Seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, premi il pulsante corrispondente.
    6. Premi **INVIA LINK DI DOWNLOAD**.
    7. Inserisci l'indirizzo email nel campo corrispondente e premi **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.

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

- **Da Google Play**

  Cerca Bitdefender Mobile Security per trovare e installare la app.

  In alternativa, inquadra il codice QR:

Codice QR

Prima di passare alle diverse fasi per la convalida, devi accettare l'Accordo di abbonamento. Prenditi qualche istante per leggere l'Accordo di abbonamento in quanto contiene i termini e le condizioni con cui è possibile utilizzare Bitdefender Mobile Security.

Tocca **CONTINUA** per passare alla finestra successiva.

Accedi al tuo account di Bitdefender

Per usare Bitdefender Mobile Security, devi collegare il tuo dispositivo a un account di Bitdefender o Facebook, Google o Microsoft, accedendo all'account direttamente dalla app. La prima volta che apri l'applicazione, ti sarà chiesto di accedere a un account.

Se hai installato Bitdefender Mobile Security dal tuo account Bitdefender, l'applicazione tenterà di accedere automaticamente a quell'account.

Per collegare il tuo dispositivo a un account di Bitdefender:

1. Inserisci l'indirizzo e-mail e la password del tuo account di Bitdefender nei campi corrispondenti. Se non hai un account di Bitdefender e vuoi crearne uno, seleziona il link corrispondente.
2. Tocca **ACCEDI**.

Per accedere utilizzando un account Facebook, Google o Microsoft, tocca il servizio che vuoi utilizzare dall'area **O ACCEDI CON**. Sarai reindirizzato alla pagina di accesso del servizio selezionato. Segui le istruzioni per collegare il tuo account a Bitdefender Mobile Security.

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

Configura la protezione

Una volta eseguito l'accesso alla app, comparirà la finestra **Configura la protezione**. Per proteggere il tuo dispositivo, ti consigliamo di seguire questi passaggi:

- **Stato dell'abbonamento.** Per usufruire della protezione di Bitdefender Mobile Security, devi attivare il tuo prodotto con un abbonamento, che indicherà per quanto tempo potrai utilizzarlo. Alla sua scadenza, l'applicazione smetterà di eseguire le sue funzioni e di proteggere il tuo dispositivo.

  Se hai un codice di attivazione, tocca **HO UN CODICE** e poi **ATTIVA**.

  Se hai eseguito l'accesso con un nuovo account di Bitdefender e non hai un codice di attivazione, puoi usare il prodotto per 14 giorni gratuitamente.
- **Protezione web.** Se il tuo dispositivo richiede l'accessibilità per attivare Protezione web, tocca **ATTIVA**. Sarai reindirizzato al menu Accessibilità. Tocca Bitdefender Mobile Security e poi attiva l'interruttore corrispondente.
- **Scansione malware.** Esegui una scansione unica per assicurarti che il tuo dispositivo sia privo di minacce. Per avviare il processo di scansione, tocca **ESAMINA ORA**.

  Non appena il processo di scansione inizierà, comparirà la dashboard. Qui puoi visualizzare lo stato di sicurezza del tuo dispositivo.

Dashboard

Tocca l'icona di Bitdefender Mobile Security nell'app drawer del dispositivo per aprire l'interfaccia dell'applicazione.

La dashboard offre informazioni sullo stato di sicurezza del tuo dispositivo e tramite Autopilot ti aiuta a migliorare la sicurezza del tuo dispositivo dandoti suggerimenti sulle varie funzionalità.

La scheda stato nella parte superiore della finestra ti informa sullo stato di sicurezza del dispositivo usando messaggi chiari e colori indicativi. Se Bitdefender Mobile Security non ha alcun avviso, la scheda dello stato è verde. Quando viene rilevato un problema di sicurezza, la scheda dello stato diventa rossa.

Per offrirti un funzionamento efficace e una maggiore protezione, eseguendo diverse attività, **Bitdefender Autopilot** si comporterà come un consulente di sicurezza personale. In base alle attività eseguite, sia che tu stia lavorando o effettuando pagamenti online, Bitdefender Autopilot ti fornirà suggerimenti contestuali basati sull'uso e le esigenze del tuo dispositivo. Ciò ti aiuterà a scoprire e usufruire dei vantaggi offerti dalle funzionalità incluse nella app Bitdefender Mobile Security.

Ogni volta che vi è un processo in esecuzione o una funzione richiede un tuo intervento, nell'interfaccia viene mostrata una scheda con maggiori informazioni e le possibili azioni.

Puoi accedere alle funzionalità di Bitdefender Mobile Security e selezionarle facilmente dalla barra di navigazione in basso:

Scansione malware
Ti consente di avviare una scansione a richiesta e attivare la funzione Esamina la memoria. Per maggiori informazioni, fai riferimento a «*Scansione malware*» (p. 285).

Protezione web
Assicura una navigazione sicura, avvisandoti in caso di eventuali pagine web potenzialmente dannose. Per maggiori informazioni, fai riferimento a «*Protezione web*» (p. 288).

VPN
Cifra le comunicazioni via Internet, aiutandoti a mantenere la tua privacy, indipendentemente dalla rete a cui sei connesso. Per maggiori informazioni, fai riferimento a «*VPN*» (p. 290).

Antifurto
Ti consente di attivare o disattivare le funzioni antifurto e di configurarne le relative impostazioni. Per maggiori informazioni, fai riferimento a «*Funzioni Antifurto*» (p. 293).

Privacy dell'account
Verifica se nei tuoi account online si è verificata un'eventuale violazione dei dati. Per maggiori informazioni, fai riferimento a «*Privacy dell'account*» (p. 297).

Blocco App
Ti consente di proteggere le applicazioni installate impostando un codice di accesso PIN. Per maggiori informazioni, fai riferimento a «*Blocco App*» (p. 299).

Rapporti
Salva un registro di tutte le azioni importanti, i cambiamenti di stato e gli altri messaggi critici relativi alle attività del tuo dispositivo. Per maggiori informazioni, fai riferimento a «*Rapporti*» (p. 304).

WearON
Comunica con il tuo smartwatch per aiutarti a trovare il telefono nel caso l'avessi smarrito o dimenticato dove l'hai lasciato. Per maggiori informazioni, fai riferimento a «*WearON*» (p. 305).

22. SCANSIONE MALWARE

Bitdefender protegge il tuo dispositivo e i tuoi dati da applicazioni dannose usando una scansione all'installazione e a richiesta.

Nota
Assicurati che il tuo dispositivo sia connesso a internet. Se il dispositivo non è connesso a internet, la scansione non inizierà.

- **Scansione all'installazione**

  Ogni volta che installi un'applicazione, Bitdefender Mobile Security la controlla con una scansione che sfrutta la tecnologia in-the-cloud. Lo stesso processo di scansione viene avviato ogni volta che le app installate sono aggiornate.

  Se l'applicazione viene giudicata pericolosa, un avviso ti segnalerà di disinstallarla. Tocca **Disinstalla** per accedere alla schermata di disinstallazione dell'applicazione.

- **Scansione a richiesta**

  Ogni volta che vuoi assicurarti che le applicazioni installate sul dispositivo siano sicure, puoi avviare una scansione a richiesta.

  Per avviare una Scansione a richiesta:

  1. Tocca **Scansione malware** nella barra di navigazione in basso.
  2. Tocca **AVVIA SCANSIONE**.

  Nota
  In Android 6, per la funzione Scansione malware sono richiesti alcuni permessi aggiuntivi. Dopo aver toccato il pulsante **AVVIA SCANSIONE**, seleziona **Consenti** per le seguenti opzioni:

  - Consenti ad **Antivirus** di effettuare e gestire le chiamate?
  - Consenti ad **Antivirus** di accedere foto, filmati e file sul tuo dispositivo?

  Puoi visualizzare l'avanzamento della scansione ed eventualmente fermarla in qualsiasi momento.

Scansione malware

Di norma, Bitdefender Mobile Security esaminerà la memoria di archiviazione interna del dispositivo, incluso eventuali schede SD inserite. In questo modo, qualsiasi applicazione pericolosa che potrebbe trovarsi sulla scheda può essere rilevata prima ancora di provocare danni.

Per disattivare la funzione Esamina la memoria:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Impostazioni**.
3. Disattiva l'interruttore **Esamina la memoria** nell'area Scansione malware.

Se viene rilevata un'eventuale applicazione dannosa, saranno mostrate ulteriori informazioni e potrai rimuoverla, toccando il pulsante **DISINSTALLA**.

La scheda Scansione malware mostra lo stato del tuo dispositivo. Quando il dispositivo è protetto, la scheda è verde. Mentre diventerà rossa, se il

dispositivo richiede una scansione o in caso di eventuali azioni che necessitano di un tuo intervento.

Se la tua versione di Android è 7.1 o superiore, puoi accedere a un collegamento a Malware Scanner così da poter eseguire scansioni più velocemente, senza aprire l'interfaccia di Bitdefender Mobile Security. Per farlo, tieni premuta l'icona di Bitdefender nella schermata Home o nel drawer Applicazioni, e seleziona l'icona .

23. PROTEZIONE WEB

Utilizzando i servizi cloud di Bitdefender, Sicurezza Web esamina le pagine we a cui accedi con il portale predefinito di Android, Google Chrome, Firefox, Opera, Opera Mini e Dolphin. Un elenco completo dei browser supportati è disponibile nella sezione Sicurezza Web.

Se un URL porta a un sito web dannoso o noto per problemi di phishing, oppure a contenuti pericolosi come spyware o virus, la pagina web viene bloccata e compare un avviso.

Puoi scegliere di ignorare l'avviso e accedere alla pagina web o tornare a una pagina sicura.

Nota

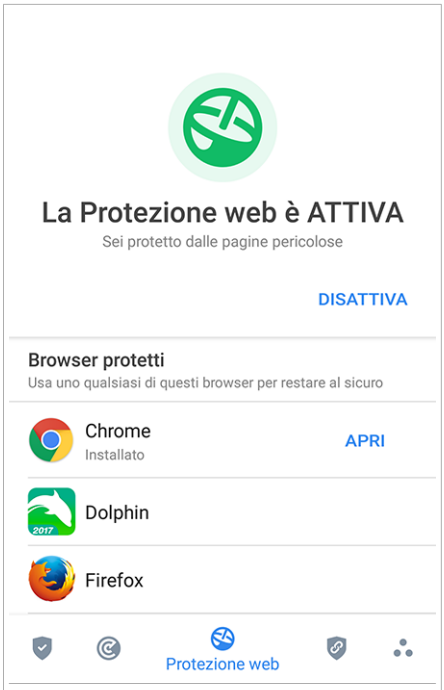
In Android 6, per la funzione Sicurezza Web sono richiesti alcuni permessi aggiuntivi.

Consenti di registrare il servizio di accessibilità e tocca **ATTIVA** quando richiesto. Tocca **Antivirus** e attiva l'interruttore, poi conferma che sei d'accordo con l'accesso al permesso del dispositivo.

Protezione web di Bitdefender è impostata per avvisarti di utilizzare Bitdefender VPN ogni volta che accedi a un sito bancario. La notifica compare nella barra di stato. Ti consigliamo di usare Bitdefender VPN mentre sei connesso al tuo account bancario così da proteggere i tuoi dati da potenziali violazioni di sicurezza.

Per disattivare la notifica di Protezione web:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Impostazioni**.
3. Disattiva il corrispondente interruttore nell'area Protezione web.



Protezione web

24. VPN

Con Bitdefender VPN puoi mantenere privati i tuoi dati ogni volta che ti connetti a reti wireless non protette mentre sei in aeroporti, centri commerciali, bar o alberghi. In questo modo, è possibile evitare situazioni spiacevoli, come furti di dati personali o tentativi di rendere accessibile il tuo indirizzo IP a pirati informatici.

Il VPN opera come una sorta di tunnel tra il tuo dispositivo e la rete a cui ti connetti, proteggendo la tua connessione, cifrando i dati usando una cifratura di tipo bancario e nascondendo il tuo indirizzo IP, ovunque ti trovi. Il tuo traffico viene reindirizzato a un server indipendente, rendendo quindi il tuo dispositivo quasi impossibile da identificare tra la miriade di altri dispositivi che stanno usando i nostri servizi. Inoltre, mentre ti connetti a Internet tramite 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 provi a utilizzare la funzionalità VPN di Bitdefender per la prima volta. Continuando a utilizzare tale funzionalità, confermi di essere a conoscenza dei regolamenti applicabili nel paese in cui ti trovi e dei rischi a cui potresti incorrere.

Ci sono due modi per attivare o disattivare Bitdefender VPN:

- Tocca **CONNETTI** nella scheda VPN della Dashboard.

  Viene mostrato lo stato di Bitdefender VPN.

- Tocca **VPN** nella barra di navigazione in basso, e poi tocca **CONNETTI**.

  Tocca **CONNETTI** ogni volta che vuoi restare protetto mentre sei conesso a reti wireless non affidabili.

  Tocca **DISCONNETTI** ogni volta che vuoi disattivare la connessione.

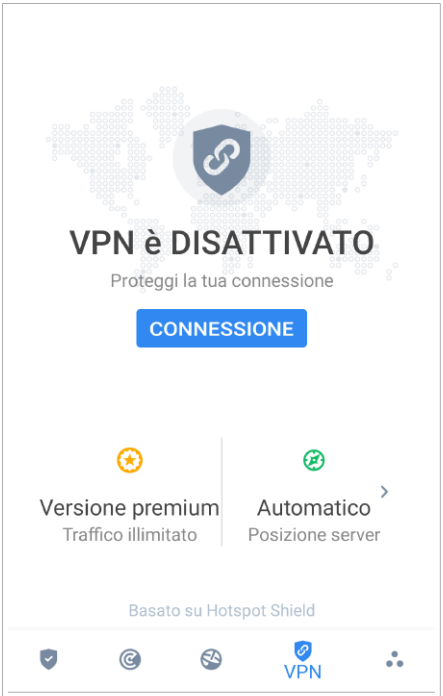
Nota
La prima volta che attivi VPN, ti verrà chiesto di consentire a Bitdefender di impostare una connessione VPN, che monitorerà il traffico di rete. Tocca **OK** per continuare.

Se la tua versione di Android è 7.1 o superiore, puoi accedere a un collegamento a Bitdefender VPN così da poter eseguire scansioni più velocemente, senza aprire l'interfaccia di Bitdefender Mobile Security. Per farlo, tieni premuta l'icona di Bitdefender nella schermata Home o nel drawer Applicazioni, e seleziona l'icona .

L'icona compare nella barra di stato quando Bitdefender VPN è attivo.

Per risparmiare la batteria, ti consigliamo di disattivare la funzionalità VPN quando non ti serve.

Se vuoi connetterti a un server a tua scelta, tocca **Posizione server** nell'interfaccia di VPN e seleziona la posizione desiderata.



VPN

Impostazioni VPN

Per una configurazione avanzata della tua VPN:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Impostazioni**.

Nell'area VPN, puoi configurare le seguenti opzioni:

- Accesso rapido a VPN - Nella barra di stato del tuo dispositivo comparirà una notifica per consentirti di attivare rapidamente VPN.
- Rete Wi-Fi aperta - Ogni volta che ti connetti a una rete Wi-Fi aperta, ti verrà segnalato nella barra di stato del tuo dispositivo di usare VPN.

25. FUNZIONI ANTIFURTO

Bitdefender può aiutarti a localizzare il tuo dispositivo e impedire che i tuoi dati personali finiscano nelle mani sbagliate.

Tutto ciò che devi fare è attivare Anti-Theft dal dispositivo e, quando necessario, accedere a **Bitdefender Central** da un qualsiasi browser web, ovunque ti trovi.

Bitdefender Mobile Security offre le seguenti funzioni Antifurto:

Localizzazione remota

Scopri la posizione attuale del tuo dispositivo su Google Maps. La posizione è aggiornata ogni 5 secondi, in modo da poterlo rintracciare, se è in movimento.

L'accuratezza della posizione dipende da come Bitdefender può rilevarla:

- Se nel dispositivo il GPS è attivato, la sua posizione può essere determinata con un'accuratezza di un paio di metri, finché resta nel raggio dei satelliti GPS (ad esempio, non dentro a un edificio).
- Se il dispositivo è in un edificio, la sua posizione può essere determinata entro decine di metri, se il Wi-Fi è attivato e ci sono reti wireless disponibili nel suo raggio d'azione.
- Diversamente, la posizione sarà determinata usando solo le informazioni dalla rete mobile, che offrono un'accuratezza non superiore a diverse centinaia di metri.

Blocco remoto

Blocca lo schermo del dispositivo e imposta un codice PIN per sbloccarlo.

Cancellazione remota

Rimuovi tutti i dati personali dal dispositivo che hai smarrito.

Invia avviso al disp. (Scream)

Invia un messaggio in remoto che comparirà sullo schermo del dispositivo oppure fallo suonare.

Se perdi il dispositivo, puoi indicare a chi lo trova come restituirlo, facendo comparire un messaggio sul suo schermo.

Se hai smarrito il tuo dispositivo e probabilmente non è molto lontano (ad esempio, da qualche parte in casa o in ufficio), quale modo migliore

di ritrovarlo, se non farlo suonare? Il dispositivo emetterà un suono, anche se è in modalità silenziosa.

Attivare Antifurto

Per attivare le funzioni dell'Anti-Theft, completa semplicemente la fase di configurazione dalla scheda Anti-Theft, disponibile nell'interfaccia.

In alternativa, puoi attivare l'Anti-Theft seguendo questi passaggi:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Anti-Theft**.
3. Tocca **ATTIVA**.
4. Per aiutarti ad attivare questa funzione, sarà attivata la seguente procedura:

   Nota
   In Android 6, la funzione Anti-Theft richiede alcuni permessi aggiuntivi. Per attivare l'opzione, segui questi passaggi:

   a. Tocca **Attiva Anti-Theft** e poi tocca **ATTIVA**.

   b. Consenti all'**Antivirus** di accedere alla posizione del tuo dispositivo.

   a. **Dai privilegi di amministratore**

      Questi privilegi sono essenziali per il funzionamento del modulo Anti-Theft e per continuare è necessario assegnarli.

   b. **Imposta PIN applicazione**

      Per impedire l'accesso non autorizzato al tuo dispositivo, occorre impostare un codice PIN. Ad ogni tentativo di accesso, sarà necessario inserire il PIN. In alternativa, su dispositivi che supportano l'autenticazione tramite impronte digitali, potrà essere utilizzata una conferma tramite impronta digitale invece del codice PIN configurato.

      Lo stesso codice PIN viene usato da Blocco App per proteggere le tue applicazioni installate.

   c. **Attiva Scatta foto**

Ogni volta che qualcuno tenta di sbloccare il tuo dispositivo senza successo con l'opzione Scatta foto attiva, Bitdefender gli scatterà una foto.

Più precisamente, ogni volta che si sbaglia per tre volte di fila a digitare il codice PIN o la password o a confermare l'impronta digitale impostati per proteggere la app, la fotocamera frontale scatta una foto. La foto viene salvata con tanto di indicazione e ora e può essere vista quando si apre Bitdefender Mobile Security la finestra Antifurto. In alternativa, puoi visualizzare la foto scattata nel tuo account di Bitdefender:

i. Vai a: https://central.bitdefender.com.

ii. Accedi al tuo account.

iii. Tocca nell'angolo in alto a sinistra della schermata e seleziona **I miei dispositivi**.

iv. Seleziona il tuo dispositivo Android, quindi la scheda **Anti-Theft**.

v. Tocca accanto a **Controlla le tue fotografie** per vedere le ultime foto scattate.

Vengono salvate solo le due foto più recenti.

Una volta attivata la funzionalità Anti-Theft, puoi attivare o disattivare i comandi del Controllo web individualmente dalla finestra Anti-Theft toccando le opzioni corrispondenti.

Utilizzare le funzioni Anti-Theft da Bitdefender Central

Nota
Tutte le funzioni di Anti-Theft richiedono che l'opzione **Dati in background** sia attivata nelle impostazioni di utilizzo dei dati del dispositivo.

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

1. Accedi a Bitdefender Central.
2. Tocca nell'angolo in alto a sinistra della schermata e seleziona **I miei dispositivi**.
3. Nella finestra **I MIEI DISPOSITIVI**, seleziona la scheda del dispositivo selezionato.

4. Seleziona la scheda **Anti-Theft**.
5. Nel campo inferiore della finestra, tocca ··· e poi il pulsante corrispondente alla funzionalità che vuoi utilizzare:

   Localizza - Mostra la posizione del dispositivo su Google Maps.

   Avviso - Digita un messaggio da far comparire sul dispositivo e/o fai suonare un allarme.

   Blocca - Blocca il dispositivo e imposta un codice PIN per sbloccarlo.

   Cancella - Elimina tutti i dati dal dispositivo.

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

   MOSTRA IP - Mostra l'ultimo indirizzo IP per il dispositivo selezionato.

Impostazioni Anti-Theft

Se desideri attivare o disattivare i comandi remoti:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Anti-Theft**.
3. Attiva o disattiva le opzioni desiderate.

26. PRIVACY DELL'ACCOUNT

Privacy dell'account di Bitdefender rileva se si sono verificate violazioni di dati negli account che utilizzi per fare pagamenti e acquisti online, o per accedere a diversi siti web e app online. I dati che potrebbero essere stati memorizzati in un account possono essere password, dati della carta di credito o informazioni bancarie, e, se non protetti correttamente, potrebbero verificarsi furti d'identità o invasioni alla privacy.

Lo stato della privacy di un account viene mostrato subito dopo la conferma.

Vengono impostati nuovi controlli automatici in background, ma è anche possibile eseguire scansioni manuali su base giornaliera.

Le notifiche saranno mostrate ogni volta che vengono scoperte nuove violazioni che includono uno degli account e-mail verificati.

Per iniziare a proteggere le informazioni personali:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Privacy account**.
3. Tocca **COME INIZIARE**.
4. Compare l'indirizzo e-mail usato per creare il tuo account Bitdefender.

   Tocca **AGGIUNGI** per continuare.

   Bitdefender deve confermare questo account prima di mostrare informazioni private. Inoltre, viene inviata un'e-mail con un codice di conferma all'indirizzo fornito.
5. Controlla la tua casella di posta e inserisci il codice che hai ricevuto nella sezione **Privacy dell'account** della tua app. Se non riesci a trovare l'e-mail di conferma nei tuoi messaggi in arrivo, controlla la cartella dello Spam.

   Viene mostrato lo stato della privacy dell'account confermato.

   Per aggiungere altri account, tocca **AGGIUNGI ACCOUNT** nella finestra Privacy account e segui i passaggi necessari.

Se in uno degli account viene rilevata una violazione, ti consigliamo di modificarne la password il prima possibile. Per creare una password sicura, segui questi suggerimenti:

- Deve contenere almeno otto caratteri.

- Includi sia caratteri minuscoli che maiuscoli.
- Aggiungi almeno un numero o simbolo, come #, @, % or !.

Una volta protetto un account coinvolto in una violazione della privacy, puoi confermare le modifiche spuntando le violazioni rilevate come **Risolto**. Per farlo:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Privacy account**.
3. Tocca l'account che hai appena protetto.
4. Tocca la violazione da cui hai protetto l'account.
5. Tocca **RISOLTO** per confermare che l'account è protetto.

Quando tutte le violazioni rilevate sono state segnate come **Risolte**, l'account non apparirà più come violato, almeno fino al rilevamento di una nuova violazione.

Per smettere di essere avvisati ogni volta che vengono eseguite scansioni automatiche:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Impostazioni**.
3. Disattiva l'interruttore corrispondente nell'area Privacy account.

27. BLOCCO APP

Le applicazioni installate, così come e-mail, foto o messaggi, possono includere dati personali che si desidera mantenere privati, limitando l'accesso ad essi in modo selettivo.

App Lock consente di bloccare l'accesso non autorizzato alle applicazioni, impostando un codice di accesso PIN. Il codice PIN impostato deve essere di almeno 4 cifre ma non più lungo di 8, ed è richiesto ogni volta che si vuole accedere alle applicazioni con restrizioni selezionate.

In alternativa, su dispositivi che supportano l'autenticazione tramite impronte digitali, potrà essere utilizzata una conferma tramite impronta digitale invece del codice PIN configurato.

Attivare Blocco App

Per limitare l'accesso alle applicazioni selezionate, configura Blocco App dalla scheda visualizzata nell'interfaccia, dopo aver attivato l'Anti-Theft.

In alternativa, puoi attivare Blocco App seguendo questi passaggi:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Blocco App**.
3. Tocca **ATTIVA**.
4. Consente a Bitdefender di accedere ai dati di utilizzo.

   Nota
   In Android 6, per la funzione Scatta foto sono richiesti alcuni permessi aggiuntivi.
   Per attivarla, consenti all'**Antivirus** di scattare foto e registrare video.

5. Torna alla app, configura il codice d'accesso e poi tocca **IMPOSTA PIN**.

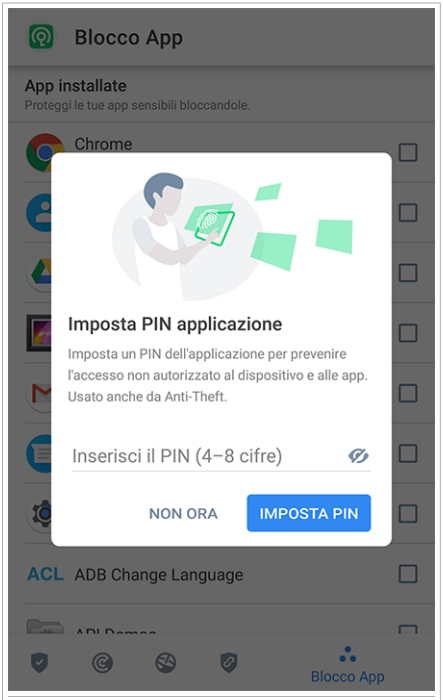
   Nota
   Questo passaggio è disponibile solo se non hai configurato in precedenza il PIN in Anti-Theft.

6. Attiva l'opzione Scatta foto per catturare un'immagine di chiunque cercherà di accedere ai tuoi dati privati.

7. Seleziona le app che vuoi proteggere.

Utilizzando un PIN o un'impronta digitale errata per cinque volte di fila, si attiverà una sessione di tempo massimo consentito di 30 secondi. In questo modo, sarà bloccato ogni tentativo di accedere alle app protette.

Nota
Lo stesso codice PIN viene usato da Antifurto per aiutarti a localizzare il tuo dispositivo.



Blocco App

Modalità Blocco

La prima volta che aggiungi una app a Blocco App, compare la schermata della modalità Blocco App. Da qui puoi scegliere quando la funzionalità Blocco App deve proteggere le applicazioni installate sul tuo dispositivo.

Puoi selezionare una delle seguenti opzioni:

- **Richiede uno sblocco ogni volta** - Ogni volta che si accede alle app bloccate, dovrà essere utilizzato il codice PIN o l'impronta digitale impostati.
- **Mantieni sbloccato fino allo spegnimento dello schermo** - L'accesso alle tue app sarà valido fino a quando lo schermo non si spegnerà.
- **Blocca dopo 30 secondi** - Puoi uscire e accedere di nuovo alle app sbloccate entro 30 secondi.

Se vuoi cambiare l'impostazione selezionata:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Impostazioni**.
3. Tocca **Richiede uno sblocco ogni volta** nell'area Blocco App.
4. Scegli l'opzione desiderata.

Impostazioni Blocco App

Per una configurazione avanzata di Blocco App:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Impostazioni**.

Nell'area Blocco App, puoi configurare le seguenti opzioni:

- **Suggerimento app sensibile** - Ricevi una notifica di blocco ogni volta che stai installato una app sensibile.
- **Richiede una sblocco ogni volta** - Scegli una delle opzioni di blocco e sblocco disponibili.
- **Sblocco rapido** - Mantieni le app sbloccate finché sei connesso a una rete Wi-Fi affidabile.
- **Tastiera casuale** - Impedisce la lettura del PIN rendendo casuale le posizioni dei numeri.

Scatta foto

Con Scatta foto di Bitdefender, puoi cogliere sul fatto amici o parenti, evitando che i loro occhi curiosi sbircino i tuoi file o le app che utilizzi.

Il suo funzionamento è davvero semplice: ogni volta che si sbaglia per tre volte di fila a digitare il codice PIN o a confermare l'impronta digitale impostati per proteggere la app, la fotocamera frontale scatta una foto. La foto viene salvata con tanto di indicazione e ora e può essere vista quando si apre Bitdefender Mobile Security e si accede alla funzione Blocco App.

Nota
Questa funzionalità è disponibile solo per telefoni dotati di una fotocamera frontale.

Per configurare la funzione Scatta foto di Blocco App:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Impostazioni**.
3. Attiva l'interruttore corrispondente nell'area Scatta foto.

Le foto scattate in caso di inserimento di un PIN errato sono mostrate nella finestra di Blocco App e possono essere visualizzate a schermo intero.

In alternativa, possono essere visualizzati nel tuo account di Bitdefender:

1. Vai a: https://central.bitdefender.com.
2. Accedi al tuo account.
3. Tocca nell'angolo in alto a sinistra della schermata e seleziona **I miei dispositivi**.
4. Seleziona il tuo dispositivo Android, quindi la scheda **Anti-Theft**.
5. Tocca accanto a **Controlla le tue fotografie** per vedere le ultime foto scattate.

Vengono salvate solo le due foto più recenti.

Per fermare l'invio delle foto scattate sul tuo account Bitdefender:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Impostazioni**.
3. Disattiva **Carica foto** nell'area Scatta foto.

Sblocco rapido

Un metodo semplice per evitare che la funzione Blocco App richieda l'inserimento del codice PIN o la conferma dell'impronta digitale per le app protette ogni volta che si accede, basta attivare Sblocco rapido.

Con Sblocco rapido, puoi impostare come affidabili le reti Wi-Fi a cui ti connetti di solito e ogni volta che le userai, le impostazioni di blocco di Blocco App saranno disattivate per le app protette.

Per configurare la funzione Sblocco rapido:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Blocco App**.
3. Tocca **AGGIUNGI** per impostare come affidabile la connessione Wi-Fi attualmente usata.

Nota
Questa impostazione è disponibile solo se la funzione Sblocco rapido è stata attivata.

Nel caso si cambiasse idea, basterà disattivare la funzione e le reti Wi-Fi impostate come affidabili saranno trattate come se non lo fossero.

28. RAPPORTI

Nei Rapporti, è possibile trovare un registro dettagliato degli eventi inerenti le attività di scansione sul proprio dispositivo.

Ogni volta che si verifica qualcosa di rilevante per la sicurezza del dispositivo, un nuovo messaggio viene aggiunto ai Rapporti.

Per accedere alla sezione Rapporti:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Rapporti**.

Nella finestra Rapporti, sono disponibili le seguenti schede:

- **RAPPORTI SETTIMANALI** - Qui puoi accedere allo stato della protezione e le attività eseguite nella settimana attuale e in quella precedente. Il rapporto della settimana viene generato ogni domenica e quando sarà disponibile, riceverai una notifica.

  In questa sezione, ogni settimana troverai un nuovo suggerimento, perciò assicurati di visitarla regolarmente per sfruttare al massimo la tua app.

  Per non ricevere più notifiche ogni volta che viene generato un rapporto:

  1. Tocca **Altro** nella barra di navigazione in basso.
  2. Tocca **Impostazioni**.
  3. Disattiva l'interruttore **Notifica nuovo rapporto** nell'area Rapporti.

- **RAPPORTO ATTIVITÀ** - Qui puoi verificare maggiori informazioni sulle attività della tua app Bitdefender Mobile Security da quando è stata installata sul tuo dispositivo Android.

  Per eliminare il rapporto attività disponibile:

  1. Tocca **Altro** nella barra di navigazione in basso.
  2. Tocca **Impostazioni**.
  3. Tocca **Cancella rapporto attività** e poi tocca **AZZERA**.

29. WEARON

Con WearON di Bitdefender, puoi trovare facilmente il tuo smartphone, nel caso l'avessi dimenticato in una sala riunioni in ufficio o su un cuscino del divano a casa. Il dispositivo può essere trovato anche se è in modalità silenziosa.

Mantieni questi funzione attivata per assicurarti di avere il tuo smartphone sempre a portata di mano.

Nota
La funzione richiede Android 4.3 e Android Wear.

Attivare WearON

Per usare WearON, devi solo connettere il tuo smartwatch all'applicazione Bitdefender Mobile Security e attivare la funzione con il seguente comando vocale:

Start:<Where is my phone>

Bitdefender WearON ha due comandi:

1. **Phone Alert**

   Con la funzione Phone Alert, puoi trovare rapidamente il tuo smartphone ogni volta che ti allontani troppo da lui.

   Se hai il tuo smartwatch con te, rileverà automaticamente la app sul tuo telefono vibrando ogni volta che sarà troppo distante e i dispositivi perderanno la connessione Bluetooth.

   Per attivare questa funzione, apri Bitdefender Mobile Security, tocca **Impostazioni generali** nel menu e seleziona l'interruttore corrispondente sotto la sezione WearON.

2. **Allarme**

   Trovare il tuo telefono non è mai stato così semplice. Ogni volta che hai dimenticato dove l'hai lasciato, tocca il comando Avvertimento sul tuo orologio, per far emettere un suono al tuo telefono.

30. INFO

Per trovare informazioni sulla versione di Bitdefender Mobile Security che hai installato, accedere e consultare l'Accordo di abbonamento e l'Informativa sulla privacy, e visualizzare le licenze open source:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Impostazioni**.
3. Tocca l'opzione desiderata nell'area Informazioni.

31. BITDEFENDER CENTRAL

Bitdefender Central è la piattaforma web 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 computer o dispositivo mobile connesso a internet, andando su https://central.bitdefender.com o direttamente dalla app Bitdefender Central sui dispositivi iOS e Android.

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 Mobile Security
  - Bitdefender Mobile Security for iOS
  - Bitdefender Antivirus for Mac
  - Linea di prodotti Bitdefender per Windows
- Gestisci e rinnova i tuoi abbonamenti di Bitdefender.
- Aggiungi nuovi dispositivi alla tua rete e gestiscili ovunque ti trovi.
- Proteggi i dispositivi nella rete e i loro dati da perdite o furti con la funzione Anti-Theft.

Accedere al tuo account Bitdefender

Ci sono due modi per accedere a Bitdefender Central

- 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 usando il tuo indirizzo e-mail e la tua 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.

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. Tocca l'icona nel lato destro superiore della schermata.
3. Tocca **account di Bitdefender** nel menu scorrevole.
4. Seleziona la scheda **Password e sicurezza**.
5. Tocca **Autenticazione a due fattori**.
6. Tocca **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. Tocca **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 computer, puoi aggiungere manualmente il codice mostrato.

   Tocca **CONTINUA**.

c. Inserisci il codice fornito dalla app o quello mostrato nel passaggio precedente e poi tocca **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. Tocca **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. Tocca **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. Tocca **FATTO**.

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

1. Tocca **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.

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. Tocca l'icona nel lato destro superiore della schermata.
3. Tocca **account di Bitdefender** nel menu scorrevole.
4. Seleziona la scheda **Password e sicurezza**.
5. Tocca **Dispositivi affidabili**.
6. Viene mostrato l'elenco con i dispositivi su cui è stato installato Bitdefender. Tocca il dispositivo desiderato.

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

I miei dispositivi

L'area **I MIEI DISPOSITIVI** nel tuo account Bitdefender 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 identificare facilmente i tuoi dispositivi, puoi personalizzarne il nome:

1. Accedi a Bitdefender Central.
2. Tocca nell'angolo in alto a sinistra della schermata e seleziona **I miei dispositivi**.
3. Tocca la scheda del dispositivo desiderato e poi tocca nell'angolo in alto a destra dello schermo.
4. Seleziona **Impostazioni**.
5. Inserisci un nuovo nome nel campo **Nome dispositivo** e seleziona **SALVA**.

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

1. Accedi a Bitdefender Central.

2. Tocca ☰ nell'angolo in alto a sinistra della schermata e seleziona **I miei dispositivi**.
3. Tocca la scheda del dispositivo desiderato e poi tocca ⋮ nell'angolo in alto a destra dello schermo.
4. Seleziona **Profilo**.
5. Tocca **Aggiungi proprietario**, poi compila i campi corrispondenti. Personalizza il profilo aggiungendo una foto e selezionando una data di nascita.
6. Tocca **AGGIUNGI** per salvare il profilo.
7. Seleziona il proprietario desiderato dall'elenco **Proprietario dispositivo** e tocca **ASSEGNA**.

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

Una volta selezionata la 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, tocca la 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 una scansione sul dispositivo in modalità remota. Tocca il pulsante **ESAMINA** 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.
- **Anti-Theft**. Nel caso smarrissi il tuo dispositivo, con la funzione Anti-Theft puoi localizzarlo e sfruttare alcune azioni in remoto. Tocca **LOCALIZZA** per rilevare la posizione del dispositivo. Sarà mostrata l'ultima posizione

nota, accompagnata da ora e data. Per maggiori dettagli su questa funzione, fai riferimento a «*Funzioni Antifurto*» (p. 293).

I miei abbonamenti

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

Controllare gli abbonamenti disponibili

Per controllare gli abbonamenti disponibili:

1. Accedi a Bitdefender Central.
2. Tocca ☰ nell'angolo in alto a sinistra dello schermo e seleziona **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.

Aggiungi un nuovo dispositivo

Se l'abbonamento copre più di un dispositivo, è possibile aggiungerne un altro e installare Bitdefender Mobile Security su di esso, come descritto in «Installazione di Bitdefender Mobile Security» (p. 280).

Rinnova abbonamento

Se mancano meno di 30 giorni alla scadenza del tuo abbonamento e hai optato per il rinnovo automatico, puoi comunque rinnovarlo manualmente seguendo questi passaggi:

1. Accedi a Bitdefender Central.
2. Tocca ☰ nell'angolo in alto a sinistra dello schermo e seleziona **I miei abbonamenti**.
3. Seleziona la scheda di abbonamento desiderata.
4. Tocca **RINNOVA** per continuare.

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

32. DOMANDE FREQUENTI

Perché Bitdefender Mobile Security richiede una connessione a internet?

L'applicazione deve comunicare con i server di Bitdefender per determinare lo stato della sicurezza delle applicazioni che controlla e delle pagine web visitate, ma anche per ricevere comandi dal tuo account Bitdefender, quando si utilizzano le funzioni Antifurto.

A cosa serve ogni permesso di Bitdefender Mobile Security?

- Accesso a Internet -> usato per la comunicazione con il cloud.
- Valutazione dello stato del telefono e dell'identità -> Usata per rilevare se il dispositivo è connesso a internet e per estrapolare determinate informazioni necessarie a creare un ID univoco per comunicare con il cloud di Bitdefender.
- Lettura e scrittura segnalibri del browser -> Il modulo Protezione web elimina i siti dannosi dalla cronologia.
- Lettura dati del registro -> Bitdefender Mobile Security rileva tracce di attività minacciose dai registri di Android.
- Posizione -> Richiesta per localizzazione remota.
- Fotocamera -> richiesta per Scatta foto.
- Memoria -> usata per consentire a Scansione malware di esaminare la scheda SD.

Come posso smettere di inviare a Bitdefender informazioni sulle app sospette?

Di norma, Bitdefender Mobile Security invia rapporti ai server di Bitdefender su app sospette che stai installando. Queste informazioni sono essenziali per migliorare il rilevamento delle minacce e possono aiutarci a offrirti un'esperienza migliore in futuro. Nel caso volessi interrompere l'invio di queste informazioni sulle app sospette:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Impostazioni**.
3. Disattiva il **Rilevamento in-the-cloud** nell'area Scansione malware.

Dove posso vedere maggiori dettagli sulle attività dell'app?

Bitdefender Mobile Security salva un rapporto di tutte le azioni importanti, i cambiamenti di stato e gli altri messaggi critici relativi alle sue attività. Per accedere e visualizzare le attività della app:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Rapporti**.

   Nella finestra RAPPORTI SETTIMANALI puoi accedere ai rapporti che vengono generati ogni settimana, mentre nella finestra RAPPORTO ATTIVITÀ puoi visualizzare maggiori informazioni sulle attività della tua app di Bitdefender.

Ho dimenticato il codice PIN impostato per proteggere la mia applicazione. What do I do?

1. Accedi a Bitdefender Central.
2. Tocca nell'angolo in alto a sinistra della schermata e seleziona **I miei dispositivi**.
3. Tocca la scheda del dispositivo desiderato e poi tocca nell'angolo in alto a destra dello schermo.
4. Seleziona **Impostazioni**.
5. Recupera il codice PIN dal campo **PIN per l'applicazione**.

Come posso modificare il codice PIN impostato per Blocco App e Anti-Theft?

Se desideri modificare il codice PIN impostato per Blocco App e Anti-Theft:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Impostazioni**.
3. Tocca **CODICE PIN** di sicurezza nell'area Anti-Theft.
4. Inserisci il codice PIN attuale.
5. Inserisci il nuovo codice PIN che vuoi impostare.

Come posso disattivare la funzionalità Blocco App?

Non c'è un'opzione per disattivare direttamente l'opzione Blocco app, ma puoi facilmente disattivarla togliendo la spunta delle caselle accanto alle app, dopo aver confermato il PIN o le impronte digitali impostate.

Come posso impostare un'altra rete wireless come affidabile?

Per iniziare, devi connettere il tuo dispositivo alla rete wireless che vuoi impostare come affidabile. Segui questi passaggi:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca **Blocco App**.
3. Tocca nell'angolo in alto a destra.
4. Tocca **AGGIUNGI** accanto alla rete che vuoi impostare come affidabile.

Come posso smettere di vedere le fotografie scattate dai miei dispositivi?

Per smettere di rendere visibili le fotografie scattate sui tuoi dispositivi:

1. Accedi a Bitdefender Central.
2. Tocca nell'angolo in alto a destra dello schermo.
3. Tocca **Il mio account** nel menu scorrevole.
4. Seleziona la scheda **Impostazioni**.
5. Disattiva l'opzione **Mostra/non mostrare le foto scattate sui tuoi dispositivi**.

Come posso mantenere sicuri i miei acquisti online?

Quando si ignorano alcuni dettagli, gli acquisti online possono comportare dei rischi elevati. Per non cadere vittima di una frode, ti consigliamo di seguire questi suggerimenti:

- Mantieni la tua app di sicurezza aggiornata.
- Invia pagamenti online solo con la protezione dell'acquirente.
- Usa una VPN quando ti connetti a internet da reti wireless pubbliche e non protette.
- Presta attenzione alle password che hai assegnato ai tuoi account online. Devono essere sicure, includendo sia lettere maiuscole che minuscole, numeri e simboli (@, !, %, #, ecc.).
- Assicurati di inviare le tue informazioni sempre con connessioni sicure. L'estensione del sito web online deve essere HTTPS:// e non HTTP://.

Quando dovrei utilizzare Bitdefender VPN?

Devi fare sempre attenzione quando accedi, scarichi o invii contenuti su internet. Per assicurarti di essere sempre al sicuro mentre navighi sul web, ti consigliamo di utilizzare Bitdefender VPN quando:

- vuoi connetterti a reti wireless pubbliche
- vuoi accedere a contenuti che normalmente sono riservati a determinate aree, indipendentemente dal fatto che ti trovi a casa o all'estero
- vuoi mantenere i tuoi dati personali privati (nomi utente, password, informazioni della carta di credito, ecc.)
- vuoi nascondere il tuo indirizzo IP

Bitdefender VPN avrà un impatto negativo sulla durata della batteria del mio dispositivo?

Bitdefender VPN è progettato per proteggere i tuoi dati personali, nascondere il tuo indirizzo IP mentre sei connesso a reti wireless non sicure e accedere a contenuti inaccessibili in determinati paesi. Per evitare un consumo non necessario della batteria del tuo dispositivo, ti consigliamo di utilizzare VPN solo quando ne hai bisogno e disconnetterti quando sei offline.

Perché riscontro rallentamenti in Internet mentre sono connesso con Bitdefender VPN?

Bitdefender VPN è stato progettato per offrirti un'esperienza di navigazione sul web leggera; tuttavia, la tua connettività a Internet o la distanza del server a cui ti connetti potrebbero causare dei rallentamenti. In questo caso, se non è obbligatorio connetterti a un server ospitato molto distante (ad esempio negli Stati Uniti o in Cina), ti consigliamo di consentire a Bitdefender VPN di connettersi automaticamente al server più vicino o trovarne uno più vicino alla tua ubicazione attuale.

Posso cambiare l'account Bitdefender collegato al dispositivo?

Sì, puoi facilmente modificare l'account di Bitdefender collegato al tuo dispositivo seguendo questi passaggi:

1. Tocca **Altro** nella barra di navigazione in basso.
2. Tocca il tuo indirizzo e-mail.
3. Tocca **Esci dal tuo account**. Se è stato impostato un codice PIN, ti sarà chiesto di inserirlo.
4. Conferma la tua scelta.
5. Inserisci l'indirizzo email e la password del tuo account nei campi corrispondenti, e tocca **ACCEDI**.

Quanto Bitdefender Mobile Security influenzerà le prestazioni e la durata della batteria del dispositivo?

Abbiamo mantenuto un basso impatto sulle prestazioni. L'applicazione si attiva solo quando serve, dopo aver installato un'applicazione, mentre si usa l'interfaccia o si esegue un controllo di sicurezza. Bitdefender Mobile Security non funziona in background mentre chiami gli amici, digiti un messaggio o giochi.

Che cos'è la funzione Amministratore dispositivo?

Amministratore dispositivo è una funzione di Android che dà a Bitdefender Mobile Security i permessi necessari per eseguire determinati compiti in remoto. Senza questi privilegi, il Blocco remoto non funzionerebbe e la cancellazione non potrebbe rimuovere completamente i tuoi dati. Se desideri rimuovere l'applicazione, assicurati di revocare tali privilegi prima della disinstallazione, andando in **Impostazioni > Sicurezza > Seleziona Amministratori dispositivo**.

Come risolvere il messaggio d'errore "No Google Token" che appare quando accedi a Bitdefender Mobile Security.

Questo errore si verifica quando il dispositivo non è associato a un account Google, oppure se associato, un problema temporaneo impedisce la connessione a Google. Prova una delle seguenti soluzioni:

- Vai a Impostazioni Android > Applicazioni > Gestisci applicazioni > Bitdefender Mobile Security e tocca **Cancella dati** Poi accedi di nuovo.
- Assicurati che il dispositivo sia associato con un account Google.

  Per controllare, andare in Impostazioni > Account & sync e verificare se un account Google è indicato sotto la voce **Gestione account**. Se non c'è, riavvia il dispositivo e riprova ad accedere a Bitdefender Mobile Security.
- Riavvia il dispositivo e riprova ad accedere.

In quali lingue è disponibile Bitdefender Mobile Security?

Al momento, Bitdefender Mobile Security è disponibile nelle seguenti lingue:

- Brasiliano
- Ceco
- Olandese
- Italiano
- Francese

- Tedesco
- Greco
- Ungherese
- Italiano
- Giapponese
- Coreano
- Polacco
- Portoghese
- Romeno
- Russo
- Spagnolo
- Svedese
- Thai
- Turco
- Vietnamita

Nelle prossime versioni saranno aggiunte altre lingue. Per cambiare la lingua dell'interfaccia di Bitdefender Mobile Security, vai alle impostazioni **Lingua & tastiera** del dispositivo e imposta la lingua che vuoi usare.

CONTATTACI

33. 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. 185) 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 Total Security» (p. 320)
- «Contattaci tramite il nostro Centro di supporto online» (p. 321)

Contattaci direttamente da Bitdefender Total Security

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

Segui questi passaggi:

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

34. 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.

34.1. 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.

34.2. 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 specifiche dal computer 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.

34.3. Portale HOTforSecurity

Il portale HOTforSecurity è una ricca fonte di informazioni sulla sicurezza informatica. Qui puoi apprendere le varie minacce a cui il computer 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.

35. CONTATTI

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.

35.1. 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

35.2. 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.

35.3. 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
E-mail: info@bitdefender.co.uk
Telefono: (+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
Telefono: +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, 15A Orhideelor Street, Sector 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.

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.

Settore di avvio:

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.

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.