

Bitdefender[®] **ANTIVIRUS PLUS 2016**



MANUALE D'USO



Bitdefender Antivirus Plus 2016 Manuale d'uso

Data di pubblicazione 02/02/2016

Diritto d'autore© 2016 Bitdefender

Avvertenze legali

Tutti i diritti riservati. Nessuna parte di questo manuale può essere riprodotta o trasmessa in alcuna forma o tramite qualsiasi strumento, elettronico o meccanico, incluse fotocopie, registrazioni, o attraverso qualsiasi informazione di archivio o sistema di recupero dati, senza il consenso scritto di un rappresentante autorizzato di Bitdefender. L'inserimento di brevi citazioni nelle recensioni è possibile solo indicando la fonte citata. Il contenuto non può essere modificato in alcun modo.

Avvertenze e Limiti. Questo prodotto e la sua documentazione sono protetti dal diritto d'autore. Le informazioni su questo documento sono fornite «così come sono» senza alcuna garanzia. Sebbene sia stata adottata ogni precauzione nella preparazione di questo documento, gli autori non hanno alcun obbligo nei confronti di alcuna persona o entità rispetto a qualsiasi perdita o danno causati o che si presume essere stati causati, direttamente o indirettamente, dalle informazioni contenute in questo prodotto.

Questo manuale contiene collegamenti a siti Internet di terze parti, che non sono sotto il controllo di Bitdefender, conseguentemente Bitdefender non è responsabile per il contenuto di qualsiasi sito collegato. Se accedi a siti Internet di terze parti, menzionati in questo manuale, lo farai assumendotene tutti i rischi. Bitdefender fornisce tali collegamenti solo come risorsa, e l'inclusione dei collegamenti non implica che Bitdefender approvi o accetti alcuna responsabilità per il contenuto dei siti di terze parti.

Marchi registrati. In questo manuale potrebbero essere citati nomi e marchi registrati. Tutti i marchi registrati e non in questo documento appartengono ai rispettivi proprietari e vengono rispettosamente riconosciuti.



Indice

Installazione	1
1. Prepararsi all'installazione	2
2. Requisiti di sistema	3
2.1. Requisiti minimi di sistema	3
2.2. Requisiti di sistema consigliati	3
2.3. Requisiti software	4
3. Installare il tuo prodotto Bitdefender	5
3.1. Installa da Bitdefender Central	5
3.2. Installa dal disco di installazione	8
Inizia	13
4. Le basi	14
4.1. Aprire la finestra di Bitdefender	14
4.2. Risolvere i problemi	15
4.2.1. Procedura guidata Risolvi ogni problema	16
4.2.2. Configurare gli avvisi di stato	17
4.3. Eventi	17
4.4. Autopilot	19
4.5. Profili e Modalità Batteria	19
4.5.1. Profili	20
4.5.2. Modalità Batteria	21
4.6. Impostazioni protette da password di Bitdefender	22
4.7. Rapporti anonimi sull'utilizzo	23
4.8. Offerte speciali e notifiche sul prodotto	24
5. Interfaccia di Bitdefender	25
5.1. Icona area di notifica	25
5.2. Finestra principale	27
5.2.1. Barra degli strumenti superiore	27
5.2.2. Pulsanti d'azione	28
5.3. I moduli di Bitdefender	29
5.3.1. Protezione	29
5.3.2. Privacy	30
5.3.3. Strumenti	31
5.4. Widget sicurezza	32
5.4.1. Eseguire la scansione di file e cartelle	33
5.4.2. Nascondi / mostra widget sicurezza	33
5.5. Rapporto sicurezza	34
5.5.1. Controllare il Rapporto sicurezza	35
5.5.2. Attivare o disattivare la notifica del Rapporto di sicurezza	36
6. Bitdefender Central	38
6.1. Accedere al tuo account Bitdefender Central	38
6.2. I miei abbonamenti	39



6.2.1. Controllare gli abbonamenti disponibili	39
6.2.2. Aggiungi un nuovo dispositivo	39
6.2.3. Rinnova abbonamento	40
6.2.4. Attiva abbonamento	40
6.3. I miei dispositivi	40
7. Mantenere aggiornato Bitdefender	43
7.1. Verificare se Bitdefender è aggiornato	43
7.2. Eseguire un aggiornamento	44
7.3. Attivare o disattivare l'aggiornamento automatico	45
7.4. Modificare le impostazioni di aggiornamento	45

Come fare 47

8. Installazione	48
8.1. Come faccio a installare Bitdefender su un secondo computer?	48
8.2. Quando dovrei reinstallare Bitdefender?	48
8.3. Dove posso scaricare il mio prodotto Bitdefender?	49
8.4. Come posso utilizzare il mio abbonamento a Bitdefender dopo aver aggiornato Windows?	49
8.5. Come posso riparare Bitdefender?	52
9. Abbonamenti	54
9.1. Quale prodotto Bitdefender sto usando?	54
9.2. Come posso attivare l'abbonamento di Bitdefender utilizzando un codice di licenza?	54
10. Bitdefender Central	56
10.1. Come posso accedere a Bitdefender Central utilizzando un altro account online?	56
10.2. Come posso cambiare la password dell'account Bitdefender Central?	56
11. Scansione con Bitdefender	58
11.1. Come posso controllare un file o una cartella?	58
11.2. Come posso eseguire una scansione del mio sistema?	58
11.3. Come posso programmare una scansione?	59
11.4. Come posso creare un'attività di scansione personale?	59
11.5. Come posso escludere una cartella dalla scansione?	60
11.6. Cosa fare quando Bitdefender rileva un file pulito come infetto?	61
11.7. Come posso verificare quali virus sono stati rilevati da Bitdefender?	62
12. Controllo privacy	64
12.1. Come posso essere certo che le mie transazioni online sono sicure?	64
12.2. Come posso eliminare un file in modo permanente con Bitdefender?	64
13. Informazioni utili	65
13.1. Come faccio a testare la mia soluzione antivirus?	65
13.2. Come posso rimuovere Bitdefender?	65
13.3. Come posso spegnere automaticamente il computer al termine della scansione?	66
13.4. Come posso configurare Bitdefender per usare una connessione a Internet tramite proxy?	67



13.5. Sto usando una versione di Windows a 32 o 64 bit?	69
13.6. Come posso visualizzare gli elementi nascosti in Windows?	69
13.7. Come posso rimuovere le altre soluzioni di sicurezza?	70
13.8. Come posso riavviare in modalità provvisoria?	71

Gestire la propria sicurezza 73

14. Protezione antivirus	74
14.1. Scansione all'accesso (protezione in tempo reale)	75
14.1.1. Attivare o disattivare la protezione in tempo reale	75
14.1.2. Impostare il livello di protezione in tempo reale	76
14.1.3. Configurare le impostazioni della protezione in tempo reale	76
14.1.4. Ripristinare le impostazioni predefinite	80
14.2. Scansione a richiesta	81
14.2.1. Controllare un file o una cartella alla ricerca di malware	81
14.2.2. Eseguire una Scansione veloce	82
14.2.3. Eseguire una scansione del sistema	82
14.2.4. Configurare una scansione personale	83
14.2.5. Procedura guidata scansione antivirus	86
14.2.6. Controllare i registri di scansione	89
14.3. Scansione automatica di supporti rimovibili	90
14.3.1. Come funziona?	90
14.3.2. Gestire la scansione di supporti rimovibili	91
14.4. Configurare le eccezioni della scansione	92
14.4.1. Escludere file o cartelle dalla scansione	92
14.4.2. Escludere estensioni di file dalla scansione	93
14.4.3. Gestire le eccezioni della scansione	94
14.5. Gestire i file in quarantena	95
14.6. Active Threat Control	96
14.6.1. Verificare le applicazioni rilevate	97
14.6.2. Attivare o disattivare Active Threat Control	97
14.6.3. Impostare la protezione di Active Threat Control	97
14.6.4. Gestire i processi esclusi	98
15. Protezione web	100
15.1. Avvisi di Bitdefender nel browser	101
16. Protezione dati	102
16.1. Eliminare i file in modo permanente	102
17. Vulnerabilità	104
17.1. Controllare il sistema per rilevare vulnerabilità	104
17.2. Usare il controllo automatico delle vulnerabilità	105
18. Protezione da Ransomware	108
18.1. Attivare o disattivare la Protezione da Ransomware	108
18.2. Proteggi i tuoi file personali dagli attacchi dei Ransomware.	109
18.3. Configurare le applicazioni attendibili	109
18.4. Configurare le applicazioni bloccate	110
18.5. Protezione all'avvio	110



19. Safepay: sicurezza per le transazioni online	111
19.1. Utilizzare Bitdefender Safepay™	112
19.2. Configurare le impostazioni	113
19.3. Gestire i segnalibri	114
19.4. Protezione hotspot per reti non sicure	115
20. Protezione di Password Manager per le tue credenziali	116
20.1. Configurare Password Manager	117
20.2. Attivare o disattivare la protezione del Password Manager	120
20.3. Gestire le impostazioni del Password Manager	120
21. Bitdefender USB Immunizer	124
Ottimizzazione sistema	125
22. Profili	126
22.1. Profilo Lavoro	127
22.2. Profilo Film	128
22.3. Profilo Gioco	129
22.4. Ottimizzazione in tempo reale	131
Risoluzione dei problemi	132
23. Risolvere i problemi più comuni	133
23.1. Il mio sistema sembra lento	133
23.2. La scansione non parte	134
23.3. Non riesco più a usare un'applicazione	137
23.4. Cosa fare quando Bitdefender blocca un sito web o un'applicazione online sicuri	138
23.5. Come aggiornare Bitdefender con una connessione a Internet lenta	139
23.6. I servizi Bitdefender non rispondono	140
23.7. L'opzione Compila automaticamente nel mio Portafoglio non funziona	140
23.8. Rimozione di Bitdefender non riuscita	142
23.9. Il sistema non si riavvia dopo aver installato Bitdefender	143
24. Rimuovere malware dal sistema	147
24.1. Modalità soccorso di Bitdefender	147
24.2. Cosa fare quando Bitdefender trova dei virus sui tuoi computer?	149
24.3. Come posso rimuovere un virus in un archivio?	151
24.4. Come posso rimuovere un virus nell'archivio delle e-mail?	152
24.5. Cosa fare se sospetti che un file possa essere pericoloso?	153
24.6. Quali sono i file protetti da password nel registro della scansione?	153
24.7. Quali sono gli elementi ignorati nel registro della scansione?	154
24.8. Quali sono i file supercompressi nel registro della scansione?	154
24.9. Perché Bitdefender ha eliminato automaticamente un file infetto?	154
Contattaci	156
25. Chiedere aiuto	157
26. Risorse online	159



26.1. Centro di supporto di Bitdefender	159
26.2. Forum supporto di Bitdefender	159
26.3. Portale HOTforSecurity	160
27. Informazioni di contatto	161
27.1. Indirizzi web	161
27.2. Distributori locali	161
27.3. Uffici di Bitdefender	161
Glossario	164



INSTALLAZIONE



1. PREPARARSI ALL'INSTALLAZIONE

Prima di installare Bitdefender Antivirus Plus 2016, completa questi passaggi preliminari per assicurarti che l'installazione funzioni senza problemi:

- Assicurati che il computer su cui desideri installare Bitdefender soddisfi i requisiti minimi di sistema. Se il computer non soddisfa i requisiti minimi di sistema, Bitdefender non sarà installato, o se installato, non funzionerà correttamente e potrà causare rallentamenti e instabilità del sistema. Per un elenco completo dei requisiti di sistema, consultare la sezione «*Requisiti di sistema*» (p. 3).
- Accedere al computer utilizzando un account Amministratore.
- Rimuovi qualsiasi altro programma simile dal computer. L'esecuzione simultanea di due programmi di sicurezza può influenzarne il funzionamento e causare problemi seri al sistema. Durante l'installazione Windows Defender sarà disattivato.
- Assicurati che il computer sia connesso a Internet durante l'installazione, anche se l'hai avviata da un CD/DVD. Se sono disponibili versioni più recenti dei file dell'applicazione inclusi nel pacchetto d'installazione, Bitdefender può scaricarli e installarli.



2. REQUISITI DI SISTEMA

Puoi installare Bitdefender Antivirus Plus 2016 solo su computer con i seguenti sistemi operativi:

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

Prima dell'installazione, assicurati che il computer soddisfi i requisiti minimi di sistema.



Nota

Per scoprire quale versione di Windows è attiva sul computer e maggiori informazioni sull'hardware, segui questi passaggi:

- In **Windows 7**, clicca con il pulsante destro su **Computer** nel desktop (o cliccando prima sul pulsante Start) e poi seleziona **Proprietà**.
- In **Windows 8 e Windows 8.1**, dal menu Start di Windows, localizza l'opzione Computer (puoi anche digitare direttamente "Computer" nella finestra di ricerca del menu Start) e poi clicca sulla sua icona con il pulsante destro. Seleziona Proprietà nel menu inferiore. Individua la sezione Sistema per trovare maggiori informazioni sul tuo sistema.
- In **Windows 10**, digita "Sistema" nella casella di ricerca della barra delle attività e clicca sulla sua icona. Individua la sezione Sistema per trovare maggiori informazioni sul tuo sistema.

2.1. Requisiti minimi di sistema

- 1 GB di spazio disponibile su disco rigido (almeno 800 MB sull'unità di sistema)
- Processore da 1.6 GHz
- 1 GB di memoria (RAM)

2.2. Requisiti di sistema consigliati

- 2 GB di spazio disponibile su disco rigido (almeno 800 MB sull'unità di sistema)
- Intel CORE Duo (2 GHz) o processore equivalente
- 2 GB di memoria (RAM)



2.3. Requisiti software

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

- Internet Explorer 10 o superiore
- Mozilla Firefox 14 o superiore
- Google Chrome 20 o superiore
- Skype 6.3 o superiore
- Yahoo! Messenger 9 o superiore



3. INSTALLARE IL TUO PRODOTTO BITDEFENDER

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

Se il tuo acquisto vale per più di un computer (per esempio hai acquistato Bitdefender Antivirus Plus 2016 per 3 PC), ripeti il processo d'installazione e attiva il prodotto con lo stesso account su ogni computer. L'account che devi utilizzare è quello che include il tuo abbonamento attivo a Bitdefender.

3.1. Installa da Bitdefender Central

Dall'account Bitdefender Central, puoi scaricare il kit d'installazione corrispondente all'abbonamento acquistato. Una volta completato il processo d'installazione, Bitdefender Antivirus Plus 2016 viene attivato.

Per scaricare Bitdefender Antivirus Plus 2016 dal tuo account Bitdefender Central, segui questi passaggi:

1. Accedi al tuo **account Bitdefender Central**
2. Seleziona la scheda **I miei dispositivi**.
3. Nella finestra **I miei dispositivi**, clicca su **INSTALLA Bitdefender**.
4. Seleziona una delle due opzioni disponibili:

● **SCARICA**

Clicca sul pulsante e salva il file d'installazione.

● **Su un altro dispositivo**

Seleziona **Windows** per scaricare il tuo prodotto Bitdefender e poi clicca su **CONTINUA**. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA**.

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

Convalidare l'installazione

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



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

Se viene rilevato un programma antivirus incompatibile o una versione precedente di Bitdefender, ti sarà chiesto di rimuoverla dal sistema. Segui le istruzioni per rimuovere il programma dal sistema, per evitare eventuali problemi in seguito. Potrebbe essere necessario riavviare il computer per completare la rimozione dei programmi antivirus rilevati.

Il pacchetto d'installazione di Bitdefender Antivirus Plus 2016 è aggiornato costantemente.



Nota

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

Una volta convalidata l'installazione, comparirà la procedura guidata della configurazione. Segui tutti i passaggi per installare Bitdefender Antivirus Plus 2016.

Fase 1 - Installazione di Bitdefender

La schermata d'installazione di Bitdefender ti consente di selezionare il tipo d'installazione che desideri eseguire.

Per un'installazione senza problemi, basta cliccare sul pulsante **Installa**. Bitdefender sarà installato nel percorso predefinito con le impostazioni standard, passando direttamente alla **Fase 3** della procedura guidata.

Se desideri configurare le impostazioni dell'installazione, clicca su **Personal..**

In questa fase possono essere eseguite due attività aggiuntive:

- Prima di procedere con l'installazione, leggi l'Accordo di licenza con l'utente finale. L'Accordo di licenza contiene i termini e le condizioni per poter utilizzare Bitdefender Antivirus Plus 2016.

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

- Mantieni attivata l'opzione **Invia rapporti anonimi sull'utilizzo**. Permettendo questa opzione, i rapporti contenenti informazioni su come il prodotto viene utilizzato sono inviati ai server Bitdefender. Queste informazioni sono essenziali per migliorare il prodotto e possono aiutarci a offrire una



migliore esperienza in futuro. I rapporti non conterranno dati confidenziali, come nome o indirizzo IP, e non saranno utilizzati per scopi commerciali.

Fase 2 - Personalizzare le impostazioni dell'installazione



Nota

Questa fase appare solo se hai selezionato di personalizzare l'installazione durante la fase precedente.

Sono disponibili le seguenti opzioni:

Percorso di installazione

Di norma, Bitdefender Antivirus Plus 2016 sarà installato in C:\Programmi\Bitdefender\Bitdefender 2016. Se desideri modificare il percorso di installazione, clicca su **Modifica** e seleziona la cartella dove vuoi installare Bitdefender.

Configura le impostazioni proxy

Bitdefender Antivirus Plus 2016 richiede l'accesso a Internet per l'attivazione del prodotto, il download di aggiornamenti per la sicurezza e il prodotto, le componenti di rilevazione in-the-cloud, ecc. Se usi una connessione proxy invece di una connessione a Internet diretta, devi selezionare questa opzione e configurare le impostazioni del proxy.

Le impostazioni possono essere importate dal browser predefinito o inserite manualmente.

Clicca su **Installa** per confermare le tue preferenze e iniziare l'installazione. Se cambiassi idea, clicca sul pulsante corrispondente **Usa predefiniti**.

Fase 3 - Installazione in corso

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

Una scansione controlla le aree critiche del sistema alla ricerca di virus, vengono scaricate ed eventualmente installate le ultime versioni dei file dell'applicazione e i servizi di Bitdefender vengono avviati. Questa fase può richiedere alcuni minuti.

Fase 4 - Fine dell'installazione

Il tuo prodotto Bitdefender è stato installato con successo.



Viene mostrato un resoconto dell'installazione. Se durante l'installazione viene rilevato e rimosso qualche malware attivo, è necessario riavviare il sistema. Clicca su **OK** per continuare.

Fase 5 - Come iniziare

Nella finestra Come iniziare, puoi verificare la validità del tuo abbonamento.

In questa fase possono essere eseguite due attività aggiuntive:

- **Acquista un nuovo abbonamento** - questo link ti reindirizza alla pagina di Bitdefender, dove puoi acquistare un nuovo abbonamento.
- **Ho un codice di attivazione** - Questo link ti reindirizza al tuo account Bitdefender Central. Digita il tuo codice di attivazione nel campo corrispondente e clicca su **INVIA**. In alternativa, puoi digitare un codice di licenza valido che sarà convertito in un abbonamento con le stesse caratteristiche, in fatto di numero di dispositivi e disponibilità residua.

Clicca su **Fine** per accedere all'interfaccia di Bitdefender Antivirus Plus 2016.

3.2. Installa dal disco di installazione

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

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



Nota

La schermata d'installazione fornisce un'opzione per copiare il pacchetto d'installazione dal disco a un dispositivo USB. Ciò è utile se devi installare Bitdefender su un computer che non ha un'unità disco (per esempio, su un netbook). Inserisci il dispositivo USB nella porta USB e clicca su **Copia su USB**. In seguito, spostati sul computer senza unità CD, inserisci il dispositivo USB nella porta USB e clicca due volte su `runsetup.exe` dalla cartella nella quale hai salvato il pacchetto di installazione.

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



Convalidare l'installazione

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

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

Se viene rilevato un programma antivirus incompatibile o una versione precedente di Bitdefender, ti sarà chiesto di rimuoverla dal sistema. Segui le istruzioni per rimuovere il programma dal sistema, per evitare eventuali problemi in seguito. Potrebbe essere necessario riavviare il computer per completare la rimozione dei programmi antivirus rilevati.

Il pacchetto d'installazione di Bitdefender Antivirus Plus 2016 è aggiornato costantemente.



Nota

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

Una volta convalidata l'installazione, comparirà la procedura guidata della configurazione. Segui tutti i passaggi per installare Bitdefender Antivirus Plus 2016.

Fase 1 - Installazione di Bitdefender

La schermata d'installazione di Bitdefender ti consente di selezionare il tipo d'installazione che desideri eseguire.

Per un'installazione senza problemi, basta cliccare sul pulsante **Installa**. Bitdefender sarà installato nel percorso predefinito con le impostazioni standard, passando direttamente alla **Fase 3** della procedura guidata.

Se desideri configurare le impostazioni dell'installazione, clicca su **Personal..**

In questa fase possono essere eseguite due attività aggiuntive:

- Prima di procedere con l'installazione, leggi l'Accordo di licenza con l'utente finale. L'Accordo di licenza contiene i termini e le condizioni per poter utilizzare Bitdefender Antivirus Plus 2016.

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



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

Fase 2 - Personalizzare le impostazioni dell'installazione



Nota

Questa fase appare solo se hai selezionato di personalizzare l'installazione durante la fase precedente.

Sono disponibili le seguenti opzioni:

Percorso di installazione

Di norma, Bitdefender Antivirus Plus 2016 sarà installato in C:\Programmi\Bitdefender\Bitdefender 2016. Se desideri modificare il percorso di installazione, clicca su **Modifica** e seleziona la cartella dove vuoi installare Bitdefender.

Configura le impostazioni proxy

Bitdefender Antivirus Plus 2016 richiede l'accesso a Internet per l'attivazione del prodotto, il download di aggiornamenti per la sicurezza e il prodotto, le componenti di rilevazione in-the-cloud, ecc. Se usi una connessione proxy invece di una connessione a Internet diretta, devi selezionare questa opzione e configurare le impostazioni del proxy.

Le impostazioni possono essere importate dal browser predefinito o inserite manualmente.

Clicca su **Installa** per confermare le tue preferenze e iniziare l'installazione. Se cambiassi idea, clicca sul pulsante corrispondente **Usa predefiniti**.

Fase 3 - Installazione in corso

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

Una scansione controlla le aree critiche del sistema alla ricerca di virus, vengono scaricate ed eventualmente installate le ultime versioni dei file dell'applicazione e i servizi di Bitdefender vengono avviati. Questa fase può richiedere alcuni minuti.



Fase 4 - Fine dell'installazione

Viene mostrato un resoconto dell'installazione. Se durante l'installazione viene rilevato e rimosso qualche malware attivo, è necessario riavviare il sistema. Clicca su **OK** per continuare.

Fase 5 - Bitdefender Central

Dopo aver completato la configurazione iniziale, comparirà la finestra Bitdefender Central. Per attivare il prodotto e utilizzare le sue funzioni online, è necessario avere un account Bitdefender Central. Per maggiori informazioni, fai riferimento a «*Bitdefender Central*» (p. 38).

Procedi in base alla tua situazione.

Ho già un account Bitdefender Central

Inserisci l'indirizzo e-mail e la password per il tuo account Bitdefender Central e clicca su **ACCEDI**.

Se hai dimenticato la password del tuo account o semplicemente vuoi cambiarla, clicca sul link **Cambia password**. Inserisci il tuo indirizzo e-mail e clicca sul pulsante **CAMBIA PASSWORD**.

Voglio creare un account Bitdefender Central

Per creare un account Bitdefender Central, clicca sul link **Registrati** nella parte inferiore della finestra. Inserisci le informazioni richieste nei campi corrispondenti e clicca sul pulsante **CREA ACCOUNT**.

I dati forniti resteranno riservati.

La password deve essere composta da almeno 8 caratteri e includere un numero.



Nota

Una volta che l'account è stato creato, puoi utilizzare l'indirizzo e-mail e la password forniti per accedere all'account all'indirizzo <https://central.bitdefender.com>.

Voglio accedere usando il mio account Microsoft, Facebook o Google

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

1. Seleziona il servizio che vuoi utilizzare. Sarai reindirizzato alla pagina di accesso del servizio.



2. Segui le istruzioni fornite dal servizio selezionato per collegare il tuo account a Bitdefender.



Nota

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

Fase 6 - Come iniziare

Nella finestra Come iniziare, puoi verificare la validità del tuo abbonamento.

In questa fase possono essere eseguite due attività aggiuntive:

- **Acquista un nuovo abbonamento** - questo link ti reindirizza alla pagina di Bitdefender, dove puoi acquistare un nuovo abbonamento.
- **Ho un codice di attivazione** - Questo link ti reindirizza al tuo account Bitdefender Central. Digita il tuo codice di attivazione nel campo corrispondente e clicca su **INVIA**. In alternativa, puoi digitare un codice di licenza valido che sarà convertito in un abbonamento con le stesse caratteristiche, in fatto di numero di dispositivi e disponibilità residua.

Clicca su **Fine** per accedere all'interfaccia di Bitdefender Antivirus Plus 2016.



INIZIA



4. LE BASI

Una volta installato Bitdefender Antivirus Plus 2016, il tuo computer sarà protetto contro tutti i tipi di malware (come virus, spyware e trojan).

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

Puoi attivare l'**Autopilot** per usufruire di una sicurezza assolutamente silenziosa, che non richiede alcuna impostazione da configurare. Tuttavia, potresti volere sfruttare le impostazioni di Bitdefender per ottimizzare e migliorare la tua protezione.

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

Bitdefender prenderà la maggior parte delle decisioni in materia di sicurezza per conto tuo, mostrandoti raramente delle finestre pop-up di avviso. Nella finestra Eventi sono disponibili maggiori dettagli sulle azioni intraprese e sulle operazioni dei programmi. Per maggiori informazioni, fai riferimento a **«Eventi» (p. 17)**.

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

Per utilizzare le funzioni online di Bitdefender Antivirus Plus 2016 e gestire i tuoi abbonamenti e dispositivi, accedi al tuo account Bitdefender Central. Per maggiori informazioni, fai riferimento a **«Bitdefender Central» (p. 38)**.

Nella sezione **«Come fare» (p. 47)** troverai una serie di istruzioni passo passo per eseguire le attività più comuni. Se dovessi riscontrare problemi nell'utilizzare Bitdefender, controlla la sezione **«Risolvere i problemi più comuni» (p. 133)** per alcune possibili soluzioni ai problemi più comuni.

4.1. Aprire la finestra di Bitdefender

Per accedere all'interfaccia principale di Bitdefender Antivirus Plus 2016, segui questi passaggi:



● In Windows 7:

1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
2. Clicca su **Bitdefender 2016**.
3. Clicca su **Bitdefender Antivirus Plus 2016** o più rapidamente, clicca due volte sull'icona di Bitdefender **B** nell'area di notifica.

● In Windows 8 e Windows 8.1:

Dal menu Start di Windows, localizza Bitdefender Antivirus Plus 2016 (puoi anche digitare direttamente "Bitdefender" nella finestra di ricerca del menu Start) e poi clicca sulla sua icona. In alternativa, apri l'applicazione sul desktop e poi clicca due volte sull'icona di Bitdefender **B** nell'area di notifica.

● In Windows 10:

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

Per maggiori informazioni sulla finestra di Bitdefender e l'icona nell'area di notifica, fai riferimento a *«Interfaccia di Bitdefender»* (p. 25).

4.2. Risolvere i problemi


Bitdefender utilizza un sistema di identificazione dei problemi per rilevare e fornire informazioni relative ai problemi che potrebbero avere effetto sulla sicurezza del computer e dei dati. Di norma, il sistema controlla solo una serie di problemi considerati molto importanti. Tuttavia è possibile configurare il sistema in base alle proprie necessità, scegliendo di quali problemi specifici si desidera essere avvisati.


I problemi rilevati includono importanti impostazioni di protezione che sono disattivate e altre condizioni che possono rappresentare un rischio per la sicurezza. Sono suddivisi in due categorie:

- **Problemi critici** - Impediscono a Bitdefender di proteggerti dai malware o rappresentano un grosso rischio alla sicurezza.
- **Problemi minori (non critici)** - Possono influenzare la tua protezione nel prossimo futuro.

L'icona di Bitdefender nell'**area di notifica** indica problemi in sospenso cambiando il suo colore come segue:



 Alcuni problemi critici influenzano la sicurezza del tuo sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.

 Alcuni problemi non critici influenzano la sicurezza del tuo sistema. Quando hai un po' di tempo, dovresti controllarli e risolverli.

Inoltre muovendo il cursore sull'icona, una finestra pop-up confermerà l'esistenza di problemi in sospeso.

Quando apri l'**interfaccia di Bitdefender**, l'area Stato di sicurezza sulla barra degli strumenti superiore indicherà la natura dei problemi che influenzano il sistema.

4.2.1. Procedura guidata Risolvi ogni problema

Per risolvere i problemi rilevati segui la procedura guidata **Risolvi ogni problema**.

1. Per aprire la procedura guidata, fai una delle seguenti operazioni:

- Clicca con il pulsante destro sull'icona di Bitdefender nell'**area di notifica** e seleziona **Visualizza i problemi di sicurezza**.
- Apri l'**interfaccia di Bitdefender** e clicca in qualsiasi punto nell'area Stato di sicurezza sulla barra degli strumenti superiore (per esempio, puoi cliccare sul link **Risolvi ogni problema!**).

2. Puoi visualizzare i problemi che influenzano la sicurezza del computer e dei dati. Tutti i problemi attuali sono stati selezionati per essere risolti.

Se non desideri risolvere subito un particolare problema, deseleziona la casella corrispondente. Ti sarà chiesto di indicare per quanto tempo posticipare la risoluzione del problema. Scegli l'opzione che desideri nel menu e clicca su **OK**. Per non monitorare più la rispettiva categoria di problemi, seleziona **Permanentemente**.

Lo stato del problema diventerà **Posticipato** e non sarà intrapresa alcuna azione per risolverlo.

3. Per risolvere i problemi selezionati, clicca su **Risolvi**. Alcuni problemi vengono risolti immediatamente. Per altri problemi verrà eseguito un assistente per poterli risolvere.

I problemi che la procedura guidata permette di risolvere possono essere raggruppati nelle seguenti categorie principali:




- **Impostazioni di sicurezza disabilitate.** Tali problemi vengono risolti immediatamente abilitando le rispettive impostazioni di sicurezza.
- **Attività di sicurezza preventiva che devi eseguire.** Nel risolvere tali problemi, una procedura guidata permette di completare con successo l'attività.

4.2.2. Configurare gli avvisi di stato

Bitdefender ti avvisa in caso venissero rilevati problemi durante l'esecuzione delle seguenti funzioni:

- Antivirus
- Aggiorna
- Sicurezza browser

Puoi configurare il sistema di avvisi per rispondere al meglio alle tue esigenze di sicurezza, selezionando di quali problemi specifici desideri essere informato. Attenersi alla seguente procedura:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Impostazioni generali** dal menu a tendina.
2. Nella finestra **Impostazioni generali**, seleziona la scheda **Avanzate**.
3. Clicca sul link **Configura avvisi di stato**.
4. Clicca sugli interruttori per attivare o disattivare gli avvisi di stato in base alle tue preferenze.


4.3. Eventi

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 negli eventi di Bitdefender, in modo simile a quando ricevi un nuovo messaggio nella casella di posta.

Gli Eventi sono uno strumento molto importante per monitorare e gestire la protezione di Bitdefender. Per esempio, puoi controllare facilmente se l'aggiornamento è stato eseguito con successo, se sono stati rilevati malware sul tuo computer, ecc. In aggiunta, se necessario, puoi intraprendere ulteriori azioni o modificare le azioni intraprese da Bitdefender.

Per accedere al registro degli Eventi, segui questi passaggi:




1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Eventi** dal menu a tendina.

I messaggi sono raggruppati in base alle diverse attività dei vari moduli di Bitdefender:

- **Aggiorna**
- **Antivirus**
- **Protezione web**
- **Vulnerabilità**
- **Protezione da Ransomware**

Ogni volta che si verifica un evento, compare un punto sull'icona  nella parte superiore dell'**interfaccia di Bitdefender**.

È disponibile un elenco di eventi per ogni categoria. Per trovare eventuali informazioni su un particolare evento nell'elenco, clicca sull'icona  e seleziona **Eventi** dal menu a tendina. I dettagli degli eventi sono indicati sul lato destro della finestra. Ogni evento è fornito delle seguenti informazioni: una breve descrizione, l'azione intrapresa da Bitdefender quando si è verificato e la data e l'ora in cui è avvenuto. Se necessario, possono essere fornite opzioni per intraprendere ulteriori azioni.

Puoi filtrare gli eventi per la loro importanza e nell'ordine in cui sono accaduti. Ci sono tre tipi di eventi filtrati dalla loro importanza, ognuno indicato da un'icona specifica:

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

Per visualizzare gli eventi che si sono verificati in un determinato intervallo, seleziona il periodo desiderato dal campo corrispondente.

Per aiutarti a gestire facilmente gli eventi registrati, ogni sezione della finestra Eventi fornisce opzioni per eliminare o segnare come letti tutti gli eventi in quella sezione.



4.4. Autopilot

Per tutti gli utenti che vogliono essere protetti dalla propria soluzione di sicurezza senza tanti problemi, Bitdefender Antivirus Plus 2016 include una modalità Autopilot.

Con l'Autopilot attivo, Bitdefender applica una configurazione di sicurezza ottimale e prende tutte le relative decisioni per te. Questo significa che non vedrai né finestre di pop-up né avvisi e non dovrai configurare alcuna impostazione.

In modalità Autopilot, Bitdefender risolve automaticamente i problemi critici, oltre ad attivare e gestire in modo silenzioso:

- Protezione antivirus, fornita da scansioni all'accesso e continue.
- Protezione web.
- Aggiornamenti automatici.

Per attivare o disattivare l'Autopilot, clicca sull'interruttore **Autopilot** nella barra degli strumenti superiore dell'**interfaccia di Bitdefender**.

Finché l'Autopilot è attivo, l'icona di Bitdefender nell'area di notifica cambia in .

Importante

Se si modifica un'impostazione gestita dall'Autopilot mentre è attivo, sarà disattivato automaticamente.

Per vedere una cronologia delle azioni eseguite da Bitdefender mentre l'Autopilot era attivo, apri la finestra **Eventi**.

4.5. Profili e Modalità Batteria

Alcune attività del computer, come giochi online o presentazioni video, richiedono una maggiore prontezza del sistema, prestazioni più elevate e nessuna interruzione. Quando il laptop funziona a batterie, si consiglia che operazioni superflue, che consumano energia aggiuntiva, siano rimandate fino a quando il laptop è connesso all'alimentazione C/A.

Per adattarsi a queste situazioni particolari, Bitdefender Antivirus Plus 2016 include due modalità operative speciali:

- **Profili**



● Modalità Batteria

4.5.1. Profili

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

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

Profilo Lavoro

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

Profilo Film


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

Profilo Gioco

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

Attivare o disattivare i profili

Per attivare o disattivare i profili, segui questi passaggi:


1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Strumenti**.
3. Clicca sul modulo **Profili**.
4. Nella finestra **Profili**, seleziona la scheda **Impostazioni profili**.
5. Attiva o disattiva i profili, cliccando sull'interruttore corrispondente.

Configura l'Autopilot per monitorare i profili

Per un'esperienza più intuitiva, puoi configurare l'Autopilot per gestire i tuoi profili operativi. Mentre sei in questa modalità, Bitdefender rileva automaticamente l'attività eseguita e applica le impostazioni di ottimizzazione del sistema e del prodotto.

Per consentire ad Autopilot di gestire i profili, segui questi passaggi:



1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Strumenti**.
3. Clicca sul modulo **Profili**.
4. Nella finestra **Profili**, seleziona la scheda **Impostazioni profili**.
5. Seleziona la casella corrispondente **Consenti all'Autopilot di gestire i miei profili**.

Se non vuoi che il tuo Profilo sia gestito automaticamente, non spuntare la casella e selezionala manualmente dall'elenco a comparsa **PROFILO** dell'interfaccia di Bitdefender.

Per maggiori informazioni su Profili, fai riferimento a «*Profili*» (p. 126)

4.5.2. Modalità Batteria


La Modalità Batteria è stata sviluppata appositamente per chi utilizza computer portatili e tablet. Il suo scopo è ridurre al minimo l'impatto del sistema e di Bitdefender sul consumo energetico, quando il livello di carica della batteria è inferiore a quello predefinito o selezionato.

Quando Bitdefender funziona in Modalità Batteria, vengono applicate le seguenti impostazioni:

- L'Aggiornamento automatico di Bitdefender è rinviato.
- Le scansioni programmate sono rinviate.
- Il **Widget sicurezza** è disattivato.

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

Per attivare o disattivare la Modalità Batteria, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Strumenti**.
3. Clicca sul modulo **Profili** e seleziona la finestra **Modalità Batteria**.



4. Attiva o disattiva la Modalità Batteria automatica, cliccando sull'interruttore corrispondente.

Trascina il cursore scorrevole corrispondente per impostare quando il sistema dovrebbe attivare la Modalità Batteria. Di norma, la modalità si attiva quando il livello di carica della batteria è inferiore al 30%.




Nota

Di solito, la Modalità Batteria viene attivata su portatili e tablet.

Configurare la Modalità Batteria

Per configurare la Modalità Batteria, segui questi passaggi:


1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Strumenti**.
3. Clicca sul modulo **Profili** e seleziona la finestra **Modalità Batteria**.
4. Attiva la funzione, cliccando sull'interruttore corrispondente.
5. Clicca sul pulsante **Configura**.
6. Seleziona le regolazioni del sistema da applicare, spuntando le seguenti opzioni:
 - Ottimizza le impostazioni del prodotto per la modalità Batteria.
 - Rimanda i programmi in background e le attività di manutenzione.
 - Posticipa aggiornamenti automatici di Windows.
 - Modifica le impostazioni dei consumi energetici per la modalità Batteria.
 - Disattiva i dispositivi esterni e le porte di rete.
7. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

4.6. Impostazioni protette da password di Bitdefender

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

Per configurare la protezione tramite password per le impostazioni di Bitdefender, segui questi passaggi:




1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Impostazioni generali** dal menu a tendina.
2. Nella finestra **Impostazioni generali**, seleziona la scheda **Impostazioni generali**.
3. Attiva la protezione con password, cliccando sull'interruttore corrispondente.
4. Inserisci la password nei due campi e poi clicca su **OK**. La password deve essere composta da almeno 8 caratteri.

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

Importante

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

Per rimuovere la protezione tramite password, segui questi passaggi:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Impostazioni generali** dal menu a tendina.
2. Nella finestra **Impostazioni generali**, seleziona la scheda **Impostazioni generali**.
3. Disattiva la protezione con password, cliccando sull'interruttore corrispondente. Digita la password e clicca su **OK**.

Nota


Per modificare la password del tuo prodotto, clicca sul link **Cambia password**.

4.7. Rapporti anonimi sull'utilizzo

Di norma, Bitdefender invia rapporti contenenti informazioni su come utilizzi il programma ai server di Bitdefender. Queste informazioni sono essenziali per migliorare il prodotto e possono aiutarci a offrire una migliore esperienza in futuro. I rapporti non conterranno dati confidenziali, come nome o indirizzo IP, e non saranno utilizzati per scopi commerciali.



Se vuoi fermare l'invio dei Rapporti anonimi sull'utilizzo, segui questi passaggi:


1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Impostazioni generali** dal menu a tendina.
2. Nella finestra **Impostazioni generali**, seleziona la scheda **Avanzate**.
3. Clicca sull'interruttore per disattivare i rapporti anonimi sull'utilizzo.

4.8. Offerte speciali e notifiche sul prodotto

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

Inoltre, le notifiche possono apparire quando effettui delle modifiche nel prodotto.

Per attivare o disattivare le offerte speciali e le notifiche sul prodotto, segui questi passaggi:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Impostazioni generali** dal menu a tendina.
2. Nella finestra **Impostazioni generali**, seleziona la scheda **Impostazioni generali**.
3. Attiva o disattiva le offerte speciali e le notifiche sul prodotto, cliccando sull'interruttore corrispondente.

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



Nota

Dopo aver disattivato le offerte speciali e le notifiche sul prodotto, Bitdefender continuerà a tenerti informato sulle offerte speciali, se stai utilizzando una versione di prova, se l'abbonamento sta per scadere o se stai usando una versione scaduta del prodotto.



5. INTERFACCIA DI BITDEFENDER

Bitdefender Antivirus Plus 2016 soddisfa le necessità di persone esperte e di principianti. L'interfaccia grafica dell'utente è quindi stata progettata per essere adatta a qualsiasi categoria di utenti.

Per visualizzare lo stato del prodotto ed eseguire le attività essenziali, l'icona di Bitdefender nell'**area di notifica** è disponibile in qualsiasi momento.

La **finestra principale** ti consente di accedere a informazioni importanti sul prodotto e ai moduli del programma, consentendoti di eseguire le attività più comuni. Dalla finestra principale, puoi accedere ai **moduli di Bitdefender**, per una configurazione più dettagliata e alcune attività di gestione avanzata, e gestire il comportamento del prodotto utilizzando l'**Autopilot** e i **Profili**.

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

5.1. Icona area di notifica


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



Nota

L'icona di Bitdefender potrebbe non essere sempre visibile. Per rendere l'icona sempre visibile, segui questi passaggi:

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

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

● In **Windows 10**:

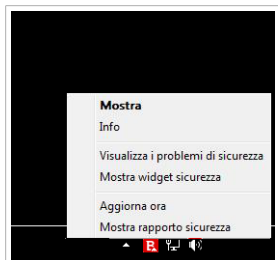
1. Clicca con il pulsante destro sulla barra delle applicazioni e seleziona **Proprietà**.
2. Clicca su **Personalizza** nella finestra della barra delle applicazioni.
3. Clicca sul link **Seleziona le icone che compaiono sulla barra delle applicazioni** nella finestra **Notifiche e azioni**.



4. Attiva l'interruttore accanto a **Bitdefender Agent**.

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




- **Mostra** - Apre la finestra principale di Bitdefender.
- **Informazioni** - Apre una finestra nella quale puoi visualizzare informazioni su Bitdefender e cercare aiuto nel caso in cui accada qualcosa di inaspettato.
- L'opzione **Visualizza i problemi di sicurezza** ti aiuta a rimuovere le vulnerabilità attuali. Se l'opzione non è disponibile, non ci sono errori da risolvere. Per maggiori informazioni, ti preghiamo di far riferimento a *«Risolvere i problemi»* (p. 15).




Icona area di notifica

- **Nascondi / Mostra widget sicurezza** - Attiva / disattiva il **widget sicurezza**.
- **Aggiorna ora** - Inizia un aggiornamento immediato. Puoi seguire lo stato di aggiornamento nel pannello Aggiornamento della **finestra principale di Bitdefender**.
- L'opzione **Mostra rapporto sicurezza** apre una finestra dove è possibile visualizzare uno stato settimanale oltre a diversi suggerimenti per il sistema. Puoi seguire i suggerimenti per migliorare la sicurezza del sistema.

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

-  Alcuni problemi critici influenzano la sicurezza del tuo sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.
-  Alcuni problemi non critici influenzano la sicurezza del tuo sistema. Quando hai un po' di tempo, dovresti controllarli e risolverli.
-  L'**Autopilot** di Bitdefender è attivo.

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



o quando altri errori interferiscono con il normale funzionamento di Bitdefender.

5.2. Finestra principale

La finestra principale di Bitdefender ti consente di eseguire le attività più comuni, risolvere rapidamente problemi di sicurezza, visualizzare informazioni sulle attività del prodotto e accedere ai vari pannelli da cui puoi configurare le impostazioni. Tutto è a pochi clic di distanza.


La finestra è organizzata in due sezioni principali:


Barra degli strumenti superiore

Qui è dove puoi verificare lo stato di sicurezza del computer, configurare il comportamento di Bitdefender in alcuni casi speciali e accedere alle attività importanti.

Area pulsanti d'azione

Qui è dove puoi accedere all'interfaccia dell'account Bitdefender Central ed eseguire diverse attività per mantenere il sistema protetto e funzionante a velocità ottimale.

L'icona  nell'angolo in basso a sinistra dell'interfaccia principale ti consente di accedere ai moduli del prodotto, in modo da poter avviare la configurazione delle impostazioni.

L'icona  nella parte superiore dell'interfaccia principale ti consente di gestire il tuo account e accedere alle funzioni online del prodotto dall'interfaccia dell'account. Da qui puoi anche accedere agli **Eventi**, al **rapporto di sicurezza** settimanale e alla pagina **Aiuto e Supporto**.

Accedi	Descrizione
Numero di giorni rimasti	Qui viene indicato il tempo rimasto prima della scadenza del tuo abbonamento attuale. Clicca sul link per aprire una finestra dove potrai visualizzare maggiori informazioni sul tuo codice di licenza o registrare il prodotto con un nuovo codice di licenza.

5.2.1. Barra degli strumenti superiore

La barra degli strumenti superiore contiene i seguenti elementi:



- L'**area Stato di sicurezza** sul lato sinistro della barra degli strumenti ti informa se ci sono problemi relativi alla sicurezza del tuo computer, aiutandoti a risolverli.

Il colore dell'area Stato sicurezza cambia in base ai problemi rilevati e ai diversi messaggi che vengono mostrati:

- L'**area è colorata di verde**. Nessun problema da risolvere. Il computer e i dati sono protetti.
- L'**area è colorata di giallo**. Alcuni problemi non critici influenzano la sicurezza del tuo sistema. Quando hai un po' di tempo, dovresti controllarli e risolverli.
- L'**area è colorata di rosso**. Alcuni problemi critici influenzano la sicurezza del tuo sistema. Devi risolvere i problemi rilevati immediatamente.

Cliccando in qualsiasi punto dell'area Stato sicurezza, puoi accedere a una procedura guidata che ti aiuterà a rimuovere facilmente qualsiasi minaccia dal computer. Per maggiori informazioni, ti preghiamo di far riferimento a *«Risolvere i problemi»* (p. 15).

- L'opzione **Autopilot** ti consente di attivare l'Autopilot, per usufruire di una sicurezza "silenziosa". Per maggiori informazioni, fai riferimento a *«Autopilot»* (p. 19).
- I **Profili** ti consentono di lavorare, usare i videogiochi o guardare un film risparmiando tempo a configurare il sistema e ritardando le attività di manutenzione. Per maggiori informazioni, fai riferimento a *«Profili»* (p. 126).

5.2.2. Pulsanti d'azione

Usando i pulsanti d'azione puoi accedere rapidamente al tuo account Bitdefender Central e lanciare funzioni importanti.

I pulsanti d'azione disponibili in quest'area sono:


- **Vai a Bitdefender Central**. Accedi al tuo account Bitdefender Central per verificare i tuoi abbonamenti ed eseguire le funzioni di sicurezza sui dispositivi che gestisci.
- **Scansione veloce**. Esegui una scansione veloce per assicurarti che il computer sia libero da virus.
- **Scansione vulnerabilità**. Esegui una scansione del computer alla ricerca di vulnerabilità per assicurarti che tutte le applicazioni installate, incluso il sistema operativo, siano aggiornate e funzionino correttamente.



- **Safepay.** Apri Bitdefender Safepay™ per proteggere i tuoi dati sensibili durante l'elaborazione delle transazioni online.
- **Aggiornamento.** Aggiorna Bitdefender per assicurarti di avere le ultime firme malware.

5.3. I moduli di Bitdefender

Il prodotto Bitdefender include una serie di moduli molto utili per garantirti la massima sicurezza mentre lavori, navighi sul web, giochi o esegui pagamenti online.

Ogni volta che vuoi accedere ai moduli o avviare la configurazione del tuo prodotto, clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.

I moduli sono suddivisi in tre schede, basate sulle funzioni che offrono:

- **Protezione**
- **Privacy**
- **Strumenti**

5.3.1. Protezione

In questa scheda puoi configurare il livello di sicurezza e impostare quali vulnerabilità del sistema devono essere risolte.

Nel pannello Protezione, puoi gestire i seguenti moduli:

Antivirus

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

Dal modulo Antivirus, puoi accedere facilmente alle seguenti attività di scansione:

- Scansione veloce
- Scansione sistema
- Gestisci scansioni
- Modalità soccorso

Per maggiori informazioni sulle attività di scansione e su come configurare la protezione antivirus, fai riferimento a **«Protezione antivirus»** (p. 74).



Protezione web

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

Per maggiori informazioni su come configurare Bitdefender per proteggere le tue attività sul web, fai riferimento a *«Protezione web»* (p. 100).

Vulnerabilità

Il modulo Vulnerabilità ti aiuta a mantenere aggiornato il sistema operativo e le applicazioni, che usi normalmente.

Clicca su **Scansione vulnerabilità** nel modulo Vulnerabilità per iniziare a identificare gli aggiornamenti critici di Windows, gli aggiornamenti delle applicazioni e le password non sicure, appartenenti agli account di Windows.

Per maggiori informazioni sulla configurazione della protezione dalle vulnerabilità, fai riferimento a *«Vulnerabilità»* (p. 104).

Protezione da Ransomware

Il modulo Protezione da Ransomware assicura che i tuoi file personali siano sempre protetti da attacchi di pirati informatici online.

Per maggiori informazioni su come configurare la Protezione da Ransomware per proteggere il tuo sistema dagli attacchi ransomware, fai riferimento a *«Protezione da Ransomware»* (p. 108).

5.3.2. Privacy

Nella scheda Privacy, puoi proteggere le tue transazioni online e mantenere sicura la tua navigazione.

Nel pannello Privacy, puoi gestire i seguenti moduli:

Protezione dati

Il modulo Protezione dati ti consente di eliminare i file in modo permanente.

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

Per maggiori informazioni sulla configurazione della Protezione dati, fai riferimento a *«Protezione dati»* (p. 102).



Gestore Password

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

Dal modulo Password Manager, puoi selezionare le seguenti funzioni:

- **Apri Portafoglio** - Apre il database del Portafoglio attuale.
- **Blocca Portafoglio** - Blocca il database del Portafoglio attuale.
- **Esporta Portafoglio** - Consente di salvare il database attuale in un dato percorso sul proprio sistema.
- **Crea nuovo Portafoglio** - Avvia una procedura guidata che ti consentirà di creare un nuovo database del Portafoglio.
- **Elimina** - Ti consente di eliminare un database del Portafoglio.
- **Impostazioni** - Qui puoi modificare il nome del database del tuo Portafoglio e impostare se sincronizzare o meno le informazioni esistenti con tutti i tuoi dispositivi.

Per maggiori informazioni sulla configurazione del Password Manager, fai riferimento a *«Protezione di Password Manager per le tue credenziali»* (p. 116).

Safepay

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

Clicca sul pulsante d'azione **Safepay** nell'interfaccia di Bitdefender per iniziare a eseguire transazioni online in un ambiente sicuro.

Per maggiori informazioni su Bitdefender Safepay™, fai riferimento a *«Safepay: sicurezza per le transazioni online»* (p. 111).

5.3.3. Strumenti

Nella scheda Strumenti, puoi configurare il tuo profilo lavorativo.

Nella scheda Strumenti, puoi gestire i seguenti moduli:

Profili

I Profili di Bitdefender ti aiutano ad avere sempre la migliore esperienza mentre lavori, guardi un film o usi un videogioco, monitorando gli strumenti operativi del prodotto e del sistema. Clicca su **Attiva adesso**



nella barra degli strumenti superiore dell'interfaccia di Bitdefender, per avviare questa funzionalità.

Bitdefender ti consente di configurare i seguenti profili:

- Profilo Lavoro
- Profilo Film
- Profilo Gioco

Per maggiori informazioni su come configurare il modulo Profili, fai riferimento a «*Profili*» (p. 126).

5.4. Widget sicurezza

Il **widget sicurezza** è un modo semplice e veloce per monitorare e controllare Bitdefender Antivirus Plus 2016. Aggiungendo questo piccolo e discreto widget sul desktop, puoi visualizzare tutte le informazioni critiche ed eseguire le attività principali in qualsiasi momento:

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



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



Alcuni problemi critici influenzano la sicurezza del tuo sistema.



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



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




Il tuo sistema è protetto.



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

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

Il lato inferiore del widget mostra il contatore degli eventi non letti (il numero di eventi rilevanti segnalati da Bitdefender, in caso ve ne fossero). Clicca sul contatore degli eventi, per esempio , nel caso di un evento non letto, per aprire la finestra degli Eventi. Per maggiori informazioni, fai riferimento a «*Eventi*» (p. 17).

5.4.1. Eseguire la scansione di file e cartelle

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

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


5.4.2. Nascondi / mostra widget sicurezza

Se non desideri più visualizzare il widget, clicca su .

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

- Dall'area di notifica:



1. Clicca con il pulsante destro sull'icona di Bitdefender nell'**area di notifica**.
 2. Clicca su **Mostra widget sicurezza** nel menu contestuale che apparirà.
- Dall'interfaccia di Bitdefender:
 1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Impostazioni generali** dal menu a tendina.
 2. Nella finestra **Impostazioni generali**, seleziona la scheda **Impostazioni generali**.
 3. Attiva l'opzione **Mostra widget sicurezza** cliccando sull'interruttore corrispondente.

5.5. Rapporto sicurezza

Il Rapporto sicurezza ti fornisce uno stato settimanale del tuo prodotto, oltre a diversi suggerimenti per migliorare la protezione del sistema. Questi suggerimenti sono importanti per la gestione della protezione globale e potrai facilmente verificare le azioni che si possono intraprendere sul sistema.

Il rapporto viene generato una volta la settimana e riassume le informazioni più importanti sulle attività del tuo prodotto, in modo da verificare facilmente tutto ciò che è successo in questo periodo di tempo.

Le informazioni offerte dal Rapporto sicurezza sono divise in due categorie:

- La sezione **Protezione** consente di visualizzare informazioni sulla protezione del sistema.

- **File esaminati**

Ti consente di visualizzare i file esaminati da Bitdefender durante la settimana. Puoi visualizzare i dettagli, come il numero di file esaminati e il numero di file puliti da Bitdefender.

Per maggiori informazioni sulla protezione antivirus, fai riferimento a **«Protezione antivirus» (p. 74)**

- **Pagine web esaminate**

Ti consente di verificare il numero di pagine web esaminate e bloccate da Bitdefender. Per impedirti di rivelare informazioni personali durante la navigazione, Bitdefender protegge il tuo traffico web.



Per maggiori informazioni sulla Protezione web, fai riferimento a *«Protezione web»* (p. 100).

● Vulnerabilità

Ti consente di identificare e risolvere facilmente le vulnerabilità, per rendere il computer più sicuro e protetto da malware e hacker.

Per maggiori informazioni sulla Scansione vulnerabilità, fai riferimento a *«Vulnerabilità»* (p. 104).

● Cronologia eventi

Ti consente di avere una panoramica di tutti i processi di scansione e dei problemi risolti da Bitdefender nel corso della settimana. Gli eventi sono suddivisi per giornata.

Per maggiori informazioni sul registro dettagliato degli eventi, inerenti l'attività del computer, seleziona **Eventi**.

- La sezione **Ottimizzazione** consente di visualizzare le informazioni relative allo spazio liberato, alle applicazioni ottimizzate e a quanta batteria hai risparmiato usando la Modalità Batteria.

● Batteria risparmiata

Ti consente di visualizzare quanta batteria hai risparmiato mentre il sistema funzionava in Modalità Batteria.

Per maggiori informazioni sulla Modalità Batteria, fai riferimento a *«Modalità Batteria»* (p. 21).

● App ottimizzate

Ti consente di visualizzare il numero di applicazioni che hai usato nei Profili.

Per maggiori informazioni sui Profili, fai riferimento a *«Profili»* (p. 126).


5.5.1. Controllare il Rapporto sicurezza

Il Rapporto sicurezza utilizza un sistema di identificazione dei problemi per rilevare e fornire informazioni sui problemi che potrebbero influenzare la sicurezza del computer e dei dati. I problemi rilevati includono importanti impostazioni di protezione che sono disattivate e altre condizioni che possono rappresentare un rischio per la sicurezza. Utilizzando il rapporto, puoi configurare alcune componenti specifiche di Bitdefender o prendere azioni preventive per proteggere il computer e i tuoi dati personali.



Per controllare il Rapporto sicurezza, segui questi passaggi:

1. Accedi al rapporto:

- Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Rapporto sicurezza** dal menu a tendina.
- Clicca con il pulsante destro sull'icona di Bitdefender nell'area di notifica e seleziona **Mostra rapporto sicurezza**.
- Una volta completato un rapporto, comparirà una finestra per avvisarti. Clicca su **Mostra** per accedere al rapporto sicurezza.

Nel browser si aprirà una pagina web in cui potrai visualizzare il rapporto.

2. Puoi verificare lo stato generale della sicurezza nella parte superiore della finestra.


3. Controlla i nostri suggerimenti in fondo alla pagina.

Il colore dell'area Stato sicurezza cambia in base ai problemi rilevati e ai diversi messaggi che vengono mostrati:

- **L'area è di colore verde.** Non ci sono problemi da risolvere. Il computer e i dati sono protetti.
- **L'area è di colore giallo.** Alcuni problemi non critici influenzano la sicurezza del sistema. Quando hai un po' di tempo, dovresti controllarli e risolverli.
- **L'area è di colore rosso.** Alcuni problemi critici influenzano la sicurezza del sistema. Devi risolvere i problemi rilevati immediatamente.

5.5.2. Attivare o disattivare la notifica del Rapporto di sicurezza

Per attivare o disattivare gli avvisi del rapporto sicurezza, segui questi passaggi:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Impostazioni generali** dal menu a tendina.
2. Nella finestra **Impostazioni generali**, seleziona la scheda **Impostazioni generali**.
3. Clicca sull'interruttore corrispondente per attivare o disattivare la notifica del Rapporto di sicurezza.



Di norma, gli avvisi del rapporto sicurezza sono attivati.




6. BITDEFENDER CENTRAL

Bitdefender Central è la piattaforma web che consente di accedere alle funzioni e ai servizi online del prodotto, oltre a eseguire in remoto alcune importanti funzioni sui dispositivi in cui è stato installato Bitdefender. Puoi accedere al tuo account Bitdefender Central da qualsiasi computer o dispositivo mobile connesso a Internet, andando su <https://central.bitdefender.com>. Una volta eseguito l'accesso, puoi utilizzare le seguenti attività:

- Scarica e installa Bitdefender su sistemi operativi Windows, OS X e Android. I prodotti che è possibile scaricare sono:
 - Bitdefender Antivirus Plus 2016
 - Bitdefender Antivirus for Mac
 - Bitdefender Mobile Security
- Gestisci e rinnova i tuoi abbonamenti di Bitdefender.
- Aggiungi nuovi dispositivi alla tua rete e gestiscili ovunque ti trovi.

6.1. Accedere al tuo account Bitdefender Central

Puoi accedere al tuo account Bitdefender Central in vari modi. In base all'attività che intendi eseguire, puoi utilizzare una delle seguenti possibilità:

- Dall'interfaccia principale di Bitdefender:
 1. Clicca sul link **Vai a Bitdefender Central** sul lato destro dell'**interfaccia di Bitdefender**.
- Da Informazioni Account:
 1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Informazioni Account** dal menu a tendina.
 2. Clicca sul link **Vai a Bitdefender Central** nella parte inferiore della finestra che si aprirà.
- 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 password.



6.2. I miei abbonamenti

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

6.2.1. Controllare gli abbonamenti disponibili

Per controllare gli abbonamenti disponibili:

1. Accedi al tuo **account Bitdefender Central**
2. Seleziona il pannello **I miei abbonamenti**.

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

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



Nota

Puoi avere uno o più abbonamenti sul tuo account, a condizione che siano per piattaforme differenti (Windows, Mac OS X o Android).

6.2.2. Aggiungi un nuovo dispositivo

Se l'abbonamento copre più di un dispositivo, è possibile aggiungerne un altro e installare Bitdefender Antivirus Plus 2016 su di esso, come segue:

1. Accedi al tuo **account Bitdefender Central**
2. Seleziona la scheda **I miei dispositivi**.
3. Nella finestra **I miei dispositivi**, clicca su **INSTALLA Bitdefender**.
4. Seleziona una delle due opzioni disponibili:

● **SCARICA**

Clicca sul pulsante e salva il file d'installazione.

● **Su un altro dispositivo**

Seleziona **Windows** per scaricare il tuo prodotto Bitdefender e poi clicca su **CONTINUA**. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA**.

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



6.2.3. Rinnova abbonamento

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

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

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

6.2.4. Attiva abbonamento

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

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

Per attivare un abbonamento utilizzando un codice di attivazione, segui questi passaggi:

1. Accedi al tuo **account Bitdefender Central**
2. Seleziona il pannello **I miei abbonamenti**.
3. Clicca sul pulsante **CODICE DI ATTIVAZIONE** e digita il codice nel campo corrispondente.
4. Clicca su **INVIA**.

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


6.3. I miei dispositivi

L'area **I miei dispositivi** nel tuo account Bitdefender Central ti consente d'installare, gestire e utilizzare in remoto il tuo prodotto Bitdefender su qualsiasi dispositivo, a condizione che sia acceso e connesso a Internet. Le




schede del dispositivo mostrano il nome del dispositivo, lo stato di protezione e la disponibilità restante nel tuo abbonamento.

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


1. Accedi al tuo **account Bitdefender Central**
2. Seleziona la scheda **I miei dispositivi**.
3. Clicca sull'icona  sulla scheda del dispositivo desiderato e seleziona **Impostazioni**.
4. Cambia il nome del dispositivo nel campo corrispondente e poi seleziona **Salva**.

Se l'Autopilot è disattivato, puoi attivarlo cliccando sull'interruttore. Clicca su **Salva** per applicare le impostazioni.

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

1. Accedi al tuo **account Bitdefender Central**
2. Seleziona la scheda **I miei dispositivi**.
3. Clicca sull'icona  nella scheda del dispositivo desiderato e seleziona **Profilo**.
4. Clicca su **Aggiungi proprietario** e poi completa i campi corrispondenti, indicando sesso e data, e aggiungendo un'immagine per il Profilo.
5. Clicca su **AGGIUNGI** per salvare il profilo.
6. Seleziona il proprietario desiderato dall'elenco **Proprietario dispositivo** e clicca su **ASSEGNA**.

Per aggiornare in remoto Bitdefender su un dispositivo, segui questi passaggi:

1. Accedi al tuo **account Bitdefender Central**
2. Seleziona la scheda **I miei dispositivi**.
3. Clicca sull'icona  sulla scheda del dispositivo desiderato e seleziona **Aggiorna**.

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



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

- **Interfaccia.** In questa finestra, puoi verificare lo stato di protezione dei tuoi prodotti Bitdefender e i giorni restanti nel tuo abbonamento. Lo stato di protezione può essere verde, quando non ci sono problemi che influenzano il tuo prodotto, oppure rosso, quando il tuo dispositivo è a rischio. Quando ci sono problemi che influenzano il tuo prodotto, clicca su **Vedi problemi** per scoprire altri dettagli. Da qui puoi risolvere manualmente i problemi che influenzano la sicurezza del tuo dispositivo.
- **Protezione.** Da questa finestra, puoi eseguire in remoto una Scansione veloce o una Scansione di sistema sui tuoi dispositivi. Clicca sul pulsante **CONTROLLA** per avviare il processo. Puoi anche verificare quanto è stata eseguita l'ultima scansione sul dispositivo e visualizzare un rapporto della scansione più recente con tutte le informazioni più importanti. Per maggiori informazioni sui due processi di scansione, fai riferimento a «*Eseguire una scansione del sistema*» (p. 82) e «*Eseguire una Scansione veloce*» (p. 82).
- **Vulnerabilità.** Per verificare le vulnerabilità di un dispositivo, come l'assenza di aggiornamenti di Windows, applicazioni datate o password poco sicure, clicca sul pulsante **CONTROLLA** nella scheda Vulnerabilità. Le vulnerabilità non possono essere corrette in remoto. Nel caso venisse rilevata una vulnerabilità, devi eseguire una nuova scansione del dispositivo e intraprendere le azioni consigliate. Per maggiori dettagli su questa funzione, fai riferimento a «*Vulnerabilità*» (p. 104).



7. MANTENERE AGGIORNATO BITDEFENDER

Tutti giorni vengono trovati e identificati nuovi malware. È quindi molto importante mantenere aggiornato Bitdefender con le firme malware più recenti.

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

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



Importante

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

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


- Se il tuo computer si collega a Internet tramite un server proxy, devi configurare le impostazioni proxy come descritto nella sezione *«Come posso configurare Bitdefender per usare una connessione a Internet tramite proxy?»* (p. 67).
- Con una connessione a Internet lenta potrebbero verificarsi degli errori durante lo scaricamento degli aggiornamenti. Per scoprire come superare tali errori, fai riferimento a *«Come aggiornare Bitdefender con una connessione a Internet lenta»* (p. 139).
- Se sei connesso a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di Bitdefender su richiesta dell'utente. Per maggiori informazioni, fai riferimento a *«Eseguire un aggiornamento»* (p. 44).

7.1. Verificare se Bitdefender è aggiornato

Per verificare quando c'è stato l'ultimo aggiornamento di Bitdefender, controlla l'**area Stato di sicurezza**, sul lato sinistro della barra degli strumenti.



Per maggiori informazioni sugli ultimi aggiornamenti, controlla gli eventi di aggiornamento:


1. Nella finestra principale, clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Eventi** dal menu a tendina.
2. Nella finestra **Eventi**, seleziona **Aggiornamento** dal corrispondente menu a tendina.

Puoi sapere quando gli aggiornamenti sono stati lanciati e avere maggiori informazioni al riguardo (se hanno avuto successo o meno, e se richiedono di riavviare il computer per completare l'installazione). Se necessario, riavvia il sistema al più presto.

7.2. Eseguire un aggiornamento

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

Per avviare un aggiornamento, esegui una delle seguenti operazioni:

- Apri l'**interfaccia di Bitdefender** e clicca sul pulsante **Aggiorna**.
- Clicca con il pulsante destro sull'icona  di Bitdefender nell'**area di notifica** e seleziona **Aggiorna ora**.


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

Importante

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

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


Per aggiornare in remoto Bitdefender su un dispositivo, segui questi passaggi:

1. Accedi al tuo **account Bitdefender Central**
2. Seleziona la scheda **I miei dispositivi**.
3. Clicca sull'icona  sulla scheda del dispositivo desiderato e seleziona **Aggiorna**.



7.3. Attivare o disattivare l'aggiornamento automatico

Per attivare o disattivare l'aggiornamento automatico, segui questi passaggi:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Impostazioni generali** dal menu a tendina.
2. Nella finestra **Impostazioni generali**, seleziona la scheda **Aggiornamento**.
3. Clicca sull'interruttore per attivare o disattivare l'Aggiornamento automatico.
4. Comparirà una finestra di avviso. Devi confermare la tua scelta selezionando dal menu per quanto tempo desideri disattivare l'aggiornamento automatico. Puoi disattivare l'aggiornamento automatico per 5, 15 o 30 minuti, per un'ora, in modo permanente o fino a un riavvio del sistema.



Avvertimento


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

7.4. Modificare le impostazioni di aggiornamento

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

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

Per modificare le impostazioni di aggiornamento, segui questi passaggi:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Impostazioni generali** dal menu a tendina.
2. Nella finestra **Impostazioni generali**, seleziona la scheda **Aggiornamento** e modifica le impostazioni in base alle tue preferenze.



Frequenza d'aggiornamento

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

Ubicazione aggiornamento

Bitdefender è configurato per aggiornarsi dai server di aggiornamento di Bitdefender su Internet. L'ubicazione dell'aggiornamento è un indirizzo Internet generico che viene automaticamente reindirizzato al server di aggiornamento più vicino di Bitdefender nel tuo paese.

Non modificare l'ubicazione dell'aggiornamento a meno che non ti sia stato consigliato da un operatore di Bitdefender o dal tuo amministratore di rete (se sei connesso a una rete aziendale).

Puoi tornare alla generica ubicazione dell'aggiornamento Internet cliccando su **Predefinito**.

Regole di esecuzione dell'aggiornamento

Puoi scegliere fra tre modi per scaricare e installare gli aggiornamenti:

- **Aggiornamento silenzioso** - Bitdefender scarica e implementa l'aggiornamento automaticamente.
- **Chiedi prima di scaricare** - Ogni volta che un aggiornamento è disponibile, ti sarà chiesto se desideri scaricarlo.
- **Chiedi prima di installare** - Ogni volta che si scarica un aggiornamento, ti sarà chiesto se desideri installarlo.

Per completare l'installazione di alcuni aggiornamenti devi riavviare il sistema. Come impostazione predefinita, se un aggiornamento richiede un riavvio, Bitdefender continuerà a funzionare con i file precedenti finché l'utente non riavvia volontariamente il computer. Questo per impedire che il processo di aggiornamento di Bitdefender interferisca con il lavoro dell'utente.

Se vuoi essere avvisato quando un aggiornamento richiede un riavvio del sistema, disattiva l'opzione **Posticipa riavvio** cliccando sull'interruttore corrispondente.



COME FARE



8. INSTALLAZIONE

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

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

Per installare Bitdefender su un secondo computer, segui questi passaggi:

1. Accedi al tuo **account Bitdefender Central**
2. Seleziona la scheda **I miei dispositivi**.
3. Nella finestra **I miei dispositivi**, clicca su **INSTALLA Bitdefender**.
4. Seleziona una delle due opzioni disponibili:

- **SCARICA**

Clicca sul pulsante e salva il file d'installazione.

- **Su un altro dispositivo**

Seleziona **Windows** per scaricare il tuo prodotto Bitdefender e poi clicca su **CONTINUA**. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA**.

5. Esegui il prodotto Bitdefender che hai scaricato. Attendi il termine del processo di installazione e chiudi la finestra.

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

8.2. Quando dovrei reinstallare Bitdefender?

In alcune situazioni, potresti dover reinstallare il tuo prodotto Bitdefender.

Alcune tipiche situazioni in cui dovrei reinstallare Bitdefender sono:

- hai reinstallato il sistema operativo.
- hai acquistato un computer nuovo.
- vuoi cambiare la lingua visualizzata nell'interfaccia di Bitdefender.

Per reinstallare Bitdefender, puoi usare il disco di installazione acquistato o scaricare una nuova versione dall'account Bitdefender Central.



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

8.3. Dove posso scaricare il mio prodotto Bitdefender?

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



Nota

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

Per installare Bitdefender dall'account Bitdefender Central, segui questi passaggi:

1. Accedi al tuo **account Bitdefender Central**
2. Seleziona la scheda **I miei dispositivi**.
3. Nella finestra **I miei dispositivi**, clicca su **INSTALLA Bitdefender**.
4. Seleziona una delle due opzioni disponibili:

● **SCARICA**

Clicca sul pulsante e salva il file d'installazione.

● **Su un altro dispositivo**

Seleziona **Windows** per scaricare il tuo prodotto Bitdefender e poi clicca su **CONTINUA**. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA**.

5. Esegui il prodotto Bitdefender che hai scaricato.

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

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

Se stai usando una versione precedente di Bitdefender puoi passare gratuitamente all'ultima versione di Bitdefender, seguendo questi passaggi:



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

Può comparire in due occasioni:

- Dopo aver aggiornato il sistema operativo con Windows Update, scopri che Bitdefender non funziona più.

In questo caso, devi installare nuovamente il prodotto utilizzando la versione più recente disponibile.

Per risolvere questa situazione, segui questi passaggi:

1. Rimuovi Bitdefender seguendo questi passaggi:

● In **Windows 7**:

- Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
- Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
- Clicca su **Rimuovi** nella finestra che comparirà e poi seleziona **Voglio reinstallarlo**.
- Clicca su **Avanti** per continuare.
- Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

● In **Windows 8 e Windows 8.1**:

- Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
- Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
- Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
- Clicca su **Rimuovi** nella finestra che comparirà e poi seleziona **Voglio reinstallarlo**.
- Clicca su **Avanti** per continuare.



- f. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.
- In **Windows 10**:
 - a. Clicca su **Start** e poi su Impostazioni.
 - b. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
 - c. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
 - d. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
 - e. Clicca su **Rimuovi** e poi seleziona **Voglio reinstallarlo**.
 - f. Clicca su **Avanti** per continuare.
 - g. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

2. Scarica il file di installazione:

- a. Accedi al tuo **account Bitdefender Central**
- b. Seleziona la scheda **I miei dispositivi**.
- c. Nella finestra **I miei dispositivi**, clicca su **INSTALLA Bitdefender**.
- d. Seleziona una delle due opzioni disponibili:

● **SCARICA**

Clicca sul pulsante e salva il file d'installazione.

● **Su un altro dispositivo**

Seleziona **Windows** per scaricare il tuo prodotto Bitdefender e poi clicca su **CONTINUA**. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA**.

3. Esegui il prodotto Bitdefender che hai scaricato.

- Hai cambiato sistema e vuoi continuare a utilizzare la protezione di Bitdefender.

In questo caso, devi installare nuovamente il prodotto utilizzando la versione più recente.

Per risolvere questa situazione:

1. Scarica il file di installazione:



- a. Accedi al tuo **account Bitdefender Central**
- b. Seleziona la scheda **I miei dispositivi**.
- c. Nella finestra **I miei dispositivi**, clicca su **INSTALLA Bitdefender**.
- d. Seleziona una delle due opzioni disponibili:

- **SCARICA**

Clicca sul pulsante e salva il file d'installazione.

- **Su un altro dispositivo**

Seleziona **Windows** per scaricare il tuo prodotto Bitdefender e poi clicca su **CONTINUA**. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA**.

2. Esegui il prodotto Bitdefender che hai scaricato.

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

8.5. Come posso riparare Bitdefender?

Se desideri riparare la tua copia di Bitdefender Antivirus Plus 2016 dal menu del pulsante Start di Windows, segui questi passaggi:

- **In Windows 7:**

1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
2. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
3. Clicca su **Ripara** nella finestra che comparirà.
Questa operazione richiederà alcuni minuti.
4. Dovrai riavviare il computer per completare il processo.

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

1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
3. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
4. Clicca su **Ripara** nella finestra che comparirà.



Questa operazione richiederà alcuni minuti.

5. Dovrai riavviare il computer per completare il processo.

● **In Windows 10:**

1. Clicca su **Start** e poi su Impostazioni.

2. Clicca sull'icona **Sistema** nelle Impostazioni e seleziona **App e funzioni**.

3. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.

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

5. Clicca su **Ripara**.

Questa operazione richiederà alcuni minuti.

6. Dovrai riavviare il computer per completare il processo.



9. ABBONAMENTI

9.1. Quale prodotto Bitdefender sto usando?

Per scoprire quale programma di Bitdefender hai installato:

1. Apri l'**interfaccia di Bitdefender**.
2. Nella parte superiore della finestra dovresti vedere uno dei seguenti:
 - Bitdefender Antivirus Plus 2016
 - Bitdefender Internet Security 2016
 - Bitdefender Total Security 2016

9.2. Come posso attivare l'abbonamento di Bitdefender utilizzando un codice di licenza?

Se hai un codice di licenza valido e vuoi utilizzarlo per attivare un abbonamento a Bitdefender Antivirus Plus 2016, ci sono due possibilità:

- Sei passato da una versione precedente di Bitdefender a quella nuova:
 1. Una volta completato l'upgrade di Bitdefender Antivirus Plus 2016, ti sarà chiesto di accedere al tuo account Bitdefender Central.
 2. Inserisci le tue credenziali di accesso e clicca su **ACCEDI**.
 3. Nella schermata del tuo account comparirà una notifica che ti confermerà la creazione di un abbonamento. L'abbonamento così creato sarà valido per i giorni restanti nel tuo codice di licenza e per lo stesso numero di utenti.

I dispositivi che stanno utilizzando versioni precedenti di Bitdefender e sono registrati con il codice di licenza che hai convertito in un abbonamento, dovranno registrare il prodotto con lo stesso account Bitdefender Central.

- Bitdefender non è stato precedentemente installato sul sistema:
 1. Una volta completata la fase di installazione, ti sarà chiesto di accedere al tuo account Bitdefender Central.
 2. Inserisci le tue credenziali di accesso e clicca su **ACCEDI**.
 3. Seleziona il pannello **I miei abbonamenti**.



4. Clicca sul pulsante **CODICE DI ATTIVAZIONE** e inserisci il tuo codice di licenza.
5. Clicca su **INVIA**. Un abbonamento con la stessa disponibilità e numero di utenti del tuo codice di licenza è stato associato al tuo account.




10. BITDEFENDER CENTRAL

10.1. Come posso accedere a Bitdefender Central utilizzando un altro account online?

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

Per utilizzare correttamente un altro account, segui questi passaggi:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Informazioni Account** dal menu a tendina.
2. Clicca sul pulsante **Cambia account** per cambiare l'account associato al computer.
3. Inserisci l'indirizzo e-mail e la password del tuo account nei campi corrispondenti e clicca su **Accedi**.




Nota

Il prodotto Bitdefender dal tuo dispositivo cambia automaticamente in base all'abbonamento associato al nuovo account Bitdefender Central.

Se non ci fosse alcun abbonamento disponibile associato al nuovo account Bitdefender Central o si volesse trasferirlo dall'account precedente, contattare il supporto tecnico di Bitdefender, come descritto nella sezione *«Chiedere aiuto»* (p. 157).

10.2. Come posso cambiare la password dell'account Bitdefender Central?

Per impostare una nuova password per il tuo account Bitdefender Central, segui questi passaggi:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Informazioni Account** dal menu a tendina.
2. Clicca sul pulsante **Cambia account** per cambiare l'account associato al computer.
Comparirà una nuova finestra.
3. Clicca sul collegamento **Cambia password**.



4. Digita l'indirizzo e-mail utilizzato per creare il tuo account Bitdefender Central e poi clicca sul pulsante **CAMBIA PASSWORD**.
5. Controlla la tua casella di posta, apri il messaggio e clicca sul link fornito.
6. Digita il tuo indirizzo e-mail nel campo corrispondente.
7. Digita la nuova password. La password deve essere composta da almeno 8 caratteri e includere dei numeri.
8. Fare clic su **Accedi**.

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



11. SCANSIONE CON BITDEFENDER

11.1. Come posso controllare un file o una cartella?

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

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


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

Tipiche situazioni in cui si userebbe questo metodo includono:

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

11.2. Come posso eseguire una scansione del mio sistema?

Per eseguire una scansione completa del sistema, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Nel modulo **Antivirus**, seleziona **Scansione sistema**.
4. Segui la procedura guidata della Scansione di sistema per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati.


Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo. Per maggiori informazioni, fai riferimento a «**Procedura guidata scansione antivirus**» (p. 86).



11.3. Come posso programmare una scansione?

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

Per programmare una scansione, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Nel modulo **Antivirus**, seleziona **Gestisci scansioni**.
4. Seleziona il tipo di scansione che vuoi programmare tra Scansione di sistema o Scansione veloce e poi clicca su **Opzioni di scansione**.

In alternativa, puoi creare un tipo di scansione che si adatti alle tue necessità, cliccando su **Nuova attività personalizzata**.

5. Attiva l'interruttore **Programma**.

Seleziona una delle opzioni corrispondenti per impostare un elenco:


- All'avvio del sistema
- Una volta
- Periodicamente

Nella finestra **Obiettivi scansione**, puoi selezionare le posizioni che vuoi esaminare.

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

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

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

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Nel modulo **Antivirus**, seleziona **Gestisci scansioni**.



4. Clicca su **Nuova Attività personalizzata**. Nella scheda **Base**, inserisci un nome per la scansione e seleziona i percorsi da controllare.
5. Se desideri configurare le opzioni di scansione in ogni dettaglio, seleziona la scheda **Avanzate**.

Puoi configurare facilmente le opzioni di scansione, impostando il livello della scansione. Trascina il cursore scorrevole lungo la barra per impostare il livello di scansione desiderato.

Puoi anche scegliere di spegnere il computer al termine della scansione, se non venisse rilevata alcuna minaccia. Ricordati che questo sarà il comportamento predefinito ogni volta che esegui questa attività.

6. Clicca su **OK** per salvare le modifiche e chiudere la finestra.
7. Usa l'interruttore corrispondente se vuoi programmare la tua attività di scansione.
8. Clicca su **Esegui scansione** e segui la **procedura guidata della scansione** per completarla. Al termine della scansione, ti sarà chiesto di scegliere quali azioni intraprendere sui file rilevati, se presenti.
9. Se lo desideri, puoi eseguire nuovamente una scansione personale precedente cliccando sulla rispettiva voce nell'elenco disponibile.

11.5. Come posso escludere una cartella dalla scansione?


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

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

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


Per aggiungere la cartella all'elenco delle eccezioni, segui questi passaggi:



1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus** e seleziona la finestra **Eccezioni**.
4. Assicurati che l'opzione **Eccezioni per i file** sia attivata cliccando sull'interruttore.
5. Clicca sul collegamento **File e cartelle escluse**.
6. Clicca sul pulsante **Aggiungi** localizzato nella parte superiore della tabella delle eccezioni.
7. Clicca su **Sfoglia**, seleziona la cartella che desideri escludere dalla scansione e quindi clicca su **OK**.
8. Clicca su **Aggiungi** e poi su **OK** per salvare le modifiche e chiudere la finestra.


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

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

1. Disattiva la protezione antivirus in tempo reale di Bitdefender:
 - a. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
 - b. Seleziona la finestra **Protezione**.
 - c. Clicca sul modulo **Antivirus**.
 - d. Nella finestra **Antivirus**, seleziona la scheda **Protezione**.
 - e. Clicca sull'interruttore per disattivare la **scansione all'accesso**.

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



2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a *«Come posso visualizzare gli elementi nascosti in Windows?»* (p. 69).
3. Ripristina il file dalla quarantena:
 - a. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
 - b. Seleziona la finestra **Protezione**.
 - c. Clicca sul modulo **Antivirus** e seleziona la finestra **Quarantena**.
 - d. Seleziona il file e clicca su **Ripristina**.
4. Aggiungi il file all'elenco delle eccezioni. Per scoprire come fare, fai riferimento a *«Come posso escludere una cartella dalla scansione?»* (p. 60).
5. Attiva la protezione antivirus in tempo reale di Bitdefender.
6. Contatta gli operatori del nostro supporto in modo da poter rimuovere la firma di rilevazione. Per scoprire come fare, fai riferimento a *«Chiedere aiuto»* (p. 157).


11.7. Come posso verificare quali virus sono stati rilevati da Bitdefender?

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

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

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

Per controllare un registro di scansione o qualsiasi infezione rilevata in un secondo momento, segui questi passaggi:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Eventi** dal menu a tendina.
2. Nella finestra **Eventi**, seleziona **Antivirus** dal corrispondente menu a tendina.



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

3. Nell'elenco degli eventi, puoi controllare quali scansioni sono state eseguite di recente. Clicca su un evento per visualizzare maggiori dettagli al riguardo.
4. Per aprire un registro di scansione, clicca su **Guarda registro**.

Se vuoi eseguire nuovamente la stessa scansione, clicca sul pulsante **Nuova scansione**.




12. CONTROLLO PRIVACY

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

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

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

Per garantire la massima sicurezza e privacy alle tue attività online, segui questi passaggi:

1. Clicca sul pulsante d'azione **Safepay** nell'**interfaccia di Bitdefender**.
2. Clicca sul pulsante  per accedere alla **tastiera virtuale**.
3. Usa la **tastiera virtuale** ogni volta che devi digitare informazioni personali, come le password.

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

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

Il Distruttore di file di Bitdefender ti aiuterà a distruggere rapidamente file o cartelle dal computer, utilizzando il menu contestuale di Windows, seguendo questi passaggi:

1. Clicca con il pulsante destro sul file o la cartella che vuoi eliminare in maniera definitiva, seleziona Bitdefender e poi **Distruttore di file**.
2. Apparirà una finestra di conferma. Clicca su **Sì** per avviare la procedura guidata del Distruttore di file.
3. Attendi che Bitdefender termini la distruzione dei file.
4. I risultati sono mostrati. Clicca su **Chiudi** per uscire dalla procedura guidata.



13. INFORMAZIONI UTILI

13.1. Come faccio a testare la mia soluzione antivirus?

Per assicurarti che il tuo prodotto Bitdefender stia funzionando correttamente, ti consigliamo di utilizzare il test Eicar.

Il test Eicar ti consente di verificare l'efficacia della tua protezione antivirus, utilizzando un file sicuro appositamente sviluppato a tale scopo.

Per testare la tua soluzione antivirus, segui questi passaggi:

1. Scarica il test dalla pagina web ufficiale dell'organizzazione EICAR <http://www.eicar.org/>.
2. Clicca sull'opzione **Anti-Malware Testfile**.
3. Clicca su **Download** nel menu a sinistra.
4. Ora dalla tabella **Download area using the standard protocol http**, clicca sul file di test **eicar.com**.
5. Sarai avvisato che la pagina a cui stai cercando di accedere contiene il file sospetto EICAR-Test-File (in realtà NON è un virus).

Cliccando sull'opzione **Conosco i rischi, quindi proseguì**, il test sarà scaricato e comparirà una finestra di Bitdefender per informarti che ha rilevato un virus.

Clicca su **Maggiori dettagli** per scoprire altre informazioni su questa azione.

Se non ricevi alcun avviso da parte di Bitdefender, ti consigliamo di contattare il supporto tecnico di Bitdefender come descritto nella sezione **«Chiedere aiuto»** (p. 157).

13.2. Come posso rimuovere Bitdefender?

Se desideri rimuovere Bitdefender Antivirus Plus 2016, segui questi passaggi:

● In Windows 7:

1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
2. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
3. Seleziona **Rimuovi** e poi seleziona **Voglio reinstallarlo**.



4. Clicca su **Avanti** per continuare.
5. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

● In **Windows 8 e Windows 8.1**:

1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
3. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
4. Seleziona **Rimuovi** e poi seleziona **Voglio reinstallarlo**.
5. Clicca su **Avanti** per continuare.
6. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

● In **Windows 10**:

1. Clicca su **Start** e poi su **Impostazioni**.
2. Clicca sull'icona **Sistema** nelle **Impostazioni** e poi seleziona **Applicazioni installate**.
3. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
5. Seleziona **Rimuovi** e poi seleziona **Voglio reinstallarlo**.
6. Clicca su **Avanti** per continuare.
7. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

13.3. Come posso spegnere automaticamente il computer al termine della scansione?


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



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

Considera questo esempio: hai finito di lavorare al computer e vuoi andare a riposare. Ti piacerebbe che Bitdefender eseguisse una scansione antim malware sull'intero sistema.

Ecco come impostare Bitdefender per spegnere il sistema al termine della scansione:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Nel modulo **Antivirus**, seleziona **Gestisci scansioni**.
4. Nella finestra **Gestisci attività di scansione**, clicca su **Nuova attività personalizzata** per inserire un nome per la scansione e selezionare i percorsi da esaminare.
5. Se desideri configurare le opzioni di scansione in ogni dettaglio, seleziona la scheda **Avanzate**.
6. Scegli di spegnere il computer al termine della scansione, se non venisse rilevata alcuna minaccia.
7. Clicca su **OK** per salvare le modifiche e chiudere la finestra.
8. Clicca sul pulsante **Esegui scansione** per avviare la scansione del tuo sistema.

Se non vengono rilevate minacce, il computer si spegnerà.

Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo. Per maggiori informazioni, fai riferimento a «*Procedura guidata scansione antivirus*» (p. 86).

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


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



Importante

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

Per gestire le impostazioni del proxy, segui questi passaggi:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Impostazioni generali** dal menu a tendina.
2. Nella finestra **Impostazioni generali**, seleziona la scheda **Avanzate**.
3. Attiva l'uso del proxy, cliccando sull'interruttore.
4. Clicca sul collegamento **Gestione proxy**.
5. Ci sono due opzioni per determinare le impostazioni proxy:
 - **Importa le impostazioni del proxy dal browser predefinito** - le impostazioni del proxy dell'utente attuale, estratte dal browser predefinito. Se il server proxy richiede un nome utente e una password, devi indicarli nei rispettivi campi.



Nota

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

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



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

Per scoprire se hai un sistema operativo a 32 o 64 bit, segui questi passaggi:

● In **Windows 7**:

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

● In **Windows 8 e Windows 8.1**:

1. Dal menu Start di Windows, localizza l'opzione **Computer** (puoi anche digitare direttamente "Computer" nella finestra di ricerca del menu Start) e poi clicca sulla sua icona con il pulsante destro.
2. Seleziona **Proprietà** nel menu inferiore.
3. Controlla in Sistema per verificare il tipo di sistema.

● In **Windows 10**:

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

13.6. Come posso visualizzare gli elementi nascosti in Windows?

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

Segui questi passaggi per mostrare gli elementi nascosti in Windows:

1. Clicca su **Start** e poi seleziona **Pannello di controllo**.

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

2. Seleziona **Opzioni cartella**.



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

In **Windows 10**:

1. Digita "Visualizza cartelle e file nascosti" nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona.
2. Seleziona **Visualizza cartelle, file e unità nascosti**.
3. Deseleziona **Nascondi estensioni per i file conosciuti**.
4. Deseleziona **Nascondi file protetti del sistema operativo**.
5. Clicca su **Applica** e poi su **OK**.

13.7. Come posso rimuovere le altre soluzioni di sicurezza?

La ragione principale per usare una soluzione di sicurezza è garantire la protezione e la sicurezza dei tuoi dati. Ma cosa succede quando si ha più di un prodotto di sicurezza sullo stesso sistema?

Usando più di una soluzione di sicurezza sullo stesso computer, il sistema diventa instabile. Il programma d'installazione di Bitdefender Antivirus Plus 2016 rileva automaticamente altri programmi di sicurezza e ti offre la possibilità di disinstallarli.

Se non hai rimosso le altre soluzioni di sicurezza durante l'installazione iniziale, segui questi passaggi:

● In **Windows 7**:

1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
2. Attendi per qualche istante, finché non compare l'elenco del software installato.
3. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.



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

● In Windows 8 e Windows 8.1:

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

● In Windows 10:

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

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

13.8. Come posso riavviare in modalità provvisoria?

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



Per avviare Windows in modalità provvisoria:

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



GESTIRE LA PROPRIA SICUREZZA



14. PROTEZIONE ANTIVIRUS

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

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

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



Importante

Per impedire ai virus di infettare il tuo computer, tieni attivata la **Scansione all'accesso**.

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

Bitdefender controlla automaticamente ogni supporto rimovibile che è collegato al computer per assicurarti di accedervi in sicurezza. Per maggiori informazioni, fai riferimento a *«Scansione automatica di supporti rimovibili»* (p. 90).

Gli utenti più esperti possono configurare le eccezioni della scansione, se non desiderano controllare determinati file o estensioni. Per maggiori informazioni, fai riferimento a *«Configurare le eccezioni della scansione»* (p. 92).

Quando rileva un virus o un malware, Bitdefender tenterà automaticamente di rimuovere il codice malware dal file infetto, ricostruendo il file originale. Questa operazione è denominata disinfezione. I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione. Per maggiori informazioni, fai riferimento a *«Gestire i file in quarantena»* (p. 95).

Se il tuo computer è stato infettato da un malware, fai riferimento a *«Rimuovere malware dal sistema»* (p. 147). Per aiutarti a ripulire il tuo computer dai malware che non possono essere rimossi dal sistema operativo Windows, Bitdefender ti offre una **Modalità soccorso**. Si tratta di un ambiente sicuro,



realizzato specificatamente per la rimozione dei malware, che ti consente di avviare il tuo computer in modo indipendente da Windows. Quando il computer parte in Modalità soccorso, i malware di Windows non sono attivi, semplificando così la loro rimozione.

Per proteggerti da applicazioni sconosciute e pericolose, Bitdefender utilizza Active Threat Control, una tecnologia euristica avanzata, che monitora continuamente le applicazioni in esecuzione sul sistema. Active Threat Control blocca automaticamente le applicazioni che mostrano un comportamento simile ai malware, per impedirgli di danneggiare il computer. Occasionalmente, applicazioni legittime potrebbero essere bloccate. In questo caso, puoi configurare Active Threat Control per non bloccare queste applicazioni di nuovo creando delle regole di eccezione. Per altre informazioni, fai riferimento a «*Active Threat Control*» (p. 96).


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

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

Le impostazioni predefinite della protezione in tempo reale assicurano una buona protezione contro i malware, con un impatto minore sulle prestazioni di sistema. Puoi modificare facilmente le impostazioni della protezione in tempo reale in base alle tue necessità passando a uno dei livelli di protezione predefiniti. O, se sei un utente avanzato, puoi configurare le impostazioni della scansione in ogni dettaglio, creando un livello di protezione personalizzato.

14.1.1. Attivare o disattivare la protezione in tempo reale

Per attivare o disattivare la protezione antimaleware in tempo reale, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus** e seleziona la finestra **Protezione**.
4. Clicca sull'interruttore per attivare o disattivare la scansione all'accesso.



5. Se vuoi disattivare la protezione in tempo reale, comparirà una finestra di avviso. Devi confermare la tua scelta selezionando dal menu per quanto tempo desideri disattivare la protezione in tempo reale. Puoi disattivare la protezione in tempo reale per 5, 15 o 30 minuti, un'ora, in modo permanente o fino a un riavvio del sistema. La protezione in tempo reale si attiverà automaticamente allo scadere del tempo indicato.




Avvertimento

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

14.1.2. Impostare il livello di protezione in tempo reale

Il livello di protezione in tempo reale definisce le impostazioni della scansione per la protezione in tempo reale. Puoi modificare facilmente le impostazioni della protezione in tempo reale in base alle tue necessità passando a uno dei livelli di protezione predefiniti.

Per impostare il livello di protezione in tempo reale, segui questi passaggi:


1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus** e seleziona la finestra **Protezione**.
4. Trascina il cursore scorrevole lungo la barra per impostare il livello di protezione desiderato. Usa la descrizione sul lato destro della barra per selezionare il livello di protezione che si adatta meglio alle tue necessità di sicurezza.

14.1.3. Configurare le impostazioni della protezione in tempo reale

Gli utenti avanzati possono trarre vantaggio dalle impostazioni di scansione offerte da Bitdefender. Puoi configurare le impostazioni della protezione in tempo reale in ogni dettaglio, creando un livello di protezione personalizzato.

Per configurare le impostazioni della protezione in tempo reale, segui questi passaggi:



1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus** e seleziona la finestra **Protezione**.
4. Clicca su **Personalizzato**.
5. Configura le impostazioni della scansione come necessario.
6. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

Informazioni sulle opzioni di scansione

Questa informazione potrebbe esserti utile:

- Se non conosci alcuni termini, verificali nel **glossario**. Puoi anche trovare informazioni utili cercando su Internet.
- **Opzione di scansione per i file a cui accedi**. Puoi impostare Bitdefender per eseguire la scansione su tutti i file a cui si accede o solo sulle applicazioni (file dei programmi). Controllare tutti i file a cui si ha avuto accesso fornisce una protezione migliore, mentre controllare solo le applicazioni può essere usato per ottenere prestazioni migliori.

Di norma, sia le cartelle locali sia quelle condivise in rete sono soggette a una scansione all'accesso. Per migliorare le prestazioni del sistema, è possibile escludere i percorsi di rete dalla scansione all'accesso.

Le applicazioni (o programmi) sono più vulnerabili agli attacchi dei malware rispetto ad altri tipi di file. Questa categoria include le seguenti estensioni dei file:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fpx; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript;



vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsn; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Scansiona all'interno degli archivi.** La scansione degli archivi è un processo lento e che richiede molte risorse, che quindi non è consigliato per la protezione in tempo reale. Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del sistema. I malware possono colpire il sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la protezione in tempo reale.

Se decidi di utilizzare questa opzione, puoi impostare un limite di dimensione massima degli archivi da controllare con la scansione all'accesso. Seleziona la casella corrispondente e digita la dimensione massima dell'archivio (in MB).

- **Opzioni di scansione per traffico e-mail e HTTP.** Per impedire il download di malware sul tuo PC, Bitdefender controlla automaticamente i seguenti punti d'entrata per i malware:

- E-mail in entrata e in uscita
- Traffico HTTP

Controllare il traffico web potrebbe rallentare leggermente la navigazione web, ma impedirà l'accesso a ogni malware tramite Internet o i download.

Sebbene non consigliabile, per aumentare le prestazioni del sistema, puoi disattivare la scansione per e-mail o web. Disattivando le opzioni di scansione corrispondenti, le e-mail e i file ricevuti o scaricati da Internet non saranno controllati, consentendo ai file infetti di essere salvati sul computer. Questa non è una minaccia particolarmente importante, perché la protezione in tempo reale bloccherà i malware quando si accede ai file infetti (apertura, spostamento, copiatura o esecuzione).

- **Scansiona i settori di avvio.** È possibile impostare Bitdefender per controllare i settori di boot del disco rigido. Questo settore del disco rigido contiene il codice necessario per inizializzare il processo di avvio del computer. Quando un virus infetta il settore di boot, il disco potrebbe non essere accessibile e potrebbe non essere possibile avviare il sistema e accedere ai dati.
- **Scansiona solo file nuovi e modificati.** Controllando solo i file modificati o nuovi, potresti migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.
- **Scansione per keylogger.** Seleziona questa opzione per eseguire una scansione del sistema alla ricerca di applicazioni keylogger. I keylogger




registrano ciò che digiti sulla tastiera per poi inviare queste informazioni tramite Internet a un hacker. L'hacker può trovare informazioni sensibili nei dati rubati, come numeri e password di un conto corrente, e usarle per ottenere benefici personali.

- **Scansione all'avvio del sistema.** Seleziona l'opzione di scansione all'avvio per eseguire la scansione del sistema all'avvio, quando tutti i suoi servizi più importanti vengono caricati. Lo scopo di questa funzione è migliorare il rilevamento dei virus all'avvio del sistema e il tempo necessario per avviare il sistema stesso.

Azioni intraprese su malware rilevati

Puoi configurare le azioni intraprese dalla protezione in tempo reale.

Per configurare tali azioni, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus** e seleziona la finestra **Protezione**.
4. Clicca su **Personalizzato**.
5. Seleziona la scheda **Azioni** e configura le impostazioni della scansione in base alle tue necessità.
6. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

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

Esegui azioni appropriate

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

- **File infetti.** File rilevati che corrispondono a firme malware infette nel database di firme malware di Bitdefender. Bitdefender tenterà automaticamente di rimuovere il codice malware dal file infetto e di ricostruire il file originale. Questa operazione è denominata disinfezione.

I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione. I file in quarantena non possono essere



eseguiti né essere aperti, annullando il rischio d'infezione. Per maggiori informazioni, fai riferimento a *«Gestire i file in quarantena»* (p. 95).



Importante

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

- **File sospetti.** I file sono stati rilevati come sospetti dall'analisi euristica. I file sospetti non possono essere disinfettati, perché non è disponibile alcuna routine di disinfezione. Saranno messi in quarantena per impedire una potenziale infezione.

Di norma, i file in quarantena sono inviati automaticamente ai laboratori di Bitdefender per essere analizzati dai ricercatori antim malware di Bitdefender. Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.

- **Archivi contenenti file infetti.**
 - Gli archivi che contengono solo file infetti sono eliminati automaticamente.
 - Se un archivio contiene sia file puliti che infetti, Bitdefender tenterà di eliminare i file infetti a condizione che possa riformare l'archivio con i file puliti. Se la ricostruzione dell'archivio non è possibile, sarai informato del fatto che non può essere intrapresa alcuna azione in modo da evitare la perdita di file puliti.

Sposta i file in quarantena

Sposta i file infetti nella quarantena. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Per maggiori informazioni, fai riferimento a *«Gestire i file in quarantena»* (p. 95).

Nega l'accesso


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

14.1.4. Ripristinare le impostazioni predefinite

Le impostazioni predefinite della protezione in tempo reale assicurano una buona protezione contro i malware, con un impatto minore sulle prestazioni di sistema.



Per ripristinare le impostazioni predefinite della protezione in tempo reale, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus** e seleziona la finestra **Protezione**.
4. Clicca su **Predefinito**.

14.2. Scansione a richiesta

L'obiettivo principale di Bitdefender è di mantenere il proprio computer privo di virus. Ciò avviene tenendo lontani i nuovi virus dal computer ed esaminando i messaggi e-mail e qualsiasi nuovo file scaricato o copiato sul sistema.

Esiste il rischio che un virus sia già contenuto nel tuo sistema, addirittura prima dell'installazione di Bitdefender. Questo è il motivo per cui suggeriamo di effettuare una scansione sul tuo computer alla ricerca di virus residenti dopo aver installato Bitdefender. Inoltre, è una buona idea effettuare frequentemente una scansione del computer, alla ricerca di virus.

La scansione su richiesta si basa sulle impostazioni della scansione. Le impostazioni della scansione specificano le opzioni della scansione e gli elementi da esaminare. Puoi eseguire la scansione del computer ogni volta che vuoi, avviando le attività predefinite o una tua scansione (attività definite dall'utente). Se desideri controllare ubicazioni particolari sul tuo computer o impostare le opzioni di scansione, configura ed esegui una scansione personale.

14.2.1. Controllare un file o una cartella alla ricerca di malware


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



14.2.2. Eseguire una Scansione veloce

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

Per eseguire una Scansione veloce, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Nel modulo **Antivirus**, seleziona **Scansione veloce**.
4. Segui la **procedura guidata della scansione antivirus** per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati. Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

O più rapidamente, clicca sul pulsante d'azione **Scansione veloce** nell'interfaccia di Bitdefender.

14.2.3. Eseguire una scansione del sistema

La Scansione del sistema esamina l'intero computer per rilevare tutti i tipi di malware che minacciano la sua sicurezza, come virus, spyware, adware, rootkit e altri.



Nota

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


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

- Assicurarsi che le firme malware di Bitdefender siano aggiornate. Eseguire la scansione con un database delle firme obsoleto può impedire a Bitdefender di rilevare nuovi malware, trovati dopo l'ultimo aggiornamento. Per maggiori informazioni, fai riferimento a **«Mantenere aggiornato Bitdefender»** (p. 43).
- Chiudere tutti i programmi aperti.




Se desideri controllare ubicazioni particolari sul tuo computer o impostare le opzioni di scansione, configura ed esegui una scansione personale. Per maggiori informazioni, fai riferimento a «*Configurare una scansione personale*» (p. 83).

Per eseguire una Scansione del sistema, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Nel modulo **Antivirus**, seleziona **Scansione sistema**.
4. Segui la **procedura guidata della scansione antivirus** per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati. Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

14.2.4. Configurare una scansione personale

Per configurare una scansione antimalware in ogni dettaglio e poi eseguirla, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Nel modulo **Antivirus**, seleziona **Gestisci scansioni**.
4. Clicca su **Nuova Attività personalizzata**. Nella scheda **Base**, inserisci un nome per la scansione e seleziona i percorsi da controllare.
5. Se desideri configurare le opzioni di scansione in ogni dettaglio, seleziona la scheda **Avanzate**. Comparirà una nuova finestra. Attenersi alla seguente procedura:
 - a. Puoi configurare facilmente le opzioni di scansione, impostando il livello della scansione. Trascina il cursore scorrevole lungo la barra per impostare il livello di scansione desiderato. Usa la descrizione sul lato destro della barra per identificare il livello di scansione che si adatta meglio alle tue necessità.

Gli utenti avanzati possono trarre vantaggio dalle impostazioni di scansione offerte da Bitdefender. Per configurare in ogni dettaglio le



opzioni della scansione, clicca su **Personalizzato**. Al termine di questa sezione trovi maggiori informazioni al riguardo.

b. Puoi anche configurare queste opzioni generali:

- **Esegui l'attività con bassa priorità**. Diminuisce la priorità del processo di scansione. Consentirai ad altri programmi di essere più veloci, incrementando il tempo necessario per terminare il processo di scansione.
- **Minimizza la Procedura guidata di scansione nell'area di notifica**. Minimizza la finestra di scansione nell'**area di notifica**. Clicca due volte sull'icona di Bitdefender per riaprirlo.
- Specifica l'azione da intraprendere se non venisse rilevata alcuna minaccia.

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

6. Se vuoi impostare un programma per le attività di scansione, usa l'interruttore **Programma** nella finestra di base. Seleziona una delle opzioni corrispondenti per impostare un elenco:

- All'avvio del sistema
- Una volta
- Periodicamente

7. Clicca su **Esegui scansione** e segui la **procedura guidata della scansione antivirus** per completare la scansione. In base ai percorsi da controllare, la scansione potrebbe richiedere un po' di tempo. Al termine della scansione, ti sarà chiesto di scegliere quali azioni intraprendere sui file rilevati, se presenti.

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

Informazioni sulle opzioni di scansione

Questa informazione potrebbe esserti utile:

- Se non conosci alcuni termini, verificali nel **glossario**. Puoi anche trovare informazioni utili cercando su Internet.
- **Controlla file**. Puoi impostare Bitdefender per eseguire la scansione su tutti i file o solo sulle applicazioni (file dei programmi). Controllare tutti i



file ti garantisce una protezione migliore, mentre controllare solo le applicazioni può essere utile per eseguire una scansione più veloce.

Le applicazioni (o programmi) sono più vulnerabili agli attacchi dei malware rispetto ad altri tipi di file. Questa categoria include le seguenti estensioni dei file: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpv; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Opzioni di scansione per archivi.** Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del sistema. I malware possono colpire il sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la protezione in tempo reale. Tuttavia, si consiglia di usare questa opzione per rilevare e rimuovere ogni minaccia potenziale, anche se non è immediata.



Nota

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

- **Scansiona i settori di avvio.** È possibile impostare Bitdefender per controllare i settori di boot del disco rigido. Questo settore del disco rigido contiene il codice necessario per inizializzare il processo di avvio del computer. Quando un virus infetta il settore di boot, il disco potrebbe non essere accessibile e potrebbe non essere possibile avviare il sistema e accedere ai dati.
- **Scansiona memoria.** Seleziona questa opzione per controllare i programmi in esecuzione nella memoria di sistema.
- **Registro di scansione.** Seleziona questa opzione per controllare le chiavi del registro. Il registro di Windows è un database che memorizza le



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

- **Scansiona i cookie.** Seleziona questa opzione per controllare i cookie memorizzati dai browser sul tuo computer.
- **Scansiona solo file nuovi e modificati.** Controllando solo i file modificati o nuovi, potresti migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.
- **Ignora keylogger commerciali.** Seleziona questa opzione se hai installato e utilizzi un programma keylogger commerciale sul tuo computer. I keylogger commerciali sono programmi legittimi di monitoraggio del computer la cui funzione elementare è registrare tutto ciò che viene digitato sulla tastiera.
- **Scansiona alla ricerca di rootkit.** Seleziona questa opzione per eseguire una scansione alla ricerca di **rootkit** e oggetti nascosti usando tale software.

14.2.5. Procedura guidata scansione antivirus

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

Nota

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

Fase 1 - Eseguire la scansione

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

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



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

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

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

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

Fase 2 - Scegliere le azioni

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



Nota

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

Gli oggetti infetti vengono mostrati in gruppi in base al malware con il quale sono stati infettati. Clicca sul collegamento corrispondente alla minaccia per trovare più informazioni sugli oggetti infetti.

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



Esegui azioni appropriate

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

- **File infetti.** File rilevati che corrispondono a firme malware infette nel database di firme malware di Bitdefender. Bitdefender tenterà automaticamente di rimuovere il codice malware dal file infetto e di ricostruire il file originale. Questa operazione è denominata disinfezione.

I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Per maggiori informazioni, fai riferimento a «*Gestire i file in quarantena*» (p. 95).



Importante

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

- **File sospetti.** I file sono stati rilevati come sospetti dall'analisi euristica. I file sospetti non possono essere disinfettati, perché non è disponibile alcuna routine di disinfezione. Saranno messi in quarantena per impedire una potenziale infezione.

Di norma, i file in quarantena sono inviati automaticamente ai laboratori di Bitdefender per essere analizzati dai ricercatori antimaleware di Bitdefender. Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.

- **Archivi contenenti file infetti.**
 - Gli archivi che contengono solo file infetti sono eliminati automaticamente.
 - Se un archivio contiene sia file puliti che infetti, Bitdefender tenterà di eliminare i file infetti a condizione che possa riformare l'archivio con i file puliti. Se la ricostruzione dell'archivio non è possibile, sarai informato del fatto che non può essere intrapresa alcuna azione in modo da evitare la perdita di file puliti.

Elimina

Rimuove i file rilevati dal disco.



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

Non fare nulla

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

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

Fase 3 - Sommario

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

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



Importante

Nella maggior parte dei casi Bitdefender disinfetta con successo i file infetti che rileva o isola l'infezione. Tuttavia, ci sono problemi che non possono essere risolti automaticamente. Se richiesto, riavvia il sistema per completare il processo di pulizia. Per maggiori informazioni e istruzioni su come rimuovere i malware manualmente, fai riferimento a *«Rimuovere malware dal sistema»* (p. 147).


14.2.6. Controllare i registri di scansione

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

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

Per controllare un registro di scansione o qualsiasi infezione rilevata in un secondo momento, segui questi passaggi:



1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Eventi** dal menu a tendina.
2. Nella finestra **Eventi**, seleziona **Antivirus** dal corrispondente menu a tendina.
Qui puoi trovare tutti gli eventi della scansione antim malware, incluso le minacce rilevate dalla scansione all'accesso, le scansioni avviate dall'utente e le variazioni di stato per le scansioni automatiche.
3. Nell'elenco degli eventi, puoi controllare quali scansioni sono state eseguite di recente. Clicca su un evento per visualizzare maggiori dettagli al riguardo.
4. Per aprire il registro della scansione, clicca su **Guarda registro**. Se vuoi eseguire nuovamente la stessa scansione, clicca sul pulsante **Nuova scansione**.

14.3. Scansione automatica di supporti rimovibili


Bitdefender rileva automaticamente quando si collega un dispositivo di archiviazione rimovibile al computer e ne esegue una scansione in background. Questa operazione è consigliata per impedire che virus e altri malware infettino il computer.

I dispositivi rilevati rientrano in una di queste categorie:

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

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

14.3.1. Come funziona?

Quando rileva un dispositivo rimovibile di archiviazione, Bitdefender inizia la scansione antim malware in background (a condizione che la scansione automatica sia attivata per quel tipo di dispositivo). Un'icona di scansione di Bitdefender  comparirà nell'**area di notifica**. Clicca sull'icona per aprire la finestra di scansione e visualizzarne l'avanzamento.



Se l'Autopilot è attivato, non dovrai preoccuparti della scansione. La scansione sarà solo registrata e le relative informazioni saranno disponibili nella finestra **Eventi**.

Se l'Autopilot è disattivato:

1. Sarai avvisato attraverso una finestra pop-up che un nuovo dispositivo è stato rilevato ed è in fase di scansione.
2. Nella maggior parte dei casi, Bitdefender rimuove automaticamente i malware rilevati o isola i file infetti mettendoli in quarantena. Se dopo la scansione ci sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.



Nota

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

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

Queste informazioni potrebbero esserti utili:


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

Per sapere come comportarti con i malware, consulta *«Rimuovere malware dal sistema»* (p. 147).

14.3.2. Gestire la scansione di supporti rimovibili

Per gestire la scansione automatica dei supporti rimovibili, segui questi passaggi:



1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus** e seleziona la finestra **Eccezioni**.

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

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

14.4. Configurare le eccezioni della scansione

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

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


Nota

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

14.4.1. Escludere file o cartelle dalla scansione

Per escludere determinati file o cartelle dalla scansione, segui questi passaggi:



1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus**.
4. Nella finestra **Antivirus**, seleziona la scheda **Eccezioni**.
5. Attiva le eccezioni della scansione per i file usando l'interruttore corrispondente.
6. Clicca sul collegamento **File e cartelle escluse**. Nella finestra che compare, puoi gestire i file e le cartelle esclusi dalla scansione.
7. Aggiungi eccezioni seguendo questi passaggi:
 - a. Clicca sul pulsante **Aggiungi** localizzato nella parte superiore della tabella delle eccezioni.
 - b. Clicca su **Sfoglia**, seleziona il file o la cartella che desideri escludere dalla scansione e quindi clicca su **OK**. In alternativa, puoi digitare (o copiare e incollare) il percorso del file o della cartella nello spazio apposito.
 - c. Di norma, il file o la cartella selezionati sono esclusi dalla scansione all'accesso e da quella su richiesta. Per cambiare quando applicare l'eccezione, seleziona una delle altre opzioni.
 - d. Clicca su **Aggiungi**.
8. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

14.4.2. Escludere estensioni di file dalla scansione

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




Importante

Usa la massima cautela nell'escludere le estensioni dalla scansione, perché tali estensioni possono rendere il computer vulnerabile ai malware.

Per escludere determinate estensioni dei file dalla scansione, segui questi passaggi:




1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus**.
4. Nella finestra **Antivirus**, seleziona la scheda **Eccezioni**.
5. Attiva le eccezioni della scansione per i file usando l'interruttore corrispondente.
6. Clicca sul collegamento **Estensioni escluse**. Nella finestra che compare, puoi gestire le estensioni dei file escluse dalla scansione.
7. Aggiungi eccezioni seguendo questi passaggi:
 - a. Clicca sul pulsante **Aggiungi** localizzato nella parte superiore della tabella delle eccezioni.
 - b. Inserisci le estensioni che vuoi escludere dalla scansione, separate da punto e virgola (;). Ecco un esempio:
`txt;avi;jpg`
 - c. Di norma, tutti i file con le estensioni indicate sono esclusi dalla scansione all'accesso e da quella su richiesta. Per cambiare quando applicare l'eccezione, seleziona una delle altre opzioni.
 - d. Clicca su **Aggiungi**.
8. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

14.4.3. Gestire le eccezioni della scansione

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

Per gestire le eccezioni della scansione, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus** e seleziona la finestra **Eccezioni**. Usa le opzioni nella sezione **File e cartelle** per gestire le eccezioni della scansione.



4. Per rimuovere o modificare le eccezioni della scansione, clicca su uno dei collegamenti disponibili. Procedi come segue:
 - Per rimuovere una voce dalla tabella, selezionala e clicca sul pulsante **Rimuovi**.
 - Per modificare una voce dalla tabella, cliccaci sopra due volte (o selezionala e clicca sul pulsante **Modifica**). Apparirà una nuova finestra, dove potrai modificare l'estensione o il percorso da escludere e il tipo di scansione dal quale escluderlo, a seconda delle necessità. Esegui i cambiamenti necessari, poi clicca su **Modifica**.
5. Per disattivare le eccezioni, usa l'interruttore corrispondente.


14.5. Gestire i file in quarantena

Bitdefender isola i file infettati da malware che non può disinfettare e i file sospetti in un'area sicura chiamata quarantena. Quando un virus è in quarantena, non può più arrecare alcun danno in quanto non può essere eseguito o letto.

Di norma, i file in quarantena sono inviati automaticamente ai laboratori di Bitdefender per essere analizzati dai ricercatori antimaleware di Bitdefender. Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.

Inoltre Bitdefender controlla i file in quarantena dopo ogni aggiornamento delle firme malware. I file puliti vengono spostati automaticamente alla loro ubicazione originale.

Per controllare e gestire i file in quarantena, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus** e seleziona la finestra **Quarantena**.
4. I file in quarantena sono gestiti automaticamente da Bitdefender in base alle impostazioni di quarantena predefinite. Anche se non consigliato, puoi modificare le impostazioni della quarantena in base alle tue preferenze.



Controlla nuovamente la quarantena dopo aggiornamento definizioni virus

Mantieni questa opzione attivata per eseguire automaticamente la scansione dei file in quarantena dopo ogni aggiornamento delle definizioni dei virus. I file puliti vengono spostati automaticamente alla loro ubicazione originale.

Invia i file sospetti in quarantena per ulteriori analisi

Tieni questa opzione attivata per inviare automaticamente i file in quarantena ai laboratori di Bitdefender. I file campioni saranno analizzati dai ricercatori antimalware di Bitdefender. Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.

Elimina i contenuti più vecchi di {30} giorni

Di norma, i file in quarantena più vecchi di 30 giorni sono eliminati automaticamente. Se vuoi modificare questo intervallo, digita un nuovo valore nel campo corrispondente. Per disattivare la rilevazione automatica dei vecchi file in quarantena, digita 0.

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

14.6. Active Threat Control

Bitdefender Active Threat Control è una tecnologia di individuazione innovativa e proattiva, che utilizza metodi euristici avanzati per rilevare nuove minacce potenziali in tempo reale.


Active Threat Control monitora continuamente le applicazioni in esecuzione sul computer, cercando azioni simili a malware. A ognuna viene assegnato un punteggio e per ogni processo viene poi assegnato un punteggio totale. Quando il punteggio totale di un processo raggiunge una certa soglia, il processo è considerato nocivo ed è bloccato automaticamente.

Se l'Autopilot è disattivato, sarai avvisato tramite una finestra pop-up sull'applicazione bloccata. Diversamente, l'applicazione sarà bloccata senza alcuna notifica. Puoi verificare quali applicazioni sono state rilevate da Active Threat Control nella finestra **Eventi**.




14.6.1. Verificare le applicazioni rilevate

Per verificare le applicazioni rilevate da Active Threat Control, segui questi passaggi:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Eventi** dal menu a tendina.
2. Nella finestra **Eventi**, seleziona **Antivirus** dal corrispondente menu a tendina.
3. Clicca su un evento per visualizzare maggiori dettagli al riguardo.
4. Se ti fidi dell'applicazione, puoi configurare Active Threat Control per non bloccarla più, cliccando su **Consenti e monitora**. Active Threat Control continuerà a monitorare le applicazioni escluse. Se un'applicazione esclusa viene rilevata a eseguire attività sospette, l'evento semplicemente sarà registrato e notificato al cloud di Bitdefender come errore di rilevazione.

14.6.2. Attivare o disattivare Active Threat Control

Per attivare o disattivare Active Threat Control, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus**.
4. Nella finestra **Antivirus**, seleziona la scheda **Protezione**.
5. Clicca sull'interruttore per attivare o disattivare Active Threat Control.

14.6.3. Impostare la protezione di Active Threat Control

Se vedi che Active Threat Control rileva spesso applicazioni legittime, devi impostare un livello di protezione più permissivo.

Per impostare la protezione di Active Threat Control, trascina il cursore scorrevole lungo la barra per impostare il livello di protezione desiderato.

Usa la descrizione sul lato destro della barra per selezionare il livello di protezione che si adatta meglio alle tue necessità di sicurezza.




Nota

Se imposti il livello di protezione più elevato, Active Threat Control richiederà un minor numero di comportamenti simili a malware per segnalare un processo. Ciò comporterà un numero più elevato di applicazioni rilevate e, allo stesso tempo, a un aumento della probabilità di falsi positivi (applicazioni legittime rilevate come dannose).

14.6.4. Gestire i processi esclusi

Puoi configurare le regole delle eccezioni per le applicazioni attendibili in modo che Active Threat Control non le blocchi, se eseguono azioni simili a malware. Active Threat Control continuerà a monitorare le applicazioni escluse. Se un'applicazione esclusa viene rilevata a eseguire attività sospette, l'evento semplicemente sarà registrato e notificato al cloud di Bitdefender come errore di rilevazione.

Per gestire le eccezioni di Active Threat Control, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus** e seleziona la finestra **Eccezioni**.
4. Clicca sul collegamento **Processi esclusi**. Nella finestra che compare, puoi gestire le eccezioni del processo di Active Threat Control.
5. Aggiungi eccezioni seguendo questi passaggi:
 - a. Clicca sul pulsante **Aggiungi** localizzato nella parte superiore della tabella delle eccezioni.
 - b. Clicca su **Sfoglia**, trova e seleziona l'applicazione che vuoi escludere e poi clicca su **OK**.
 - c. Mantieni selezionata l'opzione **Consenti**, per impedire ad Active Threat Control di bloccare l'applicazione.
 - d. Clicca su **Aggiungi**.
6. Per rimuovere o modificare le eccezioni, procedi come segue:
 - Per rimuovere una voce dalla tabella, selezionala e clicca sul pulsante **Elimina**.



- Per modificare una voce dalla tabella, cliccaci sopra due volte (o selezionala e clicca sul pulsante **Modifica**). Esegui i cambiamenti necessari, poi clicca su **Modifica**.

7. Salva le modifiche e chiudi la finestra.




15. PROTEZIONE WEB

La Protezione web di Bitdefender assicura una navigazione sicura, avvisandoti in caso di eventuali pagine web di phishing.

Bitdefender fornisce protezione web in tempo reale per:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Per configurare le impostazioni della Protezione web, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Protezione web**.

Clicca sugli interruttori per attivare o disattivare:

- Ricerca sicura, una componente che valuta i risultati delle tue ricerche e i link pubblicati sui social network, posizionando un'icona accanto a ogni risultato:

- Non dovresti visitare questa pagina web.

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

- Questa è una pagina sicura da visitare.

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

- Google
- Yahoo!
- Bing
- Baidu

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

- Facebook
- Twitter
- Controllare il traffico web SSL.



Gli attacchi più sofisticati possono usare il traffico web sicuro per ingannare le loro vittime. Si consiglia pertanto di attivare la scansione SSL.

- Protezione dalle frodi.
- Protezione da phishing.

Puoi creare un elenco di siti web che non saranno esaminati dai motori antimalware, antiphishing e antifrode di Bitdefender. L'elenco dovrebbe contenere solo siti web di cui ti fidi completamente. Ad esempio, aggiungi i siti web dove fai di solito i tuoi acquisti online.

Per configurare e gestire i siti web utilizzando la protezione web fornita da Bitdefender, clicca sul link **Whitelist**. Comparirà una nuova finestra.

Per aggiungere un sito alla whitelist, inserisci il suo indirizzo nel campo corrispondente e quindi clicca su **Aggiungi**.

Per rimuovere un sito web dall'elenco, selezionalo e clicca sul collegamento **Rimuovi** corrispondente.

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

15.1. Avvisi di Bitdefender nel browser

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

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

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

- Allontanati dalla pagina web, cliccando su **Per sicurezza torna indietro**.
- Disattiva il blocco delle pagine che contengono phishing, cliccando su **Disattiva il filtro antiphishing**.
- Disattiva il blocco delle pagine che contengono malware, cliccando su **Disattiva il filtro antimalware**.
- Aggiungi la pagina alla whitelist dell'antiphishing cliccando su **Aggiungi alla whitelist**. La pagina non sarà più controllata dai motori antiphishing di Bitdefender.
- Procedi alla pagina web, malgrado l'avvertimento, cliccando su **Sono a conoscenza dei rischi, quindi proseguì**.



16. PROTEZIONE DATI

16.1. Eliminare i file in modo permanente


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

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

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

1. Clicca con il pulsante destro sul file o la cartella che vuoi eliminare in modo permanente.
2. Seleziona **Bitdefender** > **Distruttore di file** nel menu contestuale che apparirà.
3. Apparirà una finestra di conferma. Clicca su **Sì** per avviare la procedura guidata del Distruttore di file.
4. Attendi che Bitdefender termini la distruzione dei file.
5. I risultati sono mostrati. Clicca su **Chiudi** per uscire dalla procedura guidata.

In alternativa, puoi distruggere i file dall'interfaccia di Bitdefender.

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Privacy**.
3. Nel modulo **Protezione dati**, seleziona **Distruttore file**.
4. Segui la procedura guidata del Distruttore di file:
 - a. **Aggiungi cartella(e)**
Aggiungi i file o le cartelle che vuoi rimuovere in modo permanente.
 - b. Clicca su **Avanti** e conferma di voler continuare il processo.
Attendi che Bitdefender termini la distruzione dei file.
 - c. **Risultati**



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



17. VULNERABILITÀ

Un passaggio importante nella protezione del computer contro azioni e applicazioni dannose è mantenere aggiornato il sistema operativo e le applicazioni che usi regolarmente. Dovresti anche considerare di disattivare le impostazioni di Windows che rendono il sistema più vulnerabile ai malware. Inoltre, per impedire accessi fisici non autorizzati al tuo computer, devi configurare password sicure (password che non possano essere facilmente indovinate) per ogni account di Windows.

Bitdefender controlla automaticamente il sistema alla ricerca di vulnerabilità e fornisce avvisi al riguardo. Le vulnerabilità di sistema includono quanto segue:

- applicazioni obsolete sul computer.
- aggiornamenti di Windows mancanti.
- password deboli per gli account utente di Windows.


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

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

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

17.1. Controllare il sistema per rilevare vulnerabilità

Per risolvere le vulnerabilità del sistema utilizzando l'opzione Scansione vulnerabilità, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Nel modulo **Vulnerabilità**, seleziona **Scansione vulnerabilità**.



4. Attendi che Bitdefender controlli le vulnerabilità del sistema. Per fermare il processo di scansione, clicca sul pulsante **Ignora** nella parte superiore della finestra.

O più rapidamente, clicca sul pulsante d'azione **Scansione vulnerabilità** nell'interfaccia di Bitdefender.

● **Aggiornamenti critici di Windows**

Clicca su **Mostra dettagli** per visualizzare un elenco di aggiornamenti critici di Windows che non sono installati sul computer.

Per avviare l'installazione degli aggiornamenti selezionati, clicca su **Installa aggiornamenti**. L'installazione degli aggiornamenti potrebbe richiedere un po' di tempo e alcuni potrebbero richiedere anche un riavvio del sistema per completare l'installazione. Se necessario, riavvia il sistema al più presto.

● **Aggiornamenti applicazioni**

Se un'applicazione non è aggiornata, clicca sul link **Scarica nuova versione** per scaricare la versione più recente.

Clicca su **Mostra dettagli** per visualizzare maggiori informazioni sull'applicazione che dev'essere aggiornata.

● **Password account Windows deboli**

Puoi visualizzare l'elenco degli account di Windows configurati sul tuo computer e il livello di protezione che le loro password forniscono.

Clicca su **Cambia password all'accesso** per impostare una nuova password per il tuo sistema.

Clicca su **Mostra dettagli** per modificare le password non sicure. Puoi scegliere tra chiedere di cambiare la password al prossimo accesso o cambiare subito la password direttamente. Per avere una password sicura, utilizza una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, \$ o @).


Nell'angolo in alto a destra della finestra, puoi filtrare i risultati in base alle tue preferenze.

17.2. Usare il controllo automatico delle vulnerabilità


Bitdefender controlla regolarmente e in background il sistema alla ricerca di vulnerabilità, tenendo traccia dei problemi rilevati nella finestra **Eventi**.



Per verificare e sistemare i problemi rilevati, segui questi passaggi:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Eventi** dal menu a tendina.
2. Nella finestra **Eventi**, seleziona **Vulnerabilità** dall'elenco. Seleziona eventi.
3. Puoi visualizzare informazioni dettagliate sulle vulnerabilità del sistema rilevate. In base al problema, per risolvere una vulnerabilità specifica procedi come segue:
 - Se sono disponibili aggiornamenti di Windows, clicca su **Aggiorna ora**.
 - Se gli aggiornamenti automatici di Windows sono disattivati, clicca su **Attiva**.
 - Se un'applicazione non è aggiornata, clicca su **Aggiorna ora** per trovare un link alla pagina web del distributore, da dove poter installare la versione più recente dell'applicazione.
 - Se un account utente Windows ha una password poco sicura, clicca su **Cambia password** per costringere l'utente a modificare la password al prossimo accesso, oppure cambiala direttamente. Per avere una password sicura, utilizza una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, \$ o @).
 - Se la funzione di esecuzione automatica di Windows è attivata, clicca su **Risolvi** per disattivarla.

Per configurare le impostazioni del controllo vulnerabilità, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Vulnerabilità**.
4. Clicca sull'interruttore per attivare o disattivare la Scansione vulnerabilità.



Importante

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



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

Aggiornamenti critici di Windows

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

Aggiornamenti applicazioni

Verifica se le applicazioni installate sul sistema sono aggiornate. Applicazioni datate possono essere sfruttate da software dannosi, rendendo il tuo PC vulnerabile agli attacchi esterni.

Password non sicure

Verifica se le password degli account Windows configurate sul sistema sono più o meno facili da indovinare. Impostare password difficili da indovinare (password sicure) ostacola l'accesso al tuo sistema da parte degli hacker. Una password sicura include una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, \$ o @).

Esecuzione automatica supporti

Verifica lo stato della funzione di esecuzione automatica di Windows. Questa caratteristica consente alle applicazioni di essere avviate automaticamente da unità CD, DVD, USB o altri dispositivi esterni.

Alcuni tipi di malware usano l'esecuzione automatica per diffondersi automaticamente da supporti rimovibili al PC. Ecco perché si consiglia di disattivare questa funzione di Windows.



Nota

Se disattivi il monitoraggio di una vulnerabilità particolare, i relativi problemi non saranno più registrati nella finestra Eventi.



18. PROTEZIONE DA RANSOMWARE

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

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


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

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

Utilizzando le tecnologie più recenti, la Protezione da Ransomware di Bitdefender assicura la massima integrità al sistema, proteggendo le sue zone più critiche da qualsiasi danno, senza influenzarne le prestazioni. Tuttavia, potresti anche voler proteggere i tuoi file personali, come documenti, fotografie, filmati o i file presenti sul cloud.

18.1. Attivare o disattivare la Protezione da Ransomware

Per disattivare la Protezione da Ransomware, segui questi passaggi:


1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca su **Protezione da Ransomware**.
4. Clicca sull'interruttore per attivare o disattivare la **Protezione da Ransomware**.



Ogni volta che un'applicazione tenterà di accedere a un file protetto, comparirà una finestra di Bitdefender. Puoi consentirle o negarle l'accesso.

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

Se vuoi proteggere i tuoi file personali, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Protezione da Ransomware** e poi clicca sul pulsante **Aggiungi**.
4. Vai alla cartella che vuoi proteggere e clicca su **OK** per aggiungere la cartella selezionata all'ambiente protetto.

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




Nota

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

18.3. Configurare le applicazioni attendibili

Disattiva la Protezione da Ransomware per determinate applicazioni, ma meglio aggiungere all'elenco quelle sicuramente attendibili.

Per aggiungere applicazioni attendibili alle eccezioni, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Nel modulo **Protezione da Ransomware**, seleziona **Applicazioni attendibili**.
4. Clicca su **Aggiungi** e individua le applicazioni che vuoi proteggere.




5. Clicca su **OK** per aggiungere l'applicazione selezionata all'ambiente protetto.

18.4. Configurare le applicazioni bloccate

Tra le applicazioni installate sul computer, alcune potrebbero voler accedere ai tuoi file personali.


Per limitare tali applicazioni, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Nel modulo **Protezione da Ransomware**, seleziona **Applicazioni bloccate**.
4. Clicca su **Aggiungi** e individua le applicazioni che vuoi limitare.
5. Clicca su **OK** per aggiungere l'applicazione selezionata all'elenco di quelle limitate.

18.5. Protezione all'avvio

È risaputo che molte applicazioni malware sono impostate per essere eseguite all'avvio del sistema, cosa che può danneggiare seriamente un computer. La Protezione avvio di Bitdefender esamina tutte le aree critiche del sistema prima che i file vengano caricate, non influenzandone le prestazioni. Allo stesso tempo, viene garantita una protezione da attacchi basati sull'esecuzione di codici heap o stack, inserimenti di codici o hook in determinate librerie dinamiche.

Per disattivare la Protezione all'avvio, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca su **Protezione da Ransomware**.
4. Clicca sull'interruttore per attivare o disattivare la **Protezione all'avvio**.



19. SAFEPAY: SICUREZZA PER LE TRANSAZIONI ONLINE

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

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

Bitdefender Safepay™ è prima di tutto un browser protetto, un ambiente sigillato, concepito per proteggere e mantenere private le operazioni bancarie, gli acquisti e qualsiasi altro tipo di transazione online.

Per assicurare una migliore protezione della privacy, Bitdefender Password Manager è stato integrato in Bitdefender Safepay™ per proteggere le proprie credenziali ogni volta che si desidera accedere a indirizzi privati online. Per maggiori informazioni, fai riferimento a *«Protezione di Password Manager per le tue credenziali»* (p. 116).

Bitdefender Safepay™ offre le seguenti funzioni:

- Blocca l'accesso al proprio desktop, impedendo qualsiasi tentativo di catturare delle immagini del proprio schermo.
- Protegge le tue password segrete mentre navighi online con Password Manager.
- È dotato di una tastiera virtuale che, quando viene utilizzata, rende impossibile agli hacker rilevare la combinazione di tasti premuta.
- È completamente indipendente dagli altri browser.
- È dotato di una protezione integrata degli hotspot da utilizzare quando il computer è connesso a reti Wi-Fi non protette.
- Supporta i segnalibri e consente di navigare nei propri siti bancari/commerciali preferiti.



- Non è limitato agli acquisti e alle transazioni bancarie online. Ma qualsiasi sito web può essere aperto in Bitdefender Safepay™.

19.1. Utilizzare Bitdefender Safepay™

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

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

- Dall'**interfaccia di Bitdefender**:

1. Clicca sul pulsante d'azione **Safepay** nell'interfaccia di Bitdefender.

- Da Windows:

- In **Windows 7**:

1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
2. Clicca su **Bitdefender**.
3. Clicca su **Bitdefender Safepay™**.

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

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

- In **Windows 10**:

Digita "Bitdefender Safepay™" nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona.













Nota

Se il plugin Adobe Flash Player non è installato o aggiornato, comparirà un messaggio di Bitdefender. Clicca sul pulsante corrispondente per continuare. Una volta completato il processo di installazione, per continuare le tue operazioni, dovrai riaprire manualmente il browser di Bitdefender Safepay™.

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

- Inserisci gli URL che desideri utilizzare nella barra degli indirizzi.



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

19.2. Configurare le impostazioni

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

Impostazioni generali

Scegli cosa succede quando accedi a un negozio online a un sito di online banking nel tuo browser standard:

- Apri automaticamente siti web in Safepay.
- Suggestimi di usare Safepay.
- Non suggerirmi di usare Safepay.

Elenco domini

Scegli come Bitdefender Safepay™ si comporterà quando visiti siti web di determinati domini nel tuo browser standard, aggiungendoli all'elenco dei domini e selezionando il comportamento per ciascuno:

- Apri automaticamente Bitdefender Safepay™.
- Bitdefender ti chiede ogni volta come proseguire.
- Non utilizzare mai Bitdefender Safepay™ quando visiti una pagina di quel dato dominio in un browser standard.



Bloccare le finestre pop-up

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

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

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

Per rimuovere un sito web dall'elenco, selezionalo e clicca sul collegamento **Rimuovi** corrispondente.

Attiva protezione hotspot


Attivando questa funzione, puoi avere un ulteriore livello di protezione quando ti connetti a reti Wi-Fi non sicure.

Accedi *«Protezione hotspot per reti non sicure»* (p. 115) per maggiori informazioni.

19.3. Gestire i segnalibri

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

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

1. Clicca sull'icona  accanto alla barra degli indirizzi per aprire la pagina dei Segnalibri.



Nota

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

2. Clicca sul pulsante **+** per aggiungere un nuovo segnalibro.
3. Inserisci l'URL e il nome del segnalibro, poi clicca su **Crea**. Seleziona l'opzione **Apri automaticamente in Safepay**, se desideri che la pagina salvata nei segnalibri si apra in Bitdefender Safepay™ ogni volta che vi




accedi. L'URL viene aggiunto anche nell'elenco dei domini alla pagina delle **impostazioni**.

19.4. Protezione hotspot per reti non sicure

Utilizzando Bitdefender Safepay™ quando ci si connette a reti Wi-Fi non sicure (per esempio a un hotspot pubblico), la funzione Protezione hotspot offre un ulteriore livello di sicurezza. Questo servizio codifica le comunicazioni Internet su connessioni non sicure, garantendo la propria privacy indipendentemente dalla rete a cui si è connessi.

La protezione hotspot si attiva solo se il computer è connesso a una rete non sicura.

La connessione sicura sarà inizializzata e, una volta stabilita la connessione, apparirà un messaggio nella finestra di Bitdefender Safepay™. Di fronte all'URL nella barra degli indirizzi comparirà il simbolo  per aiutarti a identificare facilmente le connessioni sicure.

Per migliorare la tua esperienza visiva di navigazione, puoi scegliere di attivare i plugin **Adobe Flash** e **Java**, cliccando su **Mostra impostazioni avanzate**.

Potrebbe essere necessario confermare l'azione.



20. PROTEZIONE DI PASSWORD MANAGER PER LE TUE CREDENZIALI

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

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

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

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

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

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

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

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

Password Manager protegge le seguenti informazioni private:

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



20.1. Configurare Password Manager

Una volta completata l'installazione e aperto il browser, una finestra pop-up ti avviserà della possibilità di utilizzare il Portafoglio per un'esperienza online più sicura.

Il Portafoglio di Bitdefender è dove puoi archiviare i tuoi dati personali.

Clicca su **Esplora** per avviare l'installazione guidata del Portafoglio. Segui la procedura guidata per completare l'installazione.

Durante questa fase possono essere eseguite due attività:

- Crea un nuovo database del Portafoglio per proteggere le tue password.

Durante la fase d'installazione, ti sarà chiesto di proteggere il tuo Portafoglio con una password principale. La nuova password dovrebbe avere almeno 7 caratteri.

Per creare una password molto sicura, utilizza almeno un numero o un simbolo e un carattere maiuscolo. Una volta impostata una password, chiunque cerchi di accedere al Portafoglio dovrà prima inserirla.

Dopo aver impostato la password principale, avrai la possibilità di sincronizzare le informazioni del Portafoglio nel cloud, in modo da utilizzarle su tutti i tuoi dispositivi.

Al termine dell'installazione, di norma vengono attivate le seguenti impostazioni del Portafoglio:

- **Salva automaticamente le credenziali nel Portafoglio.**
- **Chiedi la password principale quando apro il browser e le applicazioni.**
- **Blocca automaticamente il Portafoglio quando lascio il PC incustodito.**
- **Compila automaticamente le credenziali di accesso ogni volta.**
- **Inserisci direttamente i miei dati quando visito una pagina con dei moduli.**
- Se in precedenza hai utilizzato il Portafoglio sul tuo sistema, puoi importare un database esistente.

Esporta il database del Portafoglio

Per esportare il database del Portafoglio, segui questi passaggi:



1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Privacy**.
3. Clicca sul modulo **Password Manager** e seleziona la scheda **Portafogli**.
4. Seleziona il database del Portafoglio desiderato dalla sezione **I miei portafogli** e poi clicca sul pulsante **Esporta**.
5. Segui la procedura indicata per esportare il database del Portafoglio in una determinata posizione sul tuo sistema.




Nota

Il Portafoglio deve essere aperto, affinché il pulsante **Esporta** sia disponibile.

Crea un nuovo database del Portafoglio

Per creare un nuovo database del Portafoglio, segui questi passaggi:


1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Privacy**.
3. Clicca sul modulo **Password Manager** e seleziona la scheda **Portafogli**.
4. Clicca sull'icona + nella finestra che comparirà.
5. Nell'area **Avvia nuovo**, clicca su **Crea nuovo**.
6. Digita le informazioni richieste nei campi corrispondenti.
 - Etichetta Portafoglio - Imposta un nome unico per il database del tuo Portafoglio.
 - Password principale - Inserisci una password per il tuo Portafoglio.
 - Ridigita la password - Ridigita la password impostata.
 - Suggerimento - Inserisci un suggerimento per ricordarti la password.
7. Clicca su **Continua**.
8. In questa fase, puoi scegliere di archiviare i tuoi dati nel cloud. Selezionando **Sì**, le informazioni bancarie resteranno comunque memorizzate a livello locale sul tuo dispositivo. Scegli l'opzione che desideri e poi clicca su **Continua**.



9. Seleziona il browser web da cui vuoi importare le credenziali.
10. Clicca su **Termina**.

Sincronizzare i tuoi Portafogli nel cloud

Per attivare o disattivare la sincronizzazione dei Portafogli nel cloud, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Privacy**.
3. Clicca sul modulo **Password Manager** e seleziona la scheda **Portafogli**.
4. Seleziona il database del Portafoglio desiderato dalla sezione **I miei portafogli** e poi clicca sul pulsante **Impostazioni**.
5. Scegli l'opzione che desideri nella finestra che comparirà e poi clicca su **Salva**.



Nota

Il Portafoglio deve essere aperto, affinché il pulsante **Impostazioni** sia disponibile.

Gestisci le tue credenziali del Portafoglio

Per gestire le tue password, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Privacy**.
3. Clicca sul modulo **Password Manager** e seleziona la scheda **Portafogli**.
4. Seleziona il database del Portafoglio desiderato dalla sezione **I miei portafogli** e poi clicca sul pulsante **Apri**.

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

- Identità
- Siti web




- Online banking
- E-mail
- Applicazioni
- Reti Wi-Fi

Aggiungere/modificare le credenziali

- Per aggiungere una nuova password, seleziona la categoria desiderata in alto, clicca su **+ Aggiungi elemento**, inserisci le informazioni nei campi corrispondenti e clicca sul pulsante **Salva**.
- Per modificare una voce dalla tabella, selezionarla e fare clic sul pulsante **Modifica**.
- Per uscire, clicca su **Annulla**.
- Per rimuovere una voce, selezionala, clicca sul pulsante **Modifica** e seleziona **Elimina**.


20.2. Attivare o disattivare la protezione del Password Manager

Per attivare o disattivare la protezione del Password Manager, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Privacy**.
3. Clicca sul modulo **Password Manager**.
4. Clicca sull'interruttore **Stato del modulo** per attivare o disattivare Password Manager.

20.3. Gestire le impostazioni del Password Manager

Per configurare la password principale, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Privacy**.



3. Clicca sul modulo **Password Manager** e seleziona la scheda **Impostazioni di sicurezza**.

Sono disponibili le seguenti opzioni:

- **Chiedi la password principale quando accedo al computer.** - Quando accedi al computer, ti sarà chiesto di inserire la password principale.
- **Chiedi la password principale quando apro il browser e le applicazioni** - Quando accedi al browser o a un'applicazione, ti sarà chiesto di inserire la password principale.
- **Blocca automaticamente il Portafoglio quando lascio il PC incustodito** - Quando torni al computer dopo circa 15 minuti, ti sarà chiesto di inserire la password principale.




Importante

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

Migliora la tua esperienza

Per selezionare i browser o le applicazioni in cui desideri integrare Password Manager, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Privacy**.
3. Clicca sul modulo **Password Manager** e seleziona la scheda **Plugin**.

Controlla se un'applicazione utilizza Password Manager e migliora la tua esperienza:


- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safepay
- Skype
- Yahoo! Messenger



Configurare l'opzione **Compila automaticamente**

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

Per configurare le impostazioni dell'opzione **Compila automaticamente**, segui questi passaggi:


1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Privacy**.
3. Clicca sul modulo **Password Manager** e seleziona la scheda **Impostazioni comp. automatica**.
4. Puoi configurare le seguenti opzioni:
 - **Compila automaticamente le credenziali di accesso:**
 - **Compila automaticamente le credenziali di accesso ogni volta** - Le credenziali vengono inserite automaticamente nel browser.
 - **Lasciami scegliere quando compilare automaticamente le mie credenziali di accesso** - Ti consente di scegliere quando compilare automaticamente le credenziali nel browser.
 - **Configura la protezione delle credenziali da parte del Password Manager:**
 - **Salva automaticamente le credenziali nel Portafoglio** - Le credenziali di accesso e altre informazioni identificabili, come dati personali o il numero della carta di credito, vengono salvati e aggiornati automaticamente nel Portafoglio.
 - **Chiedi sempre** - Ti sarà chiesto ogni volta se desideri aggiungere le credenziali al Portafoglio.
 - **Non salvare, aggiornerò le informazioni manualmente** - Le credenziali possono essere aggiunte nel Portafoglio solo manualmente.
 - **Comp. automaticamente moduli:**
 - **Inserisci direttamente i miei dati quando visito una pagina con dei moduli** - Ogni volta che Bitdefender rileva la tua intenzione di eseguire



un pagamento o una registrazione online, comparirà una finestra di pop-up con le opzioni già compilate.

Gestisci le informazioni del Password Manager dal browser

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

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

Il Portafoglio di Bitdefender include le seguenti opzioni:

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



21. BITDEFENDER USB IMMUNIZER

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

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

Con USB Immunizer puoi impedire a qualsiasi unità flash formattata in NTFS, FAT32 o FAT dall'eseguire automaticamente ogni malware. Una volta che un dispositivo USB è immunizzato, i malware non possono più configurarlo per eseguire una determinata applicazione quando il dispositivo viene collegato a un computer con Windows.

Per immunizzare un dispositivo USB, segui questi passaggi:

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



Nota

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

Per impedire al computer di eseguire malware da dispositivi USB non immunizzati, disattiva la funzione di esecuzione automatica. Per maggiori informazioni, fai riferimento a *«Usare il controllo automatico delle vulnerabilità»* (p. 105).



OTTIMIZZAZIONE SISTEMA



22. PROFILI

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

Bitdefender offre i seguenti profili:

- **Profilo Lavoro**
- **Profilo Film**
- **Profilo Gioco**

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

In base alla tua attività, quando viene attivato un profilo, vengono applicate le seguenti impostazioni del prodotto:

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

In base alla tua attività, quando viene attivato un profilo, vengono applicate le seguenti impostazioni del sistema:

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




22.1. Profilo Lavoro

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

Configurare il profilo Lavoro

Per configurare le azioni da intraprendere nel profilo Lavoro, segui questi passaggi:


1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Strumenti**.
3. Clicca sul modulo **Profili**.
4. Nella finestra **Impostazioni profili**, clicca sul pulsante **Configura** nell'area Profilo Lavoro.
5. Seleziona le regolazioni del sistema da applicare, spuntando le seguenti opzioni:
 - Aumenta le prestazioni delle applicazioni
 - Ottimizza le impostazioni del prodotto per il profilo Lavoro
 - Rimanda i programmi in background e le attività di manutenzione
 - Posticipa aggiornamenti automatici di Windows
6. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

Aggiungere manualmente le applicazioni all'elenco del profilo Lavoro

Se lanciando una determinata applicazione, Bitdefender non attiva automaticamente il profilo Lavoro, puoi aggiungere manualmente l'applicazione nell'**Elenco applicazioni**.

Per aggiungere manualmente le applicazioni all'Elenco applicazioni nel profilo Lavoro:



1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Strumenti**.
3. Clicca sul modulo **Profili**, poi clicca sul pulsante **Configura** nell'area Profilo lavoro.
4. Nella finestra **Profilo Lavoro**, clicca sul link **Elenco applicazioni**.
5. Clicca su **Aggiungi** per aggiungere una nuova applicazione all'**Elenco applicazioni**.


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

22.2. Profilo Film

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

Configurare il profilo Film

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

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Strumenti**.
3. Clicca sul modulo **Profili**.
4. Nella finestra **Impostazioni profili**, clicca sul pulsante **Configura** nell'area Profilo Film.
5. Seleziona le regolazioni del sistema da applicare, spuntando le seguenti opzioni:
 - Aumenta le prestazioni dei lettori multimediali
 - Ottimizza le impostazioni del prodotto per il profilo Film
 - Rimanda i programmi in background e le attività di manutenzione
 - Posticipa aggiornamenti automatici di Windows




- Modifica le impostazioni dei consumi energetici per i film

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

Aggiungere manualmente i lettori multimediali all'elenco del profilo Film

Se lanciando un determinato lettore multimediale, Bitdefender non attiva automaticamente il profilo Film, puoi aggiungere manualmente l'applicazione nell'**Elenco lettori**.

Per aggiungere manualmente i lettori multimediali all'Elenco lettori nel profilo Film:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Strumenti**.
3. Clicca sul modulo **Profili**, poi clicca sul pulsante **Configura** nell'area Profilo film.
4. Nella finestra **Profilo Film**, clicca sul link **Elenco lettori**.
5. Clicca su **Aggiungi** per aggiungere una nuova applicazione all'**Elenco lettori**.

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


22.3. Profilo Gioco

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

Configurare il profilo Gioco

Per configurare le azioni da intraprendere nel profilo Gioco, segui questi passaggi:




1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Strumenti**.
3. Clicca sul modulo **Profili**.
4. Nella finestra **Impostazioni profili**, clicca sul pulsante **Configura** nell'area Profilo Gioco.
5. Seleziona le regolazioni del sistema da applicare, spuntando le seguenti opzioni:
 - Aumenta le prestazioni dei giochi
 - Ottimizza le impostazioni del prodotto per il profilo Gioco
 - Rimanda i programmi in background e le attività di manutenzione
 - Posticipa aggiornamenti automatici di Windows
 - Modifica le impostazioni dei consumi energetici per i giochi
6. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

Aggiungere manualmente giochi all'Elenco dei giochi

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

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

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Strumenti**.
3. Clicca sul modulo **Profili**, poi clicca sul pulsante **Configura** nell'area Profilo gioco.
4. Nella finestra **Profilo Gioco**, clicca sul link **Elenco giochi**.
5. Clicca su **Aggiungi** per aggiungere un nuovo gioco all'**Elenco giochi**.


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



22.4. Ottimizzazione in tempo reale

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

Per attivare o disattivare l'Ottimizzazione in tempo reale, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Strumenti**.
3. Clicca sul modulo **Profili** e seleziona la finestra **Impostazioni profili**.
4. Attiva o disattiva l'Ottimizzazione in tempo reale automatica, cliccando sull'interruttore corrispondente.



RISOLUZIONE DEI PROBLEMI



23. RISOLVERE I PROBLEMI PIÙ COMUNI

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

- *«Il mio sistema sembra lento»* (p. 133)
- *«La scansione non parte»* (p. 134)
- *«Non riesco più a usare un'applicazione»* (p. 137)
- *«Cosa fare quando Bitdefender blocca un sito web o un'applicazione online sicuri»* (p. 138)
- *«Come aggiornare Bitdefender con una connessione a Internet lenta»* (p. 139)
- *«I servizi Bitdefender non rispondono»* (p. 140)
- *«L'opzione Compila automaticamente nel mio Portafoglio non funziona»* (p. 140)
- *«Rimozione di Bitdefender non riuscita»* (p. 142)
- *«Il sistema non si riavvia dopo aver installato Bitdefender»* (p. 143)

Se non riesci a trovare il problema qui, o se la soluzione fornita non lo risolve, puoi contattare un operatore del supporto tecnico di Bitdefender come indicato nel capitolo *«Chiedere aiuto»* (p. 157).

23.1. Il mio sistema sembra lento

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

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

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

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



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

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

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

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




Importante

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

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

La velocità del tuo sistema e le sue prestazioni generali possono essere anche influenzate dai malware. Spyware, virus, Trojan e adware contribuiscono a diminuire le prestazioni del computer. Assicurati di controllare periodicamente il tuo sistema, almeno una volta alla settimana. Si consiglia di usare la Scansione completa di sistema di Bitdefender perché controlla tutti i tipi di malware che minacciano la sicurezza del tuo sistema, oltre a eseguire una scansione degli archivi.

Per avviare la Scansione di sistema, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Nel modulo **Antivirus**, seleziona **Scansione sistema**.
4. Segui i passaggi della procedura guidata.

23.2. La scansione non parte

Questo tipo di problema può avere due cause principali:



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

In questo caso, segui questi passaggi:

1. Rimuovi completamente Bitdefender dal sistema:

- **In Windows 7:**

- a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
- b. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
- c. Clicca su **Rimuovi** nella finestra che comparirà e poi seleziona **Voglio reinstallarlo**.
- d. Clicca su **Avanti** per continuare.
- e. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

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

- a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
- b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
- c. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
- d. Clicca su **Rimuovi** nella finestra che comparirà e poi seleziona **Voglio reinstallarlo**.
- e. Clicca su **Avanti** per continuare.
- f. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

- **In Windows 10:**

- a. Clicca su **Start** e poi su **Impostazioni**.
- b. Clicca sull'icona **Sistema** nelle **Impostazioni** e poi seleziona **Applicazioni installate**.
- c. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
- d. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.



- e. Clicca su **Rimuovi** nella finestra che comparirà e poi seleziona **Voglio reinstallarlo**.
- f. Clicca su **Avanti** per continuare.
- g. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

2. Reinstalla il tuo prodotto Bitdefender.

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

In questo caso, segui questi passaggi:

1. Rimuovi l'altra soluzione di sicurezza. Per maggiori informazioni, fai riferimento a «*Come posso rimuovere le altre soluzioni di sicurezza?*» (p. 70).
2. Rimuovi completamente Bitdefender dal sistema:

● **In Windows 7:**

- a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
- b. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
- c. Clicca su **Rimuovi** nella finestra che comparirà e poi seleziona **Voglio reinstallarlo**.
- d. Clicca su **Avanti** per continuare.
- e. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

● **In Windows 8 e Windows 8.1:**

- a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
- b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
- c. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
- d. Clicca su **Rimuovi** nella finestra che comparirà e poi seleziona **Voglio reinstallarlo**.
- e. Clicca su **Avanti** per continuare.



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

● In **Windows 10**:

a. Clicca su **Start** e poi su Impostazioni.

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

c. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.

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

e. Clicca su **Rimuovi** nella finestra che comparirà e poi seleziona **Voglio reinstallarlo**.

f. Clicca su **Avanti** per continuare.

g. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

3. Reinstalla il tuo prodotto Bitdefender.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione *«Chiedere aiuto»* (p. 157).

23.3. Non riesco più a usare un'applicazione

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

Dopo aver installato Bitdefender potrebbe verificarsi una di queste situazioni:

● Potresti ricevere un messaggio da Bitdefender che il programma sta cercando di eseguire una modifica al sistema.

● Potresti ricevere un messaggio d'errore dal programma che stai cercando di usare.


Questo tipo di situazione si verifica quando Active Threat Control rileva alcune applicazioni come nocive per errore.

L'Active Threat Control è un modulo di Bitdefender che monitora costantemente le applicazioni in esecuzione sul tuo sistema e segnala quelle con un comportamento potenzialmente dannoso. Poiché questa opzione è basata su un sistema euristico, potrebbero verificarsi dei casi in cui applicazioni legittime siano segnalate dall'Active Threat Control.



Quando si verifica questa situazione, puoi escludere la rispettiva applicazione dal controllo dell'Active Threat Control.

Per aggiungere il programma all'elenco delle eccezioni, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Antivirus** e seleziona la finestra **Eccezioni**.
4. Clicca sul collegamento **Processi esclusi**. Nella finestra che compare, puoi gestire le eccezioni del processo di Active Threat Control.
5. Aggiungi eccezioni seguendo questi passaggi:
 - a. Clicca sul pulsante **Aggiungi** localizzato nella parte superiore della tabella delle eccezioni.
 - b. Clicca su **Sfoglia**, trova e seleziona l'applicazione che vuoi escludere e poi clicca su **OK**.
 - c. Mantieni selezionata l'opzione **Consenti**, per impedire ad Active Threat Control di bloccare l'applicazione.
 - d. Clicca su **Aggiungi**.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione **«Chiedere aiuto»** (p. 157).


23.4. Cosa fare quando Bitdefender blocca un sito web o un'applicazione online sicuri

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

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

Per aggiungere un sito web alla **Whitelist**, segui questi passaggi:



1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Clicca sul modulo **Protezione web**.
4. Nella scheda **Impostazioni**, clicca sul link **Whitelist**.
5. Inserisci l'indirizzo del sito web o dell'applicazione online bloccata nel campo corrispondente e clicca su **Aggiungi**.
6. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.


A questo elenco andrebbero aggiunti solo siti web e applicazioni assolutamente affidabili. Saranno esclusi dalle scansioni eseguite dai seguenti motori: malware, phishing e frodi.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione **«Chiedere aiuto»** (p. 157).

23.5. Come aggiornare Bitdefender con una connessione a Internet lenta

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

Per mantenere aggiornato il tuo sistema con le firme Bitdefender più recenti, segui questi passaggi:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Impostazioni generali** dal menu a tendina.
2. Nella finestra **Impostazioni generali**, seleziona la scheda **Aggiornamento**.
3. Accanto a **Regole di esecuzione dell'aggiornamento**, seleziona **Chiedi prima di scaricare** dal menu a tendina.
4. Torna alla finestra principale e clicca sul pulsante d'azione **Aggiorna** nell'interfaccia di Bitdefender.
5. Seleziona solo **Aggiornamento firme** e poi clicca su **OK**.
6. Bitdefender scaricherà e installerà solo gli aggiornamenti delle firme malware.



23.6. I servizi Bitdefender non rispondono

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

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

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

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

Per risolvere questo errore, provare queste soluzioni:

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

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

Se l'errore persiste, contatta i nostri operatori del supporto tecnico per ricevere assistenza, come indicato nella sezione *«Chiedere aiuto»* (p. 157).

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

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



Per risolvere il problema, segui questi passaggi:

● **In Internet Explorer:**

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

● **In Mozilla Firefox:**

1. Apri Mozilla Firefox.
2. Clicca su Strumenti.
3. Clicca su Add-on.
4. Clicca su Estensioni.
5. Seleziona **Bitdefender Password Manager** e clicca su Attiva.

● **In Google Chrome:**

1. Apri Google Chrome.
2. Vai all'icona del menu.
3. Clicca su Impostazioni.
4. Clicca su Estensioni.
5. Seleziona **Bitdefender Password Manager** e clicca su Attiva.



Nota

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

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione *«Chiedere aiuto»* (p. 157).



23.8. Rimozione di Bitdefender non riuscita

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

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

Per rimuovere completamente Bitdefender dal sistema, segui questi passaggi:

● In Windows 7:

1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
2. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
3. Seleziona **Rimuovi** e poi seleziona **Voglio reinstallarlo**.
4. Clicca su **Avanti** per continuare.
5. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

● In Windows 8 e Windows 8.1:

1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
3. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
4. Seleziona **Rimuovi** e poi seleziona **Voglio reinstallarlo**.
5. Clicca su **Avanti** per continuare.
6. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

● In Windows 10:

1. Clicca su **Start** e poi su **Impostazioni**.
2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.



3. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
5. Seleziona **Rimuovi** e poi seleziona **Voglio reinstallarlo**.
6. Clicca su **Avanti** per continuare.
7. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

23.9. Il sistema non si riavvia dopo aver installato Bitdefender

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

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

Ecco come affrontare ogni situazione:

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

Per risolvere, segui questi passaggi:

1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a *«Come posso riavviare in modalità provvisoria?»* (p. 71).
2. Rimuovi Bitdefender dal tuo sistema:
 - In **Windows 7**:
 - a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
 - b. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
 - c. Clicca su **Rimuovi** nella finestra che comparirà e poi seleziona **Voglio reinstallarlo**.
 - d. Clicca su **Avanti** per continuare.
 - e. Attendere che il processo di disinstallazione sia terminato.
 - f. Riavvia il sistema in modalità normale.

● In **Windows 8 e Windows 8.1**:



- a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
 - b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
 - c. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
 - d. Clicca su **Rimuovi** nella finestra che comparirà e poi seleziona **Voglio reinstallarlo**.
 - e. Clicca su **Avanti** per continuare.
 - f. Attendere che il processo di disinstallazione sia terminato.
 - g. Riavvia il sistema in modalità normale.
- **In Windows 10:**
- a. Clicca su **Start** e poi su Impostazioni.
 - b. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
 - c. Trova **Bitdefender Antivirus Plus 2016** e seleziona **Disinstalla**.
 - d. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
 - e. Clicca su **Rimuovi** nella finestra che comparirà e poi seleziona **Voglio reinstallarlo**.
 - f. Clicca su **Avanti** per continuare.
 - g. Attendere che il processo di disinstallazione sia terminato.
 - h. Riavvia il sistema in modalità normale.

3. Reinstalla il tuo prodotto Bitdefender.

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

Per risolvere, segui questi passaggi:

1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a *«Come posso riavviare in modalità provvisoria?»* (p. 71).
2. Rimuovi l'altra soluzione di sicurezza dal sistema:

- **In Windows 7:**



- a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
 - b. Trova il nome del programma che desideri rimuovere e seleziona **Rimuovi**.
 - c. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.
- In **Windows 8 e Windows 8.1**:
- a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
 - b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
 - c. Trova il nome del programma che desideri rimuovere e seleziona **Rimuovi**.
 - d. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.
- In **Windows 10**:
- a. Clicca su **Start** e poi su Impostazioni.
 - b. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
 - c. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
 - d. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

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

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

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

Per risolvere, segui questi passaggi:

1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a *«Come posso riavviare in modalità provvisoria?»* (p. 71).



2. Usa l'opzione Ripristino configurazione di sistema di Windows per ripristinare il computer a uno stato precedente all'installazione del prodotto Bitdefender.
3. Riavvia il sistema in modalità normale e contatta i nostri operatori del supporto per assistenza, come indicato nella sezione *«Chiedere aiuto»* (p. 157).



24. RIMUOVERE MALWARE DAL SISTEMA

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

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

- «*Modalità soccorso di Bitdefender*» (p. 147)
- «*Cosa fare quando Bitdefender trova dei virus sui tuoi computer?*» (p. 149)
- «*Come posso rimuovere un virus in un archivio?*» (p. 151)
- «*Come posso rimuovere un virus nell'archivio delle e-mail?*» (p. 152)
- «*Cosa fare se sospetti che un file possa essere pericoloso?*» (p. 153)
- «*Quali sono i file protetti da password nel registro della scansione?*» (p. 153)
- «*Quali sono gli elementi ignorati nel registro della scansione?*» (p. 154)
- «*Quali sono i file supercompressi nel registro della scansione?*» (p. 154)
- «*Perché Bitdefender ha eliminato automaticamente un file infetto?*» (p. 154)

Se non riesci a trovare il problema qui, o se la soluzione fornita non lo risolve, puoi contattare un operatore del supporto tecnico di Bitdefender come indicato nel capitolo «*Chiedere aiuto*» (p. 157).

24.1. Modalità soccorso di Bitdefender

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

Una volta installato Bitdefender Antivirus Plus 2016, la Modalità soccorso può essere usata anche se non puoi più avviare Windows.


Avviare il tuo sistema in Modalità soccorso

Puoi accedere alla Modalità soccorso in uno dei due modi:



Dall'**interfaccia di Bitdefender**

Per accedere direttamente alla Modalità soccorso da Bitdefender, segui questi passaggi:

1. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
2. Seleziona la finestra **Protezione**.
3. Nel modulo **Antivirus**, seleziona **Modalità soccorso**.
Apparirà una finestra di conferma. Clicca su **Sì** per riavviare il computer.
4. Dopo il riavvio del computer, comparirà un menu che ti avvisa di selezionare un sistema operativo. Seleziona **Modalità soccorso di Bitdefender** e premi il tasto **Invio** per avviare un ambiente di Bitdefender da cui poter pulire la tua partizione Windows.
5. Se richiesto, premi **Invio** e seleziona la risoluzione dello schermo più vicina a quella che usi normalmente. Poi premi di nuovo **Invio**.
Tra pochi istanti la Modalità soccorso di Bitdefender si caricherà.

Avvia il computer direttamente in Modalità soccorso

Se Windows non parte più, puoi avviare il tuo computer direttamente nella Modalità soccorso di Bitdefender seguendo i passaggi sottostanti:

1. Accendi / Riavvia il tuo computer e inizia a premere la **barra spaziatrice** sulla tastiera prima che compaia il logo di Windows.
2. Comparirà un menu per avvisarti di selezionare il sistema operativo da avviare. Premi **TAB** per accedere all'area degli strumenti. Seleziona **Bitdefender Rescue Image** e premi il tasto **Invio** per avviare un ambiente di Bitdefender da cui poter pulire la tua partizione Windows.
3. Se richiesto, premi **Invio** e seleziona la risoluzione dello schermo più vicina a quella che usi normalmente. Poi premi di nuovo **Invio**.
Tra pochi istanti la Modalità soccorso di Bitdefender si caricherà.

Controllare il sistema in Modalità soccorso

Per eseguire una scansione del sistema in Modalità soccorso, segui questi passaggi:



1. Entra in Modalità soccorso, come descritto in «**Avviare il tuo sistema in Modalità soccorso**» (p. 147).
2. Comparirà il logo di Bitdefender e i motori antivirus inizieranno a essere copiati.
3. Comparirà una finestra di benvenuto. Clicca su **Continua**.
4. È stato avviato un aggiornamento delle firme antivirus.
5. Una volta completato l'aggiornamento, compare la finestra della scansione antivirus su richiesta di Bitdefender.
6. Clicca su **Controlla ora**, seleziona l'obiettivo della scansione nella finestra che compare e clicca su **Apri** per avviare la scansione.

Si consiglia di controllare la tua intera partizione di Windows.



Nota

Quando si lavora in Modalità soccorso, avrai a che fare con nomi di partizioni tipo Linux. Le partizioni del disco compariranno come sda1 che corrisponde alla partizione di Windows (C:), sda2 che corrisponde a (D:) e così via.

7. Attendi il completamento della scansione. Se venissero rilevati malware, segui le istruzioni per rimuovere la minaccia.
8. Per uscire dalla modalità soccorso, clicca con il pulsante destro in un'area libera del desktop, seleziona **Esci** nel menu che comparirà e poi seleziona se riavviare o spegnere il computer.

24.2. Cosa fare quando Bitdefender trova dei virus sui tuoi computer?

Potresti scoprire l'esistenza di un virus sul tuo computer in uno di questi modi:

- Hai controllato il tuo computer e Bitdefender ha trovato alcuni elementi infetti.
- Un avviso antivirus ti informa che Bitdefender ha bloccato uno o più virus sul tuo computer.

In tali situazioni, aggiorna Bitdefender per assicurarti di avere le ultime firme malware e avvia una Scansione del sistema per analizzarlo.




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

Avvertimento

Se sospetti che il file sia parte del sistema operativo Windows o che non sia un file infetto, non seguire questi passaggi e contatta il Servizio clienti di Bitdefender il prima possibile.

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

Il primo metodo può essere usato in modalità normale:

1. Disattiva la protezione antivirus in tempo reale di Bitdefender:
 - a. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
 - b. Seleziona la finestra **Protezione**.
 - c. Clicca sul modulo **Antivirus** e seleziona la finestra **Protezione**.
 - d. Clicca sull'interruttore per disattivare la **scansione all'accesso**.
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a *«Come posso visualizzare gli elementi nascosti in Windows?»* (p. 69).
3. Trova l'ubicazione del file infetto (controlla il registro della scansione) ed eliminalo.
4. Attiva la protezione antivirus in tempo reale di Bitdefender.

Se il primo metodo non riuscisse a rimuovere l'infezione, segui questi passaggi:

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



Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 157).

24.3. Come posso rimuovere un virus in un archivio?


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

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

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

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

Ecco come rimuovere un virus in un archivio:

1. Identifica l'archivio che include il virus, eseguendo una scansione del sistema.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
 - a. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
 - b. Seleziona la finestra **Protezione**.
 - c. Clicca sul modulo **Antivirus** e seleziona la finestra **Protezione**.
 - d. Clicca sull'interruttore per disattivare la **scansione all'accesso**.
3. Vai all'ubicazione dell'archivio e decomprimilo usando un programma di compressione, come WinZip.
4. Identifica il file infetto e lo elimina.
5. Elimina l'archivio originale per assicurarti che l'infezione sia stata rimossa completamente.
6. Ricomprimi i file in un nuovo archivio usando un'applicazione di archiviazione, come WinZip.



7. Attiva la protezione antivirus in tempo reale di Bitdefender ed esegui una scansione completa del sistema per assicurarti che non ci siano altre infezioni.



Nota

È importante notare che un virus in un archivio non è una minaccia immediata al sistema, poiché deve essere decompresso ed eseguito per infettarlo.


Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 157).

24.4. Come posso rimuovere un virus nell'archivio delle e-mail?

Bitdefender può anche identificare i virus nei database e negli archivi di e-mail presenti su disco.

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

Ecco come rimuovere un virus presente in un archivio e-mail:

1. Controlla il database e-mail con Bitdefender.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
 - a. Clicca sull'icona  nell'angolo in basso a sinistra dell'**interfaccia di Bitdefender**.
 - b. Seleziona la finestra **Protezione**.
 - c. Clicca sul modulo **Antivirus** e seleziona la finestra **Protezione**.
 - d. Clicca sull'interruttore per disattivare la **scansione all'accesso**.
3. Apri il rapporto della scansione e usa le informazioni d'identificazione (oggetto, da, a) dei messaggi infettati per localizzarli nel client e-mail.
4. Elimina i messaggi infetti. La maggior parte dei client e-mail spostano il messaggio eliminato in una cartella di recupero, dalla quale può essere recuperato. Dovresti assicurarti che il messaggio sia eliminato anche da questa cartella di ripristino.
5. Compatta la cartella di memorizzazione del messaggio infetto.



- In Outlook Express: Nel menu File, clicca su Cartella, poi Comprimi tutte le cartelle.
- Per Microsoft Outlook 2007: Nel menu File, clicca su Gestione file dati. Seleziona i file delle cartelle personali (.pst) che desideri compattare e clicca su Impostazioni. Clicca su Compatta.
- Per Microsoft Outlook 2007 / 2013: Nel menu File, clicca su Info e poi su Impostazioni account (Consente di aggiungere e rimuovere account o di modificare le impostazioni di connessione esistenti). Poi clicca su File di dati, seleziona i file delle cartelle personali (.pst) che desideri compattare e clicca su Impostazioni. Clicca su Compatta.

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione *«Chiedere aiuto»* (p. 157).

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

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

Per assicurarti che il tuo sistema sia protetto, segui questi passaggi:

1. Esegui una **Scansione del sistema** con Bitdefender. Per scoprire come fare, fai riferimento a *«Come posso eseguire una scansione del mio sistema?»* (p. 58).
2. Se il risultato della scansione non segnala nulla, ma hai ancora dubbi e vuoi essere certo che il file sia pulito, contatta gli operatori del nostro supporto tecnico per ricevere assistenza.

Per scoprire come fare, fai riferimento a *«Chiedere aiuto»* (p. 157).

24.6. Quali sono i file protetti da password nel registro della scansione?

Questa è solo una notifica per indicare che Bitdefender ha rilevato che questi file sono protetti da una password o da una qualche forma di crittografia.

In genere gli elementi protetti da password sono:

- File che appartengono a un'altra soluzione di sicurezza.



- File che appartengono al sistema operativo.

Per poter controllare i contenuti, devi estrarre o quantomeno decriptare questi file.

Qualora tali contenuti venissero estratti, la scansione in tempo reale di Bitdefender li controllerebbe automaticamente per proteggere il tuo computer. Se desideri controllare quei file con Bitdefender, devi contattare il produttore per ottenere maggiori informazioni sui file.

Ti consigliamo di ignorare quei file perché non sono una minaccia per il sistema.

24.7. Quali sono gli elementi ignorati nel registro della scansione?

Tutti i file che compaiono come Ignorati nel rapporto della scansione sono puliti.

Per prestazioni superiori, Bitdefender non controlla file che non sono stati modificati dall'ultima scansione.

24.8. Quali sono i file supercompressi nel registro della scansione?

Gli oggetti supercompressi sono elementi che non possono essere estratti dal motore di scansione o elementi per i quali la crittografia avrebbe impiegato troppo tempo, rendendo il sistema instabile.

Supercompresso significa che Bitdefender ha saltato la scansione di quell'archivio perché scompattarlo avrebbe richiesto troppe risorse di sistema. Se necessario, il contenuto sarà controllato solo durante l'accesso in tempo reale.

24.9. Perché Bitdefender ha eliminato automaticamente un file infetto?

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



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

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



CONTATTACI



25. CHIEDERE AIUTO

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

La sezione *«Risolvere i problemi più comuni»* (p. 133) fornisce le informazioni necessarie sui problemi più frequenti che potresti incontrare usando questo prodotto.


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

- «Contattaci direttamente dal tuo prodotto Bitdefender» (p. 157)
- «Contattaci tramite il nostro Centro di supporto online» (p. 158)

Contattaci direttamente dal tuo prodotto Bitdefender

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

Attenersi alla seguente procedura:

1. Clicca sull'icona  nella parte superiore dell'**interfaccia di Bitdefender** e seleziona **Aiuto e Supporto** dal menu a tendina.
2. Hai le seguenti opzioni:
 - **Documentazione del prodotto**
Accedi al nostro database e cerca le informazioni necessarie.
 - **Contatta supporto**
Usa il pulsante **Contatta supporto** per lanciare lo Strumento di supporto di Bitdefender e contattare il Servizio clienti. Puoi esplorare la procedura guidata usando il pulsante **Avanti**. Per uscire dalla procedura guidata, clicca su **Annulla**.
 - a. Seleziona la casella di accettazione e clicca su **Avanti**.
 - b. Completa il modulo di invio con i dati richiesti:



- i. Inserisci il tuo indirizzo e-mail.
 - ii. Inserisci il tuo nome completo.
 - iii. Inserisci una descrizione del problema riscontrato.
 - iv. Seleziona l'opzione **Prova a riprodurre il problema prima di inviarlo**, nel caso riscontrassi un problema con il prodotto. Continua con i passaggi richiesti.
- c. Attendi qualche minuto mentre Bitdefender raccoglie le informazioni sul prodotto. Queste informazioni aiuteranno i nostri ingegneri a trovare una soluzione al tuo problema.
- d. Clicca su **Termina** per inviare le informazioni sul Servizio clienti di Bitdefender. Sarai contattato il prima possibile.

Contattaci tramite il nostro Centro di supporto online

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

1. Visitare <http://www.bitdefender.it/support/consumer.html>.

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

2. Utilizza la barra di ricerca nella parte superiore della finestra per trovare gli articoli che possono fornire una soluzione al tuo problema. Per effettuare una ricerca, digita un termine nella barra di ricerca e clicca su **Cerca**.
3. Leggi gli articoli o i documenti rilevanti e prova le soluzioni proposte.
4. Se la soluzione non dovesse risolvere il tuo problema, vai a <http://www.bitdefender.it/support/contact-us.html> e contatta gli operatori del nostro supporto tecnico.



26. 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:

<http://www.bitdefender.it/support/consumer.html>

- Forum del supporto di Bitdefender:

<http://forum.bitdefender.com>

- Il portale di sicurezza informatica HOTforSecurity:

<http://www.hotforsecurity.com>

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

26.1. 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 dei virus, la gestione delle soluzioni di Bitdefender con spiegazioni dettagliate e molti altri articoli.

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

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

<http://www.bitdefender.it/support/consumer.html>.

26.2. Forum supporto di Bitdefender

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



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

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

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

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

26.3. Portale HOTforSecurity

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

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

La pagina web HOTforSecurity è raggiungibile all'indirizzo <http://www.hotforsecurity.com>.



27. INFORMAZIONI DI CONTATTO

Una comunicazione efficiente è la chiave di un business di successo. Negli ultimi 10 anni BITDEFENDER ha acquisito una reputazione inestimabile superando le aspettative di clienti e partner, e sforzandosi costantemente per una comunicazione sempre più efficiente. Se hai delle domande o richieste, non esitare a contattarci.

27.1. Indirizzi web

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

27.2. Distributori locali

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

Per trovare un distributore di Bitdefender nel tuo paese:

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

27.3. Uffici di Bitdefender

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



USA

Bitdefender, LLC

6301 NW 5th Way, Suite 4300

Fort Lauderdale, Florida 33309

Telefono (ufficio e vendite): 1-954-776-6262

Vendite: sales@bitdefender.com

Supporto tecnico: <http://www.bitdefender.com/support/consumer.html>

Web: <http://www.bitdefender.com>

Germania

Bitdefender GmbH

TechnoPark Schwerte

Lohbachstrasse 12

D - 58239 Schwerte

Ufficio: +49 2304 9 45 - 162

Fax: +49 2304 9 45 - 169

Vendite: vertrieb@bitdefender.de

Supporto tecnico: <http://www.bitdefender.de/support/consumer.html>

Web: <http://www.bitdefender.de>

Spagna

Bitdefender España, S.L.U.

C/Bailén, 7, 3-D

08010 Barcelona

Fax: +34 93 217 91 28

Telefono: +34 902 19 07 65

Vendite: comercial@bitdefender.es

Supporto tecnico: <http://www.bitdefender.es/support/consumer.html>

Sito Web: <http://www.bitdefender.es>

Romania

BITDEFENDER SRL

Complex DV24, Building A, 24 Delea Veche Street, Sector 2

Bucharest

Fax: +40 21 2641799

Telefono vendite: +40 21 2063470

Indirizzo e-mail ufficio vendite: sales@bitdefender.ro



Supporto tecnico: <http://www.bitdefender.ro/support/consumer.html>
Sito Web: <http://www.bitdefender.ro>

Emirati Arabi Uniti

Dubai Internet City

Building 17, Office # 160

Dubai, UAE

Telefono vendite: 00971-4-4588935 / 00971-4-4589186

Indirizzo e-mail ufficio vendite: mena-sales@bitdefender.com

Supporto tecnico: <http://www.bitdefender.com/support/consumer.html>

Sito Web: <http://www.bitdefender.com>



Glossario

Abbonamento

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

ActiveX

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

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

Adware

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

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

Aggiorna

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



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

Bitdefender dispone del proprio modulo di aggiornamento che consente la verifica manuale degli aggiornamenti oppure l'aggiornamento automatico del prodotto.

Applet Java

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

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

Archivio

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

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

Area di notifica

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

Backdoor

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



Browser

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

Client mail

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

Codice di attivazione

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

Cookie

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

E-mail

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



Elementi di avvio

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

Estensione del nome di un file

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

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

Euristico

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

Eventi

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

Falso positivo

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

File di rapporto

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



Firma virus

Caratteristica binaria di un virus, utilizzata dal programma antivirus al fine di rilevare ed eliminare il virus stesso.

IP

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

Keylogger

Un keylogger è un'applicazione che registra ogni informazione digitata.

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

Linea di comando

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

Macro virus

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

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

Minaccia avanzata persistente

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

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



Non euristico

Questo metodo di scansione si basa su specifiche firme di virus. Il vantaggio della scansione non-euristica è di non essere ingannata da ciò che potrebbe sembrare un virus, e quindi non genera falsi allarmi.

Pacchetti di programmi

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

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

Percorso

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

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

Phishing

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

Photon

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



Porta

Un'interfaccia su un computer dalla quale è possibile connettere un dispositivo. I personal computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, monitor e tastiere. Esternamente i personal computer hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

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

Ransomware

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

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

Rootkit

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

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

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



Scarica

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

Script

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

Settore di avvio:

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

Spam

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

Spyware

Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua 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 cavallo di Troia che gli utenti installano inconsapevolmente con altri applicazioni. Un modo comune per diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano



informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli spyware utilizzano memoria e risorse del sistema, le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

TCP/IP

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

Trojan

Un programma distruttivo che si maschera da applicazione benevola. Diversamente dai virus, i cavalli di Troia non si replicano ma possono comunque essere altrettanto distruttivi. Un tipo di cavallo di Troia particolarmente insidioso è un programma che dichiara di pulire i virus dal computer, ma al contrario li introduce.

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

Unità disco

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

Un drive di disco rigido legge e scrive dischi rigidi.

Un drive di floppy accede i dischi floppy.

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

Uso memoria

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



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

Virus

Un programma o parte di codice caricato sul computer a propria insaputa e che viene eseguito contro la propria volontà. La maggior parte dei virus è anche in grado di auto replicarsi. Tutti i virus informatici sono creati dall'uomo. È relativamente facile produrre un semplice virus in grado di copiare sé stesso innumerevoli volte. Persino un virus così semplice è pericoloso in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di virus ancora più pericoloso è quello in grado di trasmettere sé stesso attraverso le reti superando i sistemi di sicurezza.

Virus di boot

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

Virus polimorfico

Un virus che modifica la propria forma con ogni file che infetta. Non avendo caratteristiche binarie costanti, questi virus sono difficili da identificare.

Worm

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