# INTERNET SECURITY 2012


## Manuale d'uso

# Bitdefender Internet Security 2012
*Manuale d'uso*

Data di pubblicazione 2011.08.04



## Avvertenze legali


Bitdefender

# Indice

# 1. Installazione

## 1.1. Prepararsi all'installazione

Prima di installare Bitdefender Internet Security 2012, 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 risponde ai requisiti minimi di sistema, Bitdefender non verrà installato o se installato non funzionerà correttamente e causerà rallentamenti e instabilità del sistema.Per un elenco completo dei requisiti di sistema, fare riferimento a *«Requisiti di sistema»* (p. 1).
- 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.
- Disabilita o rimuovi qualsiasi programma firewall che possa essere in esecuzione sul computer.L'esecuzione simultanea di due programmi firewall può influenzarne il funzionamento e causare problemi seri al sistema.Durante l'installazione il firewall di Windows sarà disattivato.
- Assicurati che il tuo 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 rispetto a quelli dell'installazione, Bitdefender li scaricherà e installerà.

## 1.2. Requisiti di sistema

Puoi installare Bitdefender Internet Security 2012 solo su computer con i seguenti sistemi operativi:

- Windows XP con Service Pack 3 (32 bit)
- Windows Vista con Service Pack 2
- Windows 7 con Service Pack 1

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

Nota

Per verificare il sistema operativo sul computer e l'informazione hardware, clicca con il pulsante destro del mouse su **Risorse del computer** sul desktop e quindi seleziona **Proprietà** dal menu.

### 1.2.1. Requisiti minimi di sistema

- 1,8 GB di spazio disponibile su disco fisso (almeno 800 MB sull'unità di sistema)
- Processore da 800 MHz

- 1 GB di memoria (RAM)

### 1.2.2. Requisiti di sistema consigliati

- 2,8 GB di spazio disponibile su disco fisso (almeno 800 MB sull'unità di sistema)
- Intel CORE Duo (1,66 GHz) o processore equivalente
- Memoria (RAM):
  - 1 GB per Windows XP
  - 1,5 GB per Windows Vista e Windows 7

### 1.2.3. Requisiti software

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

- Internet Explorer 7 o superiore
- Mozilla Firefox 3.6 o superiore
- Yahoo! Messenger 8.1 o superiore
- Microsoft Outlook 2007 / 2010
- Microsoft Outlook Express e Windows Mail (su sistemi a 32 bit)
- Mozilla Thunderbird 3.0.4
- .NET framework 3

## 1.3. Installare il tuo prodotto Bitdefender

Puoi installare Bitdefender dal disco di installazione di Bitdefender oppure utilizzando un programma di installazione web scaricato sul computer dal sito di Bitdefender o da altri siti web autorizzati (ad esempio il sito web di un partner di Bitdefender o un negozio online).Il file di installazione può essere scaricato dal sito web di Bitdefender al seguente indirizzo: http://www.bitdefender.com/site/Downloads/.

- Per installare Bitdefender dal disco di installazione, inserisci il disco nel lettore.A breve dovrebbe comparire una schermata di benvenuto. Segui le istruzioni per avviare l'installazione.

**Nota**

La schermata di benvenuto 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 nel drive USB e clicca **Copia su USB**.In seguito, spostati sul computer senza unità CD, inserisci il dispositivo USB nella presa USB e clicca due volte su `runsetup.exe` dalla cartella nella quale hai salvato il pacchetto di installazione.

Se la schermata di benvenuto non compare, vai alla cartella principale del disco e clicca due volte sul file `autorun.exe`.

- Per installare Bitdefender utilizzando il programma di installazione web scaricato sul computer, individua il file e cliccaci sopra due volte.In questo modo inizierà lo scaricamento dei file di installazione. L'operazione potrebbe richiedere un po', in base al tipo di connessione Internet.

Prima 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 così i problemi che si verificano in seguito.

Nota

Potrebbe essere necessario riavviare il computer per completare la rimozione dei programmi antivirus rilevati.

Segui la procedura guidata della configurazione per installare Bitdefender Internet Security 2012.

## Fase 1 - Benvenuto

Leggi l'Accordo di licenza e seleziona **Accetta e continua**.L'Accordo di licenza contiene i termini e le condizioni per poter utilizzare Bitdefender Internet Security 2012.

Nota

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

## Fase 2 - Registra il tuo prodotto

Per completare la registrazione del tuo prodotto devi inserire un codice di licenza e creare un account MyBitdefender.È richiesta una connessione a Internet attiva.

Procedi secondo la tua situazione:

- **Ho acquistato il prodotto**

  In questo caso, registra il prodotto seguendo questi passaggi:

  1. Seleziona **Ho acquistato il prodotto e voglio registrarlo subito**.
  2. Digita il codice di licenza nel campo corrispondente.

Nota

Puoi trovare il tuo codice di licenza:

- sull'etichetta del CD/DVD.
- sulla scheda di registrazione del prodotto.
- sulla e-mail di acquisto online.

3. Digita il tuo indirizzo e-mail nel campo corrispondente.

Importante

Serve un indirizzo e-mail valido.All'indirizzo fornito sarà inviato un messaggio di conferma.

4. Clicca su **Registra ora**.

- **Voglio valutare Bitdefender**

  In questo caso, puoi usare il prodotto per un periodo di 30 giorni.Per iniziare il periodo di prova, seleziona **Desidero valutare questo prodotto**.

  Per usare le funzioni online del prodotto, devi creare un account MyBitdefender.Per creare un account, inserisci il tuo indirizzo e-mail nel campo corrispondente.All'indirizzo fornito sarà inviato un messaggio di conferma.Se possiedi già un account, inserisci l'indirizzo e-mail associato ad esso per registrare il prodotto con quell'account.

## Impostazioni personalizzate

Opzionalmente, durante questa fase puoi personalizzare le impostazioni d'installazione cliccando su **Impostazioni personalizzate**.

**Percorso installazione**

Di norma, Bitdefender Internet Security 2012 sarà installato in `C:\Programmi\Bitdefender\Bitdefender 2012`.Se desideri modificare il percorso d'installazione, clicca su **Modifica** e seleziona la cartella dove vuoi installare Bitdefender.

**Configura impostazioni proxy**

Bitdefender Internet Security 2012 richiede l'accesso a Internet per la registrazione del prodotto, il download di aggiornamenti per la sicurezza e il prodotto, la rilevazione in-the-cloud di componenti, 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 puoi inserirle manualmente.

**Attiva aggiornamento P2P**

Puoi condividere i file e le firme del prodotto con altri utenti di Bitdefender.In questo modo, gli aggiornamenti di Bitdefender possono essere eseguiti più rapidamente.Se non vuoi attivare questa caratteristica, seleziona la casella corrispondente.

Nota

Attivando questa opzione, nessuna informazione identificabile sarà condivisa.

Se durante gli aggiornamenti, desideri minimizzare l'influenza del traffico di rete sulle prestazioni di sistema, usa l'opzione di condivisione aggiornamento.Bitdefender utilizza le porte 8880 - 8889 per gli aggiornamenti peer-to-peer.

**Invia rapporti anonimi sull'utilizzo**

Di default, l'invio di Report Anonimi sull'Utilizzo è abilitato.Abilitando questa opzione, i report contenenti informazioni su come il prodotto viene utilizzato sono inviati ai server Bitdefender.Queste informazioni sono essenziali per migliorare il prodotto e posso aiutarci a offrire una migliore esperienza in futuro.I report non conterranno dati confidenziali, come il tuo nome o indirizzo IP, e non saranno utilizzati per scopi commerciali.

Clicca su **OK** per confermare le tue preferenze.

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

## Fase 3 - Avanzamento installazione

Attendi il completamento dell'installazione.Vengono mostrate informazioni dettagliate sui progressi.

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

## Fase 4 - Fine

Viene indicato un sommario dell'installazione.Se durante l'installazione viene rilevato e rimosso qualche malware attivo, è necessario riavviare il sistema.

Clicca su **Termina**.

Se il tuo computer ha Windows XP, la procedura guidata di configurazione rileverà ogni rete a cui sei connesso, chiedendoti di classificarla come Casa/Ufficio o Pubblica.

## 1.3.1. Aggiornare da una versione precedente

Se stai già usando una versione precedente di Bitdefender, ci sono due modi per passare a Bitdefender Internet Security 2012:

- Installare Bitdefender Internet Security 2012 direttamente su una versione precedente.Bitdefender rileverà la versione precedente e ti aiuterà a rimuoverla prima di installare la nuova versione.Durante l'aggiornamento dovrai riavviare il computer.
- Rimuovi la versione precedente, quindi riavvia il computer e installa la nuova versione come descritto nelle pagine precedenti.Utilizza questo metodo di aggiornamento se l'altro non ha avuto successo.

Nota

Le impostazioni del prodotto e i contenuti della quarantena non saranno importati dalla versione precedente.

# 2. Iniziare

Una volta installato Bitdefender Internet Security 2012, il tuo computer sarà protetto da ogni tipo di malware (come virus, spyware e Trojan) e minaccia web (come hacker, phishing e spam).

Di norma l'Autopilota è attivo e pertanto non serve configurare alcuna impostazione.Tuttavia, potresti volere sfruttare le impostazioni di Bitdefender per ottimizzare e migliorare la tua protezione.

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 ulteriori informazioni fare riferimento a «*Eventi*» (p. 13).

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.

Se non hai registrato il prodotto (e/o non hai creato un account di MyBitdefender) ricordati di farlo prima che il periodo di prova finisca.Devi creare un account per usare le funzioni online del prodotto.Per maggiori informazioni sulla registrazione, fai riferimento a «*Registrazione del prodotto*» (p. 8).

## 2.1. Apertura di Bitdefender in corso

Per accedere all'interfaccia principale di Bitdefender Internet Security 2012, usa il menu Start di Windows, seguendo il percorso: **Start → Tutti i programmi → Bitdefender 2012 → Bitdefender Internet Security 2012** o più rapidamente cliccando due volte sull'icona Bitdefender  presente nella barra di sistema.

Per maggiori informazioni sulla finestra di Bitdefender e l'icona nella barra di sistema, fai riferimento a «*Interfaccia di Bitdefender*» (p. 19).

## 2.2. Cosa occorre fare dopo l'installazione

Se vuoi che Bitdefender si occupi di tutte le decisioni in materia di sicurezza, tieni l'Autopilota attivo.Per ulteriori informazioni fare riferimento a «*Autopilota*» (p. 14).

Ecco un elenco di attività che potresti voler eseguire dopo l'installazione:

- 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. 36).
- Se hai installato Bitdefender su più computer nella tua rete domestica, puoi gestire tutti i prodotti di Bitdefender in remoto da un solo computer.Per ulteriori informazioni fare riferimento a «*Mappa di rete*» (p. 104).

- Se hai bambini, puoi usare il Controllo genitori per monitorare e controllare ciò che fanno con il computer e in Internet.Il Controllo genitori è attivato in modo predefinito per gli account limitati di Windows e sono applicate le regole di filtro web appropriate per gli adolescenti.Per ulteriori informazioni fare riferimento a «*Controllo genitori*» (p. 80).
- Crea delle regole di Protezione dati per impedire che i tuoi dati personali siano divulgati senza il tuo consenso.Per ulteriori informazioni fare riferimento a «*Protezione dati*» (p. 76).

## 2.3. Registrazione del prodotto

Per essere protetto da Bitdefender, devi registrare il tuo prodotto inserendo un codice di licenza e creare un account MyBitdefender.

Il codice di licenza specifica per quanto tempo puoi usare il prodotto.Non appena il codice di licenza scade, Bitdefender cessa di eseguire le sue funzioni e di proteggere il computer.

Dovresti acquistare o rinnovare un codice di licenza alcuni giorni prima della scadenza di quello attuale.Per ulteriori informazioni fare riferimento a «*Comprare o rinnovare i codici di licenza*» (p. 11).Se stai usando una versione di prova di Bitdefender, devi registrarla con un codice di licenza, per continuare a usarla dopo il periodo di prova.

Un account MyBitdefender ti dà accesso agli aggiornamenti del prodotto e ti consente di usare i servizi online offerti da Bitdefender Internet Security 2012.Se hai già un account, registra il tuo prodotto di Bitdefender con tale account.

Un account MyBitdefender ti consente di:

- Tieni aggiornato il tuo prodotto.
- Recupera il tuo codice di licenza, se dovessi perderlo.
- Contatta il Servizio clienti di Bitdefender.
- Monitora le attività dei bambini e configura le impostazioni del Controllo genitori ovunque sei.
- Proteggi il tuo account Facebook con Safego.

### 2.3.1. Inserire il tuo codice di licenza

Se durante l'installazione, hai selezionato di valutare il prodotto, puoi usarlo per un periodo di prova di 30 giorni.Per continuare a usare Bitdefender dopo la scadenza del periodo di prova, devi registrarlo con un codice di licenza.

Per registrare il prodotto con un codice di licenza o modificare il codice di licenza attuale, clicca sul collegamento **Informazioni licenza**, localizzato nella parte inferiore della finestra di Bitdefender.Comparirà la finestra di registrazione.

Puoi vedere lo stato della registrazione di Bitdefender, il codice di licenza corrente e i giorni mancanti alla scadenza della licenza.

Per registrare Bitdefender Internet Security 2012:

1. Inserisci il codice di licenza nel campo di modifica.

Nota

Puoi trovare il tuo codice di licenza:

- sull'etichetta del CD.
- sulla scheda di registrazione del prodotto.
- sulla e-mail di acquisto online.

Se non hai un codice di licenza di Bitdefender, clicca sul link fornito nella finestra per aprire una pagina web da cui potrai acquistarne uno.

2. Clicca su **Registra ora**.

## 2.3.2. Accedere a MyBitdefender

Se hai fornito un indirizzo e-mail durante l'installazione, a tale indirizzo ti è stato inviato un messaggio.Clicca sul link nell'e-mail per completare la registrazione.

Se non hai completato la registrazione, Bitdefender ti avviserà che è necessario farlo.

Importante

Dopo aver installato Bitdefender, devi accedere a un account entro 30 giorni.Altrimenti, Bitdefender non sarà più aggiornato.

Per creare o accedere a un account MyBitdefender, clicca sul collegamento **Completa la registrazione** / **MyBitdefender**, localizzato nella parte inferiore della finestra di Bitdefender.

Si aprirà la finestra MyBitdefender.Procedi secondo la tua situazione.

### Voglio creare un account MyBitdefender

Per creare con successo un account di MyBitdefender, segui questi passaggi:

1. Seleziona **Crea un nuovo account**.

   Comparirà una nuova finestra.

2. Digita le informazioni richieste nei campi corrispondenti.I dati forniti resteranno riservati.

   - **Nome** - Inserisci un nome utente per il tuo account. Questo campo è opzionale.
   - **E-mail** - Inserisci il tuo indirizzo e-mail.

- **Password** - Inserisci una password per il tuo account.La password deve avere almeno 6 caratteri.
- **Conferma password** - Ridigita la password.
- A tua scelta, Bitdefender può informarti su offerte speciali e promozioni usando l'indirizzo e-mail del tuo account.Per attivare questa opzione, seleziona **Autorizzo Bitdefender a inviarmi e-mail**.

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 http://my.bitdefender.com.

3. Clicca su **Invia**.
4. Prima di poter usare il tuo account, devi completare la registrazione.Controlla la tua posta elettronica e segui le istruzioni nell'e-mail di conferma inviata da Bitdefender.

Nota

Puoi anche accedere usando il tuo account Facebook o Google.Per maggiori informazioni, fai riferimento a«Voglio accedere usando il mio account Facebook o Google» (p. 10)

## Voglio accedere usando il mio account Facebook o Google

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

1. Clicca sull'icona del servizio che vuoi usare per accedere.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.

## Ho già un account MyBitdefender

Se in precedenza ti sei connesso a un account dal tuo prodotto, Bitdefender lo rileverà e ti farà accedere in quell'account.Puoi visionare il tuo account a http://my.bitdefender.com cliccando su **Vai a MyBitdefender**.

Se vuoi accedere a un account diverso, clicca sul collegamento corrispondente e segui le istruzioni nelle sezioni precedenti.

Se disponi già di un account attivo, ma Bitdefender non lo rileva, segui questi passaggi per accedere a quell'account:

1. Digita l'indirizzo e-mail e la password per l'account nei campi corrispondenti.

   Nota
   Se hai dimenticato la tua password, clicca su **Hai dimenticato la password?** e segui le istruzioni per recuperarla.

2. Clicca su **Accedi**.

### 2.3.3. Comprare o rinnovare i codici di licenza

Se il periodo di prova è quasi scaduto, devi acquistare un codice di licenza e registrare il prodotto.Analogamente, se il tuo codice di licenza attuale è quasi in scadenza, devi rinnovare la licenza.

Bitdefender ti avviserà quando la data di scadenza della tua licenza attuale si sta avvicinando. Segui le istruzioni nell'avviso per acquistare una nuova licenza.

Puoi visitare una pagina web dove acquistare in qualsiasi momento un codice di licenza, seguendo questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul collegamento **Informazioni licenza**, localizzato nella parte inferiore della finestra di Bitdefender, per aprire la finestra di registrazione del prodotto.
3. Clicca sul link presente nella parte inferiore della finestra.

## 2.4. Risoluzione problemi

Bitdefender utilizza un sistema d'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 come si desidera, scegliendo i problemi specifici di cui desideri ricevere una notifica.

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

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

L'icona Bitdefender nella barra di sistema indica problemi in sospeso cambiando il suo colore come segue:

**Rosso:** Si sono verificati dei problemi critici per la sicurezza del sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.

**Giallo:** La sicurezza del sistema è affetta da problemi non critici. È necessario controllare e risolvere tali problemi quando si ha tempo.

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

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

### 2.4.1. 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 Bitdefender nella barra di sistema e seleziona **Risolvi ogni problema**.In base ai problemi rilevati, l'icona è rossa (a indicare problemi critici) o gialla (a indicare problemi non critici).
   - Apri la finestra di Bitdefender e clicca in qualsiasi punto nell'area Stato di sicurezza sulla barra degli strumenti superiore (per esempio, puoi cliccare sul pulsante **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 **Posticipa** e non sarà intrapresa alcuna azione per risolverlo.
3. Per risolvere i problemi selezionati, clicca su **Avvia**. Alcuni problemi vengono risolti immediatamente. Per gli altri, verrà eseguita una procedura guidata 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.

### 2.4.2. Configurare gli avvisi di stato

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. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Generale** nel menu di sinistra e poi sulla scheda **Avanzate**.
4. Cerca e clicca sul collegamento **Configura avvisi di stato**.
5. Clicca sugli interruttori per attivare o disattivare gli avvisi di stato in base alle tue preferenze.

## 2.5. Eventi

Bitdefender tiene un registro dettagliato degli eventi riguardanti la sua attività sul computer (include anche le attività dei computer monitorati del Controllo genitori).Gli Eventi sono uno strumento molto importante per monitorare e gestire la protezione di BitdefenderPer esempio, puoi controllare facilmente se l'aggiornamento è stato eseguito con successo, se sono stati rilevati malware sul tuo computer, ecc.In aggiunta, puoi intraprendere ulteriori azioni se necessario o modificare le azioni intraprese da Bitdefender.

Per aprire la finestra Eventi, apri la finestra di Bitdefender e clicca sul pulsante **Eventi** nella barra degli strumenti superiore.

Per aiutarti a filtrare gli eventi di Bitdefender, nel menu di sinistra sono disponibili le seguenti categorie:

- **Antivirus**
- **Antispam**
- **Controllo genitori**
- **Controllo privacy**
- **Firewall**
- **Mappa di rete**
- **Aggiorna**
- **Safego**

È disponibile un elenco di eventi per ogni categoria.Per avere maggiori informazioni su un particolare evento nell'elenco, cliccaci sopra. I dettagli degli eventi sono indicati nella parte inferiore 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.Ci sono tre tipi di eventi, ognuno indicato da un'icona specifica:

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

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.

## 2.6. Autopilota

Per tutti gli utenti che dalla propria soluzione di sicurezza vogliono essere protetti senza tanti problemi, Bitdefender Internet Security 2012 è stato realizzato con una modalità Autopilota automatica.

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

In modalità Autopilota, Bitdefender risolve automaticamente i problemi critici e gestisce in modo silenzioso:

- Protezione antivirus, fornita da scansioni all'accesso e continue.
- Protezione firewall.
- Protezione della privacy, fornita dal filtro antiphishing e antimalware per la tua navigazione web.
- Aggiornamenti automatici.

Di norma, l'Autopilota viene attivato al termine dell'installazione di Bitdefender.Finché l'Autopilota è attivo, l'icona di Bitdefender nella barra di sistema cambierà in .

Per attivare o disattivare l'Autopilota, apri la finestra di Bitdefender e clicca sull'interruttore **Autopilota** nella barra degli strumenti superiore.

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

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

## 2.7. Modalità giochi e Modalità portatile

Alcune attività del computer, ad esempio giochi o presentazioni, richiedono una maggiore risposta e performance dal sistema 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 Internet Security 2012 include due modalità operative speciali:

- Modalità giochi
- Modalità portatile

### 2.7.1. Modalità giochi

La modalità giochi modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema.Le seguenti impostazioni sono applicate quando la Modalità giochi è attiva:

- Tutti gli allarmi e pop-up Bitdefender sono disabilitati.
- La Scansione all'accesso è impostata sul livello di protezione **Tollerante**.
- Scansione automatica disattivata.La Scansione automatica trova e utilizza gli intervalli in cui l'uso delle risorse di sistema scende sotto a una certa soglia per eseguire scansioni ricorrenti dell'intero sistema.
- Il firewall di Bitdefender è impostato in modalità standard (La **Modalità Paranoid** è disattivata).Questo significa che tutte le nuove connessioni (sia in entrata che in uscita) vengono consentite, indipendentemente della porta o protocollo utilizzati.
- Auto aggiornamento disattivato.
- La barra degli strumenti di Bitdefender nel tuo browser è disattivata mentre esegui giochi web.

Mentre sei in Modalità giochi, puoi visualizzare la lettera G sull'icona Bitdefender.

#### Uso della Modalità Gioco.

Di norma, Bitdefender entra automaticamente in modalità giochi quando esegui un gioco incluso nell'elenco di Bitdefender dei giochi conosciuti o quando un'applicazione passa a schermo intero.Bitdefender tornerà automaticamente alla modalità normale quando si chiude il gioco o quando l'applicazione rilevata esce dallo schermo intero.

Se si vuole attivare manualmente la Modalità giochi, utilizzare uno dei metodi seguenti:

- fare clic con il pulsante destro sull'icona di Bitdefender nella barra di sistema e selezionare **Attivare Modalità giochi**.

- Premere Ctrl+Shift+Alt+G (la hotkey di default).

Importante
Non dimenticare di disattivare la Modalità Gioco quando avete finito. Per farlo, utilizzare gli stessi metodi usati per attivarla.

### Modificare l'hotkey della Modalità giochi

Puoi entrare manualmente in Modalità giochi usando la hotkey di default Ctrl+Alt+Shift+G.Per modificare la hotkey, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Generale** nel menu di sinistra e poi sulla scheda **Impostazioni**.
4. Sotto l'opzione **Attiva tasti di scelta rapida per Modalità giochi**, imposta la combinazione di tasti desiderata:
   a. Scegliere i tasti di modifica che si vogliono usare selezionando uno dei seguenti: tasto Control (Ctrl), tasto Maiuscola (Shift) o tasto Alternare (Alt).
   b. Nel campo editabile, inserisci la lettera corrispondente al tasto regolare che vuoi usare.

   Ad esempio, se vuoi usare la hotkey Ctrl+Alt+D, devi solo controllare i tasti Ctrl e Alt e inserire la D.

Nota
Per disattivare la combinazione di tasti, disattiva l'opzione **Attiva tasti di scelta rapida per Modalità giochi**.

### Attivare o disattivare la Modalità giochi automatica

Per attivare o disattivare la Modalità giochi automatica, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Generale** nel menu di sinistra e poi sulla scheda **Impostazioni**.
4. Attiva o disattiva la Modalità giochi automatica, cliccando sull'interruttore corrispondente.

## 2.7.2. Modalità portatile

La Modalità Portatile è stata specialmente disegnata per chi usa i laptop/notebook. Il suo proposito è minimizzare l'impatto di Bitdefender sul consumo di energia mentre questi apparecchi funzionino con la batteria.Quando Bitdefender è in Modalità portatile, le funzioni Scansione automatica e Auto aggiornamento sono disattivate,

poiché richiedono più risorse di sistema e, implicitamente, aumentano il consumo di energia.

Bitdefender rileva quando il tuo portatile sta funzionando con la batteria e automaticamente va in Modalità portatile.Nello stesso modo, Bitdefender uscirà automaticamente dalla Modalità Portatile quando rileverà che il portatile non sta più lavorando con la batteria.

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

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Generale** nel menu di sinistra e poi sulla scheda **Impostazioni**.
4. Attiva o disattiva la Modalità portatile automatica, cliccando sull'interruttore corrispondente.

Se Bitdefender non è installato su un portatile, disattiva la Modalità portatile automatica.

## 2.8. Impostazioni protezione 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 della password per le impostazioni di Bitdefender, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Generale** nel menu di sinistra e poi sulla scheda **Impostazioni**.
4. Nella sezione **Impostazioni protezione da password**, attiva la protezione della password cliccando sull'interruttore.
5. Clicca sul collegamento **Cambia password**.
6. Inserisci la password nei due campi e poi clicca su **OK**.La password deve essere composta da almeno 8 caratteri.

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

Importante

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

Per rimuovere la protezione della password, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Generale** nel menu di sinistra e poi sulla scheda **Impostazioni**.
4. Nella sezione **Impostazioni protezione da password**, disattiva la protezione della password cliccando sull'interruttore.
5. Digita la password e clicca su **OK**.

## 2.9. Rapporti anonimi sull'utilizzo

Di norma, Bitdefender invia rapporti contenenti informazioni su come lo usi per i server di Bitdefender.Queste informazioni sono essenziali per migliorare il prodotto e posso aiutarci a offrire una migliore esperienza in futuro.I report non conterranno dati confidenziali, come il tuo 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. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Generale** nel menu di sinistra e poi sulla scheda **Avanzate**.
4. Disattiva i Rapporti anonimi sull'utilizzo cliccando sull'interruttore corrispondente.

## 2.10. Riparare o rimuovere Bitdefender

Se desideri riparare o rimuovere Bitdefender Internet Security 2012, segui il percorso dal menu di avvio di Windows: **Start → Tutti i programmi → Bitdefender 2012 → Ripara o Rimuovi**.

Seleziona l'azione che desideri eseguire:

- **Ripara** - per reinstallare tutte le componenti del programma.
- **Rimuovi** - per rimuovere tutte le componenti installate.

Nota
Ti consigliamo di scegliere **Rimuovi** per una reinstallazione pulita.

Attendi che Bitdefender completi l'azione che hai selezionato.Questa operazione richiederà alcuni minuti.

Dovrai riavviare il computer per completare il processo.

# 3. Interfaccia di Bitdefender

Bitdefender Internet Security 2012 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.

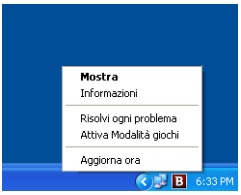
Per visualizzare lo stato del prodotto ed eseguire le attività essenziali, l'icona della barra di sistema di Bitdefender è disponibile in qualsiasi momento.

La finestra principale ti consente di accedere rapidamente ai moduli e alle informazioni importanti del prodotto, oltre a consentirti di eseguire le attività più comuni.

Per configurare il tuo prodotto Bitdefender nei dettagli ed eseguire attività di gestione avanzata, puoi trovare tutti gli strumenti che ti servono nella finestra delle impostazioni.

## 3.1. Icona barra di sistema

Per gestire tutto il prodotto più velocemente, puoi utilizzare l'icona Bitdefender nella barra delle applicazioni.Se clicchi due volte su questa icona, Bitdefender si aprirà. Inoltre, cliccando con il pulsante destro sull'icona, apparirà un menu contestuale che consentirà una rapida gestione del prodotto Bitdefender.




Icona della barra delle applicazioni

- **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.
- **Risolvi ogni problema** - aiuta a rimuovere tutte le vulnerabilità di sicurezza correnti.Se l'opzione non è disponibile, non ci sono errori da risolvere.Per ulteriori informazioni, ti preghiamo di far riferimento a «*Risoluzione problemi*» (p. 11).
- **Atttiva/Disattiva modalità giochi** - attiva / disattiva la modalità giochi.
- **Aggiorna adesso** - inizia un aggiornamento immediato.Puoi seguire lo stato di aggiornamento nel pannello Aggiornamento della finestra principale di Bitdefender.

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

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

Nessun problema critico colpisce la sicurezza del tuo sistema.Quando hai un po' di tempo, dovresti controllarli e risolverli.

Il prodotto funziona inGame Mode.

L'Autopilota di Bitdefender è attivo.

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

## 3.2. Finestra principale

La finestra principale di Bitdefender ti consente di eseguire le attività principali, risolvere rapidamente problemi di sicurezza, visualizzare informazioni sugli eventi relativi alle attività del prodotto e personalizzare le impostazioni.Tutto è a pochi clic di distanza.

La finestra è organizzata in due sezioni principali:

Barra degli strumenti superiore
: Qui puoi controllare lo stato di sicurezza del tuo computer e accedere alle attività importanti.

Area pannelli
: Qui puoi gestire i moduli principali di Bitdefender.

In aggiunta, puoi trovare diversi collegamenti utili nella parte inferiore della finestra:

| Link | Descrizione |
|---|---|
| **Feedback** | Apre una pagina web nel tuo browser dove puoi compilare un breve questionario sulla tua esperienza con il prodotto.Contiamo sui tuoi suggerimenti nel nostro costante impegno per migliorare i prodotti Bitdefender. |
| **Completa la registrazione / MyBitdefender** | Apre la finestra dell'account MyBitdefender, dove puoi creare o accedere a un account.Un account MyBitdefender è necessario per ricevere gli aggiornamenti e beneficiare delle funzioni online del tuo prodotto.Per avere altre informazioni su come creare un account e avere i relativi vantaggi, fai riferimento a *«Accedere a MyBitdefender»* (p. 9). |
| **Informazioni licenza** | Apre una finestra dove puoi visualizzare informazioni sul codice di licenza attuale e registrare il tuo prodotto con un nuovo codice di licenza. |
| **Aiuto e supporto** | Clicca su questo link se hai bisogno di aiuto con Bitdefender. |

| Link | Descrizione |
|---|---|
|  | Aggiunge dei punti di domanda in diverse aree della finestra di Bitdefender per aiutarti a trovare facilmente informazioni sui diversi elementi dell'interfaccia.<br>Sposta il cursore su un punto interrogativo per vedere alcune veloci informazioni sull'elemento accanto. |

### 3.2.1. 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 di 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 sul pulsante **Visualizza problemi** nel centro della barra degli strumenti o in qualsiasi punto nell'area di stato della sicurezza alla sua sinistra, puoi accedere a una procedura guidata che ti aiuterà a rimuovere facilmente qualsiasi minaccia dal tuo computer.Per ulteriori informazioni, ti preghiamo di far riferimento a «*Risoluzione problemi*» (p. 11).
- Il menu **Eventi** ti consente di accedere a una cronologia dettagliata degli eventi più importanti che si sono verificati durante l'attività del prodotto.Per ulteriori informazioni, ti preghiamo di far riferimento a «*Eventi*» (p. 13).
- **Impostazioni** ti consente di accedere a una finestra dove puoi configurare le impostazioni del prodotto.Per ulteriori informazioni, ti preghiamo di far riferimento a «*Finestra impostazioni*» (p. 24).
- L'opzione **Autopilota** ti consente di attivare l'Autopilota per usufruire di una sicurezza "silenziosa".Per ulteriori informazioni, ti preghiamo di far riferimento a «*Autopilota*» (p. 14).

### 3.2.2. Area pannelli

Nell'area dei pannelli puoi gestire direttamente i moduli di Bitdefender.

Puoi organizzare i pannelli come desideri.Per risistemare l'area in base alle tue necessità, trascina i singoli pannelli e rilasciali negli altri slot.

Per scorrere tra i pannelli, usa l'interruttore scorrevole sotto alla finestra dei pannelli o le frecce localizzate a destra e sinistra.

Dall'alto verso il basso, ogni pannello contiene i seguenti elementi:

- Il nome del modulo.
- Un messaggio di stato.
- L'icona del modulo.Clicca sull'icona di un modulo per configurare le sue impostazioni nella finestra impostazioni.
- Un pulsante che ti consente di eseguire funzioni importanti del modulo.
- Alcuni pannelli hanno un interruttore per consentirti di attivare o disattivare una funzione importante del modulo.

I pannelli disponibili in quest'area sono:

**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 pannello Antivirus, puoi accedere facilmente a tutte le attività di scansione importanti.Clicca su **Controlla ora** e seleziona un'attività dal menu a tendina:

- Scansione veloce
- Scansione completa
- Scansione personalizzata
- Scansione vulnerabilità
- Mod. soccorso

L'interruttore **Scansione automatica** ti consente di attivare o disattivare questa funzione.

Per maggiori informazioni sulle attività di scansione e su come configurare la protezione antivirus, fai riferimento a «*Protezione antivirus*» (p. 38).

**Firewall**

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

Cliccando su **Dettagli rete** nel pannello Firewall, puoi configurare le impostazioni di connessione alla rete.

L'interruttore Firewall ti consente di attivare o disattivare la protezione del firewall.

Avvertimento

Perché espone il tuo computer a connessioni non autorizzate, disattivare il firewall dovrebbe essere solo una misura temporanea.Riattiva il firewall il prima possibile.

Per maggiori informazioni sulla configurazione del firewall, fai riferimento a «*Firewall*» (p. 94).

**Antispam**

Il modulo antispam di Bitdefender protegge la tua casella di posta da messaggi indesiderati filtrando tutto il traffico mail POP3.

Clicca su **Gestisci** nel pannello antispam e seleziona Amici o Spammer dal menu a tendina per modificare l'elenco corrispondente.

L'interruttore antispam ti consente di attivare o disattivare la protezione antispam.

Per maggiori informazioni sulla configurazione della protezione antispam, fai riferimento a «*Antispam*» (p. 63).

**Aggiorna**

In un mondo dove i criminali informatici cercano costantemente di trovare nuovi modi per colpire, è essenziale tenere aggiornata la tua soluzione di sicurezza per essere sempre un passo avanti a loro.

Di norma, Bitdefender controlla ogni ora la presenza di eventuali aggiornamenti. Se desideri disattivare gli aggiornamenti automatici, usa l'interruttore **Auto aggiornamento** nel pannello Aggiorna.

Avvertimento

Questa è una questione critica di sicurezza. Ti consigliamo di disattivare l'aggiornamento automatico per il minimo tempo possibile. Se Bitdefender non sarà aggiornato regolarmente non sarà in grado di proteggervi dalle minacce più recenti.

Clicca sul pulsante **Aggiorna ora** sul pannello per eseguire un aggiornamento automatico.

Per maggiori informazioni sugli aggiornamenti di configurazione, fai riferimento a «*Aggiorna*» (p. 108).

**Genitori**

Bitdefender Internet Security 2012 offre un set completo di controlli per i genitori che ti aiutano a proteggere i bambini e monitorare le loro attività sul computer.

Clicca su **Gestisci account** nel pannello Controllo genitori per configurare le impostazioni per gli account Windows del computer.

Per maggiori informazioni sulla configurazione del Controllo Genitori, fare riferimento a «*Controllo genitori*» (p. 80).

**Privacy**

Il modulo Controllo privacy ti aiuta a mantenere privati i tuoi dati personali.Ti protegge mentre sei online da attacchi di phishing, tentativi di frode, sottrazione di dati personali e molto altro.

Clicca sul pulsante **Gestisci regole** nel pannello Controllo privacy per andare alla sezione Protezione dati, dove puoi configurare le regole sulla privacy.

L'interruttore antiphishing ti consente di attivare o disattivare la protezione antiphishing.

Per maggiori informazioni su come configurare Bitdefender per proteggere la tua privacy, fai riferimento a «*Controllo privacy*» (p. 73).

**Mappa di rete**

Con la Mappa di rete puoi gestire facilmente la sicurezza di tutti i computer da un solo sistema.

Per iniziare, clicca su **Gestisci** nel pannello Mappa di rete e seleziona **Attiva rete**.

Una volta che la rete è attivata, cliccando su **Gestisci** nel pannello Mappa di rete, potrai accedere alle seguenti opzioni:

- **Disattiva connessione** - Disattiva la rete.
- **Controlla tutto** - Esegue una scansione veloce o una scansione completo del sistema sui computer gestiti.
- **Aggiorna tutti i computer** - Aggiorna i prodotti di Bitdefender sui computer gestiti.

Per ulteriori informazioni fare riferimento a «*Mappa di rete*» (p. 104).

**Safego**

Per essere sempre al sicuro su Facebook, puoi accedere a Safego, la soluzione di sicurezza di Bitdefender per social network, direttamente dal tuo prodotto.

Clicca su **Attiva** per attivare e gestire Safego dal tuo account Facebook.

Se hai già attivato Safego, potrai accedere alle statistiche circa la sua attività, cliccando sul pulsante **Visualizza rapporti**.

Per ulteriori informazioni fare riferimento a «*Protezione di Safego per social network*» (p. 112).

## 3.3. Finestra impostazioni

La finestra delle impostazioni ti consente di accedere a ogni componente e personalizzazione del prodotto.Qui puoi configurare Bitdefender in ogni dettaglio.

Sulla parte sinistra della finestra c'è un menu contenente tutti i moduli di sicurezza.Ogni modulo consiste di una o più schede che permettono la configurazione

delle impostazioni di sicurezza corrispondenti oppure permettono di eseguire attività di amministrazione e di sicurezza.Il seguente elenco descrive brevemente ogni modulo.

Generale
: Ti consente di configurare le impostazioni generali del prodotto, come le impostazioni della password, la Modalità giochi, la Modalità portatile, le impostazioni del proxy e gli avvisi di stato.

Antivirus
: Ti consente di configurare la tua protezione contro i malware, rileva e risolve le vulnerabilità del tuo sistema, imposta le eccezioni per la scansione e gestisce i file in quarantena.

Antispam
: Permette di mantenere la Posta in arrivo libera da SPAM e di configurare in dettaglio le impostazioni antispam.

Controllo genitori
: Ti permette di proteggere i bambini dai contenuti inopportuni utilizzando le tue regole di accesso al computer personalizzate.

Controllo privacy
: Ti permette di prevenire il furto di dati dal computer e protegge la tua privacy mentre sei online.Configura la protezione per il browser e il programma di chat, gestisci la protezione dei dati e molto altro.

Firewall
: Ti consente di configurare le impostazioni generali e le regole del firewall, oltre alle attività di rilevazione intrusioni e monitoraggio della rete.

Mappa di rete
: Ti permette di configurare e gestire i prodotti Bitdefender installati sui computer di casa da un singolo computer.

Aggiorna
: Ti consente di configurare i dettagli del processo di aggiornamento.

In aggiunta, puoi trovare diversi collegamenti utili nella parte inferiore della finestra:

| Link | Descrizione |
|---|---|
| **Feedback** | Apre una pagina web nel tuo browser dove puoi compilare un breve questionario sulla tua esperienza con il prodotto.Contiamo sui tuoi suggerimenti nel nostro costante impegno per migliorare i prodotti Bitdefender. |
| **Completa la registrazione** / **MyBitdefender** | Apre la finestra dell'account MyBitdefender, dove puoi creare o accedere a un account.Un account MyBitdefender è necessario per ricevere gli aggiornamenti e beneficiare delle |

| Link | Descrizione |
|---|---|
| | funzioni online del tuo prodotto.Per avere altre informazioni su come creare un account e avere i relativi vantaggi, fai riferimento a «*Accedere a MyBitdefender*» (p. 9). |
| **Informazioni licenza** | Apre una finestra dove puoi visualizzare informazioni sul codice di licenza attuale e registrare il tuo prodotto con un nuovo codice di licenza. |
| **Aiuto e supporto** | Clicca su questo link se hai bisogno di aiuto con Bitdefender. |
|  | Aggiunge dei punti di domanda in diverse aree della finestra di Bitdefender per aiutarti a trovare facilmente informazioni sui diversi elementi dell'interfaccia.<br>Sposta il cursore su un punto interrogativo per vedere alcune veloci informazioni sull'elemento accanto. |

Per tornare alla finestra principale, clicca sul pulsante **Home** nell'angolo in alto a destra della finestra.

# 4. Come

Questo capitolo fornisce istruzioni per configurare passaggio dopo passaggio le impostazioni di uso comune o per completare le attività comuni con Bitdefender.Alcune argomenti includono riferimenti ad altri, dove puoi trovare informazioni dettagliate.



## 4.1. Come posso registrare una versione di prova?

Se hai installato una versione di prova, puoi usarla solo per un periodo limitato.Per continuare a usare Bitdefender dopo la scadenza del periodo di prova, devi registrare il prodotto con un codice di licenza e creare un account MyBitdefender.

- Per registrare Bitdefender, segui questi passaggi:

  1. Apri la finestra di Bitdefender.
  2. Clicca sul collegamento **Informazioni licenza** in fondo alla finestra.Comparirà la finestra di registrazione.
  3. Inserisci il codice di licenza e clicca su **Registra ora**.

Se non hai un codice di licenza, clicca sul link fornito nella finestra per visitare una pagina web da cui potrai acquistarne uno.

4. Attendi il termine del processo di registrazione e chiudi la finestra.

- Per creare un account MyBitdefender, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul collegamento **Completa la registrazione** in fondo alla finestra.Comparirà la finestra dell'account.
3. Seleziona il collegamento corrispondente per creare un nuovo account.
4. Digita le informazioni richieste nei campi corrispondenti.I dati forniti resteranno riservati.

   Clicca su **Invia**.
5. Controlla la tua posta elettronica e segui le istruzioni ricevute per completare la registrazione.

Nota
Puoi usare l'indirizzo e-mail e la password forniti per accedere al tuo account in http://my.bitdefender.com.

## 4.2. Come posso registrare Bitdefender senza una connessione a Internet?

Se hai appena acquistato Bitdefender e non hai una connessione a Internet, puoi registrare Bitdefender anche offline.

Per registrare Bitdefender con il tuo codice di licenza, segui questi passaggi:

1. Vai a un PC connesso a Internet.Per esempio, puoi usare il computer di un amico o un PC in un luogo pubblico.
2. Vai a https://my.bitdefender.com per creare un account MyBitdefender.
3. Accedi al tuo account e seleziona **Ottieni registrazione offline**.
4. Inserisci il codice di licenza che hai acquistato.
5. Clicca su **Invia** per ottenere un codice di conferma.

Importante
Prendi nota del codice di conferma.

6. Torna al tuo PC con il codice di conferma.
7. Apri la finestra di Bitdefender.

8. Clicca sul collegamento **Informazioni licenza** in fondo alla finestra.Comparirà la finestra di registrazione.
9. Seleziona l'opzione per registrare il prodotto con un codice di conferma.
10. Inserisci il codice di conferma nel campo corrispondente e clicca su **Invia**.
11. Attendi la fine della registrazione e clicca su **Termina**.

## 4.3. Come posso passare a un altro prodotto di Bitdefender 2012?

Puoi passare facilmente da un prodotto Bitdefender 2012 a un altro.

Consideriamo il seguente scenario: stai usando Bitdefender Internet Security 2012 da un po' e di recente hai deciso di passare a Bitdefender Total Security 2012 e alle funzioni extra che offre.

Tutto quello che devi fare è acquistare un codice di licenza per il prodotto Bitdefender 2012 che vuoi aggiornare e digitarlo nella finestra di registrazione del prodotto Bitdefender 2012 che stai usando attualmente.

Attenersi alla seguente procedura:

1. Apri la finestra di Bitdefender.
2. Clicca sul collegamento **Informazioni licenza** in fondo alla finestra.Comparirà la finestra di registrazione.
3. Inserisci il codice di licenza e clicca su **Registra ora**.
4. Bitdefender ti informerà che il codice di licenza è per un altro prodotto e ti darà la possibilità d'installarlo.Clicca sul collegamento corrispondente e segui la procedura per eseguire l'aggiornamento.

## 4.4. Quando dovrei reinstallare Bitdefender?

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

Alcune tipiche situazioni in cui dovresti 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 dal sito web di Bitdefender.

Durante l'installazione, ti sarà chiesto di registrare il prodotto con il tuo codice di licenza.

Se hai perso il codice di licenza, puoi accedere a https://my.bitdefender.com per recuperarlo.Digita l'indirizzo e-mail e la password per l'account nei campi corrispondenti.

## 4.5. Quando scade la protezione di Bitdefender?

Per scoprire quanti giorni mancano alla scadenza del tuo codice di licenza, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul collegamento **Informazioni licenza** in fondo alla finestra.
3. Nella finestra **Registra il tuo prodotto** puoi notare il numero rimasto di giorni.

## 4.6. Come posso rinnovare la protezione di Bitdefender?

Quando la protezione di Bitdefender sta per scadere, devi rinnovare il tuo codice di licenza.

- Segui questi passaggi per visitare un sito web dove rinnovare il tuo codice di licenza di Bitdefender:
  1. Apri la finestra di Bitdefender.
  2. Clicca sul collegamento **Informazioni licenza** in fondo alla finestra.
  3. Clicca su **Non disponi di un codice di licenza? Acquistane uno ora!**
  4. Sul tuo browser si aprirà una pagina web, da dove poter acquistare un codice di licenza di Bitdefender.

  Nota
  In alternativa, puoi contattare il rivenditore da cui hai acquistato il tuo prodotto Bitdefender.

- Segui questi passaggi per registrare Bitdefender con il nuovo codice di licenza:
  1. Apri la finestra di Bitdefender.
  2. Clicca sul collegamento **Informazioni licenza** in fondo alla finestra.Comparirà la finestra di registrazione.
  3. Inserisci il codice di licenza e clicca su **Registra ora**.
  4. Attendi il termine del processo di registrazione e chiudi la finestra.

Per maggiori informazioni, puoi contattare Bitdefender per avere assistenza, come descritto nella sezione «*Supporto*» (p. 136).

## 4.7. Quale prodotto Bitdefender sto usando?

Per scoprire quale programma di Bitdefender hai installato, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nella parte superiore della finestra dovresti vedere uno dei seguenti:
   - BitDefender Antivirus Plus 2012
   - BitDefender Internet Security 2012
   - BitDefender Total Security 2012

## 4.8. Come posso controllare un file o una cartella?

Il modo più semplice e consigliato di controllare un file o una cartella è cliccare con il pulsante destro sull'oggetto che desideri controllare e selezionare **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.Per ulteriori informazioni fare riferimento a «*Procedura guidata scansione antivirus*» (p. 48).

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.

## 4.9. Come posso eseguire una scansione del mio sistema?

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

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Antivirus**.
3. Clicca su **Controlla ora** e seleziona **Scansione completa del sistema** dal menu a tendina.
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.Per ulteriori informazioni fare riferimento a «*Procedura guidata scansione antivirus*» (p. 48).

## 4.10. Come posso creare un'attività di scansione personalizzata?

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

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

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Antivirus**.
3. Clicca su **Controlla ora** e seleziona **Scansione personalizzata** dal menu a tendina.
4. Clicca su **Aggiungi obiettivo** per selezionare i file o le cartelle da controllare.
5. Se vuoi configurare le opzioni di scansione nel dettaglio, clicca su **Opzioni di scansione**.

   Puoi configurare facilmente le opzioni di scansione, impostando il livello della scansione. Trascina l'indicatore sulla 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 **Inizia la scansione** e segui la procedura guidata della scansione antivirus per completare la scansione.Al termine della scansione, ti sarà chiesto di scegliere quali azioni intraprendere sui file rilevati, se presenti.
7. Se desideri salvare l'attività di scansione per usarla eventualmente in futuro, apri di nuovo la finestra di configurazione della scansione personalizzata.
8. Localizza la scansione che hai appena eseguito nell'elenco **Scansioni recenti**.
9. Porta il cursore del mouse sul nome della scansione e clicca sull'icona per aggiungerla all'elenco delle scansioni preferite.
10. Inserisci un nome specifico per la scansione.

## 4.11. 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. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.

3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Eccezioni**.
4. Clicca sul collegamento **File e cartelle escluse**.
5. Clicca sul pulsante **Aggiungi** localizzato nella parte superiore della tabella delle eccezioni.
6. Clicca su **Sfoglia**, seleziona la cartella che desideri escludere dalla scansione e quindi clicca su **OK**.
7. Clicca su **Aggiungi** e poi su **OK** per salvare le modifiche e chiudere la finestra.

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

In alcuni casi Bitdefender marca 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. Apri la finestra di Bitdefender.
   b. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
   c. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **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. 144).
3. Ripristina il file dalla quarantena:
   a. Apri la finestra di Bitdefender.
   b. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
   c. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **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. 32).
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. 137).

## 4.13. Come posso creare gli account utente di Windows?

Un account utente di Windows è un profilo unico che include tutte le impostazioni, i privilegi e i file personali per ogni utente.Gli account Windows consentono all'amministratore del PC domestico di controllare l'accesso di ogni utente.

Impostare gli account utente è utile quando il PC è utilizzato sia da genitori sia da bambini. Un genitore può impostare account per ogni bambino.

Scegli il sistema operativo che possiedi per scoprire come creare degli account Windows.

- Windows XP:
  1. Accedi al tuo computer come amministratore.
  2. Clicca su Start, clicca su Pannello di controllo e poi su Account utente.
  3. Clicca su Crea un nuovo account.
  4. Inserisci il nome per l'utente. Puoi usare nome e cognome, il nome di battesimo o un soprannome. Poi clicca su Avanti.
  5. Per la tipologia di account, seleziona Limitato e poi Crea account. Gli account limitati sono adatti ai bambini perché non consentono di eseguire cambiamenti importanti a livello di sistema o installare determinate applicazioni.
  6. Sarà creato il tuo nuovo account e potrai vederlo elencato nella schermata di Gestione account.
- Windows Vista o Windows 7:
  1. Accedi al tuo computer come amministratore.
  2. Clicca su Start, clicca su Pannello di controllo e poi su Account utente.
  3. Clicca su Crea un nuovo account.
  4. Inserisci il nome per l'utente. Puoi usare nome e cognome, il nome di battesimo o un soprannome. Poi clicca su Avanti.
  5. Per la tipologia di account, clicca su Standard e poi su Crea account. Gli account limitati sono adatti ai bambini perché non consentono di eseguire cambiamenti importanti a livello di sistema o installare determinate applicazioni.
  6. Sarà creato il tuo nuovo account e potrai vederlo elencato nella schermata di Gestione account.

**Nota**
Ora che hai aggiunto nuovi account utente, puoi creare le password per gli account.

## 4.14. Come posso proteggere i bambini dalle minacce online?

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

Puoi configurare il Controllo genitori per bloccare:

- pagine web inappropriate.

- accesso a Internet, durante specifici periodi di tempo (come durante le ore di studio).
- pagine web, e-mail e messaggi istantanei contenenti determinate parole.
- applicazioni come giochi, chat, programmi di condivisione file e altri.
- messaggi istantanei inviati da contatti chat diversi da quelli consentiti.

Per configurare il Controllo genitori, segui questi passaggi:

1. Creare degli account di Windows limitati (standard) per i bambini.Per ulteriori informazioni fare riferimento a *«Come posso creare gli account utente di Windows?»* (p. 33).
2. Assicurati di aver avviato il computer con un account amministratore.Solo gli utenti con diritti di amministrazione (amministratori del sistema) possono accedere e configurare il Controllo genitori.
3. Configura il Controllo genitori per gli account di Windows che saranno usati dai bambini.
   a. Apri la finestra di Bitdefender.
   b. Vai al pannello **Controllo genitori**.
   c. Clicca su **Gestisci account** e assicurati che il Controllo genitori sia attivato sull'account utente del bambino.
   d. Imposta l'età dei bambini cliccando su una delle caselle corrispondenti per l'opzione **Età**.Impostando l'età del bambino caricherai automaticamente le impostazioni considerate appropriate per quella categoria d'età, in base agli standard di sviluppo del bambino.
   e. Se desideri configurare le impostazioni del Controllo genitori in dettaglio, clicca su **Impostazioni**.

Per maggiori informazioni sull'utilizzo del Controllo Genitori, fare riferimento a *«Controllo genitori»* (p. 80).

## 4.15. Come posso sbloccare un sito web bloccato dal Controllo genitori?

Il Controllo genitori di Bitdefender ti consente di controllare i contenuti a cui accedono i bambini durante l'uso del computer.

Se imposti la categoria d'età dei bambini nel Controllo genitori e usi un solo account Windows, non potrai accedere ai siti web classificati come inappropriati per la categoria d'età selezionata.

Se il Controllo genitori blocca automaticamente l'accesso a un sito web, puoi creare una regola per consentire esplicitamente l'accesso a quel sito web.

Per consentire l'accesso a un sito web, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Controllo genitori**.
3. Clicca su **Gestisci account**.
4. Clicca sul pulsante **Impostazioni** per configurare le impostazioni dell'utente.
5. Clicca su **Consenti sito web**.
6. Inserisci l'URL del sito web nel campo **Sito web**.
7. Seleziona l'azione desiderata per questa regola - **Consenti** e clicca su **Termina** per aggiungere la regola.
8. Apri il tuo browser e accedi al sito web.

## 4.16. Come proteggo i miei dati personali?

Il Controllo privacy monitora i dati che escono dal tuo computer attraverso la navigazione web, i messaggi e-mail o chat.

Per assicurarsi che nessun dato personale lasci il computer senza il tuo consenso, è necessario creare adeguate regole di protezione dei dati.Le regole di protezione dei dati specificano le informazioni da bloccare.

Per creare una regola di protezione dati, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Controllo privacy** nel menu di sinistra e poi sulla scheda **Protezione dati**.
4. Se la **Protezione dati** è disattivata, attivala usando l'interruttore corrispondente.
5. Seleziona l'opzione **Aggiungi regola** per avviare la procedura guidata della Protezione dati.
6. Segui i passaggi della procedura guidata.

## 4.17. 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. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Generale** nel menu di sinistra e poi sulla scheda **Avanzate**.
4. Nella sezione **Impostazioni proxy**, attiva l'uso del proxy cliccando sull'interruttore.
5. Clicca sul collegamento **Gestione proxy**.
6. Ci sono due opzioni per determinare le impostazioni proxy:
   - **Importa le impostazioni del proxy dal browser predefinito** - le impostazioni del proxy dell'utente attuale, estratte dal browser predefinito. Se il server proxy richiede un nome utente e una password, devi specificarle nei campi corrispondenti.

     Nota
     Bitdefender può importare le impostazioni del proxy dai browser più diffusi, incluso le ultime versioni di 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.
7. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

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

# 5. Protezione antivirus

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

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

  La scansione all'accesso garantisce 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.

  Con la Scansione automatica attivata, non vi è alcun bisogno di eseguire manualmente le scansioni alla ricerca di malware.La Scansione automatica controllerà il tuo computer più volte, prendendo tutte le azioni opportune se dovesse rilevare malware.La Scansione automatica si avvia solo quando ci sono abbastanza risorse di sistema disponibili per non rallentare il computer.

Bitdefender controlla automaticamente ogni supporto rimovibile che è collegato al computer per assicurarti di accedervi in sicurezza.Per ulteriori informazioni fare riferimento a «*Scansione automatica di supporti removibili*» (p. 52).

Gli utenti esperti possono configurare le eccezioni della scansione se non desiderano controllare determinati file o estensioni.Per ulteriori informazioni fare riferimento a «*Configurare le eccezioni della scansione*» (p. 53).

Quando rileva un virus o un altro malware, Bitdefender tenterà automaticamente di rimuovere il codice malware dal file infetto, ricostruendo il file originale.Questa operazione si riferisce alla disinfezione.I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione.Per ulteriori informazioni fare riferimento a «*Gestire i file in quarantena*» (p. 56).

Se il tuo computer è stato infettato da un malware, fai riferimento a «*Rimuovere malware dal sistema*» (p. 128).Per aiutarti a ripulire il tuo computer dai malware che non possono essere rimossi dal sistema operativo Windows, Bitdefender ti offre una Modalità soccorso.Questo è 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 Virus Control, una tecnologia euristica avanzata, che monitora continuamente le applicazioni in esecuzione sul sistema.Active Virus 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 Virus Control per non bloccare queste applicazioni di nuovo creando delle regole di eccezione.Per altre informazioni, fai riferimento a «*Active Virus Control*» (p. 57).

Molte forme di malware sono realizzate per infettare sistemi sfruttando le loro vulnerabilità, come la mancanza di aggiornamenti del sistema operativo o la presenza di applicazioni datate.Bitdefender ti aiuta a identificare e risolvere facilmente le vulnerabilità del sistema per rendere il tuo computer più sicuro da malware e hacker.Per ulteriori informazioni fare riferimento a «*Risolvere le vulnerabilità del sistema*» (p. 59).

## 5.1. Scansione all'accesso (protezione in tempo reale)

Bitdefender fornisce una continua protezione in tempo reale contro un ampio spettro di minacce malware mediante la scansione di tutti i file utilizzati, le e-mail e le comunicazioni tramite programmi di chat (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Le impostazioni predefinite della protezione in tempo reale assicurano una buona protezione contro 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 dettaglio creando un livello di protezione personale.

### 5.1.1. Controllare i malware rilevati dalla scansione all'accesso

Per controllare i malware rilevati dalla scansione all'accesso, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Eventi** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Scansione virus**.Qui puoi trovare tutti gli eventi di scansione malware, incluso le minacce rilevate dalla scansione all'accesso, le scansioni avviate dall'utente e le variazioni di stato per le scansioni automatiche.
4. Clicca su un evento per visualizzare maggiori dettagli al riguardo.

### 5.1.2. 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. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Protezione**.
4. Trascina il pulsante scorrevole lungo la barra per impostare il livello di protezione desiderato.Usa la descrizione sul lato destro dell'ordine per selezionare il livello di protezione che si adatta meglio alle tue necessità di sicurezza.

### 5.1.3. Creare un livello di protezione personale

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

Per creare un livello di protezione personalizzato, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **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.

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.

  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; 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; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Controlla l'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 tuo sistema.Il malware può colpire il tuo sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la protezione in tempo reale.

  Se decidi di usare questa opzione, puoi impostare un limite di dimensione massima accettata 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 il traffico e-mail, web e chat.** 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 web
  - file ricevuti via Yahoo! Messenger

  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, puoi disattivare la scansione antivirus a e-mail, web o messaggistica istantanea per migliorare le prestazioni del sistema.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 il malware quando si accede ai file infetti (apertura, spostamento, copiatura o esecuzione).

- **Controlla i settori di avvio.** E' possibile impostare Bitdefender per esaminare i settori di boot del tuo disco.Questo settore del disco fisso 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.

- **Controlla solo i file nuovi e modificati.** Controllando solo i file modificati o nuovi, potresti migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.

### 5.1.4. Ripristinare le impostazioni predefinite

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

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

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Protezione**.
4. Clicca su **Default**.

### 5.1.5. Attivare o disattivare la protezione in tempo reale

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

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Protezione**.
4. Clicca sull'interruttore per attivare o disattivare la scansione all'accesso.
5. Se vuoi disattivare la protezione in tempo reale, comparirà la seguente finestra di avviso.Dovrai confermare la tua scelta selezionando dal menu per quanto tempo vuoi disattivare la protezione in tempo reale. Puoi disattivarla per 5, 15 o 30 minuti, un'ora, permanentemente o fino al riavvio del sistema.

Avvertimento

Questa è una questione di sicurezza critica. Ti consigliamo di disattivare la protezione in tempo reale per il minimo tempo possibile. Se la protezione in tempo reale non è attiva, non sarai protetto dalle minacce malware.

### 5.1.6. Azioni intraprese su malware rilevati

I file rilevati dalla protezione in tempo reale sono raggruppati in due categorie:

- **File infetti.** File rilevati che corrispondono a firme malware infette nel database di firme malware di Bitdefender.Bitdefender normalmente può rimuovere il codice

malware da un file infetto e ricostruire il file originale. Questa operazione è nota come disinfezione.

Nota

Le firme malware sono frammenti di codice estratti da campioni attuali di malware. Sono usate dai programmi antivirus per eseguire confronti di esempi e rilevare i malware.

Il database di firme malware di Bitdefender è una raccolta di firme malware aggiornato continuamente dai ricercatori malware di Bitdefender.

- **File sospetti.** I file sono stati rilevati come sospetti dall'analisi euristica.Poiché B-HAVE è una tecnologia di analisi euristica, Bitdefender non può essere sicuro che il file è in realtà infettato da un malware.I file sospetti non possono essere disinfettati, perché non è disponibile alcuna routine di disinfezione.

In base al tipo di file rilevato, le seguenti azioni vengono intraprese automaticamente:

- 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.

Importante

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

- Se viene rilevato un file sospetto, sarà messo 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 antimalware di Bitdefender.Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.

## 5.2. Scansione su richiesta

L'obiettivo principale di Bitdefender è mantenere il tuo computer privo di virus. Ciò avviene principalmente tenendo lontani i nuovi virus dal computer ed esaminando i tuoi 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 eseguire una scansione sul tuo computer alla ricerca di virus residenti dopo aver installato Bitdefender. Inoltre ti consigliamo di effettuare frequentemente una scansione del computer alla ricerca di virus.

La scansione su richiesta si basa sulle impostazioni della scansione. Le impostazioni specificano le opzioni della scansione e gli oggetti 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 personalizzata.

### 5.2.1. Scansione aut.

La scansione automatica è una scansione su richiesta che controlla in background tutti i tuoi dati alla ricerca di malware e intraprende azioni appropriate per ogni infezione rilevata.La Scansione automatica trova e utilizza gli intervalli in cui l'uso delle risorse di sistema scende sotto a una certa soglia per eseguire scansioni ricorrenti dell'intero sistema.

Vantaggi della Scansione automatica:

- L'impatto sul sistema è vicino allo zero.
- Eseguendo una prescansione dell'intero disco fisso, le future attività su richiesta saranno completate molto velocemente.
- La scansione all'accesso richiederà molto meno tempo.

Per attivare o disattivare la Scansione automatica, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Antivirus**.
3. Clicca sull'interruttore per attivare o disattivare la Scansione automatica.

### 5.2.2. 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 e seleziona **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.

### 5.2.3. Eseguire una Scansione veloce

QuickScan utilizza una scansione in-the-cloud per rilevare eventuali malware in esecuzione sul tuo sistema.In genere eseguire QuickScan 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. Apri la finestra di Bitdefender.
2. Vai al pannello **Antivirus**.
3. Clicca su **Controlla ora** e seleziona **Scansione veloce** dal menu a tendina.

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.

### 5.2.4. Eseguire una scansione completa del sistema

La Scansione completa di sistema esamina l'intero computer per rilevare tutti i tipi di malware che minacciano la sua sicurezza, come virus, spyware, adware, rootkit e altri.Se hai disattivato la Scansione automatica, si consiglia di eseguire una Scansione completa del sistema almeno una volta alla settimana.

Nota

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

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

- Assicurati che le firme malware di Bitdefender siano aggiornate. Controllare il computer con un database di firme datato potrebbe impedire a Bitdefender di rilevare i nuovi malware, nati dopo l'ultimo aggiornamento.Per ulteriori informazioni fare riferimento a «*Aggiorna*» (p. 108).
- Chiudi tutti i programmi aperti.

Se desideri controllare ubicazioni particolari sul tuo computer o impostare le opzioni di scansione, configura ed esegui una scansione personalizzata.Per ulteriori informazioni fare riferimento a «*Configurare ed eseguire una scansione personalizzata*» (p. 45).

Per eseguire una Scansione completa di sistema, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Antivirus**.
3. Clicca su **Controlla ora** e seleziona **Scansione completa del sistema** dal menu a tendina.
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.

### 5.2.5. Configurare ed eseguire una scansione personalizzata

Per configurare una scansione antimalware nei dettagli e poi eseguirla, segui questi passaggi:

1. Apri la finestra di Bitdefender.

2. Vai al pannello **Antivirus**.
3. Clicca su **Controlla ora** e seleziona **Scansione personalizzata** dal menu a tendina.
4. Se lo desideri, puoi eseguire nuovamente una scansione personalizzata precedente cliccando sulla rispettiva voce nell'elenco **Scansioni recenti** o **Scansioni preferite**.
5. Clicca su **Aggiungi obiettivo**, seleziona le caselle corrispondenti alle destinazioni in cui vuoi eseguire una scansione antimalware e clicca su **OK**.
6. Clicca su **Opzioni di scansione** se desideri configurare le opzioni della scansione.Comparirà una nuova finestra.Attenersi alla seguente procedura:
   a. Puoi configurare facilmente le opzioni di scansione, impostando il livello della scansione. Trascina l'indicatore sulla 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 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.** Riduce la priorità del processo di scansione. Permetterai ad altri programmi di essere più veloci e incrementerai il tempo necessario per finire il processo di scansione.
      - **Minimizza la Procedura guidata di scansione nella barra di sistema .** Riduce a icona la finestra di scansione sulla barra di sistema. Clicca due volte sull'icona di Bitdefender per riaprirla.
      - Specifica l'azione da intraprendere se non venisse rilevata alcuna minaccia.

   c. Clicca su **OK** per salvare le modifiche e chiudere la finestra.
7. Clicca su **Inizia la scansione** e segui la procedura guidata della scansione antivirus per completare la scansione.In base alle destinazioni 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.

## Salvare una scansione personalizzata tra le preferite

Quando configuri ed esegui una scansione personalizzata, questa è aggiunta automaticamente a un elenco limitato di scansioni recenti.Se in futuro intendi riutilizzare una scansione personalizzata, puoi scegliere di salvarla nell'elenco delle scansioni preferite dandole un nome specifico.

Per salvare una scansione personalizzata eseguita di recente nell'elenco delle scansioni preferite, segui questi passaggi:

1. Apri la finestra di configurazione della scansione personalizzata.
   a. Apri la finestra di Bitdefender.
   b. Vai al pannello **Antivirus**.
   c. Clicca su **Controlla ora** e seleziona **Scansione personalizzata** dal menu a tendina.
2. Localizza la scansione desiderata nell'elenco **Scansioni recenti**.
3. Porta il cursore del mouse sul nome della scansione e clicca sull'icona per aggiungerla all'elenco delle scansioni preferite.
4. Inserisci un nome specifico per la scansione.

Le scansioni salvate tra le preferite sono indicate con l'icona .Cliccando su questa icona, la scansione viene rimossa dall'elenco delle scansioni preferite.

## 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; 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; xlsm; 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 tuo sistema.Il malware può colpire il tuo 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.

- **Controlla i settori di avvio.** E' possibile impostare Bitdefender per esaminare i settori di boot del tuo disco.Questo settore del disco fisso 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.
- **Controlla la memoria.** Seleziona questa opzione per controllare i programmi in esecuzione nella memoria di sistema.
- **Controlla il registro.** 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.
- **Controlla cookie.** Seleziona questa opzione per controllare i cookie memorizzati dai browser sul tuo computer.
- **Controlla solo i 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.
- **Scansione per rootkit.** Seleziona questa opzione per eseguire una scansione alla ricerca di rootkit e oggetti nascosti usando tale software.

## 5.2.6. Procedura guidata scansione antivirus

Ogni volta che si inizia una scansione su richiesta (ad esempio, cliccando con il pulsante destro su una cartella e selezionando **Controlla con Bitdefender**), comparirà 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.Cercare l'icona di avanzamento della scansione nella barra delle applicazioni.Clicca su questa icona per aprire un processo di scansione e visualizzarne il progresso.

## 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).Per visualizzare altri dettagli, clicca sul collegamento **Mostra altro**.

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

**Arresto o messa in pausa della scansione.** Puoi fermare la scansione in qualsiasi momento, cliccando su **Fermare**. Verrai portato all'ultimo passaggio della procedura guidata.Per interrompere temporaneamente il processo di scansione, clicca semplicemente su **Pausa**. Per continuare la scansione, invece, dovrai cliccare su **Riprendi**.

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

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

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

## Fase 2 - Scegliere le azioni

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

Nota

Eseguendo una scansione veloce o una scansione completa del sistema, Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati durante la

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

Gli 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 corrette**

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 si riferisce alla 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 ulteriori informazioni fare riferimento a «*Gestire i file in quarantena*» (p. 56).

  Importante

  Per alcuni particolari tipologie di malware, non è possibile usare la disinfezione perché il file rilevato è interamente maligno. 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, poiché non è disponibile alcuna pratica 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 antimalware 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 «*Rimuovere malware dal sistema*» (p. 128).

## 5.2.7. Controllare i registri di scansione

Ogni volta che esegui una scansione, viene creato un registro di scansione.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 i registri di scansione in un secondo momento, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Eventi** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Scansione virus**.Qui puoi trovare tutti gli eventi di scansione malware, incluso le minacce rilevate dalla scansione all'accesso, le scansioni avviate dall'utente e le variazioni di stato per le scansioni automatiche.

4. Nell'elenco degli eventi, puoi controllare quali scansioni sono state eseguite di recente.Clicca su un evento per visualizzare maggiori dettagli al riguardo.
5. Per aprire il registro della scansione, clicca su **Guarda registro**.Il registro di scansione si aprirà nel tuo browser web predefinito.

## 5.3. Scansione automatica di supporti removibili

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.

### 5.3.1. Come funziona?

Quando rileva un dispositivo rimovibile di archiviazione, Bitdefender inizia la scansione antimalware in background (a condizione che la scansione automatica sia attivata per quel tipo di dispositivo).Un'icona di scansione di Bitdefender comparirà nella barra di sistema.Clicca su questa icona per aprire un processo di scansione e visualizzarne il progresso.

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

Se l'Autopilota 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 hanno 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.È buona cosa copiare tutti i dati importanti dal disco al tuo 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. 128).

### 5.3.2. Gestire la scansione di supporti rimovibili

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

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Eccezioni**.
4. Nella sezione **Scansione dispositivi rilevati**, scegli quali dispositivi di archiviazione vuoi controllare automaticamente.Clicca sugli interruttori per attivare o disattivare la scansione automatica.

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.

## 5.4. Configurare le eccezioni della scansione

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

### 5.4.1. Escludere file o cartelle dalla scansione

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

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Eccezioni**.
4. Attiva le eccezioni della scansione per i file usando l'interruttore corrispondente.
5. Clicca sul collegamento **File e cartelle escluse**.Nella finestra che compare, puoi gestire i file e le cartelle esclusi dalla scansione.
6. 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 al file o alla cartella nel campo Modifica.
   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'esclusione, seleziona una delle altre opzioni.
   d. Clicca su **Aggiungi**.
7. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

### 5.4.2. 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. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.

3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Eccezioni**.
4. Attiva le eccezioni della scansione per i file usando l'interruttore corrispondente.
5. Clicca sul collegamento **Estensioni escluse**.Nella finestra che compare, puoi gestire le estensioni dei file escluse dalla scansione.
6. 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'esclusione, seleziona una delle altre opzioni.
   d. Clicca su **Aggiungi**.
7. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

### 5.4.3. Gestire le eccezioni di 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 di scansione, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **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**).Comparirà una nuova finestra dove potrai modificare l'estensione o il percorso da escludere e il tipo di scansione dal quale escluderlo, secondo le necessità. Apporta le modifiche necessarie e clicca su **Modifica**.
5. Per disattivare le eccezioni, usa l'interruttore corrispondente.

## 5.5. 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 antimalware 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. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **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 in quarantena a Bitdefender 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**.

## 5.6. Active Virus Control

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

L'Active Virus 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'Autopilota 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 Virus Control nella finestra Eventi.

### 5.6.1. Verificare le applicazioni rilevate

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

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Eventi** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Active Virus Control**.
4. Clicca su un evento per visualizzare maggiori dettagli al riguardo.
5. Se ti fidi dell'applicazione, puoi configurare Active Virus Control per non bloccarla più, cliccando su **Consenti e monitora**.Active Virus Control continuerà a monitorare le applicazioni escluse. Se un'applicazione esclusa viene rilevata a eseguire attività sospette, l'evento semplicemente sarà registrato e notificato alla cloud di Bitdefender come errore di rilevazione.

### 5.6.2. Attivare o disattivare Active Virus Control

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

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Protezione**.
4. Clicca sull'interruttore per attivare o disattivare Active Virus Control.

### 5.6.3. Impostare la protezione di Active Virus Control

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

Per impostare la protezione di Active Virus Control, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Protezione**.
4. Assicurati che Active Virus Control sia attivato.
5. Trascina il pulsante scorrevole lungo la barra per impostare il livello di protezione desiderato.Usa la descrizione sul lato destro dell'ordine 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 Virus 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 pulite rilevate come dannose).

## 5.6.4. Gestire i processi esclusi

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

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

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Eccezioni**.
4. Clicca sul collegamento **Processi esclusi**.Nella finestra che compare, puoi gestire le eccezioni del processo di Active Virus Control.

Nota
Le eccezioni relative ai processi si applicano anche al Sistema di rilevazione intrusioni incluso nel firewall di Bitdefender.

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 l'opzione **Consenti** selezionata per impedire ad Active Virus 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 **Rimuovi**.
   - 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. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

## 5.7. Risolvere le vulnerabilità del sistema

Un passaggio importante nella protezione del computer contro hacker 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 offre due semplici modi per risolvere le vulnerabilità del tuo sistema:

- Puoi verificare le vulnerabilità del sistema e risolverle passaggio dopo passaggio usando la procedura guidata della **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.

### 5.7.1. Controllare il sistema per rilevare vulnerabilità

Per sistemare le vulnerabilità del sistema usando la procedura guidata della Scansione vulnerabilità, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Antivirus**.
3. Clicca su **Controlla ora** e poi seleziona **Scansione vulnerabilità**.
4. Segui la procedura guidata in sei passaggi per rimuovere le vulnerabilità dal sistema.Puoi esplorare la procedura guidata usando il pulsante **Avanti**. Per uscire, clicca su **Annulla**.

   a. **Proteggi il PC**

      Seleziona le vulnerabilità da controllare.

b. **Controllo problemi**

Attendi che Bitdefender termini di controllare le vulnerabilità del tuo sistema.

c. **Agg. Windows**

Puoi vedere l'elenco degli aggiornamenti critici e non critici di Windows che non sono attualmente installati sul computer.Seleziona gli aggiornamenti che desideri installare.

Per avviare l'installazione degli aggiornamenti selezionati, clicca su **Avanti**.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.

d. **Aggiornamenti applicazioni**

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

e. **Password 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 **Risolvi** 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 @).

f. **Sommario**

Qui puoi visualizzare il risultato dell'operazione.

## 5.7.2. Usare il controllo automatico delle vulnerabilità

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

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

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Eventi** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Vulnerabilità**.
4. 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** per aprire la procedura guidata della Scansione vulnerabilità e installarli.

- 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 **Sistema 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 esecuzione automatica di Windows è attivata, clicca su **Disattiva** per disattivarla.

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

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Vulnerabilità**.
4. Clicca sull'interruttore per attivare o disattivare la Scansione vulnerabilità automatica.

   Importante
   Per essere avvertito automaticamente sulle vulnerabilità del sistema o delle applicazioni, mantieni la **Scansione vulnerabilità automatica** 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 regolari di Windows**
   Verifica se il sistema operativo Windows ha gli ultimi aggiornamenti di sicurezza di Microsoft.

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

   **Password deboli**
   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.

# 6. Antispam

Spam è un termine usato per descrivere ogni e-mail non richiesta.Lo spam rappresenta un problema in continua crescita, sia per i privati che per le aziende. Non è piacevole, non vorresti che i tuoi figli lo vedessero, potrebbe penalizzarti (per aver sprecato troppo tempo o per aver ricevuto mail pornografiche in ufficio) e non puoi impedire alla gente di inviarlo. La miglior cosa da fare, ovviamente, è di fermarne la ricezione. Sfortunatamente lo Spam si presenta sotto molte forme e dimensioni e ce n'è veramente tanto in giro.

L'antispam di Bitdefender impiega notevoli innovazioni tecnologiche e filtri standard dell'industria antispam per eliminare lo spam prima che raggiunga la Posta in arrivo dell'utente.Per ulteriori informazioni fare riferimento a «*Approfondimenti antispam*» (p. 63).

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

Nota

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

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

- In Microsoft Outlook, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Posta eliminata**.La cartella **Spam** è creata durante l'installazione di Bitdefender.
- In Outlook Express e Windows Mail, i messaggi spam sono spostati direttamente nella cartella **Posta eliminata**.
- In Mozilla Thunderbird, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Cestino**.La cartella **Spam** è creata durante l'installazione di Bitdefender.

Se usi altri client di posta, devi creare una regola per spostare i messaggi e-mail segnati come`[spam]`da Bitdefender in una cartella personale di quarantena.

## 6.1. Approfondimenti antispam

### 6.1.1. Filtri Antispam

Il motore antispam di Bitdefender incorpora diversi filtri che assicurano l'assenza di SPAM nella tua casella di posta: Elenco amici, Elenco Spammer, Filtro Carattere, Filtro link, Filtro firme, Filtro NeuNet (euristico) e rilevazione in-the-cloud.

## Elenco amici / Elenco spammer

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

Nota

Raccomandiamo di aggiungere i nomi dei tuoi amici e gli indirizzi e-mail all'**elenco Amici**. Bitdefender non blocca i messaggi di chi è nell'elenco e aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

## Filtro Carattere

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

## Filtro link

La maggior parte dei messaggi Spam contiene link a vari siti web. Questi siti solitamente contengono ulteriore pubblicità e la possibilità di acquistare oggetti e, alle volte, vengono usati per phishing.

Bitdefender mantiene un database di tali link.Il filtro link esamina ogni URL contenuto in un messaggio con il suo database. Se corrisponde, il messaggio viene etichettato come SPAM.

## Filtro firme

I ricercatori antispam di Bitdefender analizzano costantemente le e-mail spam e rilasciano firme spam per consentirne la rilevazione.

Il filtro firme controlla le e-mail contro ogni firma di spam nel database locale.Se c'è una corrispondenza, il messaggio è segnato come SPAM.

Nota

A differenza degli altri filtri, il filtro firme non può essere disattivato indipendentemente dalla protezione antispam.

## Filtro Euristico

Il **Filtro NeuNet (euristico)** esegue una serie di test a tutte le componenti del messaggio (ovvero, non solo l'intestazione ma anche il corpo del messaggio sia in formato HTML che di testo), alla ricerca di parole, frasi, link o altri elementi caratteristici dello spam.In base ai risultati dell'analisi, l'e-mail riceverà un punteggio spam.

Se il punteggio spam supera il livello di soglia, il messaggio è considerato SPAM.Il livello di soglia è definito dal livello di sensibilità antispam.Per ulteriori informazioni fare riferimento a «*Impostare il livello di sensibilità*» (p. 71).

Il filtro rileva inoltre messaggi segnati come ESPLICITAMENTE SESSUALE: nell'oggetto e li etichetta come SPAM.

Nota

Dal 19 maggio 2004 lo spam contenente materiale a sfondo sessuale deve includere l'avviso SEXUALLY-EXPLICIT: nell'oggetto, diversamente sarà passibile di sanzioni per violazione della legge federale.

### Rilevamento in-the-cloud

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

Le e-mail sono controllate in the cloud solo se i filtri antispam locali non forniscono un risultato conclusivo.

## 6.1.2. Operazione antispam

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

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

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

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

Il Filtro link confronterà i link trovati nell'e-mail con i link del database di Bitdefender relativo a link spam noti. In caso di corrispondenza, l'e-mail sarà considerata spam.

Poi, il filtro firme controllare le e-mail contro ogni firma di spam nel database locale.Se c'è una corrispondenza, il messaggio è segnato come SPAM.

Il Filtro NeuNet (Euristico) prenderà in carico il messaggio e-mail ed eseguirà una serie di test su tutte le componenti del messaggio, alla ricerca di parole, frasi, collegamenti o altre caratteristiche tipiche dello spam.In base ai risultati dell'analisi, l'e-mail riceverà un punteggio spam.

Nota

Se l'e-mail è marcata come SEXUALLY EXPLICIT nella riga del soggetto, Bitdefender la considererà come SPAM.

Se il punteggio spam supera il livello di soglia, il messaggio è considerato SPAM.Il livello di soglia è definito dal livello di protezione antispam.Per ulteriori informazioni fare riferimento a «*Impostare il livello di sensibilità*» (p. 71).

Se i filtri locali antispam non forniscono un risultato finale, l'e-mail è controllata usando una rilevazione in-the-cloud, che decide se il messaggio è spam o legittimo.

### 6.1.3. Aggiornamenti antispam

Ogni volta che viene eseguito un aggiornamento, nuove firme per link ed e-mail spam note sono aggiunte ai database.Questo aiuterà a incrementare l'effettività del tuo motore Antispam.

Per proteggerti contro gli spammer, Bitdefender può effettuare aggiornamenti automatici. Mantieni attivata l'opzione di **Aggiornamento automatico**.

### 6.1.4. Programmi e protocolli di posta elettronica supportati

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

- Microsoft Outlook 2007 / 2010
- Microsoft Outlook Express e Windows Mail (su sistemi a 32 bit)
- Mozilla Thunderbird 3.0.4

## 6.2. Attivare o disattivare la protezione antispam

Per attivare o disattivare la protezione antispam, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Antispam**.
3. Clicca sull'interruttore per attivare o disattivare la protezione antispam.

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

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

Importante

Bitdefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo.Per un elenco completo di applicazioni di posta supportate, fare riferimento a «*Programmi e protocolli di posta elettronica supportati*» (p. 66).

Qui di seguito la spiegazione di ogni pulsante:

**È spam** - indica che l'e-mail selezionata è spam.L'e-mail sarà spostata immediatamente alla cartella **Spam**.Se i servizi cloud antispam sono attivati, il messaggio è inviato alla cloud di Bitdefender per ulteriori analisi.

**Non è spam** - indica che l'e-mail selezionata non è spam e Bitdefender non deve marcarla.L'e-mail sarà spostata dalla cartella **Spam** alla **Posta in arrivo**.Se i servizi cloud antispam sono attivati, il messaggio è inviato alla cloud di Bitdefender per ulteriori analisi.

Importante

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

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

**Aggiungi amico** - aggiunge il mittente dell'e-mail selezionata all'elenco Amici.Può essere necessario premere **OK** per confermare.Riceverai sempre e-mail provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

**Spammer** - apre l'**elenco Spammer**, che contiene tutti gli indirizzi e-mail dai quali non vuoi ricevere messaggi, indipendentemente dal loro contenuto.Per ulteriori informazioni fare riferimento a «*Configurazione dell'elenco Spammer*» (p. 70).

**Amici** - apre l'**elenco Amici** che contiene tutti gli indirizzi e-mail dai quali desideri ricevere sempre i messaggi, indipendentemente dal loro contenuto.Per ulteriori informazioni fare riferimento a «*Configurazione dell'elenco Amici*» (p. 69).

**Impostazioni** - apre una finestra dove puoi configurare i filtri antispam e le impostazioni della barra degli strumenti.

### 6.3.1. Indicare gli errori di rilevazione

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

1. Apri il tuo client e-mail.
2. Vai alla cartella posta indesiderata, dove vengono spostati i messaggi spam.

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

## 6.3.2. Indicare messaggi spam non rilevati

Se utilizzi un client di posta supportato, puoi facilmente indicare quali messaggi e-mail sarebbero dovuti essere rilevati come spam. Facendo ciò si migliora considerevolmente l'efficienza del filtro antispam.Attenersi alla seguente procedura:

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

## 6.3.3. Configurare le impostazioni della barra degli strumenti

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

Le impostazioni sono suddivise in due categorie:

- Nella categoria **Regole e-mail**, puoi configurare le regole per la gestione delle e-mail spam rilevate da Bitdefender
  - **Sposta messaggio in Posta eliminata** (solo per Microsoft Outlook Express / Windows Mail)

    Nota
    In Microsoft Outlook / Mozilla Thunderbird, i messaggi spam rilevati sono spostati automaticamente nella cartella Spam, localizzata in Posta eliminata / Cestino.

  - **Etichetta i messaggi di spam come 'letti'** - etichetta i messaggi di spam come letti in modo automatico, in modo tale da non disturbare quando questi vengono ricevuti.

- Nella categoria **Notifiche**, puoi scegliere se visualizzare o no le finestre di conferma quando clicchi sui pulsanti **Aggiungi Spammer** e **Aggiungi Amico** nella barra degli strumenti antispam.Le finestre di conferma possono impedire di aggiungere accidentalmente i mittenti all'elenco Amici / Spammer.

## 6.4. Configurazione dell'elenco Amici

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

Nota

Qualsiasi mail in arrivo da un indirizzo contenuto nell'**elenco Amici**, sarà automaticamente consegnato alla tua Posta in arrivo senza alcun ulteriore processo.

Per configurare e gestire l'elenco Amici:

- Se stai usando Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, clicca sul pulsante **Amici** nella barra degli strumenti antispam di Bitdefender integrata nel tuo client e-mail.
- In alternativa, segui questi passaggi:
  1. Apri la finestra di Bitdefender.
  2. Vai al pannello **Antispam**.
  3. Clicca su **Gestisci** e seleziona **Amici** dal menu.

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

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

- @domain.com, *domain.com e domain.com - tutte le e-mail provenienti da domain.com raggiungeranno la tua **Posta in arrivo** indipendentemente dal loro contenuto;
- *domain* - tutte le e-mail provenienti da domain (non importa il suffisso del dominio) raggiungeranno la tua **Posta in arrivo** indipendentemente dal loro contenuto;
- *com - tutte le e-mail con il suffisso di dominio com raggiungeranno la tua **Posta in arrivo** indipendentemente dal loro contenuto;

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

Per eliminare un elemento dall'elenco, clicca sul collegamento **Rimuovi** corrispondente.Per eliminare tutti gli elementi dall'elenco clicca su **Cancella lista** e quindi su **Sì** per confermare.

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

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

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

## 6.5. Configurazione dell'elenco Spammer

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

Per configurare e gestire l'elenco Spammer:

- Se stai usando Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, clicca sul pulsante **Spammer** nella barra degli strumenti antispam di Bitdefender integrata nel tuo client e-mail.
- In alternativa, segui questi passaggi:
  1. Apri la finestra di Bitdefender.
  2. Vai al pannello **Antispam**.
  3. Clicca su **Gestisci** e seleziona **Spammer** dal menu.

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

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

- @domain.com, *domain.com e domain.com - tutte le e-mail provenienti da domain.com saranno marcate come Spam;
- *domain* - tutte le e-mail provenienti da domain (indipendentemente dai suffissi del dominio) saranno marcate come Spam;
- *com - tutte le e-mail con il suffisso di dominio com saranno marcate come Spam.

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

### Avvertimento

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

Per eliminare un elemento dall'elenco, clicca sul collegamento **Rimuovi** corrispondente.Per eliminare tutti gli elementi dall'elenco clicca su **Cancella lista** e quindi su **Sì** per confermare.

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

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

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

## 6.6. Impostare il livello di sensibilità

Se noti che alcune e-mail legittime sono segnate come spam, o che molte e-mail spam non sono rilevate, puoi provare a modificare il livello di sensibilità antispam per risolvere il problema.Tuttavia, piuttosto che cambiare indipendentemente il livello di sensibilità, si consiglia di leggere prima «*Il filtro antispam non funziona correttamente*» (p. 120) e seguire le istruzioni per correggere il problema.

Per impostare il livello di sensibilità dell'antispam, segui questi passaggi:

1. Apri Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antispam** nel menu di sinistra e poi sulla scheda **Impostazioni**.
4. Usa la descrizione sul lato destro dell'ordine per selezionare il livello di sensibilità che si adatta meglio alle tue necessità di sicurezza.La descrizione ti informa anche di ogni azione aggiuntiva che dovresti intraprendere per evitare problemi potenziali o per aumentare l'efficienza della rilevazione antispam.

## 6.7. Configurare i filtri locali antispam

Come descritto in «*Approfondimenti antispam*» (p. 63), Bitdefender usa una combinazione di diversi filtri antispam per identificare lo spam.I filtri antispam sono pre-configurati per una protezione ottimale.

Importante

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

Per configurare i filtri antispam locali, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antispam** nel menu di sinistra e poi sulla scheda **Impostazioni**.
4. Clicca sugli interruttori per attivare o disattivare i filtri locali antispam.

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

## 6.8. Configurare la rilevazione in-the-cloud

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

Per configurare la rilevazione in-the-cloud, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antispam** nel menu di sinistra e poi sulla scheda **Cloud**.
4. Clicca sull'interruttore per attivare o disattivare la rilevazione in-the-cloud.
5. Campioni di e-mail legittime o spam possono essere inviati alla cloud di Bitdefender, indicando errori di rilevazione o messaggi spam non rilevati. Ciò contribuisce a migliorare la rilevazione antispam di Bitdefender.Configura l'invio di un'e-mail campione alla cloud di Bitdefender selezionando le opzioni desiderate.

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

# 7. Controllo privacy

Le tue informazioni personali sono un bersaglio costante per i cyber criminali.Poiché le minacce si sono estese a quasi tutto l'intero spettro di attività online, messaggi e-mail, chat e navigazione web non protetti possono comportare il rilascio di informazioni in grado di compromettere la propria privacy.

Il Controllo privacy di Bitdefender affronta tutte queste minacce con una moltitudine di componenti.

- Protezione antiphishing - offre un set completo di funzioni che proteggono la tua esperienza di navigazione web, come ad esempio evitare la diffusione di informazioni personali a siti web fraudolenti camuffati da siti legittimi.
- Protezione dati - Non consente di divulgare i tuoi dati personali dal computer senza il tuo consenso.Controlla le e-mail e i messaggi istantanei inviati dal tuo computer, oltre a qualsiasi dato inviato tramite pagine web, bloccando qualsiasi informazione protetta dalle regole di Protezione dati impostate.
- Crittografia chat - crittografa le conversazioni chat per assicurarsi che il contenuto resti privato.

## 7.1. Protezione antiphishing

L'antiphishing di Bitdefender ti impedisce di svelare informazioni personali mentre navighi su Internet, avvertendoti delle potenziali pagine web con phishing.

Bitdefender fornisce protezione antiphishing in tempo reale per:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger

Per configurare le impostazioni antiphishing, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Controllo Privacy** nel menu di sinistra e poi sulla scheda **Antiphishing**.

Le impostazioni sono suddivise in due categorie.

**Funzioni barra strumenti**

Clicca sugli interruttori per attivare o disattivare:

- Mostrare la barra degli strumenti di Bitdefender nel browser web.

- Ricerca sicura, un componente che classifica i risultati delle tue ricerche tramite Google, Bing e Yahoo! oltre ai link di Facebook e Twitter, posizionando un'icona accanto a ogni risultato.

  Non dovresti visitare questa pagina web.

  Questa pagina web può contenere contenuti pericolosi. Se decidi di visitarla, presta la massima cautela.

  Questa è una pagina sicura da visitare.

- 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 per browser web**

Clicca sugli interruttori per attivare o disattivare:

- Protezione dalle frodi.
- Protezione da phishing.
- Protezione per chat.

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

Per configurare e gestire la white list antiphishing, clicca sul collegamento **White list**.Comparirà una nuova finestra.

Per aggiungere un sito alla white list, 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.

### 7.1.1. Protezione di Bitdefender nel browser

Bitdefender si integra direttamente attraverso una barra degli strumenti intuitiva e di facile uso nei seguenti web browser:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera

La barra degli strumenti di Bitdefender non è la tipica barra degli strumenti del browser.L'unica cosa che aggiunge al browser è una piccola linguetta nella parte superiore di ogni pagina web.Cliccaci sopra per vedere la barra degli strumenti.

La barra degli strumenti di Bitdefender include le seguenti componenti:

**Valutazione pagina**

In base a come Bitdefender classifica la pagina web che stai visualizzando, sul lato sinistro della barra degli strumenti viene indicata una delle seguenti valutazioni:

- Il messaggio "Questa pagina non è sicura" compare su uno sfondo rosso. Dovresti uscire subito dalla pagina web.
- Il messaggio "Si consiglia cautela" compare su uno sfondo arancio. Questa pagina web potrebbe avere contenuti pericolosi.Se decidi di visitarlo, usa la massima cautela.
- Il messaggio "Questa pagina è sicura" compare su uno sfondo verde. La pagina è sicura e può essere visitata.

**Sandbox**

Clicca per lanciare il browser in un ambiente creato da Bitdefender, isolandolo dal sistema operativo. Impedisce alle minacce basate sui browser di sfruttare le vulnerabilità dei browser per ottenere il controllo del tuo sistema.Usa SandBox quando visiti pagine web che ritieni possano contenere malware.

Nota
Sandbox non è disponibile sui computer con Windows XP.

**Impostazioni**

Clicca per selezionare le singole caratteristiche da attivare o disattivare:

- Filtro antiphishing
- Filtro antimalware
- Ricerca Sicura

**Interruttore di accensione**

Per attivare/disattivare completamente le funzioni della barra degli strumenti, clicca sul lato destro della barra stessa.

## 7.1.2. 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:

- Resta alla larga dalla pagina web.
- Procedi alla pagina web, malgrado l'avvertimento, cliccando su **Sono a conoscenza dei rischi, quindi prosegui**.
- Aggiungi la pagina alla white list dell'antiphishing cliccando su **Aggiungi alla white list**.La pagina non sarà più controllata dai motori antiphishing di Bitdefender.

## 7.2. Protezione dati

La Protezione dati impedisce la diffusione di dati sensibili quando sei online.

Considera un semplice esempio: hai creato una regola di Protezione dati che protegge il tuo numero di carta di credito.Se uno spyware in qualche modo riesce a installarsi sul tuo computer, non può inviare il tuo numero di carta di credito via e-mail, chat o tramite pagine web.Inoltre, il bambino non può usarlo per fare acquisti online o comunicarlo a persone incontrate sul web.

### 7.2.1. Info su Protezione dati

Che sia la tua e-mail o il numero della tua carta di credito, quando finiscono nelle mani sbagliate tali informazioni possono recarti danno: puoi ritrovarti affogato nei messaggi di spam o addirittura con il tuo conto bancario in rosso.

Basandosi sulle regole create da te, la Protezione dati esegue la scansione del traffico web, e-mail e chat in uscita dal tuo computer, cercando specifiche sequenze di caratteri (ad esempio, il tuo numero di carta di credito). In caso di coincidenza, la pagina web, l'e-mail o il messaggio istantaneo vengono bloccati.

Puoi creare regole per proteggere ogni informazione che consideri personale o confidenziale, dal tuo numero di telefono o l'indirizzo e-mail, fino alle informazioni sul tuo conto bancario.Viene fornito un supporto Multi-utente, in modo che gli utenti che accedano ad altri account di Windows possano configurare e usare le proprie regole.Se il proprio account Windows è un account amministratore, le regole create possono essere configurate per essere applicate anche quando altri utenti del computer accedono ai rispettivi account utente Windows.

### 7.2.2. Configurare la Protezione dati

Se vuoi usare la Protezione dati, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Controllo privacy** nel menu di sinistra e poi sulla scheda **Protezione dati**.
4. Assicurati che la Protezione dati sia attivata.

5. Crea regole per proteggere i tuoi dati sensibili.Per ulteriori informazioni fare riferimento a «*Creare regole di protezione dati*» (p. 77).

## Creare regole di protezione dati

Per creare una regola, clicca sul pulsante **Aggiungi regola** e segui la procedura guidata di configurazione.Puoi esplorare la procedura guidata usando i pulsanti **Avanti** e **Indietro**.Per uscire dalla procedura guidata, clicca su **Annulla**.

1. **Imposta il tipo di regola e i dati**

   Devi impostare i seguenti parametri:

   - **Nome regola** - inserisci il nome della regola nel campo di modifica.
   - **Tipo di regola** - scegli il tipo di regola (indirizzo, nome, carta di credito, PIN, SSN, ecc).
   - **Dati regola** - inserisci i dati da proteggere nel campo di modifica.Ad esempio, se desideri proteggere la tua carta di credito, inserisci tutto o parte del numero in questo campo.

     Importante

     Inserendo meno di tre caratteri, ti sarà chiesto di convalidare i dati. Ti consigliamo di inserire almeno tre caratteri per evitare il blocco erroneo di messaggi e pagine web.

   Tutti i dati inseriti sono crittografati. Per una sicurezza maggiore, non inserire tutti i dati che desideri proteggere.

2. **Seleziona i tipi di traffico e utenti**

   a. Seleziona il traffico che desideri esaminare con Bitdefender.

      - **Scansione web (traffico HTTP)** - controlla il traffico HTTP (web) e blocca i dati in uscita corrispondenti ai dati della regola.
      - **Scansione e-mail (traffico SMTP)** - esamina il traffico SMTP (e-mail) e blocca le e-mail in uscita contenenti i dati della regola.
      - **Scansione traffico chat** - controlla il traffico chat e blocca i messaggi in uscita contenenti i dati della regola.

      Puoi scegliere di applicare la regola solo se i dati della regola corrispondono completamente oppure se le maiuscole/minuscole corrispondono.

   b. Specifica gli utenti a cui si applica la regola.

      - **Solo per me (utente attuale)** - la regola si applica solo all'account utente attuale.
      - **Account utente limitati** - la regola si applica all'utente attuale e a tutti gli account di Windows limitati.

- **Tutti gli utenti** - la regola si applica a tutti gli account di Windows.

3. **Definizione regola**

   Inserisci una breve descrizione della regola nel campo di modifica.Siccome i dati bloccati (serie di caratteri) non vengono mostrati in plain text quando si accede alla regola, la descrizione dovrebbe aiutarti a identificarla facilmente.

   Clicca su **Termina**.La regola apparirà nella tabella.

D'ora in poi, qualsiasi tentativo di inviare i dati indicati (via e-mail, chat o una pagina web) fallirà.Nella finestra Eventi sarà visualizzato un valore, indicando che Bitdefender ha impedito che contenuti relativi all'identità venissero inviati.

### 7.2.3. Amministrazione delle regole

Per gestire le regole della Protezione dati:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Controllo privacy** nel menu di sinistra e poi sulla scheda **Protezione dati**.

Puoi visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionala e clicca sul pulsante **Rimuovi regola**.

Per modificare una regola, selezionala e clicca sul pulsante **Modifica regola**. Comparirà una nuova finestra.Qui puoi modificare il nome, la definizione e i parametri della regola (tipo, dati e traffico). Clicca su **OK** per salvare le modifiche.

## 7.3. Crittografia chat

I contenuti dei tuoi messaggi istantanei dovrebbero restare tra te e il tuo partner di chat.Crittografando le tue conversazioni, puoi assicurarti che chiunque tenti di intercettarle durante l'invio da te ai tuoi contatti, non sarà in grado di leggerne il contenuto.

Di norma, Bitdefender esegue la crittografia di tutte le tue sessioni chat, purché:

- Il tuo partner di chat ha una versione di Bitdefender installata che supporta la Crittografia Chat, e la Crittografia Chat è abilitata per l'applicazione usata per chattare.
- Tu e la persona con cui vuoi chattare usate Yahoo! Messenger.

Importante

Bitdefender non cifrerà una conversazione se uno degli utenti in chat utilizza un'applicazione chat via web come Meebo.

Per configurare la crittografia della chat:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Controllo Privacy** nel menu di sinistra e poi sulla scheda **Crittografia**.

Di norma, la Crittografia chat è attivata.Puoi disattivare la Crittografia chat cliccando sull'interruttore corrispondente.

# 8. Controllo genitori

Il Controllo genitori di Bitdefender ti permette di controllare l'accesso a Internet e ad applicazioni specifiche di ogni utente che possieda un account nel sistema.

Puoi configurare il Controllo genitori per bloccare:

- pagine web inappropriate.
- accesso a Internet, durante specifici periodi di tempo (come durante le ore di studio).
- pagine web, e-mail e messaggi istantanei contenenti determinate parole.
- applicazioni come giochi, chat, programmi di condivisione di file e altri.
- messaggi istantanei inviati da contatti chat diversi da quelli consentiti.

Importante

Solo gli utenti con diritti di amministrazione (amministratori del sistema) possono accedere e configurare il Controllo genitori.Per essere sicuro che solo tu possa modificare le impostazioni del Controllo genitori per qualsiasi utente, puoi proteggerle mediante una password.

Una volta configurato il Controllo genitori, puoi scoprire facilmente ciò che i bambini fanno sul computer.

Anche quando non sei a casa, puoi sempre verificare le attività dei bambini e modificare le impostazioni del Controllo genitori, usando il Controllo genitori remoto.

## 8.1. Configurazione Controllo genitori

Prima di configurare il Controllo genitori, crea degli account utente di Windows separati per i bambini. In questo modo potrai sapere esattamente cosa sta facendo ognuno di loro sul computer. Dovresti creare degli account utente limitati (standard), in modo che non possano modificare le impostazioni del Controllo genitori.Per ulteriori informazioni fare riferimento a *«Come posso creare gli account utente di Windows?»* (p. 33).

Se i bambini possono accedere ai loro computer con un account di amministratore, devi configurare una password per proteggere le impostazioni del Controllo genitori.Per ulteriori informazioni fare riferimento a *«Impostazioni protezione da password di Bitdefender»* (p. 17).

Per configurare il Controllo genitori:

1. Assicurati di aver avviato il computer con un account amministratore.Solo gli utenti con diritti di amministrazione (amministratori del sistema) possono accedere e configurare il Controllo genitori.
2. Apri la finestra di Bitdefender.

3. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
4. Clicca su **Controllo genitori** nel menu di sinistra e poi sulla scheda **Account**.Qui puoi selezionare e configurare le impostazioni del Controllo genitori di ogni account di Windows.Se il Controllo genitori è attivato, puoi visualizzare la categoria d'età selezionata e lo stato dei controlli per genitori (che saranno descritti qui di seguito).

Per configurare il Controllo genitori per un account utente specifico:

1. Usa l'interruttore per attivare il Controllo genitori per quell'account utente.
2. Imposta l'età dei bambini cliccando su una delle caselle corrispondenti per l'opzione **Età**.Impostando l'età del bambino caricherai automaticamente le impostazioni considerate appropriate per quella categoria d'età, in base agli standard di sviluppo del bambino.
3. Se desideri configurare le impostazioni del Controllo genitori in dettaglio, clicca su **Impostazioni**.Clicca su una scheda per configurare la caratteristica corrispondente del Controllo genitori:
   - **Web** - per filtrare la navigazione web e impostare limiti temporali nell'accesso a Internet usando il Controllo web.
   - **Applicazioni** - configura il Controllo applicazioni per bloccare o limitare l'accesso a determinate applicazioni.
   - **Parole chiave** - per filtrare l'accesso a web, e-mail e chat in base alle parole chiave usando il Controllo parole chiave.
   - **Chat** - configura il Controllo Chat per consentire o bloccare la chat con determinati contatti su Yahoo! Messenger.
   - **Categorie** - blocca determinate categorie di contenuti web usando il Filtro categorie.

   Per chiudere la finestra delle impostazioni del Controllo genitori, clicca sul pulsante X nell'angolo in alto a destra.Le impostazioni che hai configurato sono state salvate automaticamente.

Per configurare le opzioni di monitoraggio attività e il Controllo genitori remoto, vai alla scheda **Impostazioni**.Configura le opzioni di monitoraggio come necessario:

**Invia notifiche attività via e-mail**
Viene inviata una notifica e-mail ogni volta che il Controllo genitori di Bitdefender blocca un'attività.Prima devi configurare le impostazioni di notifica.

**Salva registro del traffico Internet**
Registra i siti web visitati dagli utenti per cui è abilitato il Controllo genitori.

Per ulteriori informazioni fare riferimento a «*Monitorare le attività dei bambini*» (p. 87).

Se desideri monitorare e controllare in remoto le attività dei bambini con il computer e Internet, attiva il Controllo genitori remoto usando l'interruttore.Per ulteriori informazioni fare riferimento a «*Controllo genitori remoto*» (p. 89).

### 8.1.1. Controllo web

Il Controllo web ti aiuta a bloccare i siti web con contenuti inappropriati e a impostare restrizioni temporali nell'utilizzo di Internet.

Per configurare il Controllo web per un account utente specifico:

1. Accedi alla finestra delle impostazioni del Controllo genitori di Bitdefender per quell'account utente.
2. Clicca sulla scheda **Web**.
3. Usa l'interruttore per attivare il Controllo web.
4. Se lo desideri, puoi creare regole personali per consentire o bloccare l'accesso a specifici siti web.Se il Controllo genitori blocca automaticamente l'accesso a un sito web, puoi creare una regola per consentire esplicitamente l'accesso a quel sito web.
5. Puoi impostare un limite di tempo per l'utilizzo di Internet da parte dei bambini.Per ulteriori informazioni fare riferimento a «Limitare gli intervalli di accesso a Internet» (p. 83).

#### Creare le regole del Controllo web

Per permettere o bloccare l'accesso a un sito web, segui questi passaggi:

1. Clicca su **Consenti sito web** o **Blocca sito web**.
2. Inserisci l'URL del sito web nel campo **Sito web**.
3. Seleziona l'azione desiderata per questa regola - **Consenti** oppure **Blocca**.
4. Clicca su **Termina** per aggiungere la regola.

#### Gestire le regole del Controllo web

Le regole del Controllo web configurate sono elencate in una tabella nella parte inferiore della finestra. Per ogni regola del Controllo web sono elencati l'indirizzo del sito web e lo stato attuale.

Per eliminare una regola, selezionala e clicca su **Rimuovi**.

Per modificare una regola, cliccaci sopra due volte (o selezionala e clicca su **Modifica**.Effettua i cambiamenti necessari nella finestra di configurazione.

### Limitare gli intervalli di accesso a Internet

Nella sezione Programma accesso web, puoi impostare dei limiti di tempo per l'uso di Internet da parte dei bambini.

Per bloccare completamente l'accesso a Internet, seleziona **Blocca l'accesso al web**.

Per limitare l'accesso a Internet in determinati momenti della giornata:

1. Seleziona **Accesso al web limitato**.
2. Clicca su **Cambia programma**.
3. Seleziona dalla griglia gli intervalli di tempo durante i quali bloccare l'accesso a Internet.Puoi cliccare sulle singole caselle oppure puoi cliccare e trascinare per coprire periodi più lunghi.Per avviare una nuova selezione, clicca su **Blocca tutto** o su **Permetti tutto**.
4. Clicca su **Salva**.

Nota
Bitdefender eseguirà gli aggiornamenti ogni ora anche se l'accesso web fosse bloccato.

## 8.1.2. Controllo applicazioni

Il **Controllo applicazioni** ti aiuta a bloccare qualsiasi applicazione in esecuzione. Giochi, programmi di chat, oltre ad altre categorie di software e minacce che possono essere bloccati. Le applicazioni bloccate sono così protette da ogni modifica e non possono essere copiate o spostate.Puoi bloccare le applicazioni permanentemente o solo per determinati periodi di tempo, ad esempio quando i bambini dovrebbero fare i compiti.

Per configurare il Controllo applicazioni per un account utente specifico:

1. Accedi alla finestra delle impostazioni del Controllo genitori di Bitdefender per quell'account utente.
2. Clicca sulla scheda **Applicazioni**.
3. Usa l'interruttore per attivare il Controllo applicazioni.
4. Crea regole per le applicazioni che vuoi bloccare o a cui vuoi limitare l'accesso.

### Creazione regole di Controllo applicazioni

Per bloccare o limitare l'accesso a un'applicazione segui questi passaggi:

1. Clicca su **Blocca** o **Limita**.
2. Clicca su **Sfoglia** per localizzare l'applicazione di cui desideri bloccare/restringere l'accesso.Le applicazioni installate normalmente si trovano nella cartella `C:\Programmi`.

3. Seleziona l'azione della regola:
   - **Blocca permanentemente** per bloccare completamente l'accesso all'applicazione.
   - **Blocca in base ad un programma** per limitare l'accesso a determinati intervalli di tempo.

   Se scegli di restringere l'accesso piuttosto che bloccare completamente l'applicazione, devi anche selezionare dalla griglia i giorni e gli intervalli di tempo durante i quali l'accesso sarà bloccato.Puoi cliccare sulle singole caselle oppure puoi cliccare e trascinare per coprire periodi più lunghi.Per avviare una nuova selezione, clicca su **Blocca tutto** o su **Permetti tutto**.
4. Clicca su **Salva** per aggiungere la regola.

### Gestire le regole del Controllo applicazioni

Le regole del Controllo applicazioni che sono state configurate sono elencate in una tabella nella parte inferiore della finestra. Per ogni regola del Controllo applicazioni viene elencato il nome dell'applicazione, il percorso e lo stato attuale.

Per eliminare una regola, selezionala e clicca su **Rimuovi**.

Per modificare una regola, cliccaci sopra due volte (o selezionala e clicca su **Modifica**.Effettua i cambiamenti necessari nella finestra di configurazione.

## 8.1.3. Controllo parole chiave

Il Controllo parole chiave aiuta a bloccare l'accesso degli utenti a messaggi e-mail, pagine web e messaggi istantanei che contengono parole specifiche.Utilizzando il Controllo parole chiave, puoi impedire ai bambini di vedere parole o frasi inappropriate quando sono online.In più, puoi assicurarti che non saranno inoltrate informazioni personali (come indirizzo di casa o numeri di telefono) alle persone che incontrano su Internet.

Nota
Il Controllo parole chiave per la chat è disponibile solo per Yahoo! Messenger.

Per configurare il Controllo parole chiave per un account utente specifico:

1. Accedi alla finestra delle impostazioni del Controllo genitori di Bitdefender per quell'account utente.
2. Clicca sulla scheda **Parole chiave**.
3. Usa l'interruttore per attivare il Controllo parole chiave.
4. Creare regole per il Controllo delle Parole Chiave è utile affinché non vengano mostrate parole inappropriate o non vengano inviate informazioni importanti.

## Creazione regole del Controllo parole chiave

Per bloccare una parola o una frase, segui questi passaggi:

1. Clicca su **Blocca parola chiave**.
2. Informazioni sulle parole chiave.
   - **Categoria Parola chiave** - scrivi il nome della regola in questo campo.
   - **Parola Chiave** - digita la parola o la frase che vuoi bloccare. Se vuoi che solo intere parole vengano rilevate, seleziona la casella **Corrispondenza totale**.
3. Seleziona il Tipo di Filtraggio.
   - **Blocca visualizzazione** - seleziona questa opzione per le regole create per impedire che parole inappropriate possano essere visualizzate.
   - **Blocca inoltro** - seleziona questa opzione per le regole create per prevenire che informazioni importanti siano inviate.
4. Seleziona il tipo di traffico che Bitdefender dovrà analizzare alla ricerca della parola specificata.

| Opzione | Descrizione |
|---|---|
| **Web** | Le pagine web che contengono la parola chiave sono bloccate. |
| **E-mail** | I messaggi e-mail che contengono la parola chiave sono bloccati. |
| **Chat** | I messaggi istantanei che contengono la parola chiave sono bloccati. |

5. Clicca su **Termina** per aggiungere la regola.

D'ora in poi, ogni tentativo di inviare dati specifici (attraverso le e-mail, i messaggi istantanei o su una pagina web) fallirà. Sarà mostrato un messaggio di avviso indicante che Bitdefender ha impedito l'invio di contenuti personali.

## Gestione regole del Controllo parole chiave

Nella tabella sono elencate le regole del Controllo parole chiave che sono state configurate. Per ogni regola sono fornite informazioni dettagliate.

Per eliminare una regola, selezionala e clicca su **Rimuovi**.

Per modificare una regola, cliccaci sopra due volte (o selezionala e clicca su **Modifica**.Effettua i cambiamenti necessari nella finestra di configurazione.

### 8.1.4. Controllo Chat

Il Controllo chat ti permette di specificare i contatti chat con i quali i bambini possono chattare.

Nota
Il Controllo Chat è disponibile solo per Yahoo! Messenger.

Per configurare il Controllo chat per un account utente specifico:

1. Accedi alla finestra delle impostazioni del Controllo genitori di Bitdefender per quell'account utente.
2. Clicca sulla scheda **Chat**.
3. Usa l'interruttore per attivare il Controllo chat.
4. Seleziona il metodo di filtraggio preferito e, in base alla tua scelta, crea regole appropriate.
   - **Consenti la chat con tutti i contatti, eccetto quelli nell'elenco**

     In questo caso, devi specificare gli ID chat da bloccare (persone con cui i bambini non dovrebbero parlare).
   - **Blocca la chat con tutti i contatti, eccetto quelli nell'elenco**

     In questo caso, devi specificare gli ID chat con cui il bambino può esplicitamente chattare.Per esempio, puoi consentire la chat con i tuoi familiari, gli amici di scuola o i vicini di casa.

     Questa seconda opzione è consigliata se il bambino ha meno di 14 anni.

#### Creare regole di controllo chat

Per permettere o bloccare la messaggistica istantanea con un contatto, segui questi passaggi:

1. Clicca su **Blocca ID IM** o su **Consenti ID IM**.
2. Digita l'indirizzo e-mail o il nome utente utilizzato dal contatto IM nel campo **E-mail o ID IM**.
3. Seleziona l'azione desiderata per questa regola - **Consenti** oppure **Blocca**.
4. Clicca su **Termina** per aggiungere la regola.

#### Gestire le regole di controllo della chat

Le regole del Controllo chat configurate sono indicate nella tabella nel lato inferiore della finestra.

Per eliminare una regola, selezionala e clicca su **Rimuovi**.

Per modificare una regola, cliccaci sopra due volte (o selezionala e clicca su **Modifica**.Effettua i cambiamenti necessari nella finestra di configurazione.

### 8.1.5. Filtro categorie

Il Filtro categorie filtra dinamicamente l'accesso ai siti web in base ai loro contenuti.Attivando il Controllo genitori e impostando l'età dei bambini, il Filtro categorie viene configurato automaticamente per bloccare l'accesso alle categorie di siti web considerati inappropriati per l'età dei bambini.Questa configurazione è adatta alla maggior parte dei casi.

Se desideri controllare maggiormente i contenuti Internet a cui i bambini possono accedere, puoi selezionare quali categorie di siti web bloccare con il Filtro categorie.

Per controllare e configurare in dettaglio le impostazioni del Filtro categorie per un determinato account utente, segui questi passaggi:

1. Accedi alla finestra delle impostazioni del Controllo genitori di Bitdefender per quell'account utente.
2. Clicca sulla scheda **Categorie**.
3. Il Controllo categorie è attivato di default. Anche se non consigliato, puoi scegliere di disattivare il Controllo categorie e configurare autonomamente un elenco di determinati siti web da bloccare usando il Controllo web.
4. Puoi verificare quali categorie web sono bloccate automaticamente o limitate per il gruppo d'età attualmente selezionato.Per esempio, se lo stato della categoria Motori di ricerca è **Bloccato**, il bambino non potrà usare alcun motore di ricerca.Se non sei soddisfatto delle impostazioni di default, puoi configurarle a tuo piacimento.

   Per modificare l'azione configurata per una categoria specifica di contenuti web, clicca sullo stato attuale e seleziona l'azione desiderata dal menu.

## 8.2. Monitorare le attività dei bambini

Bitdefender permette di controllare ciò che fanno i bambini al computer anche quando non sei presenti.

Di norma, quando il Controllo genitori è abilitato, le attività dei bambini vengono annotate. In questo modo, puoi sempre scoprire esattamente quali siti web hanno visitato, quali applicazioni hanno usato e quali attività sono state bloccate dal Controllo genitori.

Puoi anche configurare Bitdefender per inviare notifiche via e-mail ogni volta che il Controllo genitori blocca un'attività.

### 8.2.1. Verificare i registri del Controllo genitori

Per verificare le attività recenti dei bambini sul computer, accedi ai registri del Controllo genitori.Attenersi alla seguente procedura:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Eventi** nella barra degli strumenti superiore.
3. Clicca su **Controllo genitori** sul menu a sinistra.

Nota

Se non condividi il computer con i bambini, puoi configurare la rete domestica di Bitdefender in modo da accedere in remoto ai registri del Controllo genitori (dal tuo computer).Per ulteriori informazioni fare riferimento a «*Mappa di rete*» (p. 104).

I rapporti del Controllo genitori forniscono informazioni dettagliate riguardo l'attività dei bambini sul computer e internet.Le informazioni sono organizzate in diverse tabelle:

**Eventi**

Ti aiuta a trovare informazioni dettagliate sull'attività di Controllo genitori (per esempio, quando il Controllo genitori è stato attivato / disattivato, quali eventi sono stati bloccati).

Clicca su un evento per visualizzare maggiori dettagli al riguardo.

**Uso applicazione**

Ti aiuta a scoprire le applicazioni usate di recente dai bambini.

Puoi filtrare le informazioni in base all'utente e il periodo.Clicca su un evento per visualizzare maggiori dettagli al riguardo.

**Rapporto Internet**

Ti aiuta a scoprire quali siti web i tuoi bambini hanno visitato di recente.

Puoi filtrare le informazioni in base all'utente e il periodo.Clicca su un evento per visualizzare maggiori dettagli al riguardo.

### 8.2.2. Configurare le notifiche e-mail

Per ricevere e-mail di notifica quando il Controllo genitori blocca un'attività:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Controllo genitori** nel menu di sinistra e poi sulla scheda **Impostazioni**.
4. Attiva l'opzione **Invia notifiche attività via e-mail** usando l'interruttore corrispondente.

5. Ti sarà richiesto di configurare le impostazioni dell'account e-mail. Clicca su **Sì** per aprire la finestra di configurazione.

   Nota
   Puoi aprire la finestra di configurazione in un secondo momento cliccando su **Impostazioni notifiche**.

6. Inserisci l'indirizzo e-mail in cui vuoi ricevere le notifiche e-mail.
7. Configura le impostazioni e-mail del server usato per inviare le notifiche relative alle e-mail.Ci sono tre opzioni per configurare le impostazioni e-mail:

   **Usa le impostazioni del client mail corrente**
   Questa opzione è selezionata di norma quando Bitdefender riesce a importare le impostazioni del server mail dal tuo client di posta.

   **Selezionale da uno dei server conosciuti**
   Seleziona questa opzione se hai un account e-mail con uno dei servizi e-mail Internet nell'elenco.

   **Desidero configurare da solo le impostazioni del server**
   Se conosci le impostazioni del server mail, seleziona questa opzione e configura le impostazioni come segue:

   - **Server SMTP in Uscita** - digita l'indirizzo del server di posta utilizzato per inviare i messaggi e-mail.
   - Se il server usa una porta diversa rispetto alla porta 25 predefinita, digita il numero della porta nel campo corrispondente.
   - Se il server richiede l'autenticazione, seleziona la casella di controllo **Il mio server SMTP richiede l'autenticazione** e digita il nome utente e la password nei campi corrispondenti.
   - Se il server richiede una connessione sicura SSL, seleziona la casella **Usa SSL**.

8. Clicca su **Test settaggi** per confermare le impostazioni. Se durante la conferma dovessi rilevare qualche problema, ti sarà comunicato cosa fare per risolverlo.
9. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

## 8.3. Controllo genitori remoto

Il Controllo genitori remoto ti consente di monitorare le attività dei bambini e cambiare le impostazioni del Controllo genitori, anche quando non sei a casa.Tutto ciò che ti serve è un computer con accesso a Internet e un browser web.

Il Controllo genitori remoto offre un buon metodo per controllare ciò che i bambini fanno online, senza essere invadenti.

### 8.3.1. Prerequisiti per l'uso del Controllo genitori remoto

Per usare il Controllo genitori remoto, i seguenti prerequisiti devono essere soddisfatti:

1. Installa Bitdefender Internet Security 2012 o Bitdefender Total Security 2012 sul computer dei bambini.
2. Assicurati di completare la registrazione del prodotto associando il tuo prodotto a un account MyBitdefender.Per ulteriori informazioni fare riferimento a «*Registrazione del prodotto*» (p. 8).
3. Attiva il Controllo genitori remoto.
4. Il computer dal quale vuoi accedere al Controllo genitori remoto deve essere connesso a Internet.

### 8.3.2. Attivazione Controllo genitori remoto

Per attivare il Controllo genitori remoto:

1. Accedi al computer su cui è installato Bitdefender usando un account da amministratore.Puoi usare lo stesso account che hai usato per installare il programma.
2. Apri la finestra di Bitdefender.
3. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
4. Clicca su **Controllo genitori** nel menu di sinistra e poi sulla scheda **Impostazioni**.
5. Attiva il Controllo genitori remoto usando l'interruttore corrispondente.Il Controllo genitori remoto sarà attivato per tutti gli account utente sul sistema.

### 8.3.3. Accesso Controllo genitori remoto

Puoi accedere al Controllo genitori remoto accedendo al tuo account di MyBitdefender.

1. Su un computer con accesso a Internet, apri un browser web e vai a:

   https://my.bitdefender.com
2. Accedi al tuo account usando il tuo nome utente e la password.
3. Nel pannello Servizi, clicca su **Assistenza per genitori** per accedere alla dashboard del Controllo genitori remoto.
4. Puoi vedere tutti i tuoi computer su cui è attivo il Controllo genitori remoto e i rispettivi account.Per ogni account utente sono disponibili tre pulsanti:

   - **Avvisi** - Per controllare quali attività sono state bloccate dal rispettivo account dal tuo ultimo accesso.

- **Attività** - Per controllare le attività recenti dei bambini.
- **Impostazioni** - Per cambiare le impostazioni del Controllo genitori per il rispettivo account utente.

Cliccando su uno di questi pulsanti aprirai la pagina del Controllo genitori remoto di quell'account utente.

### 8.3.4. Monitorare in remoto le attività dei bambini

Prima di poter monitorare in remoto le attività sul computer e in Internet dei bambini, devi attivare il Controllo genitori remoto sul loro computer.Per ulteriori informazioni fare riferimento a «*Attivazione Controllo genitori remoto*» (p. 90).

Per verificare in remoto cosa stanno facendo i bambini sul computer:

1. Su un computer con accesso a Internet, apri un browser web e vai a:

   https://my.bitdefender.com

2. Accedi al tuo account usando il tuo nome utente e la password.
3. Nel pannello Servizi, clicca su **Assistenza per genitori** per accedere alla dashboard del Controllo genitori remoto.
4. Trova l'account usato dal bambino e clicca su uno di questi pulsanti:
   - **Avvisi** - Per controllare quali attività sono state bloccate dal rispettivo account dal tuo ultimo accesso.
   - **Attività** - Per controllare le attività recenti dei bambini.

Nella pagina degli avvisi, puoi scoprire quali siti web, applicazioni o contatti chat sono stati bloccati dal tuo ultimo accesso.Per rimuovere una restrizione, clicca sul pulsante **Consenti** corrispondente.

Nella pagina Attività, puoi trovare informazioni utili sulle attività recenti dei bambini:

- che sono i siti web più visitati e più bloccati.
- che sono le applicazioni più eseguite e più bloccate.
- che sono gli ID chat più contattati e più bloccati.

Puoi bloccare direttamente un sito web, un'applicazione o un ID chat cliccando sul collegamento **Blocca** corrispondente.

Per filtrare i dati visualizzati, clicca sul menu **Mostra** e seleziona l'opzione desiderata.

### 8.3.5. Modificare in remoto le impostazioni del Controllo genitori

Prima di poter cambiare in remoto le impostazioni del Controllo genitori configurate per i bambini, devi attivare il Controllo genitori remoto sul loro computer.Per ulteriori informazioni fare riferimento a «*Attivazione Controllo genitori remoto*» (p. 90).

Per modificare in remoto le impostazioni del Controllo genitori:

1. Su un computer con accesso a Internet, apri un browser web e vai a:

   https://my.bitdefender.com

2. Accedi al tuo account di Bitdefender usando il tuo nome utente e la password.
3. Nel pannello Servizi, clicca su **Assistenza per genitori** per accedere alla dashboard del Controllo genitori remoto.Puoi visualizzare tutti gli account utente per i quali è attivo il Controllo genitori remoto.
4. Trova l'account usato dal bambino e clicca su uno di questi pulsanti:
   - **Avvisi** - Per controllare l'elenco delle attività bloccate di recente e rimuovere le restrizioni.
   - **Attività** - Per monitorare le attività recenti dei bambini e bloccare quelle non desiderate.
   - **Impostazioni** - Per cambiare le impostazioni del Controllo genitori per il rispettivo account utente.
5. Imposta e rimuove le restrizioni in base alle esigenze.

## Limitare gli intervalli di accesso a Internet

Puoi specificare quando è consentito al bambino di accedere a Internet usando le opzioni del **Programma accesso web** nella pagina **Impostazioni**.

Per limitare l'accesso a Internet in determinati momenti della giornata:

1. Seleziona dalla griglia gli intervalli di tempo durante i quali bloccare l'accesso a Internet.Per avviare una nuova selezione, clicca su **Blocca tutto** o su **Permetti tutto**.
2. Clicca su **Salva**.

Per bloccare completamente l'accesso a Internet, clicca sul collegamento **Blocca tutto** sotto alla tabella degli orari e poi su **Salva**.

I cambiamenti saranno configurati e applicati al computer del bambino dopo la prossima sincronizzazione con il sito web del Controllo genitori remoto (entro un massimo di 10 minuti).

## Bloccare siti web

Per bloccare un sito web:

1. Vai alla pagina **Impostazioni**.
2. Inserisci il sito web nel campo corrispondente.
3. Clicca su **Invia**.Il sito web sarà aggiunto all'elenco delle azioni in sospeso.Se cambiassi idea, clicca sul pulsante **Annulla azione** corrispondente.

Nota

In alternativa, puoi andare alla pagina **Attività**, controllare l'elenco dei siti web visitati e cliccare sul pulsante **Blocca** corrispondente, se vuoi bloccare un sito web.

La regola sarà configurata e applicata al computer del bambino dopo la prossima sincronizzazione con il sito web del Controllo genitori remoto (entro un massimo di 10 minuti).

## Bloccare i contatti chat

Per bloccare i messaggi istantanei con un contatto specifico:

1. Vai alla pagina **Impostazioni**.
2. Inserisci l'ID chat nel campo corrispondente.
3. Clicca su **Blocca**.L'ID chat sarà aggiunta all'elenco delle azioni in sospeso.Se cambiassi idea, clicca sul pulsante **Annulla azione** corrispondente.

Nota

In alternativa, puoi andare alla pagina **Attività**, controllare l'elenco dei contatti chat con cui il bambino ha chattato e cliccare sul pulsante **Blocca** corrispondente quando trovi un contatto indesiderato.

La regola sarà configurata e applicata al computer del bambino dopo la prossima sincronizzazione con il sito web del Controllo genitori remoto (entro un massimo di 10 minuti).

## Bloccare le applicazioni

Per bloccare un'applicazione:

1. Vai alla pagina **Attività**.
2. Controlla la lista delle applicazioni eseguite e clicca sul pulsante **Blocca** corrispondente quando trovi un'applicazione non desiderata.

La regola sarà configurata e applicata al computer del bambino dopo la prossima sincronizzazione con il sito web del Controllo genitori remoto (entro un massimo di 10 minuti).

## Sbloccare siti web, applicazioni o contatti chat

La pagina Avvisi mostra i siti web, le applicazioni e gli ID chat che sono stati bloccati dal Controllo genitori.Per rimuovere una restrizione, clicca sul pulsante **Consenti** corrispondente.La restrizione sarà rimossa dal computer del bambino dopo la prossima sincronizzazione con il sito web del Controllo genitori remoto (entro un massimo di 10 minuti).

# 9. Firewall

Il Firewall protegge il computer da connessioni interne o esterne non autorizzate.È abbastanza simile a una guardia a un cancello: tiene traccia dei tentativi di connessione e decide chi far entrare e chi bloccare.

Nota

Un firewall è essenziale se disponi di una connessione a banda larga o ADSL.

Se il computer ha Windows Vista o Windows 7, Bitdefender assegna automaticamente un tipo di rete a ogni nuova connessione di rete che rileva.Su computer con Windows XP, ti sarà chiesto di selezionare il tipo di rete.Per scoprire altre informazioni sulle impostazioni del firewall per ogni tipo di rete e come modificare le impostazioni della rete, fai riferimento a «*Configurare le impostazioni di connessione della rete*» (p. 95).

Il firewall di Bitdefender utilizza un set di regole per filtrare i dati trasmessi al e dal sistema.Le regole sono suddivise in 3 categorie:

Regole generali

Regole che determinano i protocolli tramite i quali sono consentite le comunicazioni.

Viene usato un set di regole predefinito che fornisce una protezione ottimale.Puoi modificare le regole, consentendo o negando le connessioni su determinati protocolli.

Regole applicazione

Le regole che determinano come ogni applicazione può accedere alle risorse di rete e a Internet.

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

Regole adattatore

Regole che determinano se il computer può comunicare con determinati altri computer.

Devi creare regole per consentire o bloccare il traffico specifico.

Una protezione aggiuntiva è fornita dal Sistema di rilevazione intrusioni (IDS).IDS monitora la rete e le attività del sistema per rilevare attività pericolose o violazione delle policy.Può rilevare e bloccare tentativi di modificare i file critici di sistema, i file di Bitdefender o le voci del registro, l'installazione di driver malware e gli attacchi eseguiti con l'inserimento di codice (inserimento di DLL).

Bitdefender di norma è configurato per intraprendere automaticamente le azioni consigliate per la tua protezione, senza importunarti. Se desideri essere informato

e decidere la migliore azione da intraprendere quando un'applicazione richiede l'accesso a Internet o mostra un comportamento sospetto, devi attivare la modalità Paranoid.

## 9.1. Attivare o disattivare la protezione del firewall

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

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Firewall**.
3. Clicca sull'interruttore firewall.

Avvertimento

Perché espone il tuo computer a connessioni non autorizzate, disattivare il firewall dovrebbe essere solo una misura temporanea.Riattiva il firewall il prima possibile.

## 9.2. Configurare le impostazioni di connessione della rete

Per visualizzare e modificare le impostazioni di connessione della rete, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Firewall**.
3. Clicca su **Dettagli rete**.

Comparirà una nuova finestra.Il grafico nella parte superiore della finestra mostra informazioni in tempo reale sul traffico in entrata e in uscita.

Sotto al grafico, per ogni connessione di rete sono mostrate le seguenti informazioni.

- **Tipo di rete** - il tipo di rete a cui è connesso il tuo computer.Bitdefender applica un set base di impostazioni del firewall secondo il tipo di rete a cui sei connesso.

  Puoi cambiare il tipo, aprendo il menu a tendina **Tipo di rete** e selezionare uno dei tipi disponibili dall'elenco.

| Tipo di rete | Descrizione |
|---|---|
| **Di fiducia** | Disabilita il firewall per il relativo adattatore. |
| **Casa/Ufficio** | Consente tutto il traffico tra il tuo computer e quelli nella rete locale. |
| **Pubblica** | Tutto il traffico viene filtrato. |
| **Non sicura** | Blocca completamente la rete e il traffico Internet attraverso il relativo adattatore. |

- **Modalità invisibile** - se si può essere rilevati da altri computer o meno.

  Per configurare la modalità mascheramento clicca sulla freccia dalla colonna **Modalità mascheramento** e seleziona l'opzione desiderata.

| Opzione Invisibile | Descrizione |
|---|---|
| **Attiva** | La Modalità Invisibile è attiva.Il tuo computer è invisibile sia dalla rete locale che da Internet. |
| **Inattiva** | La Modalità Invisibile è disattivataTutti possono pingare e rilevare il tuo computer dalla rete locale o da Internet. |
| **Remoto** | Il tuo computer non può essere rilevato da Internet.Gli utenti della rete locale possono pingare e rilevare il tuo computer. |

- **Generico** - se delle regole generiche vengono applicate a questa connessione.

  Se l'indirizzo IP dell'adattatore di rete è stato cambiato, Bitdefender modifica il tipo di rete di conseguenza.Se desideri mantenere la stessa tipologia, clicca sulla freccia dalla colonna **Generico** e seleziona **Sì**.

## 9.3. Sistema di rilevazione intrusioni

Per configurare il Sistema di rilevazione intrusioni, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Firewall** nel menu di sinistra e poi sulla scheda **Impostazioni**.
4. Per attivare il Sistema di rilevazione intrusioni, clicca sull'interruttore corrispondente.
5. Trascina il pulsante scorrevole lungo la barra per impostare il livello di aggressività desiderato.Usa la descrizione sul lato destro dell'ordine per selezionare il livello di protezione che si adatta meglio alle tue necessità di sicurezza.

Puoi verificare quali applicazioni sono state rilevate dal Sistema di rilevazione intrusioni nella finestra Eventi.

Se ci sono applicazioni di cui ti fidi e non vuoi che il Sistema di rilevazione intrusioni le controlli, puoi aggiungere delle regole di eccezione per loro.Per escludere un'applicazione dalla scansione, segui i passaggi descritti nella sezione *«Gestire i processi esclusi»* (p. 58).

Nota

Il funzionamento del Sistema di rilevazione intrusioni è legato a quello dell'Active Virus Control.Le regole di eccezione per il processo si applicano a entrambi i sistemi.

## 9.4. Configurare impostazioni traffico

Per configurare le impostazioni del traffico, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Firewall** nel menu di sinistra e poi sulla scheda **Impostazioni**.

Le seguenti caratteristiche possono essere attivate o disattivate nella sezione **Traffico**.

- **Abilita il supporto condivisione connessione Internet (ICS)** - abilita il supporto per la condivisione della connessione Internet (ICS).

  Nota

  Questa opzione non abilita automaticamente ICS sul sistema, ma consente solo questo tipo di connessione nel caso tu la abilitassi dal tuo sistema operativo.

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

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

- **Aumenta la verbosità del registro** - aumenta la verbosità del registro del firewall.

  Bitdefender conserva un registro esauriente di eventi riguardanti l'utilizzo del modulo Firewall (attivare/disattivare il firewall, bloccare il traffico, modificare le impostazioni) o generati dalle attività rilevate da questo modulo (scansione delle porte, blocco di tentativi di connessione o del traffico secondo le regole).Puoi accedere al registro dalla finestra **Attività firewall** cliccando su **Rapporto**.

- **Monitora connessioni Wi-Fi** - se si è connessi a una rete wireless, mostra delle finestre informative relative a determinati eventi sulla rete (ad esempio, quando un nuovo computer accede alla rete).

## 9.5. Regole generali

Ogni volta che si trasmettono dati su Internet, sono usati determinati protocolli.

Le regole generali ti consentono di configurare i protocolli su cui è consentito il traffico.Per modificare le regole, segui questi passaggi:

1. Apri la finestra di Bitdefender.

2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Firewall** nel menu di sinistra e poi sulla scheda **Avanzate**.
4. Nelle regole del firewall, clicca su **Regole generali**.

Comparirà una nuova finestra.Sono mostrate le regole attuali.

Per modificare una regola, clicca sulla sua freccia corrispondente nella colonna **Azione** e seleziona **Consenti** o **Nega**.

**DNS su UDP / TCP**
Consenti o blocca DNS su UDP e TCP.

Di norma, questo tipo di connessione è consentita.

**ICMP / ICMPv6 in ingresso**
Consenti o blocca i messaggi ICMP / ICMPv6.

I messaggi ICMP sono spesso usati dagli hacker per eseguire attacchi contro le reti informatiche.Di norma, questo tipo di connessione è bloccata.

**Inviare e-mail**
Consenti o blocca l'invio di e-mail via SMTP.

Di norma, questo tipo di connessione è consentita.

**Navigazione web HTTP**
Consenti o blocca la navigazione web HTTP.

Di norma, questo tipo di connessione è consentita.

**Connessioni desktop remote in ingresso**
Consenti o blocca l'accesso ad altri computer alle connessioni desktop remote.

Di norma, questo tipo di connessione è consentita.

**Traffico Windows Explorer su HTTP / FTP**
Consenti o blocca il traffico HTTP e FTP da Windows Explorer.

Di norma, questo tipo di connessione è bloccata.

## 9.6. Regole applicazione

Per visualizzare e gestire le regole del firewall che controllano l'accesso delle applicazioni alle risorse di rete e a Internet, clicca su **Regole applicazione**.

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Firewall** nel menu di sinistra e poi sulla scheda **Avanzate**.
4. Nelle regole del Firewall, clicca su **Regole applicazione**.

Puoi visualizzare i programmi (processi) per i quali sono state create le regole del firewall nella tabella.Per vedere le regole create per un'applicazione specifica, clicca

sulla casella + accanto alla relativa applicazione o semplicemente cliccaci sopra due volte.

Per ogni regola sono visualizzate le seguenti informazioni:

- **Tipologie di processo/rete** - le tipologie di processo e adattatore di rete sulle quali vengono applicate le regole.Le regole sono create automaticamente per filtrare l'accesso alla rete o a Internet attraverso tutti gli adattatori.Puoi creare nuove regole manualmente o modificare regole esistenti per filtrare l'accesso alla rete o a Internet di un'applicazione attraverso un adattatore specifico (ad esempio, un adattatore di rete wireless).
- **Protocollo** - il protocollo IP al quale si applica la regola.Potrai visualizzare uno dei seguenti:

| Protocollo | Descrizione |
|---|---|
| **Qualsiasi** | Include tutti i protocolli IP. |
| **TCP** | Transmission Control Protocol – Il Protocollo TCP abilita due host a stabilire una connessione e a scambiarsi pacchetti di dati. TCP garantisce la consegna dei dati e anche le garanzie che i pacchetti saranno consegnati nello stesso ordine in cui sono stati inviati. |
| **UDP** | User Datagram Protocol – UDP è un IP progettato per prestazioni hig. I giochi e altre applicazioni video utilizzano spesso UDP. |
| **Un numero** | Rappresenta un protocollo IP specifico (diverso da TCP e UDP).Puoi trovare l'elenco completo dei numeri di protocolli IP assegnati su http://www.iana.org/assignments/protocol-numbers. |

- **Azione** - se all'applicazione è permesso o vietato l'accesso alla rete o a Internet sotto le circostanze specificate.

Per gestire le regole, usa i pulsanti nella parte inferiore della finestra:

- **Aggiungi regola** - apre la finestra Aggiungi regola applicazione, dove puoi creare una nuova regola.
- **Modifica regola** - apre la finestra Modifica regola applicazione dove puoi modificare le impostazioni di una regola selezionata.
- **Rimuovi regola** - elimina la regola selezionata.

## Aggiungere / modificare le regole applicazione

Per aggiungere o modificare una regola applicazione, clicca sul pulsante corrispondente.Comparirà una nuova finestra. Procedi come segue:

- **Percorso del Programma.** Clicca su **Sfoglia** e seleziona l'applicazione sulla quale applicare la regola.

- **Indirizzo Locale.** Specifica l'indirizzo IP locale e la porta sui quali sarà applicata la regola.Se hai più di un adattatore di rete, puoi deselezionare la casella **Qualsiasi** e digitare un indirizzo IP specifico.
- **Indirizzo Remoto.** Specifica l'indirizzo IP remoto e la porta sui quali sarà applicata la regola.Per filtrare il traffico tra il tuo computer e un computer specifico, deseleziona la casella **Qualsiasi** e digita il suo indirizzo IP.
- **Tipo di rete.** Seleziona il tipo di rete a cui si applica la regola.
- **Eventi.** In base al protocollo selezionato, scegli gli eventi di rete sui quali la regola sarà applicata.I seguenti eventi possono essere tenuti in conto:

| Evento | Descrizione |
|---|---|
| **Connessione** | Scambio preliminare di messaggi standard usati da protocolli orientati alla connessione (come il TCP) per stabilire una connessione.Con protocolli orientati alla connessione, il traffico di dati tra due computer accade solo dopo che la connessione è stabilita. |
| **Traffico** | Flusso di dati tra due computer. |
| **In ascolto** | Stato in cui un'applicazione monitorizza la rete in attesa di stabilire una connessione o di ricevere informazioni da un'applicazione pari. |

- **Protocollo.** Seleziona dal menu il protocollo IP sul quale la regola sarà applicata.
  - Se desideri che la regola venga applicata a tutti i protocolli, seleziona **Qualsiasi**.
  - Se desideri che la regola venga applicata a TCP, seleziona **TCP**.
  - Se desideri che la regola venga applicata a UDP, seleziona **UDP**.
  - Se desideri che la regola venga applicata su un protocollo specifico, seleziona **Altro**.Comparirà un campo di modifica.Digita il numero assegnato al protocollo che desideri filtrare nel campo di modifica.

Nota

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

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

| Direzione | Descrizione |
|---|---|
| **In uscita** | La regola sarà applicata solo per il traffico in uscita. |

| Direzione | Descrizione |
|---|---|
| **In entrata** | La regola sarà applicata solo per il traffico in entrata. |
| **Entrambi** | La regola sarà applicata in entrambe le direzioni. |

- **Versione IP.** Seleziona dal menu la versione IP (IPv4, IPv6 o altre) alla quale sarà applicata la regola.
- **Autorizzazione.** Seleziona uno dei permessi disponibili:

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

## 9.7. Regole adattatore

Per ogni connessione di rete puoi configurare zone sicure e non sicure.

Una zona di fiducia è un dispositivo di cui ti fidi completamente, per esempio un computer o una stampante.Tutto il traffico tra il computer e un dispositivo affidabile è consentito.Per condividere delle risorse con un computer specifico in una rete wireless non sicura, aggiungerli come computer consentiti.

Una zona non sicura è un dispositivo con cui non vuoi proprio comunicare.

Per visualizzare e gestire le zone sui tuoi adattatori di rete, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Firewall** nel menu di sinistra e poi sulla scheda **Avanzate**.
4. Nelle regole del Firewall, clicca su **Regole adattatore**.

Comparirà una nuova finestra.Le zone di rete attuali sono mostrate in base all'adattatore.

Per gestire le zone, usa i pulsanti nella parte superiore della finestra:

- **Agg. zona** - apre la finestra Aggiungi indirizzo IP, dove puoi creare una nuova zona per un adattatore selezionato.
- **Modifica zona** - apre la finestra Modifica regola dove puoi modificare le impostazioni di una zona selezionata.
- **Rimuovi zona** - elimina la zona selezionata.

### Aggiungere / modificare le zone

Per aggiungere o modificare una zona, clicca sul pulsante corrispondente.Comparirà una nuova finestra con gli indirizzi IP dei dispositivi connessi alla rete.Procedi come segue:

1. Seleziona l'indirizzo IP del computer che vuoi aggiungere o digita un indirizzo o un intervallo di indirizzi nella casella di testo.
2. Seleziona l'azione:
   - **Consenti** - per consentire tutto il traffico tra il tuo computer e quello selezionato.
   - **Rifiuta** - per bloccare tutto il traffico tra il tuo computer e quello selezionato.
3. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

## 9.8. Monitorare le attività della rete

Per monitorare l'attività della rete / Internet corrente (su TCP e UDP) ordinata per applicazioni e aprire il registro del firewall di Bitdefender, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Firewall** nel menu di sinistra e poi sulla scheda **Avanzate**.
4. In Attività di rete, clicca su **Attività firewall**.

Comparirà una nuova finestra.Puoi visualizzare il traffico totale generato dall'applicazione. Per ogni applicazione, puoi visualizzare le connessioni e le porte aperte, così come le statistiche riguardanti la velocità del traffico in uscita e in entrata e la quantità totale di dati inviati / ricevuti.

Accanto a ogni connessione è indicata un'icona.Il significato delle icone è come segue:

- Indica una connessione in uscita.
- Indica una connessione in entrata.
- Indica una porta aperta sul tuo computer.

La finestra presenta l'attività della rete corrente / Internet in tempo reale. Se le connessioni o le porte fossero chiuse, potreste vedere che le statistiche corrispondenti sarebbero opache e che, alla fine, scomparirebbero.La stessa cosa accade a tutte le statistiche corrispondenti a un'applicazione che genera traffico o ha delle porte aperte e che tu chiudi.

Per un elenco esauriente di eventi riguardanti l'utilizzo del modulo Firewall (abilitare/disabilitare il firewall, bloccare il traffico, modificare le impostazioni) o generati dalle attività rilevate da questo modulo (scansione delle porte, blocco di

tentativi di connessione o del traffico secondo le regole), visualizza il file di rapporto del firewall Bitdefender cliccando su **Rapporto**.L'ubicazione del file del registro è `?\Programmi\File comuni\Bitdefender\Bitdefender Firewall\bdfirewall.txt`.

## 9.9. Usare la modalità Paranoid

Bitdefender Internet Security 2012 è stato progettato per essere il meno invadente possibile.In condizioni normali, non devi decidere se consentire o bloccare connessioni o azioni intraprese da applicazioni in esecuzione sul tuo sistema.Bitdefender prenderà tutte le decisioni per te.

Se desideri avere il controllo completo delle decisioni intraprese, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Firewall** nel menu di sinistra e poi sulla scheda **Avanzate**.
4. Attiva la **modalità Paranoid** cliccando sull'interruttore corrispondente.

Finché la modalità Paranoid è attiva, ogni volta che si verifica una delle seguenti situazioni ti sarà chiesto come comportarti:

- Un'applicazione tenta di connettersi a Internet.
- Un'applicazione prova a eseguire un'azione considerata sospetta dal Sistema di rilevazione intrusioni o da Active Virus Control.

L'avviso contiene informazioni relative all'applicazione e al comportamento rilevato.Devi selezionare **Consenti** o **Nega** usando il pulsante corrispondente.

# 10. Mappa di rete

Il modulo Rete ti permette di gestire i prodotti Bitdefender installati sui computer di casa da un singolo computer.

Per essere in grado di gestire i prodotti Bitdefender installati sui computer di casa, devi seguire questi passaggi:

1. Attiva la rete di Bitdefender sul tuo computer.Imposta il tuo computer come **server**.
2. Vai su ogni computer che desideri gestire e aggiungere alla rete (imposta la password).Imposta ogni computer come **normale**.
3. Torna al tuo computer e aggiungi i computer che desideri gestire.

## 10.1. Attivare la rete di Bitdefender

Per attivare la rete di Bitdefender, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Mappa di rete** nel menu di sinistra.
4. Clicca su **Abilita rete**.Ti sarà chiesto di configurare la password di gestione per la mappa di rete.
5. Inserisci la stessa password in ognuno dei campi corrispondenti.
6. Imposta il ruolo del computer nella mappa di rete di Bitdefender:
   - **Computer server** - seleziona questa opzione sul computer che sarà usato per gestire tutti gli altri.
   - **Computer normale** - seleziona questa opzione sui computer che saranno gestiti dal server.
7. Clicca su **OK**.

   Puoi vedere il nome del computer comparire nella mappa di rete.

   Compare il pulsante **Disattiva connessione**.

Nota

Puoi anche attivare la mappa di rete dalla finestra principale di Bitdefender:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Mappa di rete**.
3. Clicca su **Gestisci** e seleziona **Attiva rete** dal menu a tendina.

## 10.2. Aggiungere computer alla rete di Bitdefender

Qualsiasi computer sarà aggiunto automaticamente alla rete se soddisfa i seguenti requisiti:

- la mappa di rete di Bitdefender è stata attivata.
- il ruolo è stato impostato su computer normale.
- la password impostata abilitando la rete è la stessa impostata dal computer server.

Nota

In qualsiasi momento puoi controllare la mappa di rete alla ricerca di computer che soddisfano i criteri cliccando sul pulsante **Trova automaticamente**.

Per aggiungere manualmente un computer alla mappa di rete di Bitdefender dal computer server, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Mappa di rete** nel menu di sinistra.
4. Clicca su **Aggiungi Computer**.
5. Digita la password di gestione e clicca su **OK**.Comparirà una nuova finestra.

   Puoi vedere l'elenco dei computer in questa rete.Il significato dell'icona è il seguente:

    Indica un computer online senza prodotti Bitdefender installati.

    Indica un computer online con Bitdefender installato.

    Indica un computer offline con Bitdefender installato.
6. Esegui una delle seguenti azioni:
   - Seleziona dall'elenco il nome del computer da aggiungere.
   - Digita l'indirizzo IP o il nome del computer da aggiungere nel campo corrispondente.
7. Clicca su **Aggiungi**.
8. Digita la password di gestione configurata sul rispettivo computer.
9. Clicca su **OK**.Se hai fornito la password corretta, il nome del computer selezionato comparirà nella mappa di rete.

## 10.3. Gestire la rete di Bitdefender

Una volta creata con successo una mappa di rete di Bitdefender, puoi gestire tutti i prodotti Bitdefender dal computer server.

Per eseguire più attività su tutti i computer in gestione, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Mappa di rete**.
3. Clicca su **Gestisci** e seleziona i pulsanti corrispondenti dal menu a tendina:
   - **Disattiva connessione** - Ti consente di disattivare la rete.
   - **Controlla tutto** - ti permette di eseguire la scansione contemporaneamente su tutti i computer gestiti.
   - **Aggiorna tutti i computer** - ti permette di aggiornare contemporaneamente tutti i computer gestiti.

Prima di eseguire un'attività su un particolare computer, ti sarà chiesto di fornire la password per la gestione locale.Digita la password di gestione e clicca su **OK**.

Per visualizzare l'intera Mappa di rete e accedere a tutte le attività di gestione, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Mappa di rete** nel menu di sinistra.

Se muovi il cursore su un computer nella mappa di rete, puoi vedere una breve informazione su di esso (indirizzo IP, numero di problemi che colpiscono la sicurezza del sistema, stato della registrazione di Bitdefender).

Se clicchi sul nome di un computer nella mappa di rete, puoi visualizzare tutte le funzioni di amministrazione che si possono eseguire sul computer remoto.

**Registra prodotto**
Permette di registrare Bitdefender sul computer inserendo un codice di licenza.

**Configura password per impost. prodotto**
Permette di creare una password per limitare l'accesso alle impostazioni Bitdefender sul PC.

**Esegui un'attività di scansione su richiesta**
Permette di eseguire una scansione su richiesta sul computer remoto. Puoi compiere una qualsiasi delle seguenti attività di scansione: Scansione veloce o Scansione completa del sistema.

**Risolvi ogni problema**
Permette di risolvere i problemi che influenzano la sicurezza del computer seguendo la procedura guidata della funzione Risolvi ogni problema.

**Aggiorna ora**
Avvia il processo di aggiornamento per il prodotto Bitdefender installato sul computer.

**Imposta profilo Controllo genitori**
Permette di impostare la categoria di età da usare per il filtro web del Controllo genitori su questo computer.

**Imposta come server di aggiorn. per questa rete**
Permette di impostare il computer come server di aggiornamento per tutti i prodotti Bitdefender installati sui computer della rete.Utilizzando questa opzione si ridurrà il traffico Internet, poiché un solo computer della rete si collegherà a Internet per scaricare gli aggiornamenti.

**Rimuovi PC dalla mappa di rete**
Permette di rimuovere il PC dalla rete.

Nota

Se programmi di eseguire più funzioni, puoi selezionare **Non mostrare di nuovo questo messaggio durante questa sessione**.Selezionando questa opzione non ti sarà più chiesta la password durante la sessione corrente.

# 11. Aggiorna

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

Se sei connesso a Internet con banda larga o ADSL, Bitdefender si prenderà cura di sé da solo. Di norma, esso cercherà aggiornamenti, ogni volta che avvierai il computer e ogni **ora**dopo l'avvio.Se viene rilevato un aggiornamento, questo è automaticamente scaricato e installato sul computer.

Il processo di aggiornamento è eseguito al volo, ciò significa che i file da aggiornare sono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto, nello stesso tempo, ogni vulnerabilità sarà 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. 36).
- Se non hai una connessione a Internet, puoi aggiornare Bitdefender manualmente, come descritto nella sezione *«Il mio computer non è connesso a Internet. Come posso aggiornare Bitdefender?»* (p. 119).Il file per l'aggiornamento manuale viene rilasciato una volta alla settimana.
- 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. 119).
- Se sei connesso a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di Bitdefender su richiesta dell'utente.Per ulteriori informazioni fare riferimento a *«Eseguire un aggiornamento»* (p. 109).

## 11.1. Verificare se Bitdefender è aggiornato

Per verificare se la protezione di Bitdefender è aggiornata, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Aggiorna**.
3. La data dell'ultimo aggiornamento è mostrata proprio sotto il nome del pannello.

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

1. Nella finestra principale, clicca su **Eventi** nella barra degli strumenti superiore.
2. Clicca su **Aggiorna** nel menu di sinistra.

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

## 11.2. Eseguire un aggiornamento

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

Per avviare un aggiornamento, esegui una delle seguenti operazioni:

- Apri la finestra di Bitdefender, vai al pannello **Aggiornamento** e clicca su **Aggiorna ora**.
- Clicca con il pulsante destro sull'icona di Bitdefender nella barra di sistema e seleziona **Aggiorna ora**.

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

Importante
Può essere necessario riavviare il computer una volta completato l'aggiornamento. Noi consigliamo di farlo il più presto possibile.

## 11.3. Attivare o disattivare l'aggiornamento automatico

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

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Aggiorna**.
3. Clicca sull'interruttore per attivare o disattivare l'Aggiornamento automatico.
4. Scegliendo di disattivare l'aggiornamento automatico, comparirà una finestra di avviso.Devi confermare la tua scelta selezionando dal menu per quanto tempo vuoi che l'aggiornamento automatico sia disattivato. Puoi disattivare l'aggiornamento automatico per 5, 15 o 30 minuti, per un'ora, permanentemente o fino al riavvio del sistema.

Avvertimento

Questa è una questione critica di sicurezza. Ti consigliamo di disattivare l'aggiornamento automatico per il minimo tempo possibile. Se Bitdefender non sarà aggiornato regolarmente non sarà in grado di proteggervi dalle minacce più recenti.

## 11.4. Modificare impostazioni 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. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Aggiorna** nel menu di sinistra.
4. Modifica le impostazioni in base alle tue preferenze.

### Ubicazione aggiornamento

Bitdefender è configurato per aggiornarsi dai server di aggiornamento di Bitdefender su Internet.L'ubicazione di aggiornamento è `http://upgrade.bitdefender.com`, 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).

Se a casa hai installato Bitdefender su più computer, puoi predisporre una rete domestica di Bitdefender e quindi designare uno dei computer come server di aggiornamento.Informazioni dettagliate sono fornite in «*Mappa di rete*» (p. 104). Il programma di Bitdefender installato sul server di aggiornamento designato sarà aggiornato tramite Internet. I programmi di Bitdefender sugli altri computer riceveranno gli aggiornamenti dal server di aggiornamento locale (la cui ubicazione sarà cambiata di conseguenza automaticamente).Questa configurazione è intesa a ridurre il traffico Internet e ottimizzare gli aggiornamenti.

Puoi tornare alla generica ubicazione di aggiornamento Internet cliccando su **Default**.

### Regole esecuzione aggiornamento

Puoi scegliere tra 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 eseguire il download.
- **Chiedi prima di installare** - ogni volta che si scarica un aggiornamento, ti sarà chiesto se 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.

## Aggiornamenti P2P

Oltre al normale meccanismo di aggiornamento, Bitdefender utilizza anche un sistema intelligente di condivisione dell'aggiornamento basato su un protocollo peer-to-peer (P2P) per distribuire gli aggiornamenti delle firme malware tra gli utenti di Bitdefender.

Puoi attivare o disattivare le opzioni di aggiornamento P2P usando gli interruttori corrispondenti.

**Usa sistema di aggiornamento P2P**
Attiva questa opzione per scaricare gli aggiornamenti delle firme malware da altri utenti di Bitdefender utilizzando il sistema di aggiornamento P2P.Bitdefender utilizza le porte 8880 - 8889 per gli aggiornamenti peer-to-peer.

**Distribuire i file di Bitdefender**
Attiva questa opzione per condividere le firme malware più recenti disponibili sul tuo computer con altri utenti di Bitdefender.

# 12. Protezione di Safego per social network

Ti fidi dei tuoi amici online.Ma ti fidi dei loro computer?Usa la protezione di Safego per social network per proteggere il tuo account e i tuoi amici dalle minacce online.

Safego è un'applicazione Facebook sviluppata da Bitdefender per tenere al sicuro il tuo account di social network.Il suo compito è controllare i link che ricevi dai tuoi amici Facebook e monitorare le impostazioni sulla privacy del tuo account.

Nota
Per usare questa caratteristica serve un account MyBitdefender.
Per ulteriori informazioni fare riferimento a *«Registrazione del prodotto»* (p. 8).

Queste sono le sue caratteristiche principali:

- controlla automaticamente i messaggi nelle tue notizie alla ricerca di link pericolosi.
- protegge il tuo account dalle minacce online.

  Quando rileva un post o un commento che non è nient'altro che spam, phishing o malware, riceverai un messaggio di avvertimento.
- avvisa i tuoi amici su eventuali link sospetti pubblicati nelle loro notizie.
- ti aiuta a costruire una rete sicura di amici usando la funzione **Friend'O'Meter**.
- ottieni un controllo dello stato di sicurezza del sistema fornito da Bitdefender QuickScan.

Per accedere a Safego dal tuo prodotto di Bitdefender, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Safego**.
3. Clicca su **Attiva**.Sarai indirizzato al tuo account.

   Se hai già attivato Safego, potrai accedere alle statistiche circa la sua attività, cliccando sul pulsante **Visualizza rapporti**.
4. Usa le tue informazioni di accesso a Facebook per connetterti all'applicazione Safego.
5. Consenti a Safego di accedere al tuo account Facebook.

# 13. Risoluzione dei problemi

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.



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 «*Supporto*» (p. 136).

## 13.1. 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 ulteriori informazioni fare riferimento a «*Come posso rimuovere le altre soluzioni di sicurezza?*» (p. 142).

- **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 ulteriori informazioni fare riferimento a «*Requisiti minimi di sistema*» (p. 1).

- **Le tue unità disco fisso sono troppo frammentate.**

  Un'eccessiva frammentazione rallenta l'accesso ai file e diminuisce le prestazioni del sistema.

  Per deframmentare il disco usando il tuo sistema operativo Windows, segui questo percorso dal menu start di Windows: **Start → Tutti i programmi → Accessori → Utilità di sistema → Utilità di deframmentazione dischi**.

## 13.2. 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:
     a. Vai a http://www.bitdefender.com/uninstall e scarica il programma di disinstallazione sul computer.
     b. Esegui il programma di disinstallazione utilizzando privilegi di amministratore.
     c. Riavvia il computer.
  2. Reinstalla Bitdefender sul sistema.

- **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 ulteriori informazioni fare riferimento a «*Come posso rimuovere le altre soluzioni di sicurezza?*» (p. 142).
  2. Rimuovi completamente Bitdefender dal sistema:
     a. Vai a http://www.bitdefender.com/uninstall e scarica il programma di disinstallazione sul computer.
     b. Esegui il programma di disinstallazione utilizzando privilegi di amministratore.
     c. Riavvia il computer.
  3. Reinstalla Bitdefender sul sistema.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 137).

## 13.3. 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.

Potresti imbatterti in 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 il modulo Active Virus Control per errore contrassegna alcune applicazioni come nocive.

L'Active Virus Control è un modulo di Bitdefender che monitora costantemente le applicazioni in esecuzione sul tuo sistema e segnala quelle con un comportamento potenzialmente maligno.Poiché questa opzione è basata su un sistema euristico, potrebbero verificarsi dei casi in cui applicazioni legittime siano rilevate dall'Active Virus Control.

Quando si verifica questa situazione, puoi escludere la rispettiva applicazione dal controllo dell'Active Virus Control.

Per aggiungere il programma all'elenco delle eccezioni, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **Eccezioni**.
4. Clicca sul collegamento **Processi esclusi**.Nella finestra che compare, puoi gestire le eccezioni del processo di Active Virus 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 l'opzione **Consenti** selezionata per impedire ad Active Virus 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. 137).

## 13.4. Non riesco a connettermi a Internet

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

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

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Firewall** nel menu di sinistra e poi sulla scheda **Avanzate**.
4. Nelle regole del Firewall, clicca su **Regole applicazione**.
5. Per aggiungere una regola applicazione, clicca sul pulsante corrispondente.
6. Clicca su **Sfoglia** e seleziona l'applicazione sulla quale applicare la regola.
7. Seleziona tutti i tipi di rete disponibili.
8. Vai ad **Autorizzazione** e seleziona **Consenti**.

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 137).

## 13.5. Non riesco ad accedere a un dispositivo nella mia rete

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

In questo caso, la miglior soluzione è configurare Bitdefender per consentire automaticamente le connessioni da e per il rispettivo dispositivo.Per ogni connessione di rete puoi configurare una speciale zona di fiducia.

Una zona di fiducia è un dispositivo del quale ti fidi completamente.Tutto il traffico tra il computer e un dispositivo affidabile è consentito.Per condividere le risorse con dispositivi specifici, come computer o stampanti, aggiungili alle zone sicure.

Per aggiungere una zona di fiducia ai tuoi adattatori di rete, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Firewall** nel menu di sinistra e poi sulla scheda **Avanzate**.
4. Nelle regole del Firewall, clicca su **Regole adattatore**.
5. Per aggiungere una zona, clicca sul pulsante corrispondente.Comparirà una nuova finestra con gli indirizzi IP dei dispositivi connessi alla rete.

6. Seleziona l'indirizzo IP del computer o della stampante che vuoi aggiungere o digita un indirizzo o un intervallo di indirizzi nella casella di testo.
7. Vai ad **Autorizzazione** e seleziona **Consenti**.

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

Controllare altre potenziali cause, ad esempio le seguenti:

- Il firewall su un altro computer potrebbe bloccare la condivisione di file e stampante con il tuo computer.
  - Se viene utilizzato il firewall di Windows, puoi configurarlo per permettere la condivisione di file e stampanti nel seguente modo: apri la finestra delle impostazioni di Windows Firewall, vai alla scheda **Eccezioni** e seleziona la casella **Condivisione file e stampanti**.
  - Se viene utilizzato un altro programma firewall, fare riferimento alla sua documentazione o al file della guida.
- Condizioni generiche che possono impedire l'utilizzo o la connessione a una stampante condivisa:
  - Potrebbe essere necessario accedere a un account di amministratore di Windows per poter accedere alla stampante condivisa.
  - Potrebbero essere state impostate delle autorizzazioni per la stampante condivisa che permettono l'accesso solo a specifici computer e utenti.Se stai condividendo la tua stampante, controlla le autorizzazioni impostate per la stampante per verificare che l'utente dell'altro computer sia autorizzato ad accedervi.Se stai provando a collegarti a una stampante condivisa, controlla insieme all'utente dell'altro computer di disporre delle autorizzazioni al collegamento alla stampante.
  - La stampante collegata al proprio computer o all'altro computer non è condivisa.
  - La stampante condivisa non è stata aggiunta al computer.

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

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 137).

## 13.6. Internet è lento

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

Per risolvere questa situazione, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Firewall** e clicca sull'interruttore per disattivarlo.
3. Verifica se la tua connessione a Internet è migliorata con il firewall di Bitdefender disattivato.
   - Se hai ancora una connessione a Internet lenta, il problema potrebbe non essere causato da Bitdefender. Contatta il tuo fornitore di servizi Internet per verificare se la connessione è attiva.

     Se ricevi conferma dal tuo fornitore di servizi Internet che la connessione è operativa e il problema persiste, contatta Bitdefender come descritto nella sezione «*Chiedere aiuto*» (p. 137).
   - Se la connessione a Internet è migliorata dopo aver disattivato il firewall di Bitdefender, segui questi passaggi:
     a. Apri la finestra di Bitdefender.
     b. Vai al pannello **Firewall** e clicca sull'interruttore per attivarlo.
     c. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
     d. Clicca su **Firewall** nel menu di sinistra e poi sulla scheda **Impostazioni**.
     e. Vai a **Condivisione connessione a Internet** e clicca sull'interruttore per attivarla.
     f. Vai a **Blocca port scan** e clicca sull'interruttore per disattivarlo.
     g. Clicca sul pulsante **Home** nella barra degli strumenti superiore.
     h. Vai al pannello **Firewall** e clicca su **Dettagli rete**.
     i. Vai a **Tipo di rete** e seleziona **Casa/Ufficio**.
     j. Vai a **Mod. mascheramento** e impostala su **Remoto**. Imposta l'opzione **Generico** su **Sì**.
     k. Chiudi Bitdefender, riavvia il sistema e verifica la velocità della connessione a Internet.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 137).

## 13.7. 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. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Aggiorna** nel menu di sinistra e poi sulla scheda **Aggiorna**.
4. Nell'opzione **Regole esecuzione aggiornamento**, seleziona **Chiedi prima di scaricare**.
5. Clicca sul pulsante **Home** nella barra degli strumenti superiore.
6. Vai al pannello **Aggiorna** e clicca su **Aggiorna ora**.
7. Seleziona solo **Aggiornamenti firme** e poi clicca su **OK**.
8. Bitdefender scaricherà e installerà solo gli aggiornamenti delle firme malware.

## 13.8. Il mio computer non è connesso a Internet. Come posso aggiornare Bitdefender?

Se il tuo computer non è connesso a Internet, devi scaricare manualmente gli aggiornamenti su un computer con accesso a Internet e poi trasferirli al tuo computer usando un dispositivo rimuovibile, come una chiavetta USB.

Attenersi alla seguente procedura:

1. Su un computer con accesso a Internet, apri un browser web e vai a:

   http://www.bitdefender.com/site/view/Desktop-Products-Updates.html

2. Nella colonna **Aggiornamento manuale**, clicca sul collegamento corrispondente all'architettura del tuo sistema e prodotto.Se non sai se la tua versione di Windows sia a 32 o 64 bit, fai riferimento a *«Sto usando una versione di Windows a 32 o 64 bit?»* (p. 143).
3. Salva il file chiamato `weekly.exe` sul sistema.
4. Trasferire il file scaricato su un dispositivo rimuovibile come una chiave USB, e poi al tuo computer.
5. Clicca due volte sul file e segui la procedura guidata.

## 13.9. 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 Bitdefender nella barra di sistema 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:

- Si sta installando un aggiornamento importante.
- 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. Riavvia il computer e aspetta alcuni attimi fino a quando Bitdefender è caricato. Apri Bitdefender per vedere se l'errore persiste.Riavviare il computer di solito risolve il problema.
3. Controlla che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di Bitdefender. Se così fosse, ti consigliamo di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente Bitdefender.

   Per ulteriori informazioni fare riferimento a «*Come posso rimuovere le altre soluzioni di sicurezza?*» (p. 142).

Se l'errore persiste, contatta i nostri operatori del supporto tecnico per ricevere assistenza, come indicato nella sezione «*Chiedere aiuto*» (p. 137).

## 13.10. Il filtro antispam non funziona correttamente

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

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

### 13.10.1. I messaggi legittimi sono contrassegnati come [spam]

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

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

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

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

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

   **Nota**

   Bitdefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo.Per un elenco completo di applicazioni di posta supportate, fare riferimento a *«Programmi e protocolli di posta elettronica supportati»* (p. 66).

2. Diminuisci il livello di protezione antispam. Diminuendo il livello di protezione, il filtro antispam avrà bisogno di maggiori indicazioni di spam per classificare un messaggio e-mail come spam.Utilizza questa soluzione solo se molti messaggi legittimi (inclusi i messaggi commerciali richiesti) vengono rilevati scorrettamente come spam.

#### Aggiungi contatti all'elenco Amici

Se stai utilizzando un'applicazione di posta supportata, puoi facilmente aggiungere i mittenti dei messaggi legittimi all'elenco amici.Attenersi alla seguente procedura:

1. Nell'applicazione di posta seleziona un messaggio e-mail inviato dal mittente che desideri aggiungere all'elenco Amici.
2. Clicca sul pulsante **Aggiungi Amico** sulla barra degli strumenti antispam di Bitdefender.

3. Può essere richiesto di accettare gli indirizzi aggiunti all'elenco Amici.Seleziona **Non mostrare di nuovo questo messaggio** e clicca su **OK**.

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

Se utilizzi un'applicazione di posta differente, puoi aggiungere i contatti all'elenco Amici dall'interfaccia di Bitdefender.Attenersi alla seguente procedura:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Antispam**.
3. Clicca su **Gestisci** e seleziona **Amici** dal menu.Apparirà la finestra di configurazione.
4. Digita l'indirizzo e-mail da cui vuoi sempre ricevere i messaggi e clicca su **Aggiungi**.Puoi aggiungere quanti indirizzi e-mail desideri.
5. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

## Indica errori di rilevamento

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

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

## Diminuisci il livello di protezione antispam

Per diminuire il livello di protezione antispam, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Vai a **Antispam** nel menu a sinistra.

4. Spostare il selettore verso il basso lungo la scala.

## 13.10.2. Molti messaggi spam non vengono rilevati

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

Prova le seguenti soluzioni:

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

   Nota

   Bitdefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo.Per un elenco completo di applicazioni di posta supportate, fare riferimento a «*Programmi e protocolli di posta elettronica supportati*» (p. 66).

2. Aggiungi spammer all'elenco Spammer. I messaggi e-mail ricevuti dagli indirizzi nell'elenco Spammer sono contrassegnati automaticamente come [spam].
3. Aumenta il livello di protezione antispam. Aumentando il livello di protezione, il filtro antispam avrà bisogno di minori indicazioni di spam per classificare un messaggio e-mail come spam.

### Indica messaggi spam non rilevati

Se utilizzi un client di posta supportato, puoi facilmente indicare quali messaggi e-mail sarebbero dovuti essere rilevati come spam. Facendo ciò si migliora considerevolmente l'efficienza del filtro antispam.Attenersi alla seguente procedura:

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

### Aggiungi spammer a elenco Spammer

Se stai utilizzando un'applicazione di posta supportata, puoi facilmente aggiungere i mittenti dei messaggi di spam all'elenco Spammer.Attenersi alla seguente procedura:

1. Apri il tuo client e-mail.
2. Vai alla cartella posta indesiderata, dove vengono spostati i messaggi spam.

3. Seleziona i messaggi contrassegnati come [spam] da Bitdefender.
4. Clicca sul pulsante **Aggiungi Spammer** sulla barra degli strumenti antispam di Bitdefender.
5. Può essere richiesto di accettare gli indirizzi aggiunti all'elenco degli Spammer.Seleziona **Non mostrare di nuovo questo messaggio** e clicca su **OK**.

Se stai utilizzando un'applicazione di posta differente, puoi aggiungere manualmente gli spammer all'elenco Spammer dall'interfaccia di Bitdefender. Si tratta di un metodo conveniente solo quando ricevi diversi messaggi spam dallo stesso indirizzo e-mail.Attenersi alla seguente procedura:

1. Apri la finestra di Bitdefender.
2. Vai al pannello **Antispam**.
3. Clicca su **Gestisci** e seleziona **Spammer** dal menu.Apparirà la finestra di configurazione.
4. Digita l'indirizzo e-mail dello spammer e poi clicca su **Aggiungi**.Puoi aggiungere quanti indirizzi e-mail desideri.
5. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

### Aumenta il livello di protezione antispam

Per aumentare il livello di protezione antispam, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Clicca su **Antispam** nel menu a sinistra.
4. Spostare il selettore verso l'alto lungo la scala.

## 13.10.3. Il Filtro antispam non rileva alcun messaggio spam

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

- La protezione antispam potrebbe essere disattivata.Per verificare lo stato di protezione antispam, apri la finestra Bitdefender e verifica l'interruttore nel pannello **Antispam**.

  Se l'antispam è disattivato, questa è la causa dei problemi.Clicca sull'interruttore per attivare o disattivare la protezione antispam.

- La protezione antispam di Bitdefender è disponibile solo per client e-mail configurati per ricevere messaggi e-mail tramite il protocollo POP3.Questo vuol dire che:

- I messaggi e-mail ricevuti tramite servizi e-mail web (ad esempio Yahoo, Gmail, Hotmail o altri) non sono filtrati per spam da Bitdefender.
- Se il tuo client e-mail è configurato per ricevere messaggi e-mail usando un protocollo diverso da POP3 (per esempio, IMAP4), il filtro antispam di Bitdefender non verifica se siano spam.

Nota

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

- Bitdefender Internet Security 2012 non esegue la scansione del traffico POP3 di Lotus Notes.

Una soluzione possibile consiste nel riparare o reinstallare il prodotto. Tuttavia puoi contattare Bitdefender per ricevere supporto, come descritto nella sezione «*Supporto*» (p. 136).

## 13.11. Rimozione di Bitdefender non riuscita

Questo articolo permette di risolvere gli errori che potrebbero verificarsi nella rimozione di Bitdefender.Vi sono due possibili situazioni:

- Durante la rimozione compare una schermata di errore.La schermata fornisce un pulsante per avviare uno strumento di disinstallazione che pulirà il sistema.
- La rimozione si blocca e il sistema potrebbe congelarsi.Clicca su **Annulla** per annullare la rimozione. Se non dovesse funzionare, riavvia 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:

1. Vai a http://www.bitdefender.com/uninstall e scarica il programma di disinstallazione sul computer.
2. Esegui il programma di disinstallazione utilizzando privilegi di amministratore.
3. Riavvia il computer.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 137).

## 13.12. 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 una 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. 143).
  2. Rimuovi Bitdefender dal tuo sistema:
     a. Vai a http://www.bitdefender.com/uninstall e scarica il programma di disinstallazione sul computer.
     b. Esegui il programma di disinstallazione utilizzando privilegi di amministratore.
     c. Riavvia il computer.
  3. Riavvia il sistema in modalità normale e reinstalla 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. 143).
  2. Rimuovi Bitdefender dal tuo sistema:
     a. Vai a http://www.bitdefender.com/uninstall e scarica il programma di disinstallazione sul computer.
     b. Esegui il programma di disinstallazione utilizzando privilegi di amministratore.
     c. Riavvia il computer.
  3. 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.
  4. 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. 143).
2. Usa l'opzione Ripristino configurazione di sistema di Windows per ripristinare il computer a uno stato precedente all'installazione del prodotto Bitdefender.Per scoprire come fare, fai riferimento a «*Come posso usare il Ripristino di sistema in Windows?*» (p. 144).
3. Riavvia il sistema in modalità normale e contatta i nostri operatori del supporto per assistenza, come indicato nella sezione «*Chiedere aiuto*» (p. 137).

# 14. 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. 128)
- «*Cosa fare quando Bitdefender trova dei virus sui tuoi computer?*» (p. 130)
- «*Come posso rimuovere un virus in un archivio?*» (p. 131)
- «*Come posso rimuovere un virus nell'archivio delle e-mail?*» (p. 132)
- «*Cosa fare se sospetti che un file possa essere pericoloso?*» (p. 133)
- «*Come pulire i file infetti in System Volume Information*» (p. 133)
- «*Quali sono i file protetti da password nel registro della scansione?*» (p. 134)
- «*Quali sono gli elementi ignorati nel registro della scansione?*» (p. 135)
- «*Quali sono i file supercompressi nel registro della scansione?*» (p. 135)
- «*Perché Bitdefender ha eliminato automaticamente un file infetto?*» (p. 135)

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 «*Supporto*» (p. 136).

## 14.1. 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 Internet Security 2012, 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:

Dalla finestra di Bitdefender

Per accedere direttamente alla Modalità soccorso da Bitdefender, segui questi passaggi:

1. Vai al pannello **Antivirus**.
2. Clicca su **Controlla ora** e seleziona **Modalità soccorso** dal menu a tendina.

Comparirà una finestra di conferma. Clicca su **Sì** per riavviare il computer.

3. Dopo il riavvio del computer, comparirà un menu che ti avvisa di selezionare un sistema operativo.Seleziona **Bitdefender Rescue Image** e premi il tasto **Invio** per avviare un ambiente di Bitdefender da cui poter pulire la tua partizione Windows.
4. 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.

Nota

Questo metodo non è disponibile sui computer con Windows XP.

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. 128).
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, comparirà 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.

## 14.2. 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 completa del sistema per analizzarlo.

Al termine della scansione completa, 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. Apri la finestra di Bitdefender.
   b. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
   c. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **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. 144).

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. 143).
2. Mostra gli elementi nascosti in Windows.
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. 137).

## 14.3. 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 completa del sistema.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Apri la finestra di Bitdefender.
   b. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
   c. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **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. 137).

## 14.4. 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. Apri la finestra di Bitdefender.
   b. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
   c. Clicca su **Antivirus** nel menu di sinistra e poi sulla scheda **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.
   - In Microsoft Outlook: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.

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. 137).

## 14.5. 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 completa di sistema** con Bitdefender.Per scoprire come fare, fai riferimento a «*Come posso eseguire una scansione del mio sistema?*» (p. 31).
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. 137).

## 14.6. Come pulire i file infetti in System Volume Information

La cartella System volume information è una zona sul tuo disco fisso creata dal sistema operativo e usata da Windows per archiviare informazioni importanti relative alla configurazione del sistema.

I motori di Bitdefender possono rilevare qualsiasi file infetto archiviato nella cartella System Volume Information, ma essendo un'area protetta potrebbe non essere possibile rimuoverli.

I file infetti rilevati nelle cartelle del Ripristino configurazione di sistema compariranno nel registro della scansione come segue:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

Per rimuovere completamente e immediatamente i file infetti o i file nell'archivio dati, disattiva e attiva nuovamente l'opzione Ripristino configurazione di sistema.

Quanto il Ripristino configurazione di sistema è disattivato, tutti i punti di ripristino sono rimossi.

Quando il Ripristino configurazione di sistema viene attivato nuovamente, vengono creati nuovi punti di ripristino come richiesto dalla programmazione e dagli eventi.

Per disabilitare il Ripristino configurazione di sistema, segui questi passaggi:

- **Per Windows XP:**

  1. Segui questo percorso: **Start → Tutti i programmi → Accessori → Utilità di sistema → Ripristino configurazione di sistema**

2. Clicca su **Impostazioni Ripristino configurazione di sistema** sul lato sinistro della finestra.
3. Seleziona la casella **Disattiva Ripristino configurazione di sistema** su tutte le unità e clicca su **Applica**.
4. Quando ricevi l'avviso che tutti i punti di ripristino esistenti saranno eliminati, clicca su **Sì** per continuare.
5. Per attivare il Ripristino configurazione di sistema, deseleziona la casella **Disattiva Ripristino configurazione di sistema** su tutte le unità e clicca su **Applica**

- **Per Windows Vista:**
  1. Segui questo percorso: **Start** → **Pannello di controllo** → **Sistema e manutenzione** → **Sistema**
  2. Nel pannello a sinistra, clicca su **Protezione sistema**.

     Se è richiesta una password da amministratore o una conferma, digita la password o fornisci la conferma.
  3. Per disattivare il Ripristino configurazione di sistema deseleziona le caselle corrispondenti per ogni unità e clicca su **Ok**.
  4. Per attivare il Ripristino configurazione di sistema seleziona le caselle corrispondenti per ogni unità e clicca su **OK**.
- **Per Windows 7:**
  1. Clicca su **Start**, clicca col pulsante destro su **Risorse del computer** e poi clicca su **Proprietà**.
  2. Clicca sul collegamento **Protezione sistema** nel pannello a sinistra.
  3. Nelle opzioni di **Protezione sistema**, seleziona tutte le unità e clicca su **Configura**.
  4. Seleziona **Disattiva il sistema di protezione** e clicca su **Applica**.
  5. Clicca su **Elimina**, clicca su **Continua** una volta richiesto e poi clicca su **OK**.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 137).

## 14.7. 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.

## 14.8. 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.

## 14.9. 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.

## 14.10. 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 maligno. 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.

# 15. Ottenere aiuto

## 15.1. Supporto

Bitdefender si sforza di fornire 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 rapidamente una soluzione o una risposta.O, se preferisci, 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.

### 15.1.1. 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/site/Main/contactForm/
- Forum del supporto di Bitdefender:http://forum.bitdefender.com
- il portale di sicurezza Malware City:http://www.malwarecity.com

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

#### Centro di supporto di Bitdefender

Il Centro di supporto di Bitdefender è un archivio online di informazioni sui prodotti Bitdefender.Registra, in un formato facilmente accessibile, le notifiche sui risultati di 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 in http://www.bitdefender.it/site/Main/contactForm/.

#### 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 **Home & Home Office** per accedere alla sezione dedicata ai prodotti per utenti standard.

### Portale Malware City

Il portale Malware City è una ricca fonte di informazioni sulla sicurezza del computer. Qui puoi apprendere le varie minacce a cui il computer è esposto quando ti connetti a Internet (malware, phishing, spam, cyber-criminali).Un dizionario utile che ti aiuta a comprendere i termini che non conosci, relativi alla sicurezza del computer.

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 di Malware City è http://www.malwarecity.com.

## 15.1.2. Chiedere aiuto

La sezione **Risoluzione dei problemi** ti 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. 137)
- «Contattaci tramite il nostro Centro di supporto online» (p. 138)

Importante

Per contattare il Servizio clienti di Bitdefender devi registrare il prodotto di Bitdefender.Per ulteriori informazioni fare riferimento a *«Registrazione del prodotto» (p. 8)*.

### 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. Apri la finestra di Bitdefender.
2. Clicca sul collegamento **Aiuto e supporto**, localizzato nell'angolo in basso a destra della finestra.
3. Hai le seguenti opzioni:
   - Leggi gli articoli o i documenti rilevanti e prova le soluzioni proposte.
   - Lancia una ricerca nel nostro database per le informazioni che cerchi.
   - Usa il pulsante **Contatta supporto** per eseguire lo strumento di supporto e contattare il Servizio clienti.Puoi esplorare la procedura guidata usando il pulsante **Avanti**. Per uscire, 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. Scegli il tuo paese dal menu corrispondente.
        iv. Inserisci una descrizione del problema riscontrato.
     c. Attendi qualche minuto mentre Bitdefender raccoglie le informazioni sul prodotto. Queste informazioni aiuteranno i nostri tecnici 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.com/help.Il Centro di supporto di Bitdefender include molti articoli che contengono soluzioni ai problemi inerenti Bitdefender.
2. Seleziona il tuo prodotto dalla colonna sulla sinistra e cerca nel Centro di Supporto di Bitdefender gli articoli che possono fornire una soluzione al tuo problema.
3. Leggi gli articoli o i documenti rilevanti e prova le soluzioni proposte.
4. Se la soluzione non risolve il problema, usa il link nell'articolo per contattare il Servizio clienti di Bitdefender.
5. Contatta un rappresentante di supporto Bitdefender tramite e-mail, chat o telefono.

## 15.2. Contatti

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, sforzandosi costantemente per una comunicazione sempre più efficiente. Se hai delle domande o richieste, non esitare a contattarci.

### 15.2.1. Indirizzi web

Dipartimento vendite: sales@bitdefender.com
Centro di supporto:http://www.bitdefender.it/site/Main/contactForm/
Documentazione: documentation@bitdefender.com
Distributori locali:http://www.bitdefender.com/partners
Programma partner: partners@bitdefender.com
Contatti stampa: pr@bitdefender.com
Carriere: 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

### 15.2.2. 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/site/Partnership/list/.
2. Le informazioni di contatto dei distributori locali di Bitdefender dovrebbero apparire automaticamente. Se non fosse così, seleziona il paese in cui risiedi per visualizzare le informazioni.
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.

### 15.2.3. Uffici di Bitdefender

Gli uffici di Bitdefender sono pronti a rispondere a qualunque richiesta riguardo le loro aree operative, sia di natura commerciale sia generale. I loro rispettivi indirizzi e contatti sono elencati sotto.

#### U.S.A

**Bitdefender, LLC**
PO Box 667588

Pompano Beach, Fl 33066
Telefono (ufficio e vendite): 1-954-776-6262
Vendite: sales@bitdefender.com
Supporto tecnico: http://www.bitdefender.it/site/Main/contactForm/
Web: http://www.bitdefender.com

### UK e Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
E-mail: info@bitdefender.co.uk
Tel.: +44 (0) 8451-305096
Vendite: sales@bitdefender.co.uk
Supporto tecnico: http://www.bitdefender.it/site/Main/contactForm/
Web: http://www.bitdefender.co.uk

### Germania

**Bitdefender GmbH**
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Ufficio: +49 2301 91 84 0
Vendite: vertrieb@bitdefender.de
Supporto tecnico: http://kb.bitdefender.de
Web: http://www.bitdefender.de

### Spagna

**Bitdefender España, S.L.U.**
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Fax: +34 93 217 91 28
Tel.: +34 902 19 07 65
Vendite: comercial@bitdefender.es
Supporto tecnico: http://www.bitdefender.es/ayuda
Sito: http://www.bitdefender.es

### Romania

**BITDEFENDER SRL**
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799

Telefono vendite: +40 21 2063470
Indirizzo e-mail ufficio vendite: sales@bitdefender.ro
Supporto tecnico: http://www.bitdefender.ro/suport
Sito: http://www.bitdefender.ro

# 16. Informazioni utili

Questo capitolo presenta alcune procedure importanti che devi conoscere prima di iniziare a risolvere ogni problema tecnico.

Risolvere una situazione tecnica in Bitdefender richiede alcune conoscenze di Windows, perciò i prossimi passaggi sono strettamente correlati al sistema operativo Windows.



## 16.1. 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 Internet Security 2012 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:

- Per **Windows XP**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Aggiungi / Rimuovi programmi**.
  2. Attendi per qualche istante, finché non compare l'elenco del software installato.
  3. Trova il nome del programma che desideri rimuovere e seleziona **Rimuovi**.
  4. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.
- Per **Windows Vista** e **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.

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.

## 16.2. 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.

## 16.3. 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:

- Per **Windows XP**:
  1. Clicca su **Start**.
  2. Individua **Risorse del computer** nel menu **Start**.
  3. Clicca con il pulsante destro su **Risorse del computer** e seleziona **Proprietà**.
  4. Se vedi l'opzione **x64 Edition** indicata sotto la voce **Sistema**, stai usando una versione a 64 bit di Windows XP.

     Se non vedi l'opzione **x64 Edition**, stai usando una versione di XP a 32 bit.
- Per **Windows Vista** e **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.

## 16.4. Come posso usare il Ripristino di sistema in Windows?

Se non riesci ad avviare il computer in modalità normale, puoi avviarlo in modalità provvisoria e usare il Ripristino configurazione di sistema per ripristinare il computer a una configurazione precedente avviabile senza errori.

Per eseguire il Ripristino configurazione di sistema, devi accedere a Windows come amministratore.

Per usare il Ripristino configurazione di sistema, segui questi passaggi:

- In Windows XP:
  1. Avvia Windows in modalità provvisoria.
  2. Segui questo percorso dal menu Start di Windows: **Start → Tutti i programmi → Utilità di sistema → Ripristino configurazione di sistema**.
  3. Nella pagina del **Ripristino di configurazione di sistema**, seleziona **Ripristina uno stato precedente del computer** e poi clicca su Avanti.
  4. Segui i passaggi della procedura guidata e dovresti poter riavviare il sistema in modalità normale.
- In Windows Vista e Windows 7:
  1. Avvia Windows in modalità provvisoria.
  2. Segui questo percorso dal menu Start di Windows: **Tutti i programmi → Accessori → Utilità di sistema → Ripristino configurazione di sistema**.
  3. Segui i passaggi della procedura guidata e dovresti poter riavviare il sistema in modalità normale.

## 16.5. 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**, vai al **Pannello di controllo** e seleziona **Opzioni cartella**.
2. Vai alla scheda **Visualizza**.
3. Seleziona **Mostra contenuto delle cartelle di sistema** (solo per Windows XP).
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**.

# Glossario

**ActiveX**

ActiveX è una modalità di scrittura dei programmi affinché possano essere invocati da altri programmi e sistemi operativi. La tecnologia ActiveX viene utilizzata con Microsoft Internet Explorer per generare pagine web interattive che sembrino e si comportino come applicazioni e non come semplici pagine statiche. Con gli elementi ActiveX, gli utenti possono chiedere o rispondere a domande, adoperare pulsanti ed interagire in altri modi con la pagina web. I controlli ActiveX vengono 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**

L'adware è spesso combinato con un'applicazione host offerta senza spese quando l'utente accetta l'adware. Le applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove si spiega il proposito dell'applicazione. Non viene commessa quindi alcuna offesa o scortesia.

Comunque, i pop-up di avvertimento possono rappresentare un fastidio e in alcuni casi riducono il funzionamento del sistema. Inoltre, le informazioni raccolte da queste applicazioni possono causare inconvenienti alla privacy degli utenti, non completamente ben informati sui termini dell'accordo di licenza.

**Aggiorna**

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

Bitdefender dispone 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, dovrai specificare il nome dell'applet e la dimensione (lunghezza e larghezza, in pixel) che l'applet può utilizzare. Quando si accede alla pagina web, il browser scarica l'applet 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, nonostante gli applet vengano lanciati sul client, essi 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.

**Backdoor**

Breccia nella sicurezza di un programma deliberatamente implementata dal costruttore 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 venditore a scopo di manutenzione.

**Barra di sistema**

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

**Browser**

Abbreviazione di browser web, un'applicazione software utilizzata per localizzare e visualizzare pagine web. I due browser più noti sono Netscape Navigator e Microsoft Internet Explorer. Entrambi sono browser grafici, ovvero in grado di visualizzare sia elementi grafici che testo. Inoltre, i browser più moderni possono presentare informazioni multimediali, incluso suoni e video, nonostante richiedano i plug-in per alcuni formati.

**Client mail**

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

**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 dei tuoi interessi e gusti online. In questo regno, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è di fornire direttamente ciò che si dichiara essere il proprio interesse. 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. Dall'altra parte, implica, in effetti, un "tracciamento" di dove si va e di cosa si seleziona. Comprensibilmente in questo modo nascerà un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come uno "SKU number"

(il codice a barre sul retro delle confezioni che vengono passati alla scansione della cassa). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

**Download**
Per copiare dati (solitamente un file intero) da un'origine principale su un dispositivo periferico. Il termine viene spesso utilizzato per descrivere un processo di copia di un documento da un servizio online sul computer di un utente. Si può inoltre riferire al processo di copiatura di un file da un file server di rete su un computer della rete.

**E-mail**
Posta elettronica. Servizio che invia messaggi ai computer attraverso reti locali o globali.

**Elementi di startup**
Qualsiasi file posizionato in questa cartella si aprirà quando il computer viene avviato. Ad esempio, una schermata di avvio, un file sonoro da eseguire quando il computer si avvia la prima volta, un'agenda-calendario, oppure programmi applicativi che possono essere elementi di startup. Normalmente in questa cartella viene posizionato un alias di un file, anziché il 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 del nome del file, come Unix, VMS e MS-DOS. Sono normalmente composti da una a tre lettere (alcuni vecchi supporti OS non più di tre). Esempi: "c" per codici sorgente C, "ps" per PostScript, "txt" per testi arbitrari.

**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 venire ingannata dalle nuove varianti dei virus esistenti. Può comunque occasionalmente segnalare codici sospetti in programmi normali, generando "falsi positivi".

**Eventi**
Azione oppure avvenimento rilevato da un programma. Gli eventi possono rappresentare azioni dell'utente, come cliccare con il mouse o premere un tasto sulla tastiera oppure avvenimenti del sistema, ad esempio memoria insufficiente.

**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 mantiene un file di rapporto che elenca i percorsi esaminati, 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 alfine 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, infatti, possono essere usati 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**

Tipo di virus del computer 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.

**Memoria**

Aree di archiviazione interne nel computer. Il termine memoria identifica l'archiviazione dei dati sotto forma di chip; la parola storage (archiviazione) viene utilizzata per la memoria su nastri o su dischi. Ogni computer dispone di un certo quantitativo di memoria fisica, solitamente chiamata memoria principale oppure RAM.

**Non euristico**

Questo metodo di scansione si basa su specifiche firme di virus. Il vantaggio della scansione non-euristica è di non essere ingannato da ciò che potrebbe sembrare un virus e non genera falsi allarmi.

**Pacchetti di programmi**

File in formato compresso. Molti sistemi operativi e molte applicazioni contengono comandi che vi consentono di impaccare un file in modo da occupare meno memoria. Ad esempio, supponiamo che abbiate un file di testo che contenga dieci caratteri spazio consecutivi. Normalmente occuperebbe dieci byte di memoria.

Un programma che impacca i file sostituirebbe gli spazi con un carattere speciale serie_di_spazi seguito dal numero di spazi sostituiti. In questo caso i dieci spazi occuperebbero solo due byte. Questa è solo una tecnica di impaccaggio – ce ne sono molte altre.

**Percorso**

Le esatte direzioni per raggiungere un file su un computer. Queste direzioni vengono solitamente descritte attraverso il sistema di casellario gerarchico dall'alto al basso.

La strada tra due punti qualsiasi, come ad esempio il canale di comunicazioni tra due computer.

**Phishing**

L'atto d'inviare una mail a un utente fingendo di essere una ditta legittima e affermata, nel tentativo di truffarlo, facendogli cedere informazioni private che saranno usate per furti d'identità. L'e-mail indirizza gli utenti a visitare una pagina web, dove gli viene chiesto di aggiornare informazioni personali, come password e carte di credito, numero della previdenza sociale e del conto in banca, che questa legittima organizzazione ha già. In ogni caso, la pagina web è finta, e organizzata soltanto per rubare i dati dell'utente.

**Porta**

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

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

**Rootkit**

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

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

I rootkit non sono maligni per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando rootkit. Comunque, essi vengono principalmente utilizzati per nascondere malware o per celare la presenza di un intruso nel sistema. Se combinati al 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 log ed evitare il rilevamento.

**Script**

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

**Settore di boot**

Un settore all'inizio di ogni disco che identifica l'architettura del disco (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**

Posta elettronica pubblicitaria. Generalmente conosciuto come qualsiasi e-mail non richiesta.

**Spyware**

Qualsiasi programma che raccoglie di nascosto informazioni sull'utente attraverso la sua connessione internet, senza che l’utente se ne accorga, normalmente a scopo pubblicitario. Le applicazioni Spyware generalmente sono inserite come una componente nascosta di programmi freeware o shareware, scaricabili da Internet. Tuttavia, è importante segnalare che la maggioranza delle applicazioni shareware o freeware non contengono spyware. Una volta installato, lo spyware monitora le attività dell’utente su Internet e trasmette queste informazioni di nascosto a qualcun altro. Lo spyware può anche raccogliere informazione su indirizzi mail e addirittura password e numeri di carta di credito.

Lo spyware è simile a un Cavallo di Troia che gli utenti installano senza volere quando installano qualcos'altro. Un modo comune di diventare vittime di spyware è scaricare certi file peer-to-peer, scambiando prodotti attuali.

Oltre a questioni di etica e privacy, lo spyware sottrae risorse di memoria del computer, "mangiandosi" larghezza di banda dal momento in cui invia informazione alla sua "casa" usando la connessione internet dell'utente. Poiché lo spyware sta usando memoria e risorse del sistema, le applicazioni eseguite in background possono portare al blocco del sistema o all'instabilità.

**TCP/IP**

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di networking 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 traffico di instradamento.

**Trojan**

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 del computer ma che al contrario li introduce.

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

**Unità disco**

È un dispositivo che legge e scrive dei dati su un disco.

Un drive di disco rigido legge e scrive dischi rigidi.

Un drive di floppy accede i dischi floppy.

Le unità disco possono essere interne (incorporate all'interno di un computer) oppure esterne (collocate in un meccanismo separato e connesso al computer).

**Virus**

Un programma o una parte di codice caricato sul computer a tua insaputa e che viene eseguito contro la tua 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 se 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 se stesso attraverso le reti superando i sistemi di sicurezza.

**Virus di boot**

Un virus che infetta il settore di boot di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infetto con un virus di boot, farà sì che il virus venga attivato nella memoria. Da quel momento in poi, ogni volta che si esegue il boot del sistema, il virus sarà attivo nella memoria.

**Virus polimorfico**

Un virus che modifica la propria forma con ogni file che infetta. Poiché non dispongono di caratteristiche binarie costanti, tali virus sono difficili da identificare.

**Worm (baco)**

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