

# Bitdefender<sup>®</sup> **ANTIVIRUS FOR MAC**



**MANUALE  
D'USO**





# Bitdefender Antivirus for Mac

## Guida dell'utente

Data di pubblicazione 24/11/2022

Diritto d'autore © 2022 Bitdefender

## Avviso legale

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

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

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

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

**Bitdefender®**



# Indice

<b>Informazioni su questa guida .....</b>	<b>1</b>
Finalità e destinatari .....	1
Come usare questo manuale .....	1
Convenzioni usate in questo manuale .....	1
Convenzioni tipografiche .....	1
Avvertenze .....	2
Richiesta di commenti .....	2
<b>1. Cos'è Bitdefender Antivirus for Mac .....</b>	<b>4</b>
<b>2. Installazione e rimozione .....</b>	<b>5</b>
2.1. Requisiti di sistema .....	5
2.2. Installazione di Bitdefender Antivirus for Mac .....	5
2.2.1. Fase di installazione .....	6
2.3. Rimuovere Bitdefender Antivirus for Mac. ....	9
<b>3. Iniziare .....</b>	<b>11</b>
3.1. Aprire Bitdefender Antivirus for Mac .....	11
3.2. Finestra principale della app .....	11
3.3. Icona app nel Dock .....	13
3.4. Menu di navigazione .....	13
3.5. Modalità scura .....	14
<b>4. Proteggersi da software dannoso .....</b>	<b>15</b>
4.1. Consigli .....	15
4.2. Eseguire una scansione sul Mac .....	16
4.3. Procedura guidata per la scansione .....	17
4.4. Quarantena .....	18
4.5. Bitdefender Shield (protezione in tempo reale) .....	19
4.6. Scansione eccezioni .....	19
4.7. Protezione web .....	20
4.7.1. Attivare le estensioni di TrafficLight .....	20
4.7.2. Gestire le impostazioni delle estensioni .....	21
4.7.3. Valutazione delle pagine e avvisi .....	21
4.8. Anti-tracker .....	21
4.8.1. Attivare Bitdefender Anti-tracker .....	22
4.8.2. Interfaccia di Anti-tracker .....	22
4.8.3. Disattivare Bitdefender Anti-tracker .....	23
4.8.4. Consentire la tracciatura di un sito web .....	23
4.9. Safe Files .....	24
4.9.1. Accesso applicazioni .....	25
4.10. Time Machine Protection .....	25
4.10.1. Attivare o disattivare Time Machine Protection .....	26



4.11. Risoluzione problemi .....	26
4.12. Notifiche .....	27
4.13. Aggiornamenti .....	28
4.13.1. Richiedere un aggiornamento .....	28
4.13.2. Ottenere gli aggiornamenti tramite server proxy .....	29
4.13.3. Fare l'upgrade a una nuova versione .....	29
4.13.4. Trovare informazioni su Bitdefender Antivirus for Mac .....	29
<b>5. VPN .....</b>	<b>31</b>
5.1. Informazioni su VPN .....	31
5.2. Aprire VPN .....	31
5.3. Interfaccia .....	32
5.4. Abbonamenti .....	34
<b>6. Configurare le preferenze .....</b>	<b>36</b>
6.1. Accedere alle preferenze .....	36
6.2. Preferenze di protezione .....	36
6.3. Preferenze avanzate .....	37
6.4. Offerte speciali .....	37
<b>7. Informazioni su Bitdefender Central .....</b>	<b>38</b>
7.1. Accedere a Bitdefender Central .....	38
7.2. Autenticazione a due fattori .....	39
7.2.1. Attivare l'autenticazione a due fattori .....	39
7.3. Aggiungere dispositivi affidabili .....	40
7.4. I miei dispositivi .....	41
7.4.1. Aggiungere un nuovo dispositivo .....	41
7.4.2. Personalizza il tuo dispositivo .....	42
7.4.3. Azioni in remoto .....	43
7.5. Attività .....	44
7.6. I miei abbonamenti .....	44
7.6.1. Controllare gli abbonamenti disponibili .....	45
7.6.2. Attiva abbonamento .....	45
7.6.3. Rinnova abbonamento .....	45
7.7. Notifiche .....	47
<b>8. Domande frequenti .....</b>	<b>48</b>
<b>9. Ottenere aiuto .....</b>	<b>53</b>
9.1. Richiesta d'aiuto .....	53
9.2. Risorse online .....	53
9.2.1. Centro di supporto di Bitdefender .....	53
9.2.2. La community di esperti di Bitdefender .....	54
9.2.3. Bitdefender Cyberpedia .....	54
9.3. Informazioni di contatto .....	55
9.3.1. Distributori locali .....	55



**Glossario ..... 56**



## INFORMAZIONI SU QUESTA GUIDA

### Finalità e destinatari

Questo manuale è destinato a tutti gli utenti Macintosh che hanno scelto Bitdefender Antivirus for Mac come soluzione di sicurezza per i propri computer. Le informazioni presentate in questo manuale non sono rivolte solo agli esperti di computer, ma a chiunque sia in grado di usare un Macintosh.

Scoprirai come configurare e utilizzare Bitdefender Antivirus for Mac per proteggerti da minacce e altri software dannosi. Inoltre, apprendrai come sfruttare al meglio Bitdefender.

Buona lettura e speriamo che lo troverai utile.

### Come usare questo manuale

Questo manuale presenta alcuni argomenti principali:

[Iniziare \(pagina 11\)](#)

Inizia a usare Bitdefender Antivirus for Mac e la sua interfaccia utente.

[Proteggerti da software dannoso \(pagina 15\)](#)

Apprendi come usare Bitdefender Antivirus for Mac per proteggerti dai software dannosi.

[Configurare le preferenze \(pagina 36\)](#)

Apprendi maggiori informazioni sulle preferenze di Bitdefender Antivirus for Mac.

[Ottenere aiuto \(pagina 53\)](#)

Dove cercare e ottenere un aiuto in caso di difficoltà.

### Convenzioni usate in questo manuale

#### Convenzioni tipografiche

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



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

## Avvertenze

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



### Nota

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



### Importante

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



### Avvertimento

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

## Richiesta di commenti

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



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





## 1. COS'È BITDEFENDER ANTIVIRUS FOR MAC

Bitdefender Antivirus for Mac è un potente scanner antivirus, che può rilevare e rimuovere ogni tipo di software dannoso ("minacce"), tra cui:

- ☐ ransomware
- ☐ adware
- ☐ virus
- ☐ spyware
- ☐ Trojan
- ☐ keylogger
- ☐ worm

Questa applicazione non solo rileva e rimuove le minacce per Mac, ma anche quelle per Windows, impedendo quindi di inviare accidentalmente file infetti a familiari, amici e colleghi che utilizzano un PC.



## 2. INSTALLAZIONE E RIMOZIONE

Questo capitolo include i seguenti argomenti:

- Requisiti di sistema (pagina 5)
- Installazione di Bitdefender Antivirus for Mac (pagina 5)
- Rimuovere Bitdefender Antivirus for Mac. (pagina 9)

### 2.1. Requisiti di sistema

Puoi installare Bitdefender Antivirus for Mac su computer Macintosh con OS X Yosemite (10.10) o versioni successive.

Il tuo Mac deve avere un minimo di 1 GB di spazio disponibile sul disco rigido.

Per registrare e aggiornare Bitdefender Antivirus for Mac è richiesta una connessione a Internet.



#### Nota

Bitdefender Anti-tracker e Bitdefender VPN possono essere installati solo su sistemi con macOS 10.12 o versioni successive.



#### Come scoprire la versione del tuo macOS e le informazioni hardware sul tuo Mac

Clicca sull'icona Apple nell'angolo in alto a sinistra dello schermo e seleziona Informazioni su **questo Mac**. Nella finestra che comparirà, potrai visualizzare la versione del tuo sistema operativo e altre informazioni utili. Clicca su **Resoconto di sistema** per informazioni più dettagliate sull'hardware.

### 2.2. Installazione di Bitdefender Antivirus for Mac

La app Bitdefender Antivirus for Mac può essere installata dal tuo account Bitdefender come segue:

1. Accedi come amministratore.
2. Vai in: <https://central.bitdefender.com>.
3. Accedi al tuo account Bitdefender utilizzando il tuo indirizzo e-mail e la tua password.



4. Seleziona il pannello **I miei dispositivi** e clicca su **INSTALLA PROTEZIONE**.
5. Seleziona una delle due opzioni disponibili:
  - **Proteggi questo dispositivo**
    - a. Seleziona questa opzione e poi il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, clicca sul pulsante corrispondente.
    - b. Salva il file di installazione.
  - **Proteggi altri dispositivi**
    - a. Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.
    - b. Clicca su **INVIA LINK DI DOWNLOAD**.
    - c. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA E-MAIL**.

Nota che il link di download generato è valido solo per le prossime 24 ore. Se il link dovesse scadere, dovrai generarne uno nuovo seguendo gli stessi passaggi.
    - d. Sul dispositivo su cui vuoi installare il tuo prodotto Bitdefender, controlla l'account e-mail che hai digitato e poi clicca sul pulsante di download corrispondente.
6. Esegui il prodotto Bitdefender che hai scaricato.
7. Completa tutti i passaggi dell'installazione.

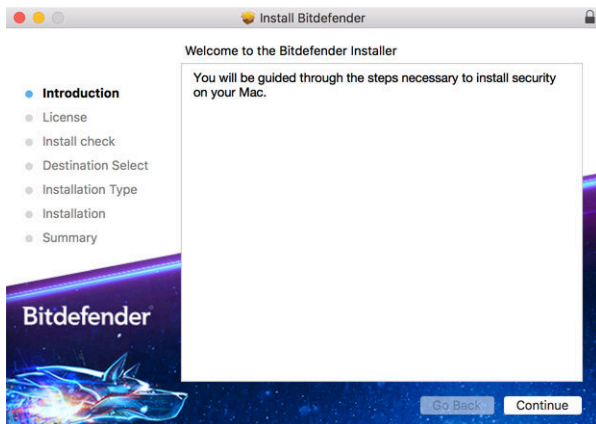
### 2.2.1. Fase di installazione

Per installare Bitdefender Antivirus for Mac:

1. Clicca sul file scaricato. Sarà lanciato il programma d'installazione, che ti guiderà attraverso il processo d'installazione.
2. Segui la procedura guidata dell'installazione.

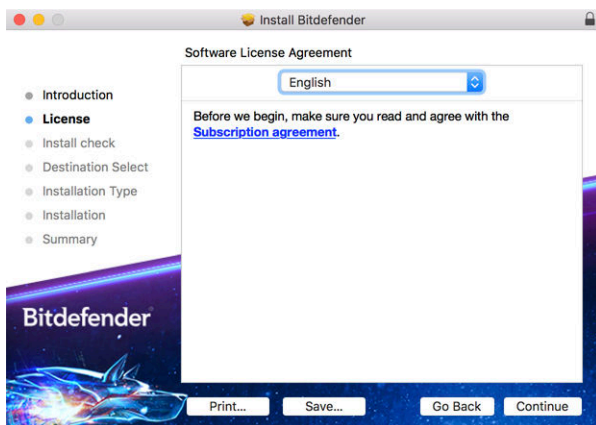


## Passo 1 - Finestra di benvenuto



Clicca su **Continua**.

## Passo 2 - Leggi l'Accordo di Abbonamento



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

Da questa finestra puoi anche selezionare la lingua con cui vuoi installare il prodotto.

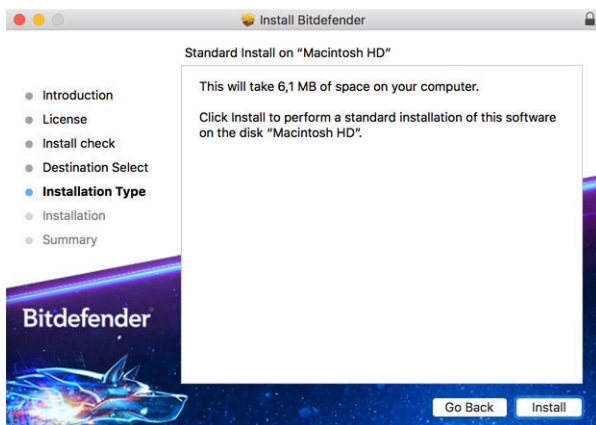
Clicca su **Continua** e poi su **Accetto**.



## Importante

Se non accetti i termini, clicca su **Continua** e poi su **Rifiuta** per annullare l'installazione e uscire dal relativo programma.

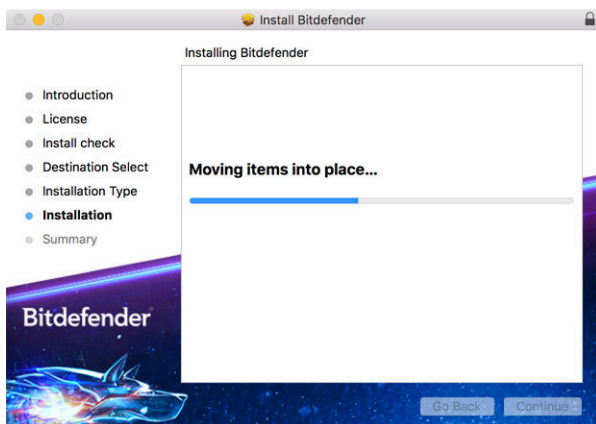
## Passo 3 - Inizia l'installazione



Bitdefender Antivirus for Mac sarà installato in Macintosh HD/Library/Bitdefender. Non è possibile modificare il percorso di installazione.

Clicca su **Installa** per avviare l'installazione.

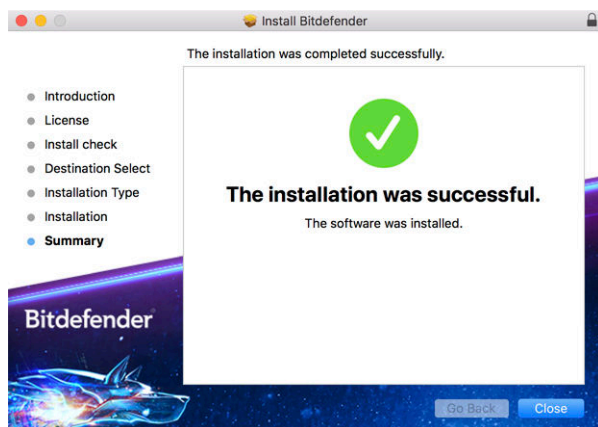
## Fase 4 - Installazione di Bitdefender Antivirus for Mac





Attendi la fine dell'installazione e clicca su **Continua**.

## Passaggio 5 - Fine



Clicca su **Chiudi** per chiudere la finestra del programma d'installazione.

Ora hai completato la fase d'installazione.



### Importante

- Se stai installando Bitdefender Antivirus for Mac su macOS High Sierra 10.13.0 o una versione successiva, comparirà la notifica **Estensione del sistema bloccata**. Questa notifica ti informa che le estensioni firmate da Bitdefender sono state bloccate e dovrai attivarle manualmente. Clicca su OK per continuare. Nella finestra di Bitdefender Antivirus for Mac che comparirà, clicca sul link **Security & Privacy**. Clicca su **Consenti** nella parte inferiore della finestra o seleziona Bitdefender SRL dall'elenco e clicca su **OK**.
- Se stai installando Bitdefender Antivirus for Mac su macOS Mojave 10.14 o una versione più recente, comparirà una nuova finestra, informandoti che devi **garantire a Bitdefender pieno accesso al disco e consentire il caricamento a Bitdefender**. Segui le istruzioni su schermo per configurare correttamente il prodotto.

## 2.3. Rimuovere Bitdefender Antivirus for Mac.

Essendo un'applicazione complessa, Bitdefender Antivirus for Mac non può essere rimossa in modo tradizionale, semplicemente trascinando l'icona dell'applicazione dalla cartella **Applicazioni** al Cestino.



Per rimuovere Bitdefender Antivirus for Mac, segui questi passaggi:

1. Apri una finestra di **Finder** e vai alla cartella **Applicazioni**.
2. Apri la cartella Bitdefender in **Applicazioni** e poi clicca due volte su **BitdefenderUninstaller**.
3. Seleziona l'opzione di disinstallazione preferita.



### Nota

Se stai cercando di rimuovere solo la app Bitdefender VPN, seleziona solo **Disinstalla VPN**.

4. Clicca su **Disinstalla** e attendi il completamento del processo.
5. Clicca su **Chiudi** per terminare.



### Importante

In caso di errore, puoi contattare il Servizio clienti di Bitdefender come descritto in [Richiesta d'aiuto \(pagina 53\)](#).




## 3. INIZIARE

Questo capitolo include i seguenti argomenti:

- [Aprire Bitdefender Antivirus for Mac \(pagina 11\)](#)
- [Finestra principale della app \(pagina 11\)](#)
- [Icona app nel Dock \(pagina 13\)](#)
- [Menu di navigazione \(pagina 13\)](#)
- [Modalità scura \(pagina 14\)](#)

### 3.1. Aprire Bitdefender Antivirus for Mac


Puoi aprire Bitdefender Antivirus for Mac in diversi modi.

- Clicca sull'icona di Bitdefender Antivirus nel Launchpad.
- Clicca sull'icona  nella barra del menu e seleziona **Apri interfaccia Antivirus**.
- Apri una finestra di Finder, vai in Applicazioni e clicca due volte sull'icona di **Bitdefender Antivirus for Mac**.



#### Importante

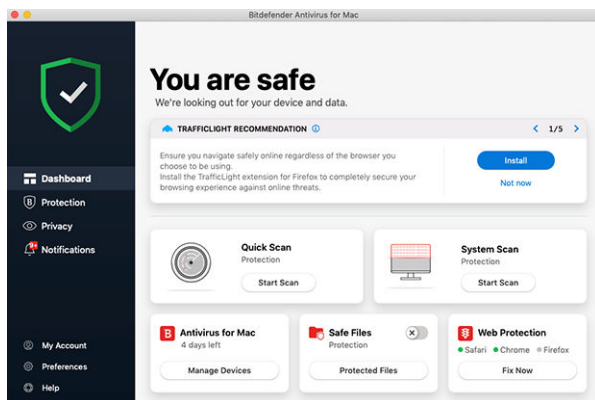
La prima volta che si apre Bitdefender Antivirus for Mac su macOS Mojave 10.14 o una versione più recente, comparirà un suggerimento di protezione. Tali suggerimenti compaiono perché ci servono i permessi per esaminare l'intero sistema alla ricerca di minacce. Per darci i permessi, devi accedere come amministratore e seguire questi passaggi:

1. Clicca sul link **Preferenze di sistema**.
2. Clicca sull'icona  e poi inserisci le tue credenziali di amministratore.
3. Si aprirà una nuova finestra. Trascina il file **BDLDaemon** nell'elenco delle app autorizzate.

### 3.2. Finestra principale della app

Bitdefender Antivirus for Mac soddisfa sia le necessità degli utenti esperti che quelle dei principianti. L'interfaccia grafica è quindi stata progettata per essere adatta a qualsiasi categoria di utenti.





Per apprendere l'interfaccia di Bitdefender, in alto a sinistra comparirà una procedura guidata introduttiva contenente maggiori dettagli su come interagire con il prodotto e configurarlo correttamente. Scegli la giusta parentesi angolare per continuare con la guida, o **Salta il tour** per chiudere la procedura guidata.

La barra di stato nella parte superiore della finestra ti informa sullo stato di sicurezza del sistema usando messaggi chiari e colori indicativi. Se Bitdefender Antivirus for Mac non ha alcun avviso, la scheda dello stato è verde. Quando viene rilevato un problema di sicurezza, la scheda dello stato diventa rossa. Per maggiori dettagli sui problemi e come risolverli, fai riferimento a [Risoluzione problemi \(pagina 26\)](#).

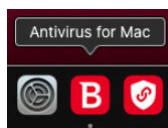
Per offrirti un funzionamento efficace e una maggiore protezione mentre esegui diverse attività, **Bitdefender Autopilot** agirà come tuo consulente di sicurezza personale. In base alle attività eseguite, sia che tu stia lavorando o effettuando pagamenti online, Bitdefender Autopilot ti fornirà suggerimenti contestuali basati sull'uso e le esigenze del tuo dispositivo. Ciò ti aiuterà a scoprire e usufruire dei vantaggi offerti dalle funzionalità incluse nella app Bitdefender Antivirus for Mac.

Dal menu di navigazione sul lato sinistro puoi accedere alle sezioni di Bitdefender per una configurazione dettagliata e attività amministrative avanzate (schede **Protezione** e **Privacy**), notifiche, il tuo **account Bitdefender** e la zona delle **Preferenze**. Inoltre, puoi contattarci (scheda **Aiuto**) se avessi delle domande o dovesse apparire qualcosa di inatteso.










### 3.3. Icona app nel Dock

L'icona di Bitdefender Antivirus for Mac può essere notata nel Dock non appena si apre la app. L'icona nel Dock ti fornisce un facile modo per esaminare file e cartelle alla ricerca di minacce. Basta trascinare e rilasciare il file o la cartella sull'icona del Dock e la scansione inizierà immediatamente.



### 3.4. Menu di navigazione

Sul lato sinistro dell'interfaccia di Bitdefender si trova il menu di navigazione, che ti consente di accedere rapidamente alle funzionalità di Bitdefender necessarie per la gestione del prodotto. In quest'area sono disponibili le seguenti schede:

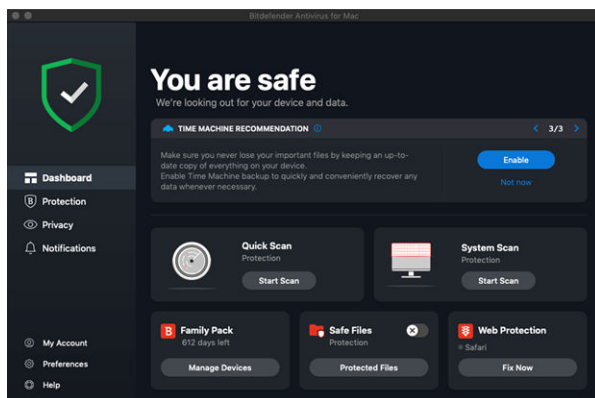
-  **Dashboard.** Da qui puoi risolvere rapidamente eventuali problemi di sicurezza, visualizzare suggerimenti in base alle esigenze del tuo sistema e l'utilizzo del prodotto, eseguire azioni rapide e andare al tuo account Bitdefender per gestire i dispositivi che hai aggiunto al tuo abbonamento Bitdefender.
-  **Protezione.** Da qui, puoi eseguire attività di scansione antivirus, aggiungere file all'elenco delle eccezioni, proteggere file e app da attacchi ransomware, proteggere i tuoi backup Time Machine, e configurare la protezione durante la navigazione su Internet.
-  **Privacy.** Da qui, puoi aprire la app Bitdefender VPN e installare l'estensione Anti-tracker nel tuo browser web.
-  **Notifiche.** Da qui, puoi visualizzare maggiori dettagli sulle azioni intraprese sui file esaminati.
-  **Il mio account.** Da qui, puoi visualizzare il tuo account Bitdefender e l'abbonamento con cui il tuo dispositivo è protetto, nonché cambiare il tuo account, se necessario.
-  **Preferenze.** Da qui, puoi configurare le impostazioni di Bitdefender.
-  **Aiuto.** Da qui, ogni volta che ti serve assistenza nel risolvere una situazione con il tuo prodotto Bitdefender, puoi contattare il Supporto



tecnico. Puoi anche lasciarci un tuo feedback per aiutarci a migliorare il prodotto.

## 3.5. Modalità scura

Per proteggere gli occhi da bagliori e luci mentre si lavora di notte o in condizioni di scarsa luminosità, Bitdefender Antivirus for Mac supporta la modalità scura per Mojave 10.14 e versioni successive. I colori dell'interfaccia sono stati ottimizzati per poter usare il Mac senza sforzare gli occhi. L'interfaccia di Bitdefender Antivirus for Mac si regola automaticamente in base alle impostazioni video del tuo dispositivo.





## 4. PROTEGGERSI DA SOFTWARE DANNOSO

Questo capitolo include i seguenti argomenti:

- Consigli (pagina 15)
- Eseguire una scansione sul Mac (pagina 16)
- Procedura guidata per la scansione (pagina 17)
- Quarantena (pagina 18)
- Bitdefender Shield (protezione in tempo reale) (pagina 19)
- Scansione eccezioni (pagina 19)
- Protezione web (pagina 20)
- Anti-tracker (pagina 21)
- Safe Files (pagina 24)
- Time Machine Protection (pagina 25)
- Risoluzione problemi (pagina 26)
- Notifiche (pagina 27)
- Aggiornamenti (pagina 28)

### 4.1. Consigli

Per tenere il tuo sistema sempre privo di minacce e impedire un'infezione accidentale di altri sistemi, segui questi consigli:

- Mantieni attivato **Bitdefender Shield**, per consentire la scansione automatica dei file di sistema da parte di Bitdefender Antivirus for Mac.
- Mantieni il tuo prodotto Bitdefender Antivirus for Mac aggiornato con gli ultimi aggiornamenti del prodotto e delle informazioni delle minacce.
- Controlla regolarmente e risolvi i problemi segnalati da Bitdefender Antivirus for Mac. Per informazioni dettagliate, fai riferimento a [Risoluzione problemi \(pagina 26\)](#).
- Controlla il registro degli eventi riguardanti le attività di Bitdefender Antivirus for Mac sul tuo computer. Ogni volta che accade qualcosa



di rilevante per la sicurezza del sistema o dei dati, viene aggiunto un nuovo messaggio nell'area delle notifiche di Bitdefender. Per maggiori dettagli, accedere a [Notifiche \(pagina 27\)](#).

- Dovresti seguire questi consigli:
  - Prendi l'abitudine di controllare i file che scarichi da periferiche di memorizzazione esterne (come una chiavetta USB o un CD), specialmente se non ne conosci l'origine.
  - Se hai un file DMG, montalo e poi controllane il contenuto (i file all'interno del volume/immagine montata).

Il modo più semplice per controllare un file, una cartella o un volume è di trascinarli e lasciarli sulla finestra di Bitdefender Antivirus for Mac o nell'icona sul Dock.

Non è necessaria nessun'altra configurazione o azione. Tuttavia, se lo desideri, puoi modificare le impostazioni e le preferenze dell'applicazione in base alle tue esigenze. Per maggiori informazioni, fai riferimento a [Configurare le preferenze \(pagina 36\)](#).

## 4.2. Eseguire una scansione sul Mac

Oltre alla funzione **Bitdefender Shield**, che monitora regolarmente le app installate, cercando azioni simili a minacce e impedendo a nuove minacce di accedere al sistema, puoi eseguire una scansione sul tuo Mac o esaminare determinati file in qualsiasi momento.

Il modo più semplice per controllare un file, una cartella o un volume è di trascinarli e lasciarli sulla finestra di Bitdefender Antivirus for Mac o nell'icona sul Dock. Comparirà la procedura guidata della scansione, che ti guiderà attraverso il processo di scansione.

Puoi avviare una scansione anche in questo modo:

1. Clicca su **Protezione** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Seleziona la scheda **Antivirus**.
3. Clicca su uno dei tre pulsanti di scansione per avviare la scansione desiderata.
  - **Scansione veloce** - Cerca eventuali minacce nei punti più vulnerabili del sistema (per esempio nelle cartelle contenenti



documenti, file scaricati, messaggi di posta e altri file temporanei di ciascun utente).

- **Scansione di sistema** - Esegue un controllo dell'intero sistema alla ricerca di eventuali minacce. Saranno controllati anche tutti i mount connessi.

## **Nota**

In base alla misura del disco fisso, controllare l'intero sistema potrebbe richiedere un po' di tempo (fino a un'ora o persino di più). Per ottenere prestazioni migliori, si consiglia di non avviare questa attività mentre se ne eseguono altre piuttosto esigenti in termini di risorse di sistema (come ad esempio una sessione di editing video).

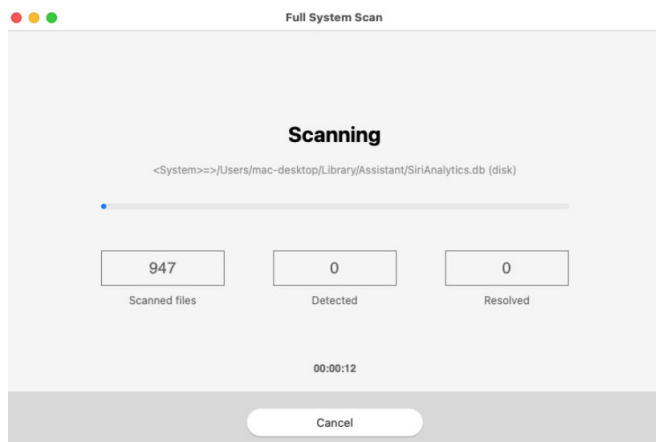
Se preferisci, puoi scegliere di non controllare determinati volumi montati, aggiungendoli all'elenco delle **Eccezioni** dalla finestra Protezione.

- **Scansione personalizzata** - Ti aiuta a controllare file, cartelle o volumi particolari in cerca di eventuali minacce.

Puoi anche avviare una Scansione veloce o di sistema dalla Dashboard.

## 4.3. Procedura guidata per la scansione

Ogni volta che avvii una scansione, comparirà la relativa procedura guidata di Bitdefender Antivirus for Mac.





Durante ogni scansione, vengono mostrate informazioni in tempo reale sulle minacce eventualmente rilevate e risolte.

Attendere che Bitdefender Antivirus for Mac finisca la scansione.

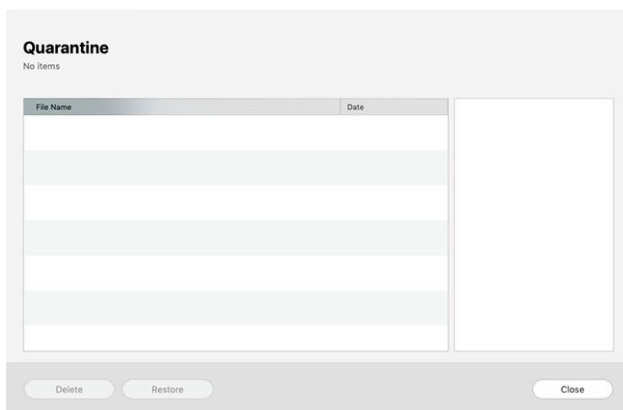


### Nota

La durata del processo dipende dalla complessità della scansione.

## 4.4. Quarantena

Bitdefender Antivirus for Mac consente di isolare i file infetti o sospetti in un'area sicura, chiamata quarantena. Quando una minaccia è in quarantena, non può più arrecare alcun danno, in quanto non può essere eseguita o letta.



La sezione Quarantena mostra tutti i file attualmente isolati nella cartella Quarantena.

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

Per visualizzare un elenco con tutti gli elementi aggiunti alla quarantena:

1. Clic **Protezione** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Clicca su **Apri** nel pannello **Quarantena**.



## 4.5. Bitdefender Shield (protezione in tempo reale)

Bitdefender fornisce una protezione in tempo reale da una vasta gamma di minacce esaminando tutte le app installate, le loro versioni aggiornate e i file nuovi e modificati.

Per disattivare la protezione in tempo reale:

1. Clicca su **Preferenze** nel menu di navigazione nell'interfaccia di Bitdefender.
2. Disattiva **Bitdefender Shield** nella finestra **Protezione**.



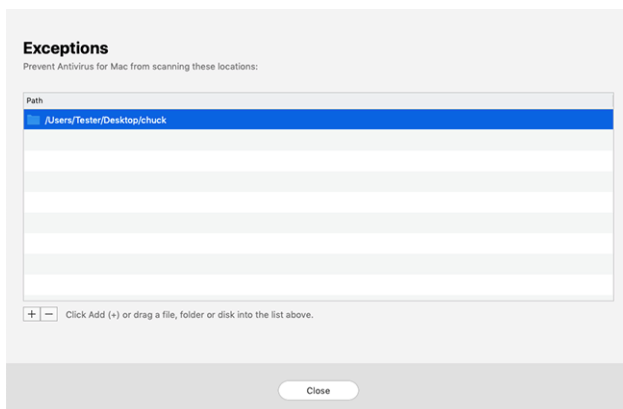
### Avvertimento

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

## 4.6. Scansione eccezioni

Se lo desideri, puoi configurare Bitdefender Antivirus for Mac per non controllare determinati file e cartelle o anche interi volumi. Per esempio, potresti voler escludere dalla scansione:

- ☐ File che sono stati identificati per errore come infetti (conosciuti come falsi positivi)
- ☐ File che causano errori di scansione
- ☐ Backup dei volumi







L'elenco delle eccezioni contiene i percorsi che sono stati esclusi dalla scansione.

Per accedere all'elenco delle eccezioni:

1. Clic **Protezione** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Clicca su **Apri** nel pannello **Eccezioni**.

Ci sono due modi per impostare un'eccezione di scansione:

- ☐ Trascina e rilascia un file, una cartella o un volume sull'elenco delle eccezioni.
- ☐ Clicca sul pulsante con il segno più (+), posizionato sotto l'elenco delle eccezioni. Poi, seleziona il file, la cartella o il volume da escludere dalla scansione.

Per rimuovere un'eccezione, selezionala dall'elenco e clicca sul pulsante con il segno meno (-), posizionato sotto l'elenco delle eccezioni.

## 4.7. 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.

### 4.7.1. Attivare le estensioni di TrafficLight


Per attivare le estensioni di TrafficLight:

1. Clicca su **Risolvi ora** nella scheda **Protezione web** nella Dashboard.
2. Si aprirà la finestra **Protezione web**.  
Comparirà il browser web rilevato che hai installato sul tuo sistema. Per installare l'estensione di TrafficLight sul tuo browser, clicca su **Ottieni estensione**.
3. Ora raggiungerai l'indirizzo:  
<https://bitdefender.com/solutions/trafficlight.html>
4. Seleziona **Free Download** (Scarica gratuitamente).



5. Segui i passaggi per installare l'estensione di TrafficLight corrispondente al tuo browser.

### 4.7.2. Gestire le impostazioni delle estensioni


Per proteggerti da ogni tipo di minaccia che potresti incontrare durante la tua navigazione web, è disponibile una vasta gamma di funzioni. Per accedervi, clicca sull'icona di TrafficLight accanto alle impostazioni del browser e poi clicca sul pulsante  **Impostazioni**:

#### ○ Impostazioni di Bitdefender TrafficLight

- Protezione web - Ti impedisce di accedere a siti web utilizzati per attacchi di malware, tentativi di phishing e frodi.
- Analisi risultati della ricerca - Segnala eventuali siti web rischiosi tra i risultati della tua ricerca.

#### ○ Eccezioni




Se sei sul sito web che vuoi aggiungere alle eccezioni, clicca su **Aggiungi questo sito web all'elenco**.

Se vuoi aggiungere un altro sito web, inserisci il suo indirizzo nel campo corrispondente, e clicca su .

Non comparirà alcun avviso in caso di minacce presenti sulle pagine escluse. Ecco perché in questa lista devi indicare solo siti web affidabili.

### 4.7.3. Valutazione delle pagine e avvisi

In base a come TrafficLight classifica la pagina web che stai visualizzando, in quest'area sarà mostrata una delle seguenti icone:

-  Questa è pagina sicura da visitare. Puoi continuare il tuo lavoro.
-  Questa pagina web può contenere contenuti pericolosi. Presta la massima cautela se decidi di visitarla.
-  Dovresti abbandonare subito questo pagina web in quanto contiene malware o altre minacce.

In Safari, lo sfondo delle icone di TrafficLight è nero.

## 4.8. Anti-tracker

Molti siti web che visiti utilizzano tracker per ottenere informazioni sul tuo comportamento, per condividerle con aziende di terze parti o mostrarti



pubblicità più rilevanti per te. Quindi, i possessori dei siti web guadagnano per essere in grado di fornirti contenuti gratuitamente o continuare a operare. Oltre a raccogliere informazioni, i tracker possono rallentare la tua esperienza di navigazione oppure occupare la tua banda.

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

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

- ☐ Google Chrome
- ☐ Mozilla Firefox
- ☐ Safari

I tracker che rileviamo vengono raggruppati nelle seguenti categorie:


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

### 4.8.1. 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.

### 4.8.2. Interfaccia di Anti-tracker

Quando l'estensione Bitdefender Anti-tracker viene attivata, compare l'icona  accanto alla barra di ricerca nel tuo browser web. Ogni volta





che visiti un sito web, sull'icona si può notare un contatore, che indica i tracker rilevati e bloccati. Per maggiori dettagli sui tracker bloccati, clicca sull'icona per aprire l'interfaccia. Accanto al numero dei tracker bloccati, puoi visualizzare il tempo richiesto per il caricamento della pagina e le categorie di appartenenza dei tracker rilevati. Per vedere l'elenco dei siti web che stanno usando la tracciatura, clicca sulla categoria desiderata.

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

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



### 4.8.3. Disattivare Bitdefender Anti-tracker


Per disattivare Bitdefender Anti-tracker dal tuo browser web:

1. Apri il tuo browser web.
2. Clicca sull'icona  accanto alla barra dell'indirizzo nel tuo browser web.
3. Clicca sull'icona  nell'angolo in alto a destra.
4. Usa l'interruttore corrispondente per disattivarlo.  
L'icona Bitdefender diventa grigia.

### 4.8.4. Consentire la tracciatura di un sito web

Se desideri lasciare attivata la tracciatura mentre visiti un determinato sito web, puoi aggiungere questo indirizzo alle eccezioni nel seguente modo:

1. Apri il browser web.
2. Clicca sull'icona  accanto alla barra di ricerca.
3. Clicca il  icona nell'angolo in alto a destra.
4. Se ti trovi sul sito Web che desideri aggiungere alle eccezioni, fai clic su **Aggiungi il sito web corrente all'elenco**.

Se desideri aggiungere un altro sito web, digita il suo indirizzo nel campo corrispondente, quindi fai clic su .



## 4.9. Safe Files

Un Ransomware è un programma dannoso che colpisce i sistemi vulnerabili bloccandoli e chiedendo denaro agli utenti per riavere il controllo dei propri sistemi. Questo programma dannoso agisce in maniera molto scaltra, mostrando falsi messaggi per allarmare l'utente, spingendoli al pagamento delle cifre richieste.

Utilizzando le tecnologie più moderne, Bitdefender assicura l'integrità del sistema proteggendone le aree critiche da attacchi ransomware senza influenzarne le prestazioni. Tuttavia, potresti voler proteggere anche i tuoi file personali, come documenti, fotografie o filmati, impedendone l'accesso ad applicazioni non affidabili. Con Bitdefender Safe Files, puoi proteggere i tuoi file personali e configurare le app autorizzate a effettuare modifiche nei tuoi file protetti, bloccando tutte le altre.

Per aggiungere successivamente file all'ambiente protetto:

1. Clic **Protezione** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Anti-Ransomware**.
3. Clicca su **File protetti** nell'area Safe Files.
4. Clicca sul pulsante con il segno più (+), posizionato sotto l'elenco dei file protetti. Poi, seleziona un file, una cartella o un volume da proteggere da eventuali attacchi ransomware.

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

Di norma, le cartelle Immagini, Documenti, Desktop e Download sono protette dagli attacchi di ogni minaccia.



### Nota

Le cartelle personali possono essere protette solo per gli utenti attuali. Unità esterne, oltre a file di sistema e delle applicazioni, non possono essere aggiunti all'ambiente protetto.

Riceverai un avviso ogni volta che una app sconosciuta con un comportamento anomalo cercherà di modificare i file che hai aggiunto. Clicca su **Consenti** o **Blocca** per aggiungerla all'elenco delle **Applicazioni gestite**.



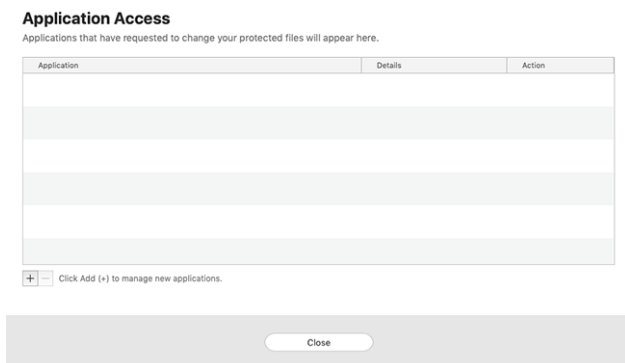
### 4.9.1. Accesso applicazioni

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

1. Clic **Protezione** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona il **Anti ransomware** scheda.
3. Clicca su **Accesso applicazione** nell'area Safe Files.
4. Cambia lo stato in Consenti accanto alla app bloccata.

Anche le app impostate su Consenti possono essere bloccate.

Usa il metodo trascina e rilascia o clicca sul segno più (+) per aggiungere altre app all'elenco.



## 4.10. Time Machine Protection

Bitdefender Time Machine Protection serve come ulteriore livello di sicurezza per l'unità di backup, incluso tutti i file che hai deciso di archiviare, 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.



### 4.10.1. Attivare o disattivare Time Machine Protection

Per attivare o disattivare Time Machine Protection:

1. Clicca su **Protezione** nel menu di navigazione nell'**interfaccia di Bitdefender**.
2. Seleziona il **Anti ransomware** scheda.
3. Attiva o disattiva l'interruttore **Time Machine Protection**.

## 4.11. Risoluzione problemi

Bitdefender Antivirus for Mac rileva automaticamente e ti informa sui problemi che possono influenzare la sicurezza del sistema e dei dati. In questo modo, puoi risolvere facilmente e in maniera tempestiva ogni rischio per la sicurezza.

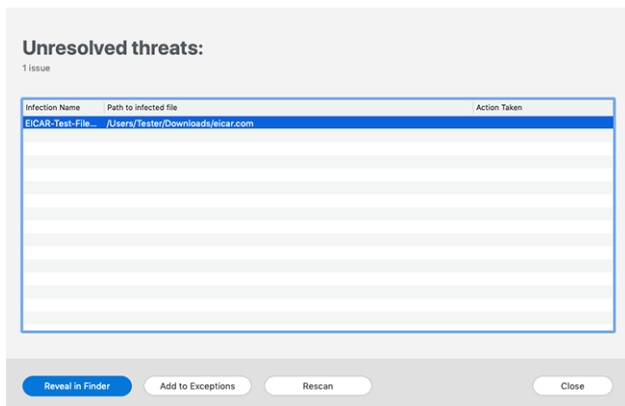
Risolvere i problemi indicati da Bitdefender Antivirus for Mac è un modo rapido e semplice per assicurare una protezione ottimale al tuo sistema e ai tuoi dati.

I problemi rilevati includono:

- Il nuovo aggiornamento sulle informazioni delle minacce non è stato scaricato dai nostri server.
- Sul tuo sistema sono state rilevate delle minacce e il prodotto non ha potuto disinfettarle automaticamente.
- La protezione in tempo reale è stata disattivata.

Per controllare e correggere i problemi rilevati:

1. Se Bitdefender non ha alcun avviso, la barra di stato è verde. Quando viene rilevato un problema di sicurezza, la barra di stato cambia il suo colore, diventando rossa.
2. Verifica la descrizione per maggiori informazioni.
3. Quando viene rilevato un problema, clicca sul pulsante corrispondente per intervenire.



L'elenco delle minacce non risolte viene aggiornato dopo ogni scansione del sistema, indipendentemente se la scansione è stata eseguita automaticamente in background o avviata da te.

Puoi scegliere di intraprendere le seguenti azioni sulle minacce non risolte:

- **Elimina manualmente.** Intraprendi questa azione per rimuovere le infezioni manualmente.
- **Aggiungi alle eccezioni.** Questa azione non è disponibile per le minacce trovate negli archivi.


## 4.12. Notifiche

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

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





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

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

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

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

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

## 4.13. Aggiornamenti

Ogni giorno vengono trovate e identificate nuove minacce. Ecco perché è molto importante mantenere Bitdefender Antivirus for Mac sempre aggiornato con i nuovi aggiornamenti delle informazioni delle minacce.

Gli aggiornamenti delle informazioni delle minacce sono eseguiti al volo, ciò significa che i file da aggiornare sono sostituiti progressivamente. In questo modo, l'aggiornamento non interesserà l'operatività del prodotto, e, allo stesso tempo, ogni vulnerabilità sarà esclusa.

- Se Bitdefender Antivirus for Mac è aggiornato, può rilevare tutte le ultime minacce scoperte e pulire i file infetti.
- Se Bitdefender Antivirus for Mac non è aggiornato, non potrà rilevare e rimuovere le nuove minacce scoperte da Bitdefender Labs.

### 4.13.1. 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.

### 4.13.2. Ottenere gli aggiornamenti tramite server proxy

Bitdefender Antivirus for Mac può essere aggiornato solo attraverso server proxy che non richiedono autenticazione. Non è necessario configurare alcuna impostazione del programma.

Se ti connetti a Internet attraverso un server proxy che richiede l'autenticazione, devi passare a una normale connessione Internet diretta per ottenere gli aggiornamenti delle informazioni delle minacce.

### 4.13.3. Fare l'upgrade a una nuova versione

Occasionalmente, rendiamo disponibili aggiornamenti del prodotto per aggiungere nuove funzioni e miglioramenti, o per risolvere eventuali problemi. Tali aggiornamenti potrebbero richiedere un riavvio del sistema per avviare l'installazione dei nuovi file. Di norma, se un aggiornamento richiede un riavvio del computer, Bitdefender Antivirus for Mac continuerà a funzionare con i file precedenti fin quando il sistema non sarà riavviato. In questo caso, il processo di aggiornamento non interferirà con le attività dell'utente.

Quando l'aggiornamento di un prodotto viene completato, una finestra di pop-up ti informerà di riavviare il sistema. Se hai saltato questa notifica, puoi cliccare su **Riavvia per aggiornare** dalla barra dei menu oppure riavviare il sistema manualmente.

### 4.13.4. 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 **Informazioni su Antivirus for Mac**.



## 5. VPN

Questo capitolo include i seguenti argomenti:

- [Informazioni su VPN \(pagina 31\)](#)
- [Aprire VPN \(pagina 31\)](#)
- [Interfaccia \(pagina 32\)](#)
- [Abbonamenti \(pagina 34\)](#)

### 5.1. 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.

La app VPN può essere installata dal tuo prodotto Bitdefender e usata ogni volta che vuoi aggiungere un ulteriore livello di protezione per la tua connessione. La VPN serve come una sorta di tunnel tra il tuo dispositivo e la rete a cui ti connetti per proteggere la tua connessione, cifrando i dati usando una cifratura di livello bancario e nascondendo il tuo indirizzo IP ovunque sei. Il tuo traffico viene reindirizzato attraverso un server separato. Ciò rende il tuo dispositivo quasi impossibile da essere identificato attraverso la miriade di altri dispositivi che stanno usando i nostri servizi. Inoltre, connettendoti a Internet tramite Bitdefender VPN, potrai accedere a contenuti che normalmente sono vietati in determinate aree.




#### Nota

Alcuni paesi applicano una censura di Internet e quindi l'utilizzo delle VPN sul loro territorio è proibito per legge. Per evitare conseguenze legali, potrebbe comparire un messaggio di avviso quando cerchi di usare la app 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.

### 5.2. Aprire VPN

Ci sono tre modi per aprire la app di Bitdefender VPN:



- Clicca su **Privacy** nel menu di navigazione nell'**interfaccia di Bitdefender**.  
Clicca su **Apri** nella scheda Bitdefender VPN.
- Clicca sull'icona  nella bara del menu.
- Vai alla cartella Applicazioni, apri la cartella Bitdefender e poi clicca due volte sull'icona di 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.



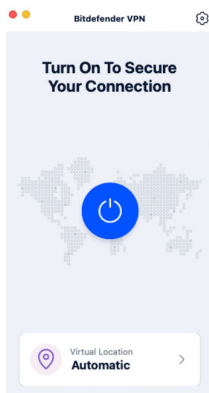
### Nota

La app Bitdefender VPN può essere installata solo su macOS Sierra (10.12.6), macOS High Sierra (10.13.6), macOS Mojave (10.14) o versioni successive del sistema operativo.

## 5.3. Interfaccia

L'interfaccia di VPN mostra lo stato della app, connessa o disconnessa. L'ubicazione del server per gli utenti con la versione gratuita viene impostata automaticamente da Bitdefender sul server più appropriato, mentre gli utenti premium hanno la possibilità di modificare la posizione del server a cui desiderano connettersi, selezionandola dall'elenco Posizioni virtuali. Per maggiori dettagli sugli abbonamenti a VPN, fai riferimento a [Abbonamenti \(pagina 34\)](#).

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.



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 sul tuo account Bitdefender e sull'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:
  - **Generale**
    - Notifiche - Mostra le notifiche del prodotto.
    - Esegui all'avvio - Lancia automaticamente Bitdefender VPN all'accesso.
    - Rapporti del prodotto - Invia rapporti anonimi sul prodotto per aiutarci a migliorare la tua esperienza e le tue capacità protettive.
  - **Avanzate**
    - Interruzione Internet - questa funzionalità interrompe temporaneamente tutto il traffico Internet se la connessione VPN dovesse cadere accidentalmente.
    - Ad blocker e Anti-tracker - Blocca gli annunci pubblicitari e i tracker per offrirti un'esperienza web più fluida e veloce.
    - Split tunneling - I siti web selezionati eviteranno la VPN e accederanno a Internet direttamente.



## Nota

Clicca su **Gestisci** e poi su **Aggiungi siti web** per aggiungere pagine web a questo elenco.

- Connessione automatica - Ti connetti automaticamente alla VPN quando:
  - Ti connetti a una rete Wi-Fi pubblica o non affidabile.
  - Viene avviata una app di condivisione dei file peer-to-peer.
- **Supporto** - Raggiungerai la 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.

## 5.4. Abbonamenti

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

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

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

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

Bitdefender VPN è un prodotto multiplatforma, disponibile nei prodotti Bitdefender compatibili con Windows, macOS, Android e iOS. Una volta effettuato l'upgrade al piano premium, potrai usare il tuo abbonamento



su tutti i prodotti, a condizione che tu acceda con lo stesso account Bitdefender.





## 6. CONFIGURARE LE PREFERENZE

Questo capitolo include i seguenti argomenti:

- [Accedere alle preferenze \(pagina 36\)](#)
- [Preferenze di protezione \(pagina 36\)](#)
- [Preferenze avanzate \(pagina 37\)](#)
- [Offerte speciali \(pagina 37\)](#)

### 6.1. Accedere alle preferenze

Per aprire la finestra delle Preferenze di Bitdefender Antivirus for Mac:

- Esegui una delle seguenti azioni:
  - Clic **Preferenze** nel menu di navigazione dell'interfaccia di Bitdefender.
  - Clicca su Bitdefender Antivirus for Mac nella barra dei menu e seleziona **Preferenze**.

### 6.2. Preferenze di protezione

La finestra delle preferenze di protezione ti consente di configurare l'approccio generale alla scansione. Puoi configurare le azioni intraprese sui file infetti o sospetti, e altre impostazioni generali.

- **Bitdefender Shield.** Bitdefender Shield offre una protezione in tempo reale da una vasta gamma di minacce esaminando tutte le app installate, le loro versioni aggiornate e i file nuovi e modificati. Non ti consigliamo di disattivare Bitdefender Shield, ma se devi farlo, fallo per il minor tempo possibile. Se Bitdefender Shield è disattivato, non avrai più alcuna protezione dalle minacce.
- **Esamina solo i file nuovi e modificati.** Seleziona questa casella per fare in modo che Bitdefender Antivirus for Mac controlli solo i file che non sono stati già controllati o che sono stati modificati dall'ultima scansione.

Puoi scegliere di non applicare questa impostazione per la scansione trascina e rilascia personalizzata, deselegionando la casella corrispondente.



- **Non esaminare i contenuti nei backup.** Seleziona questa casella per escludere i file dei backup dalla scansione. Se i file infetti vengono ripristinati più tardi, Bitdefender Antivirus for Mac li rileverà automaticamente, intraprendendo l'azione appropriata.

### 6.3. Preferenze avanzate

Puoi scegliere quale azione generale intraprendere per tutti i problemi ed elementi sospetti trovati durante un processo di scansione.

#### Azione per elementi infetti

- **Prova a disinfettare o spostare in quarantena** - Se vengono rilevati file infetti, Bitdefender tenterà di disinfettarli (rimuovendo il codice dannoso) o spostarli in quarantena.
- **Non fare nulla** - Nessuna azione verrà intrapresa sui file rilevati.

#### Azione per elementi sospetti

- **Sposta i file in quarantena** - Se vengono rilevati file sospetti, Bitdefender li sposterà in quarantena.
- **Non intraprendere alcuna azione** - Non verrà intrapresa alcuna azione sui file rilevati.

### 6.4. Offerte speciali

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

Per attivare o disattivare le notifiche sulle offerte speciali:

1. Clic **Preferenze** nel menu di navigazione dell'interfaccia di Bitdefender.
2. Seleziona la scheda **Altro**.
3. Attiva o disattiva l'interruttore **Le mie offerte**.



#### Nota

Di norma, l'opzione **Le mie offerte** è attivata.



## 7. 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 Android e iOS.

Per installare la app Bitdefender Central sui tuoi dispositivi:

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

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

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

### 7.1. 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:
1. Apri la app Bitdefender Central che hai installato.



### Nota

In questo materiale abbiamo incluso le opzioni che puoi trovare nell'interfaccia web.


## 7.2. Autenticazione a due fattori

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

### 7.2.1. 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  in alto a destra dello schermo.
  3. Clicca su **account 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.  
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.

### 7.3. 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. Accesso [Bitdefender centrale](#).
2. Clicca il  icona nella parte in alto a destra dello schermo.
3. Clic **Account di Bitdefender** nel menu della diapositiva.
4. Seleziona il **Password e sicurezza** scheda.
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.

## 7.4. 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.

### 7.4.1. Aggiungere un nuovo dispositivo

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

1. Accesso [Bitdefender centrale](#).
2. Seleziona il **I miei dispositivi** pannello, quindi toccare **INSTALLA LA PROTEZIONE**.
3. Scegli una delle due opzioni disponibili:
  - **Proteggi questo dispositivo**  
Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, tocca il pulsante corrispondente.
  - **Proteggi altri dispositivi**  
Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, tocca il pulsante corrispondente.  
Clicca su **INVIA LINK DI DOWNLOAD**. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA E-MAIL**. Nota che il




link di download generato è valido solo per le prossime 24 ore. Se il link dovesse scadere, dovrai generarne uno nuovo seguendo gli stessi passaggi.

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


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

### 7.4.2. Personalizza il tuo dispositivo

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

1. Accesso [Bitdefender centrale](#).
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. Accesso [Bitdefender centrale](#).
2. Seleziona il **I miei dispositivi** pannello.
3. Toccare la scheda del dispositivo desiderato, quindi il  icona nell'angolo in alto a destra dello schermo.
4. Seleziona **Profilo**.
5. Clicca su **Aggiungi proprietario** e 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**.



### 7.4.3. Azioni in remoto

Per aggiornare Bitdefender in remoto su un dispositivo:

1. Accesso [Bitdefender centrale](#).
2. Seleziona il **I miei dispositivi** pannello.
3. Toccare la scheda del dispositivo desiderato, quindi il  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:

- **Dashboard.** In questa finestra, puoi visualizzare maggiori dettagli sul dispositivo selezionato, 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. In caso di problemi sul dispositivo, clicca sulla freccia a tendina nella parte superiore dell'area dello stato per scoprire maggiori dettagli. Qui
- **Protezione.** Da questa finestra puoi eseguire una scansione veloce o di sistema sui tuoi dispositivi in modalità remota. Clicca sul pulsante **ESAMINA** per avviare il processo. Puoi anche verificare quando è stata eseguita l'ultima scansione sul dispositivo oltre a un rapporto sulla stessa, con tutte le informazioni più importanti.
- **Ottimizzatore.** Qui puoi migliorare in remoto le prestazioni di un dispositivo esaminando, rilevando e rimuovendo rapidamente i file inutili. Clicca sul pulsante **INIZIA** e seleziona le aree che vuoi ottimizzare. Clicca di nuovo sul pulsante **INIZIA** per avviare il processo di ottimizzazione. Clicca su **Altri dettagli** per accedere a un rapporto dettagliato sui problemi risolti.
- **Anti-Theft.** In caso di smarrimento, perdita o furto, con la funzionalità Anti-Theft puoi localizzare il tuo dispositivo e intraprendere alcune azioni in remoto. Clicca su **LOCALIZZA** per scoprire la sua posizione. Sarà mostrata l'ultima posizione nota, insieme all'ora e alla data.





- **Vulnerabilità.** Per controllare un dispositivo alla ricerca di vulnerabilità, come aggiornamenti di Windows non installati, app datate o password deboli, clicca sul pulsante **ESAMINA** nella scheda Vulnerabilità. Le vulnerabilità non possono essere risolte in remoto. Nel caso fosse rilevata una qualche vulnerabilità, devi eseguire una nuova scansione sul dispositivo e intraprendere tutte le azioni necessarie. Clicca su **Altri dettagli** per accedere a un rapporto dettagliato sui problemi trovati.

## 7.5. Attività

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

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

- **I miei dispositivi.** Qui puoi visualizzare il numero di dispositivi connessi accanto al proprio stato di protezione. Per risolvere i problemi in remoto sui dispositivi rilevati, clicca su **Risolvi problemi** e poi 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.

## 7.6. I miei abbonamenti

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



## 7.6.1. Controllare gli abbonamenti disponibili

Per controllare gli abbonamenti disponibili:

1. Accesso [Bitdefender centrale](#).
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 utilizzano.

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).

## 7.6.2. Attiva abbonamento

Un abbonamento può essere attivato durante la fase di 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. Accesso [Bitdefender centrale](#).
2. Seleziona il **le mie sottoscrizioni** pannello.
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.

## 7.6.3. Rinnova abbonamento

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

1. Accesso [Bitdefender centrale](#).



2. Seleziona il **le mie sottoscrizioni** pannello.
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.



## 7.7. Notifiche

Per aiutarti a ricevere tutte le ultime informazioni 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.



## 8. DOMANDE FREQUENTI

### Come posso provare Bitdefender Antivirus for Mac prima di acquistare un abbonamento?

Sei un nuovo cliente di Bitdefender e vorresti provare il nostro prodotto prima di acquistarlo? Il periodo di prova dura 30 giorni ed è possibile continuare a utilizzare il prodotto installato, solo se acquisti un abbonamento a Bitdefender. Per provare Bitdefender Antivirus for Mac, devi:

1. Crea un account Bitdefender, seguendo questi passaggi:
  - a. Vai a: <https://central.bitdefender.com>.
  - b. Inserisci le informazioni richieste nei campi corrispondenti. I dati forniti resteranno riservati.
  - c. Prima di procedere ulteriormente devi accettare i Termini di utilizzo. Accedi ai Termini di utilizzo e leggili attentamente, in quanto contengono i termini e le condizioni con cui puoi utilizzare Bitdefender.  
Inoltre, potrai accedere e leggere l'Informativa sulla privacy.
  - d. Clicca su **CREA ACCOUNT**.
2. Scarica Bitdefender Antivirus for Mac come segue:
  - a. Seleziona il **I miei dispositivi** pannello, quindi fare clic su **INSTALLA LA PROTEZIONE**.
  - b. Scegli una delle due opzioni disponibili:
    - **Proteggi questo dispositivo**
      - i. Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.
      - ii. Salva il file di installazione.
    - **Proteggi altri dispositivi**
      - i. Seleziona questa opzione, quindi seleziona il proprietario del dispositivo. Se il dispositivo appartiene a qualcun altro, fai clic sul pulsante corrispondente.



- ii. Clic **INVIA IL LINK PER IL DOWNLOAD**.
- iii. Digita un indirizzo email nel campo corrispondente e fai clic **INVIA UNA EMAIL**.  
Si noti che il collegamento per il download generato è valido solo per le prossime 24 ore. Se il link scade, dovrai generarne uno nuovo seguendo gli stessi passaggi.
- iv. Sul dispositivo su cui desideri installare il tuo prodotto Bitdefender, controlla l'account e-mail che hai digitato, quindi fai clic sul pulsante di download corrispondente.

c. Esegui il prodotto Bitdefender che hai scaricato.

### **Ho un codice di attivazione. Come posso aggiungere la sua validità al mio abbonamento?**

Se hai acquistato un codice di attivazione da uno dei nostri rivenditori o l'hai ricevuto in regalo, puoi aggiungere la sua disponibilità al tuo abbonamento a Bitdefender.

Per attivare un abbonamento utilizzando un codice di attivazione, attenersi alla seguente procedura:

1. Accesso [Bitdefender centrale](#).
2. Seleziona il **le mie sottoscrizioni** pannello.
3. Clicca il **CODICE DI ATTIVAZIONE** pulsante, quindi digitare il codice nel campo corrispondente.
4. Clic **ATTIVARE** continuare.

Ora l'estensione è visibile nel tuo account Bitdefender e nel tuo prodotto Bitdefender Antivirus for Mac installato, nel lato in basso a destra della schermata.

### **Il registro della scansione indica che ci sono ancora alcuni elementi non risolti. Come posso rimuoverli?**

Gli elementi non risolti nel registro della scansione possono essere:

- ☐ archivi ad accesso limitato (xar, rar, ecc.)  
**Soluzione:** usa l'opzione **Svela in Finder** per trovare il file ed eliminarlo manualmente. Assicurati di svuotare il Cestino.
- ☐ caselle di posta ad accesso limitato (Thunderbird, ecc.)



**Soluzione:** usa l'applicazione per rimuovere l'elemento contenente il file infetto.

○ Contenuti nei backup

**Soluzione:** attiva l'opzione **Non esaminare i contenuti nei backup** nelle preferenze della Protezione o **Aggiungi a eccezioni** i file rilevati.

Se i file infetti venissero ripristinati in un secondo momento, Bitdefender Antivirus for Mac li rileverà automaticamente, adottando tutti i provvedimenti necessari.



### Nota

I file ad accesso limitato sono file che solo Bitdefender Antivirus for Mac può aprire, ma non può comunque modificarli.

### Dove posso visualizzare maggiori dettagli sulle attività del prodotto?

Bitdefender salva un registro di tutte le azioni importanti, i cambiamenti di stato e gli altri messaggi critici relativi alle sue attività. Per accedere a tali informazioni, clicca su **Notifiche** nel menu di navigazione nell'interfaccia di Bitdefender.

### Posso aggiornare Bitdefender Antivirus for Mac attraverso un server proxy?

Bitdefender Antivirus for Mac può aggiornarsi solo tramite server proxy che non richiedono l'autenticazione. Non è necessario configurare alcuna impostazione del programma.

Se ti connetti a Internet tramite un server proxy che richiede l'autenticazione, devi passare regolarmente a una connessione Internet diretta per ottenere gli aggiornamenti delle informazioni sulle minacce.

### Come posso rimuovere Bitdefender Antivirus for Mac?

Per rimuovere Bitdefender Antivirus for Mac, segui questi passaggi:

1. Apri una finestra di **Finder** e vai alla cartella Applicazioni.
2. Apri la cartella Bitdefender e poi clicca due volte su BitdefenderUninstaller.
3. Clic **Disinstalla** e attendere il completamento del processo.
4. Clic **Vicino** finire.



## Importante

Se c'è un errore, puoi contattare l'assistenza clienti di Bitdefender come descritto in [Richiesta d'aiuto \(pagina 53\)](#).

### Come posso rimuovere le estensioni di TrafficLight dal mio browser web?

- Per rimuovere le estensioni di TrafficLight da Mozilla Firefox, segui questi passaggi:
  1. Vai in **Strumenti** e seleziona **Add-on**.
  2. Seleziona **Estensioni** sulla colonna a sinistra.
  3. Seleziona l'estensione e clicca su **Rimuovi**.
  4. Riavvia il browser per completare il processo di rimozione.
- Per rimuovere le estensioni di TrafficLight da Google Chrome, segui questi passaggi:
  1. In alto a destra, clicca su **Altri** ⋮.
  2. Vai in **Altri strumenti** e seleziona **Estensioni**.
  3. Clicca sull'icona **Rimuovi** 🗑️ accanto all'estensione che desideri rimuovere.
  4. Clicca su **Rimuovi** per confermare il processo di rimozione.
- Per rimuovere Bitdefender TrafficLight da Safari, segui questi passaggi:
  1. Vai in **Preferenze** o premi **Command-Comma(,)**.
  2. Seleziona **Estensioni**.  
Comparirà un elenco con le estensioni installate.
  3. Seleziona l'estensione Bitdefender TrafficLight e clicca su **Disinstalla**.
  4. Clicca nuovamente su **Disinstalla** per confermare il processo di rimozione.

### Quando devo utilizzare Bitdefender VPN?

Devi fare sempre attenzione quando accedi, scarichi o invii contenuti su internet. Per assicurarti di essere sempre al sicuro mentre navighi sul web, ti consigliamo di utilizzare Bitdefender VPN quando:





- vuoi connetterti a reti wireless pubbliche
- vuoi accedere a contenuti che normalmente sono riservati a determinate aree, indipendentemente dal fatto che ti trovi a casa o all'estero
- vuoi mantenere i tuoi dati personali privati (nomi utente, password, informazioni della carta di credito, ecc.)
- vuoi nascondere il tuo indirizzo IP

### **Bitdefender VPN avrà un impatto negativo sulla durata della batteria del mio dispositivo?**

Bitdefender VPN è progettato per proteggere i tuoi dati personali, nascondere il tuo indirizzo IP mentre ti connetti a reti wireless non sicure e accedere a contenuti inaccessibili in determinati paesi. Per evitare un consumo non necessario della batteria del tuo dispositivo, ti consigliamo di utilizzare VPN solo quando ne hai bisogno e disconnetterti quando sei offline.

### **Perché riscontro rallentamenti in Internet durante la connessione con Bitdefender VPN?**

Bitdefender VPN è stato progettato per offrirti un'esperienza di navigazione sul web leggera; tuttavia, la tua connettività a Internet o la distanza del server a cui ti connetti potrebbero causare dei rallentamenti. In questo caso, se non è obbligatorio connetterti a un server ospitato molto distante (ad esempio negli Stati Uniti o in Cina), ti consigliamo di consentire a Bitdefender VPN di connettersi automaticamente al server più vicino o trovarne uno più vicino alla tua ubicazione attuale.



## 9. OTTENERE AIUTO

### 9.1. Richiesta d'aiuto

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

### 9.2. Risorse online

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

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

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

#### 9.2.1. Centro di supporto di Bitdefender

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

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



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

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

### 9.2.2. La community di esperti di Bitdefender

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

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

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

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

### 9.2.3. Bitdefender Cyberpedia

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

La pagina web di Bitdefender Cyberpedia è disponibile qui:

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



## 9.3. Informazioni di contatto

Una comunicazione efficiente è la chiave per un business di successo. Dal 2001 BITDEFENDER ha stabilito una reputazione indiscutibile impegnandosi costantemente per una migliore comunicazione in modo da superare le aspettative dei nostri clienti e partner. In caso di domande, non esitate a contattarci direttamente tramite il ns [Centro di supporto di Bitdefender \(pagina 53\)](#).

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

### 9.3.1. Distributori locali

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

Per trovare un distributore di Bitdefender nel tuo paese:

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



## GLOSSARIO

### **Codice di attivazione**

È una chiave univoca che può essere acquistata al dettaglio e utilizzata per attivare un prodotto o servizio specifico. Un codice di attivazione consente l'attivazione di un abbonamento valido per un certo periodo di tempo e numero di dispositivi e può essere utilizzato anche per estendere un abbonamento con la condizione da generare per lo stesso prodotto o servizio.

### **ActiveX**

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

### **Minaccia persistente avanzata**

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

### **Adware**

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



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

### **Archivio**

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

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

### **Porta sul retro**

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

### **Settore di avvio**

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

### **Avvio virus**

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

### **Botnet**

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

### **Navigatore**

Abbreviazione di browser Web, un'app software utilizzata per individuare e visualizzare pagine Web. I browser più diffusi includono Microsoft Internet



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

### **Attacco di forza bruta**

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

### **Riga di comando**

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

### **Biscotti**

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

### **Cyber bullismo**

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

### **Dizionario Attacco**

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



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

### **Unità disco**

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

### **Scaricamento**

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

### **E-mail**

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

### **Eventi**

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

### **Exploit**

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

### **Falso positivo**

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

### **Estensione del nome file**

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





### **Euristico**

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

### **Vaso di miele**

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

### **IP**

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

### **Applet Java**

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

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

### **Registratore di tasti**

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



### **Virus a macroistruzione**

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

### **Cliente di posta**

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

### **Memoria**

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

### **Non euristico**

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

### **Predatori online**

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

### **Programmi confezionati**

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

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



### **Sentiero**

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

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

### **Phishing**

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

### **Fotone**

Photon è una tecnologia di Bitdefender innovativa e discreta, progettata per minimizzare l'impatto della tua soluzione di sicurezza sulle prestazioni del sistema. Monitorando in background l'attività del PC, crea degli schemi di utilizzo, per ottimizzare i processi di avvio e scansione.

### **Virus polimorfo**

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

### **Porta**

Un'interfaccia su un computer alla quale puoi connettere un supporto. I PC hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, schermi e tastiere. Esternamente hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

Nelle reti TCP/IP e UDP, un endpoint per una connessione logica. Il numero della porta identifica di che tipo di porta si tratta. Ad esempio, la porta 80 viene usata per il traffico HTTP.

### **Ransomware**

Un ransomware è un programma dannoso che prova a sottrarre illecitamente denaro agli utenti bloccando i loro sistemi vulnerabili.



CryptoLocker, CryptoWall e TeslaWall sono solo alcune delle varianti che cercano di bloccare i sistemi personali degli utenti.

L'infezione può partire, aprendo e-mail di spam, scaricando gli allegati di un messaggio o installando determinate applicazioni, il tutto lasciando l'utente ignaro di ciò che sta accadendo sul suo sistema. Gli autori di ransomware puntano a colpire soprattutto gli utenti normali e le aziende.

### **File di rapporto**

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

### **Rootkit**

Un rootkit è una serie di strumenti software che offre accesso a livello di amministratore a un sistema. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la propria presenza in modo da non dover essere visti dai veri amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, i login e i log. Possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche, se incorporano il software adeguato.

I rootkit non sono dannosi per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando i rootkit. Comunque, vengono principalmente utilizzati per nascondere minacce o per celare la presenza di un intruso nel sistema. Se combinati alle minacce, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e registri, ed evitare il rilevamento.

### **Script**

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

### **Spam**

Messaggi di posta elettronica o newsgroup indesiderati. Generalmente conosciuti come e-mail non desiderate.

### **Spyware**



Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessione a Internet, senza che questo se ne accorga, di solito per scopi pubblicitari. Le applicazioni spyware in genere sono incluse come componente nascosta di programmi freeware o shareware, che possono essere scaricati da Internet. Tuttavia, occorre segnalare che la maggioranza delle applicazioni shareware o freeware non includono alcun programma spyware. Una volta installato, uno spyware monitora le attività dell'utente su Internet e trasmette di nascosto tali informazioni a qualcun altro. Gli spyware possono anche raccogliere informazioni su indirizzi e-mail o addirittura password e numeri di carta di credito.

Gli spyware sono simili a un Trojan che gli utenti installano inconsapevolmente installando altre applicazioni. Un modo comune per diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli spyware utilizzano memoria e risorse del sistema, le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

### **Articoli di avvio**

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

### **Abbonamento**

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

### **Area di notifica**

Introdotta con Windows 95, la barra degli strumenti è situata nella barra delle applicazioni di Windows (in genere in basso vicino all'orologio) e contiene icone miniaturizzate per un accesso veloce a funzioni di sistema come fax, stampante, modem, volume e molto altro. Clicca due volte o



clicca con il pulsante destro su un'icona per visualizzare e accedere a dettagli e controlli.

### **TCP/IP**

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di rete largamente utilizzati su Internet, che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il relativo traffico.

### **Minaccia**

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

### **Aggiornamento delle informazioni sulle minacce**

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

### **Troiano**

Un programma distruttivo che si maschera da applicazione benevola. A differenza di programmi software dannosi e worm, i trojan non si replicano ma possono essere altrettanto distruttivi. Un tipo di minaccia Trojan particolarmente insidiosa è un programma che dichiara di pulire le minacce dal computer, ma al contrario le introduce.

Il termine deriva dalla storia dell'Iliade di Omero, dove i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, durante la notte, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

### **Aggiornamento**



Una nuova versione di un prodotto software o hardware creato per sostituire una versione precedente dello stesso prodotto. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul computer; diversamente non sarà possibile installare l'aggiornamento.

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

### **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.

### **Verme**

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