Bitdefender®

INTERNET SECURITY 2018

MANUALE D'USO

Bitdefender Internet Security 2018
Manuale d'uso

Data di pubblicazione 25/05/2018

Diritto d'autore© 2018 Bitdefender

Avvertenze legali

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

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

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

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

Bitdefender

Indice

Installazione 1

1. Prepararsi all'installazione 2

2. Requisiti di sistema 3
   2.1. Requisiti minimi di sistema 3
   2.2. Requisiti di sistema consigliati 3
   2.3. Requisiti software 4

3. Installare il tuo prodotto Bitdefender 5
   3.1. Installa da Bitdefender Central 5
   3.2. Installa dal disco di installazione 7

Iniziare 12

4. Le basi 13
   4.1. Aprire la finestra di Bitdefender 14
   4.2. Risolvere i problemi 15
      4.2.1. Procedura guidata problemi di sicurezza 16
      4.2.2. Configurare gli avvisi di stato 16
   4.3. Notifiche 17
   4.4. Autopilot 18
   4.5. Profili 18
      4.5.1. Configura l'attivazione automatica dei profili 19
   4.6. Impostazioni protette da password di Bitdefender 20
   4.7. Rapporti anonimi sull'utilizzo 21
   4.8. Notifiche offerte speciali 21

5. Interfaccia di Bitdefender 22
   5.1. Icona area di notifica 22
   5.2. Finestra principale 24
      5.2.1. Stato 25
      5.2.2. Barra laterale sinistra 25
      5.2.3. I pulsanti azione e accesso per la sezione delle funzionalità 26
      5.2.4. Barra inferiore 27
   5.3. Le sezioni di Bitdefender 27
      5.3.1. **Protezione** 28
      5.3.2. **Privacy** 30
   5.4. Widget sicurezza 31
      5.4.1. Eseguire la scansione di file e cartelle 33
      5.4.2. Nascondi / mostra widget sicurezza 33
   5.5. Attività 33
      5.5.1. Controllare il Rapporto sicurezza 35
      5.5.2. Attivare o disattivare la notifica del Rapporto di sicurezza 36

6. Bitdefender Central 37
   6.1. Accedere a Bitdefender Central 37
   6.2. I miei abbonamenti 38

6.2.1. Controllare gli abbonamenti disponibili . . . 38
6.2.2. Aggiungi un nuovo dispositivo . . . 38
6.2.3. Rinnova abbonamento . . . 39
6.2.4. Attiva abbonamento . . . 39
6.3. I miei dispositivi . . . 40
6.4. Il mio Account . . . 42
6.5. Notifiche . . . 42

7. Mantenere aggiornato Bitdefender . . . 43
7.1. Verificare se Bitdefender è aggiornato . . . 43
7.2. Eseguire un aggiornamento . . . 44
7.3. Attivare o disattivare l'aggiornamento automatico . . . 45
7.4. Modificare le impostazioni di aggiornamento . . . 45
7.5. Aggiornamenti costanti . . . 47

Come fare . . . 48

8. Installazione . . . 49
8.1. Come faccio a installare Bitdefender su un secondo computer? . . . 49
8.2. Come posso reinstallare Bitdefender? . . . 49
8.3. Dove posso scaricare il mio prodotto Bitdefender? . . . 50
8.4. Come posso modificare la lingua del mio prodotto Bitdefender? . . . 51
8.5. Come posso utilizzare il mio abbonamento a Bitdefender dopo aver aggiornato Windows? . . . 53
8.6. Come posso fare l'upgrade alla versione più recente di Bitdefender? . . . 55

9. Abbonamenti . . . 57
9.1. Come posso attivare l'abbonamento di Bitdefender utilizzando un codice di licenza? . . . 57

10. Bitdefender Central . . . 59
10.1. Come posso accedere a Bitdefender Central utilizzando un altro account online? . . . 59
10.2. Come posso disattivare i messaggi di aiuto di Bitdefender Central? . . . 59
10.3. Ho dimenticato la password del mio account Bitdefender. Come posso cambiarla? . . . 60
10.4. Come posso gestire le sessioni di accesso associate al mio account di Bitdefender? . . . 61

11. Scansione con Bitdefender . . . 62
11.1. Come posso controllare un file o una cartella? . . . 62
11.2. Come posso eseguire una scansione del mio sistema? . . . 62
11.3. Come posso programmare una scansione? . . . 63
11.4. Come posso creare un'attività di scansione personale? . . . 63
11.5. Come posso escludere una cartella dalla scansione? . . . 64
11.6. Cosa fare quando Bitdefender rileva un file pulito come infetto? . . . 65
11.7. Come posso verificare quali minacce sono state rilevate da Bitdefender? . . . 66

12. Parental Advisor . . . 68
12.1. Come posso proteggere i bambini dalle minacce online? . . . 68
12.2. Come posso impedire che i bambini accedano a un sito web? . . . 69

12.3. Come posso impedire ai bambini di usare un gioco? 70
12.4. Come posso impedire che il bambino entri in contatto con persone sconosciute? 70
12.5. Come posso impostare un luogo come sicuro o vietato per il bambino? 72
12.6. Come posso impedire al bambino di accedere ai dispositivi assegnati nei giorni di scuola? 74
12.7. Come posso impedire al bambino di accedere ai dispositivi assegnati nelle serate dei giorni di scuola? 73
12.8. Come posso impedire al bambino di accedere ai dispositivi assegnati nei fine settimana? 74
12.9. Come rimuovere un profilo di un bambino 74

13. Protezione della Privacy 76
13.1. Come posso essere certo che le mie transazioni online sono sicure? 76
13.2. Come posso usare i File Vault? 76
13.3. Come posso eliminare un file in modo permanente con Bitdefender? 78
13.4. Come posso proteggere la mia webcam da accessi non autorizzati? 78

14. Informazioni utili 80
14.1. Come posso testare la mia soluzione di sicurezza? 80
14.2. Come posso rimuovere Bitdefender? 80
14.3. Come posso rimuovere Bitdefender VPN? 81
14.4. Come posso spegnere automaticamente il computer al termine della scansione? 82
14.5. Come posso configurare Bitdefender per usare una connessione a Internet tramite proxy? 83
14.6. Sto usando una versione di Windows a 32 o 64 bit? 84
14.7. Come posso visualizzare gli elementi nascosti in Windows? 85
14.8. Come posso rimuovere le altre soluzioni di sicurezza? 86
14.9. Come posso riavviare in modalità provvisoria? 87

Gestire la propria sicurezza 89

15. Protezione antivirus 90
15.1. Scansione all'accesso (protezione in tempo reale) 91
15.1.1. Attivare o disattivare la protezione in tempo reale 91
15.1.2. Configurare le impostazioni avanzate della protezione in tempo reale . . . 91
15.1.3. Ripristinare le impostazioni predefinite 95
15.2. Scansione a richiesta 96
15.2.1. Controllare un file o una cartella alla ricerca di minacce 97
15.2.2. Eseguire una Scansione veloce 97
15.2.3. Eseguire una scansione del sistema 97
15.2.4. Configurare una scansione personale 98
15.2.5. Procedura guidata scansione antivirus 101
15.2.6. Controllare i registri di scansione 105
15.3. Scansione automatica di supporti rimovibili 105
15.3.1. Come funziona? 106
15.3.2. Gestire la scansione di supporti rimovibili 107
15.4. Esamina file hosts 107
15.5. Configurare le eccezioni della scansione 108

15.5.1. Escludere file e cartelle dalla scansione ... 108
15.5.2. Escludere estensioni di file dalla scansione ... 109
15.5.3. Gestire le eccezioni della scansione ... 110
15.6. Gestire i file in quarantena ... 110

16. Difesa da minacce avanzate ... 113
16.1. Attivare o disattivare Advanced Threat Defense ... 113
16.2. Verificare gli attacchi ransomware rilevati ... 113
16.3. Verificare le app sospette rilevate ... 114
16.4. Aggiungere processi alle eccezioni ... 114

17. Protezione web ... 115
17.1. Avvisi di Bitdefender nel browser ... 116

18. Antispam ... 118
18.1. Approfondimenti antispam ... 119
18.1.1. Filtri Antispam ... 119
18.1.2. Operazione antispam ... 119
18.1.3. Programmi e protocolli di posta elettronica supportati ... 120
18.2. Attivare o disattivare la protezione antispam ... 120
18.3. Usare la barra degli strumenti antispam nella finestra del tuo client e-mail ... 120
18.3.1. Indicare gli errori di rilevazione ... 121
18.3.2. Indicare messaggi spam non rilevati ... 122
18.3.3. Configurare le impostazioni della barra degli strumenti ... 122
18.4. Configurazione dell'elenco Amici ... 123
18.5. Configurazione dell'elenco Spammer ... 124
18.6. Configurare i filtri locali antispam ... 125
18.7. Configurare le impostazioni cloud ... 126

19. Firewall ... 128
19.1. Attivare o disattivare la protezione del firewall ... 128
19.2. Gestire le regole delle app ... 129
19.3. Gestire le impostazioni di connessione ... 132
19.4. Configurare le impostazioni avanzate ... 133

20. Vulnerabilità ... 134
20.1. Controllare il sistema per rilevare vulnerabilità ... 134
20.2. Usare il controllo automatico delle vulnerabilità ... 136
20.3. Wi-Fi Security Advisor ... 138
20.3.1. Attivare o disattivare le notifiche di Wi-Fi Security Advisor ... 138
20.3.2. Configurare la rete Wi-Fi di casa ... 139
20.3.3. Wi-Fi pubblica ... 139
20.3.4. Controllare le informazioni sulle reti Wi-Fi ... 140

21. Protezione webcam ... 142
21.1. Attivare o disattivare la Protezione webcam ... 142
21.2. Configurare la Protezione webcam ... 142
21.3. Aggiungere app all'elenco della Protezione webcam ... 143

22. Safe files ... 145
22.1. Attivare o disattivare Safe files ... 145
22.2. Proteggi i tuoi file personali dagli attacchi dei Ransomware. ... 146

22.3. Configurare l'accesso alle app 146
22.4. Protezione all'avvio 147

23. Crittografia file 148
23.1. Gestire i File Vault 148
23.2. Creare i File Vault 148
23.3. Importare un File Vault 149
23.4. Aprire i File Vault 149
23.5. Aggiungere file ai Vault 150
23.6. Bloccare i Vault 151
23.7. Rimuovere file dai Vault 151
23.8. Cambiare la password del Vault 152

24. Protezione di Password Manager per le tue credenziali 153
24.1. Crea un nuovo database del Portafoglio 154
24.2. Importa un database esistente 154
24.3. Esporta il database del Portafoglio 155
24.4. Sincronizzare i tuoi Portafogli nel cloud 155
24.5. Gestisci le tue credenziali del Portafoglio 156
24.6. Attivare o disattivare la protezione del Password Manager 157
24.7. Gestire le impostazioni del Password Manager 157

25. VPN 161
25.1. Installare VPN 161
25.2. Aprire VPN 162
25.3. Interfaccia di VPN 162
25.4. Abbonamenti 163

26. Safepay: sicurezza per le transazioni online 164
26.1. Utilizzare Bitdefender Safepay™ 165
26.2. Configurare le impostazioni 166
26.3. Gestire i segnalibri 168

27. Protezione dati 169
27.1. Eliminare i file in modo permanente 169

28. Parental Advisor 171
28.1. Accedere a Parental Advisor - BAMBINI 171
28.2. Aggiungere il profilo dei propri bambini 172
28.2.1. Assegnare più dispositivi allo stesso profilo 173
28.2.2. Associare il Parental Advisor a Bitdefender Central 174
28.2.3. Monitorare le attività dei bambini 175
28.2.4. Configurazione delle Impostazioni Generali 176
28.2.5. Modificare un profilo 176
28.2.6. Rimuovere un profilo 177
28.3. Configurare i profili del Parental Advisor 177
28.3.1. Attività 178
28.3.2. Applicazioni 178
28.3.3. Siti web 179
28.3.4. Contatti telefono 179
28.3.5. Posizione bambino 180
28.3.6. Social network 181

28.3.7. Calendario 182
29. Bitdefender USB Immunizer 184

Ottimizzazione sistema 185

30. Profili 186
30.1. Profilo Lavoro 187
30.2. Profilo Film 188
30.3. Profilo Gioco 189
30.4. Profilo rete Wi-Fi pubblica 191
30.5. Profilo Modalità Batteria 191
30.6. Ottimizzazione in tempo reale 192

Risoluzione dei problemi 194

31. Risolvere i problemi più comuni 195
31.1. Il mio sistema sembra lento 195
31.2. La scansione non parte 197
31.3. Non posso più usare una app 199
31.4. Cosa fare quando Bitdefender blocca un sito web o un'applicazione online sicuri 200
31.5. Cosa fare se Bitdefender rilevasse un'applicazione sicura come ransomware 201
31.6. Non riesco a connettermi a Internet 201
31.7. Non riesco ad accedere a un dispositivo nella mia rete 202
31.8. Internet è lento 204
31.9. Come aggiornare Bitdefender con una connessione a Internet lenta 205
31.10. I servizi Bitdefender non rispondono 206
31.11. Il filtro antispam non funziona correttamente 206
31.11.1. I messaggi legittimi sono contrassegnati come [spam] 207
31.11.2. Molti messaggi spam non vengono rilevati 209
31.11.3. Il Filtro antispam non rileva alcun messaggio spam 211
31.12. L'opzione Compila automaticamente nel mio Portafoglio non funziona 212
31.13. Rimozione di Bitdefender non riuscita 213
31.14. Il sistema non si riavvia dopo aver installato Bitdefender 214

32. Rimuovere le minacce dal sistema 218
32.1. Bitdefender Modalità di soccorso (Ambiente di soccorso in Windows 10) 218
32.2. Cosa fare quando Bitdefender trova delle minacce sul computer? 222
32.3. Come posso rimuovere una minaccia in un archivio? 224
32.4. Come posso rimuovere una minaccia in un archivio di e-mail? 225
32.5. Cosa fare se sospetti che un file possa essere pericoloso? 226
32.6. Quali sono i file protetti da password nel registro della scansione? 226
32.7. Quali sono gli elementi ignorati nel registro della scansione? 227
32.8. Quali sono i file supercompressi nel registro della scansione? 227
32.9. Perché Bitdefender ha eliminato automaticamente un file infetto? 228

Contattaci 229

33. Chiedere aiuto 230
34. Risorse online 233
34.1. Centro di supporto di Bitdefender 233
34.2. Forum supporto di Bitdefender 233
34.3. Portale HOTforSecurity 234
35. Contatti 235
35.1. Indirizzi web 235
35.2. Distributori locali 235
35.3. Uffici di Bitdefender 235
Glossario 238

INSTALLAZIONE

1. PREPARARSI ALL'INSTALLAZIONE

Prima di installare Bitdefender Internet Security 2018, completa questi passaggi preliminari per assicurarti che l'installazione funzioni senza problemi:

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

2. REQUISITI DI SISTEMA

Puoi installare Bitdefender Internet Security 2018 solo su computer con i seguenti sistemi operativi:

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

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

Nota

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

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

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

2.1. Requisiti minimi di sistema

- 1.5 GB di spazio disponibile su disco rigido
- Dual core 1,6 GHz
- 1 GB di memoria (RAM)

2.2. Requisiti di sistema consigliati

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

2.3. Requisiti software

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

- Microsoft Edge 40 e superiore
- Internet Explorer 10 e superiore
- Mozilla Firefox 51 e superiore
- Google Chrome 34 e superiore
- Skype 6.3 e superiore
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 e superiore

3. INSTALLARE IL TUO PRODOTTO BITDEFENDER

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

Se il tuo acquisto vale per più di un computer (per esempio hai acquistato Bitdefender Internet Security 2018 per 3 PC), ripeti il processo d'installazione e attiva il prodotto con lo stesso account su ogni computer. L'account che devi utilizzare è quello che include il tuo abbonamento attivo a Bitdefender.

3.1. Installa da Bitdefender Central

Da Bitdefender Central puoi scaricare il kit d'installazione corrispondente all'abbonamento acquistato. Una volta completato il processo d'installazione, Bitdefender Internet Security 2018 viene attivato.

Per scaricare Bitdefender Internet Security 2018 da Bitdefender Central:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **I miei dispositivi** e clicca su **INSTALLA PROTEZIONE LOCALE**.
3. Seleziona una delle due opzioni disponibili:
   - **SCARICA**

     Clicca sul pulsante e salva il file d'installazione.
   - **Su un altro dispositivo**

     Seleziona **Windows** per scaricare il tuo prodotto Bitdefender e poi clicca su **CONTINUA**. Inserisci un indirizzo e-mail nel campo corrispondente e clicca su **INVIA**.
4. Attendi il completamento del download e poi esegui il programma d'installazione.

Convalidare l'installazione

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

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

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

Il pacchetto d'installazione di Bitdefender Internet Security 2018 è aggiornato costantemente.

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

Una volta convalidata l'installazione, comparirà la relativa procedura guidata. Segui tutti i passaggi per installare Bitdefender Internet Security 2018.

Fase 1 - Installazione di Bitdefender

Prima di procedere con l'installazione, devi accettare l'Accordo di abbonamento. Prenditi qualche istante per leggere l'Accordo di abbonamento in quanto contiene i termini e le condizioni con cui è possibile utilizzare Bitdefender Internet Security 2018.

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

In questa fase possono essere eseguite due attività aggiuntive:

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

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

Fase 2 - Installazione in corso

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

Una scansione controlla le aree critiche del sistema alla ricerca di minacce, le ultime versioni dei file della app vengono scaricate e installate, e i servizi di Bitdefender vengono avviati. Questa fase può richiedere alcuni minuti. Clicca su **SALTA SCANSIONE** se vuoi eseguire la scansione del sistema più tardi. Per maggiori informazioni sull'esecuzione di una scansione di sistema, fai riferimento a «*Eseguire una scansione del sistema*» (p. 97).

Fase 3 - Fine dell'installazione

Il tuo prodotto Bitdefender è stato installato con successo.

Viene mostrato un resoconto dell'installazione. Se durante l'installazione viene rilevata e rimossa una minaccia attiva, è necessario riavviare il sistema. Clicca su **INIZIA A USARE Bitdefender** per continuare.

Fase 4 - Come iniziare

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

Clicca su **FINE** per accedere all'interfaccia di Bitdefender Internet Security 2018.

3.2. Installa dal disco di installazione

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

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

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

Se la tua connessione a Internet è lenta o il tuo sistema non è proprio connesso a Internet, clicca sul pulsante **Installa da CD/DVD**. In questo caso, sarà installato il prodotto Bitdefender disponibile sul disco e successivamente sarà scaricata una nuova versione dai server di Bitdefender tramite un aggiornamento.

Convalidare l'installazione

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

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

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

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

Una volta convalidata l'installazione, comparirà la relativa procedura guidata. Segui tutti i passaggi per installare Bitdefender Internet Security 2018.

Fase 1 - Installazione di Bitdefender

Prima di procedere con l'installazione, devi accettare l'Accordo di abbonamento. Prenditi qualche istante per leggere l'Accordo di abbonamento in quanto contiene i termini e le condizioni con cui è possibile utilizzare Bitdefender Internet Security 2018.

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

In questa fase possono essere eseguite due attività aggiuntive:

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

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

Fase 2 - Installazione in corso

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

Le aree critiche del tuo sistema vengono esaminate per trovare eventuali minacce e i servizi di Bitdefender vengono avviati. Questa fase può richiedere alcuni minuti. Clicca su **SALTA SCANSIONE** se vuoi eseguire la scansione del sistema più tardi. Per maggiori informazioni sull'esecuzione di una scansione di sistema, fai riferimento a «*Eseguire una scansione del sistema*» (p. 97).

Fase 3 - Fine dell'installazione

Viene mostrato un resoconto dell'installazione. Se durante l'installazione viene rilevata e rimossa una minaccia attiva, è necessario riavviare il sistema. Clicca su **INIZIA A USARE Bitdefender** per continuare.

Fase 4 - Account Bitdefender

Dopo aver completato la configurazione iniziale, comparirà la finestra account Bitdefender. Per attivare il prodotto e utilizzare le sue funzioni online, è necessario avere un account Bitdefender. Per maggiori informazioni, fai riferimento a «*Bitdefender Central*» (p. 37).

Procedi in base alla tua situazione.

Voglio creare un account Bitdefender

Inserisci le informazioni richieste nei campi corrispondenti e clicca sul pulsante **CREA ACCOUNT**.

I dati forniti resteranno riservati.

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

Prima di continuare, leggi i Termini di servizio di Bitdefender.

Nota

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

Ho già un account di Bitdefender

Clicca su **Accedi** e inserisci il tuo indirizzo e-mail e la tua password di account Bitdefender.

Clicca su **ACCEDI** per continuare.

Se hai dimenticato la password del tuo account o semplicemente vuoi cambiarla, clicca sul link **Ho dimenticato la mia password**. Inserisci il tuo indirizzo e-mail e clicca sul pulsante **HO DIMENTICATO LA PASSWORD**. Verifica il tuo account e-mail e segui le istruzioni fornite per impostare una nuova password per il tuo account Bitdefender.

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

Voglio accedere usando il mio account Microsoft, Facebook o Google

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

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

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

Fase 5 - Attiva il prodotto

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

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

Procedi secondo la tua situazione:

- Ho un codice di attivazione

  In questo caso, attiva il prodotto seguendo questi passaggi:

  1. Inserisci il codice di attivazione nel campo **Ho un codice di attivazione** e clicca su **CONTINUA**.

Nota
Puoi trovare il codice di attivazione:
- Sull'etichetta del CD/DVD.
- Sulla scheda di registrazione del prodotto.
- Nella e-mail di acquisto online.

2. **Voglio valutare Bitdefender**

   In questo caso, puoi usare il prodotto per un periodo di 30 giorni. Per iniziare il periodo di prova, seleziona **Non ho un abbonamento e voglio provare il prodotto gratuitamente**, poi clicca su **CONTINUA**.

Fase 6 - Come iniziare

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

Clicca su **FINE** per accedere all'interfaccia di Bitdefender Internet Security 2018.

INIZIARE

4. LE BASI

Una volta installato Bitdefender Internet Security 2018, il tuo computer sarà protetto da ogni tipo di minaccia (come malware, spyware, ransomware, exploit, botnet e Trojan) e minacce web (come hacker, phishing e spam).

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

Connettersi a reti wireless pubbliche di aeroporti, centri commerciali, bar o alberghi senza protezione potrebbe essere pericoloso per il tuo dispositivo e i tuoi dati. Principalmente, perché eventuali impostori potrebbero osservare le tue attività e trovare il momento migliore per sottrarre dati personali, ma anche perché chiunque può vedere il tuo indirizzo IP, rendendo quindi il tuo dispositivo la probabile vittima di futuri attacchi informatici. Per evitare questo tipo di spiacevoli situazioni, installa e usa la app «*VPN*» (p. 161).

Puoi memorizzare le tue password e gli account online, salvandoli con «*Protezione di Password Manager per le tue credenziali*» (p. 153) in un Portafoglio. Con una sola password principale puoi proteggere la tua privacy da eventuali intrusi che potrebbero tentare di sottrarti del denaro.

«*Protezione webcam*» (p. 142)Impedisce alle app non affidabili di accedere alla tua videocamera, bloccando così ogni tentativo di prenderne il controllo. In base alle scelte degli utenti di Bitdefender, l'accesso delle app più popolari alla tua webcam sarà consentito o bloccato.

Per proteggerti da potenziali occhi indiscreti, quando il dispositivo è connesso a una rete wireless non protetta, Bitdefender analizza il suo livello di sicurezza e, se necessario, fornisce suggerimenti per aumentare la sicurezza delle tue attività online. Per maggiori istruzioni su come proteggere i tuoi dati personali, fai riferimento al «*Wi-Fi Security Advisor*» (p. 138).

I tuoi file personali salvati in locale, come documenti, fotografie o filmati, e anche quelli memorizzati nel cloud, ora possono restare sempre al sicuro dalle minacce moderne e più pericolose, meglio conosciute come ransomware. Per informazioni su come proteggere i file personali, fai riferimento a «*Safe files*» (p. 145).

Mentre lavori, usi un videogioco o guardi un film, Bitdefender può offrirti un'esperienza continuativa, posticipando eventuali attività di manutenzione, eliminando ogni interruzione e regolando gli effetti visivi del sistema. Puoi beneficiare di tutte queste opzioni, attivando e configurando i «*Profili*» (p. 186).

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

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

Per utilizzare le funzioni online di Bitdefender Internet Security 2018 e gestire i tuoi abbonamenti e dispositivi, accedi al tuo account Bitdefender. Per maggiori informazioni, fai riferimento a «*Bitdefender Central*» (p. 37).

Nella sezione «Come fare» (p. 48) troverai una serie di istruzioni passo passo per eseguire le attività più comuni. Se dovessi riscontrare problemi nell'utilizzare Bitdefender, controlla la sezione «*Risolvere i problemi più comuni*» (p. 195) per alcune possibili soluzioni ai problemi più comuni.

4.1. Aprire la finestra di Bitdefender

Per accedere all'interfaccia principale di Bitdefender Internet Security 2018, segui questi passaggi:

- In **Windows 7**:
  1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
  2. Clicca su **Bitdefender 2018**.
  3. Clicca su **Bitdefender Internet Security 2018** o più rapidamente, clicca due volte sull'icona di Bitdefender nell'area di notifica.
- In **Windows 8 e Windows 8.1**:

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

- In **Windows 10**:

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

Per maggiori informazioni sulla finestra di Bitdefender e l'icona nell'area di notifica, fai riferimento a «*Interfaccia di Bitdefender*» (p. 22).

4.2. Risolvere i problemi

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

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

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

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

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

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

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

4.2.1. Procedura guidata problemi di sicurezza

Per risolvere i problemi rilevati segui la procedura guidata **Problemi di sicurezza**.

1. Per aprire la procedura guidata, fai una delle seguenti operazioni:
   - Clicca con il pulsante destro sull'icona di Bitdefender nell'area di notifica e seleziona **Visualizza i problemi di sicurezza**.
   - Apri l'interfaccia di Bitdefender e clicca in qualsiasi punto dell'area Stato sicurezza nella barra degli strumenti superiore.
2. Puoi visualizzare i problemi che influenzano la sicurezza del computer e dei dati. Tutti i problemi attuali sono stati selezionati per essere risolti.

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

   Lo stato del problema diventerà **Posticipato** e non sarà intrapresa alcuna azione per risolverlo.
3. Per risolvere i problemi selezionati, clicca su **Risolvi**. Alcuni problemi vengono risolti immediatamente. Per altri problemi verrà eseguito un assistente per poterli risolvere.

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

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

4.2.2. Configurare gli avvisi di stato

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

- Antivirus
- Firewall
- Aggiornamento

- Sicurezza browser

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **AVANZATE**.
3. Clicca sul link **Configura avvisi di stato**.
4. Clicca sugli interruttori per attivare o disattivare gli avvisi di stato in base alle tue preferenze.

4.3. Notifiche

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

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

Per accedere al registro delle notifiche, clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender. Ogni volta che si verifica un evento critico, sull'icona compare un contatore.

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

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

Clicca su ogni scheda per scoprire maggiori dettagli sugli eventi generati. Cliccando una sola volta su ciascun titolo di un evento, vengono mostrati alcuni dettagli: una breve descrizione, l'azione intrapresa da Bitdefender

quando è successo e la data e l'ora in cui si è verificato. Se necessario, possono essere fornite opzioni per intraprendere ulteriori azioni.

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

4.4. Autopilot

Per tutti gli utenti che vogliono essere protetti dalla propria soluzione di sicurezza senza tanti problemi, Bitdefender Internet Security 2018 include una modalità Autopilot.

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

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

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

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

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

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

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

4.5. Profili

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

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

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

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

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

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

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

Profilo rete Wi-Fi pubblica
: Vengono applicate le impostazioni del prodotto per usufruire di una protezione totale mentre si è connessi a una rete wireless non sicura.

Profilo Modalità Batteria
: Vengono applicate le impostazioni del prodotto, bloccando ogni attività in background per risparmiare il consumo della batteria.

4.5.1. Configura l'attivazione automatica dei profili

Per un'esperienza più intuitiva, puoi configurare Bitdefender per gestire i tuoi profili operativi. In questo caso, Bitdefender rileva automaticamente l'attività eseguita e applica le impostazioni di ottimizzazione del sistema e del prodotto.

Per consentire a Bitdefender di attivare i profili:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **PROFILI**.

3. Usa l'interruttore corrispondente per attivare **Attiva i profili automaticamente**.

Se non desideri che i Profili siano attivati automaticamente, disattiva l'interruttore.

Per attivare manualmente un profilo, clicca sull'interruttore ATTIVA/INATTIVA corrispondente. È possibile attivare manualmente un solo profilo alla volta.

Per maggiori informazioni sui Profili, fai riferimento a «*Profili*» (p. 186)

4.6. Impostazioni protette da password di Bitdefender

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

Per configurare la protezione password per le impostazioni di Bitdefender:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Nella finestra **GENERALE**, attiva la **Protezione password**, cliccando sull'interruttore corrispondente.
3. Inserisci la password nei due campi e poi clicca su **OK**. La password deve essere composta da almeno 8 caratteri.

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

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

Per rimuovere la protezione della password:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Nella finestra **GENERALE**, disattiva la protezione della password, cliccando sull'interruttore corrispondente.
3. Inserisci la password e clicca su **OK**.

Nota

Per modificare la password del tuo prodotto, clicca sul link **Cambia password**. Digita la tua password attuale e clicca su *OK*. Nella nuova finestra che comparirà, digita la nuova password che vuoi utilizzare d'ora in poi per limitare l'accesso alle tue impostazioni di Bitdefender.

4.7. Rapporti anonimi sull'utilizzo

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

Nel caso volessi bloccare l'invio di rapporti di utilizzo anonimi:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **AVANZATE**.
3. Clicca sull'interruttore ATTIVA/INATTIVA.

4.8. Notifiche offerte speciali

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

Per attivare o disattivare le notifiche sulle offerte speciali:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Nella finestra **GENERALE**, clicca sull'interruttore ATTIVA/INATTIVA corrispondente.

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

5. INTERFACCIA DI BITDEFENDER

Bitdefender Internet Security 2018 soddisfa le necessità di persone esperte e di principianti. L'interfaccia grafica dell'utente è quindi stata progettata per essere adatta a qualsiasi categoria di utenti.

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

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

La finestra principale ti consente di gestire il comportamento del prodotto usando Autopilot, ti dà accesso a informazioni importanti sul prodotto e ti permette di eseguire alcune attività più comuni. Dalla barra laterale sinistra puoi accedere al tuo account Bitdefender e alle sezioni di Bitdefender dedicata a una configurazione più dettagliata e ad alcune attività gestionali avanzate.

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

5.1. Icona area di notifica

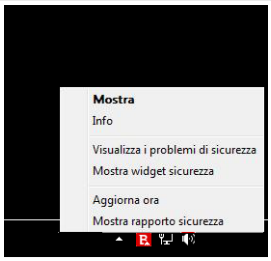
Per gestire tutto il prodotto più velocemente, puoi utilizzare l'icona di Bitdefender nell'area di notifica.

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

- In **Windows 7, Windows 8 e Windows 8.1**:
  1. Clicca sulla freccia nell'angolo in basso a destra dello schermo.
  2. Clicca su **Personalizza...** per aprire la finestra delle icone dell'area di Notifica.
  3. Seleziona l'opzione **Mostra icone e notifiche** per l'**icona dell'agente di Bitdefender**.
- In **Windows 10**:

1. Clicca con il pulsante destro sulla barra delle applicazioni e seleziona **Proprietà**.
2. Clicca su **Personalizza** nella finestra della barra delle applicazioni.
3. Clicca sul link **Seleziona le icone che compaiono sulla barra delle applicazioni** nella finestra **Notifiche e azioni**.
4. Attiva l'interruttore accanto a **Bitdefender Agent**.

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



Icona della barra delle applicazioni

- **Mostra** - Apre la finestra principale di Bitdefender.
- **Info** - Apre una finestra in cui puoi visualizzare maggiori informazioni su Bitdefender, dove cercare aiuto nel caso dovesse verificarsi qualcosa di inaspettato e rivedere l'Accordo di abbonamento, i componenti di terze parti e l'Informativa sulla privacy.
- L'opzione **Visualizza i problemi di sicurezza** ti aiuta a rimuovere le vulnerabilità attuali. Se l'opzione non è disponibile, non ci sono errori da risolvere. Per informazioni dettagliate, fai riferimento a «*Risolvere i problemi*» (p. 15).
- **Nascondi / Mostra widget sicurezza** - Attiva / disattiva il widget sicurezza.
- **Aggiorna ora** - Inizia un aggiornamento immediato. Puoi seguire lo stato di aggiornamento nel pannello Aggiornamento della finestra principale di Bitdefender.
- L'opzione **Mostra rapporto sicurezza** apre una finestra dove è possibile visualizzare uno stato settimanale oltre a diversi suggerimenti per il sistema. Puoi seguire i suggerimenti per migliorare la sicurezza del sistema.

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

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

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

5.2. Finestra principale

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

La finestra è organizzata in quattro sezioni principali:

Stato
: Qui è dove puoi verificare lo stato di sicurezza del computer, lanciare un aggiornamento e configurare l'Autopilot.

Barra laterale sinistra
: Questo menu ti consente di accedere e gestire il tuo account Bitdefender oltre a diverse funzionalità online, oppure alternarti tra le tre sezioni principali del prodotto. Da qui, puoi accedere anche alle notifiche, il rapporto di sicurezza settimanale, le impostazioni generali e le sezioni di Supporto.

I pulsanti azione e accesso per la sezione delle funzionalità
: Da qui puoi eseguire diverse attività per mantenere sempre protetto il tuo sistema. Inoltre, puoi accedere alle funzionalità di Bitdefender per configurare il prodotto per conto tuo.

Barra inferiore
: Qui è dove puoi installare facilmente Bitdefender sugli altri dispositivi, sempre che il tuo abbonamento abbia abbastanza slot disponibili.

5.2.1. Stato

La sezione stato include i seguenti elementi:

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

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

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

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

- L'opzione **AUTOPILOT** ti consente di attivare una protezione ottimale e usufruire di una sicurezza silenziosa. Per informazioni dettagliate, fai riferimento a «*Autopilot*» (p. 18).
- L'opzione **AGGIORNA ORA** ti consente di eseguire un aggiornamento del prodotto ogni volta che vuoi assicurarti di avere il database di informazioni sulle minacce più aggiornato. Per informazioni dettagliate, fai riferimento a «*Mantenere aggiornato Bitdefender*» (p. 43).
- L'opzione **Attiva profilo** mostra il profilo attuale attivato nel tuo prodotto Bitdefender. Per informazioni dettagliate, fai riferimento a «*Profili*» (p. 186).

5.2.2. Barra laterale sinistra

Nella barra laterale sinistra sono disponibili alcune icone che ti consentono di accedere al tuo account Bitdefender, le sezioni del prodotto, il rapporto sulle attività, le notifiche, le impostazioni generali e il supporto tecnico.

I nomi delle icone sono visibili cliccando sull'icona ☰, come segue:

- **Protezione**. I pulsanti azione **Scansione veloce** e **Scansione vulnerabilità** diventano visibili nell'angolo in basso a sinistra dell'interfaccia di Bitdefender. Inoltre, diventano visibili informazioni sulle applicazioni bloccate, oltre alle minacce e agli attacchi rilevati. Clicca sul link **VEDI FUNZIONALITÀ** per accedere alla sezione della configurazione.
- **Privacy**. I pulsanti azione **Safepay** e **VPN** diventano visibili nell'angolo in basso a sinistra dell'interfaccia di Bitdefender. Inoltre, vengono mostrate informazioni sui Portafogli e i File Vault rilevati. Clicca sul link **VEDI FUNZIONALITÀ** per accedere alla sezione della configurazione.
- **Attività**. Qui puoi vedere le attività del prodotto negli ultimi 30 giorni e accedere al rapporto di sicurezza che viene generato ogni sette giorni.
- **Notifiche**. Da qui, puoi accedere alle notifiche già generate.
- **Account**. Sono disponibili maggiori dettagli sul tuo account Bitdefender e sull'abbonamento attuale. Accedi al tuo account Bitdefender per verificare i tuoi abbonamenti ed eseguire le funzioni di sicurezza sui dispositivi che gestisci.
- **Impostazioni**. Da qui, puoi accedere alle impostazioni generali.
- **Supporto**. Da qui, se hai bisogno di assistenza per risolvere un determinato problema con Bitdefender Internet Security 2018, puoi contattare l'assistenza tecnica di Bitdefender.

5.2.3. I pulsanti azione e accesso per la sezione delle funzionalità

Usando i pulsanti azione, puoi lanciare rapidamente alcune attività importanti. I pulsanti azione diventano visibili nell'angolo in basso a sinistra dell'interfaccia di Bitdefender selezionando una delle due sezioni: **Protezione** e **Privacy** nella barra laterale sinistra.

In base alla sezione scelta, i pulsanti azione visibili in quest'area possono essere:

- **Scansione veloce**. Esegui una scansione veloce per assicurarti che il computer sia libero da minacce.

- **Scansione vulnerabilità**. Esegui una scansione del computer alla ricerca di vulnerabilità per assicurarti che tutte le applicazioni installate, incluso il sistema operativo, siano aggiornate e funzionino correttamente.
- **Safepay**. Apri Bitdefender Safepay™ per proteggere i tuoi dati sensibili durante l'elaborazione delle transazioni online.
- **VPN**. Apri Bitdefender VPN per aggiungere un ulteriore livello di protezione mentre ti connetti a Internet.

5.2.4. Barra inferiore

Per iniziare a proteggere altri dispositivi:

1. Clicca sul link **INSTALLA SU UN ALTRO DISPOSITIVO**.

   Sarai reindirizzato alla pagina web account Bitdefender. Assicurati di aver eseguito l'accesso con le tue credenziali.

2. Nella finestra che comparirà, seleziona il sistema operativo desiderato e poi clicca su **CONTINUA**.

3. Digita l'indirizzo e-mail a cui inviare il link di download per la piattaforma scelta.

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

- Bitdefender Internet Security 2018 su dispositivi Windows.
- Bitdefender Antivirus for Mac su dispositivi macOS.
- Bitdefender Mobile Security su dispositivi Android.
- Bitdefender Mobile Security su dispositivi iOS.
- Il Parental Advisor di Bitdefender su macOS, iOS e dispositivi Android.

5.3. Le sezioni di Bitdefender

Il prodotto Bitdefender include tre sezioni divise con funzionalità utili per garantirti la massima sicurezza mentre lavori, navighi sul web, giochi o esegui pagamenti online.

Quando vuoi utilizzare le funzionalità di una determinata sezione o iniziare a configurare il prodotto, accedi alle seguenti icone situate sulla barra laterale sinistra dell'interfaccia di Bitdefender:

- Protezione

- Privacy

5.3.1. Protezione

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

Le funzionalità che puoi gestire nella sezione Protezione sono:

ANTIVIRUS

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

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

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

Per maggiori informazioni sulle attività di scansione e su come configurare la protezione antivirus, fai riferimento a «*Protezione antivirus*» (p. 90).

PROTEZIONE WEB

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

Per maggiori informazioni su come configurare Bitdefender per proteggere le tue attività sul web, fai riferimento a «*Protezione web*» (p. 115).

FIREWALL

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

Per maggiori informazioni sulla configurazione del firewall, fai riferimento a «*Firewall*» (p. 128).

ADVANCED THREAT DEFENSE

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

Per maggiori informazioni su come tenere il sistema al sicuro dalle minacce, fai riferimento a «*Difesa da minacce avanzate*» (p. 113).

ANTISPAM

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

Per maggiori informazioni sulla protezione antispam, fai riferimento a «*Antispam*» (p. 118).

VULNERABILITÀ

La funzionalità Vulnerabilità ti aiuta a mantenere costantemente aggiornati il sistema operativo e le applicazioni che usi regolarmente, oltre a identificare le reti wireless poco sicure a cui ti connetti.

Clicca su **Scansione vulnerabilità** nella funzionalità Vulnerabilità per iniziare a identificare gli aggiornamenti critici di Windows, gli aggiornamenti delle applicazioni, le password non sicure appartenenti agli account di Windows e le reti wireless pericolose.

Clicca su **Wi-Fi Security Advisor** per visualizzare l'elenco delle reti wireless a cui ti connetti, oltre alla nostra valutazione della reputazione per ciascuna di esse e le azioni che puoi intraprendere per restare protetto da potenziali intrusioni non autorizzate.

Per maggiori informazioni sulla configurazione della protezione dalle vulnerabilità, fai riferimento a «*Vulnerabilità*» (p. 134).

SAFE FILES

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

Per maggiori informazioni su come configurare Safe files per proteggere i tuoi file personali dagli attacchi ransomware, fai riferimento a «*Safe files*» (p. 145).

5.3.2. Privacy

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

Le funzionalità che puoi gestire nella sezione Privacy sono:

VPN

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

Per maggiori informazioni su questa funzionalità, fai riferimento a «*VPN*» (p. 161).

CRITTOGRAFIA FILE

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

Per trovare maggiori informazioni su come creare unità logiche (o vault) crittografate e protette da password sul computer, fai riferimento a «*Crittografia file*» (p. 148).

PROTEZIONE WEBCAM

La Protezione webcam di Bitdefender protegge la tua webcam, bloccandone l'accesso da parte di app non affidabili.

Per maggiori informazioni su come tenere la webcam al sicuro da accessi indesiderati, fai riferimento a «*Protezione webcam*» (p. 142).

GESTORE PASSWORD

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

Per maggiori informazioni sulla configurazione del Password Manager, fai riferimento a «*Protezione di Password Manager per le tue credenziali*» (p. 153).

SAFEPAY

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

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

Per maggiori informazioni su Bitdefender Safepay™, fai riferimento a «*Safepay: sicurezza per le transazioni online*» (p. 164).

Parental Advisor

Il Parental Advisor di Bitdefender ti consente di monitorare le attività dei bambini sul computer. In caso di contenuti inappropriati, puoi decidere di limitare l'accesso a Internet o a determinate applicazioni.

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

Per maggiori informazioni sulla configurazione del Parental Advisor, fai riferimento a «*Parental Advisor*» (p. 171).

PROTEZIONE DATI

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

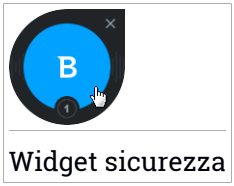
Per maggiori informazioni sulla configurazione della Protezione dati, fai riferimento a «*Protezione dati*» (p. 169).

5.4. Widget sicurezza

Il **widget sicurezza** è un modo semplice e veloce per monitorare e controllare Bitdefender Internet Security 2018. Aggiungendo questo piccolo e discreto widget sul desktop, puoi visualizzare tutte le informazioni critiche ed eseguire le attività principali in qualsiasi momento:

- apri la finestra principale di Bitdefender.
- Monitorare le attività di scansione in tempo reale.
- Monitorare lo stato di sicurezza del sistema e risolvere ogni eventuale problema.
- mostra quando è in corso un aggiornamento.
- Visualizzare le notifiche e accedere agli ultimissimi eventi segnalati da Bitdefender.

- Eseguire una scansione di file o cartelle, trascinando e rilasciando uno o più elementi sul widget.



Widget sicurezza

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

Alcuni problemi critici influenzano la sicurezza del tuo sistema.

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

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

Il tuo sistema è protetto.

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

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

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

5.4.1. Eseguire la scansione di file e cartelle

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

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

5.4.2. Nascondi / mostra widget sicurezza

Se non desideri più visualizzare il widget, clicca su .

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

- Dall'area di notifica:
  1. Clicca con il pulsante destro sull'icona di Bitdefender nell'area di notifica.
  2. Clicca su **Mostra widget sicurezza** nel menu contestuale che apparirà.
- Dall'interfaccia di Bitdefender:
  1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
  2. Seleziona la scheda **GENERALE**.
  3. Attiva l'opzione **Mostra widget sicurezza** cliccando sull'interruttore corrispondente.

Di norma, il widget sicurezza di Bitdefender è disattivato.

5.5. Attività

La finestra Attività mostra informazioni sulle azioni intraprese da Bitdefender sul tuo dispositivo negli ultimi 30 giorni. Qui puoi verificare quali applicazioni, minacce e attacchi sono stati bloccati durante tale periodo e se si è verificato un eventuale attacco ransomware.

È possibile anche accedere al rapporto sulla sicurezza, che fornisce uno stato settimanale per il prodotto oltre a vari consigli su come migliorare la

protezione del sistema, cliccando sul link corrispondente. Questi suggerimenti sono importanti per la gestione della protezione globale e potrai facilmente verificare le azioni che si possono intraprendere sul sistema.

Il rapporto viene generato una volta la settimana e riassume le informazioni più importanti sulle attività del tuo prodotto, in modo da verificare facilmente quali eventi siano avvenuti in questo periodo di tempo.

Le informazioni offerte dal Rapporto sicurezza sono suddivise in tre categorie:

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

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

    Per maggiori informazioni sulla protezione antivirus, fai riferimento a «*Protezione antivirus*» (p. 90)
  - **Pagine web esaminate**

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

    Per maggiori informazioni sulla Protezione web, fai riferimento a «*Protezione web*» (p. 115).
  - **Vulnerabilità**

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

    Per maggiori informazioni sulla Scansione vulnerabilità, fai riferimento a «*Vulnerabilità*» (p. 134).
  - **Cronologia eventi**

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

    Per maggiori informazioni sul registro dettagliato degli eventi, inerenti l'attività del computer, seleziona «*Notifiche*» (p. 17).

- La sezione **Privacy** - Visualizza le informazioni relative alla privacy del sistema.
  - **File nel Vault**

    Ti consente di visualizzare quanti file sono protetti da accessi indesiderati.

    Per trovare maggiori informazioni su come creare unità logiche (o vault) crittografate e protette da password sul computer, fai riferimento a «*Crittografia file*» (p. 148).
- La sezione **Ottimizzazione** consente di visualizzare le informazioni relative allo spazio liberato, alle applicazioni ottimizzate e a quanta batteria hai risparmiato usando il profilo Modalità Batteria.
  - **Batteria risparmiata**

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

    Per maggiori informazioni sul profilo Modalità Batteria, fai riferimento a «*Profilo Modalità Batteria*» (p. 191).
  - **App ottimizzate**

    Ti consente di visualizzare il numero di app che hai usato sotto i Profili.

    Per maggiori informazioni sui Profili, fai riferimento a «*Profili*» (p. 186).

5.5.1. Controllare il Rapporto sicurezza

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

Per controllare il Rapporto sulla sicurezza:

1. Accedi al rapporto:
   - Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.

Clicca sul link **Rapporto sicurezza** nell'angolo in basso a destra della finestra Rapporto attività.

- Clicca con il pulsante destro sull'icona di Bitdefender nell'area di notifica e seleziona **Mostra rapporto sicurezza**.
- Una volta completato un rapporto, comparirà una finestra per avvisarti. Clicca su **Mostra** per accedere al rapporto attività.

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

2. Puoi verificare lo stato generale della sicurezza nella parte superiore della finestra.
3. Controlla i nostri suggerimenti in fondo alla pagina.

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

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

5.5.2. Attivare o disattivare la notifica del Rapporto di sicurezza

Per attivare o disattivare la notifica del rapporto sulla sicurezza:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Nella finestra **GENERALE**, clicca sull'interruttore ATTIVA/INATTIVA corrispondente.

   Di norma, gli avvisi del rapporto sicurezza sono attivati.

6. BITDEFENDER CENTRAL

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

- Scarica e installa Bitdefender su sistemi operativi Windows, macOS, iOS e Android. I prodotti che è possibile scaricare sono:
  - Bitdefender Internet Security 2018
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security per Android
  - Bitdefender Mobile Security for iOS
  - Bitdefender Parental Advisor
- Gestisci e rinnova i tuoi abbonamenti di Bitdefender.
- Aggiungi nuovi dispositivi alla tua rete e gestiscili ovunque ti trovi.
- Configura le impostazioni di Parental Advisor per i dispositivi dei bambini e monitora le loro attività ovunque ti trovi.

6.1. Accedere a Bitdefender Central

Ci sono diversi modi per accedere a Bitdefender Central. In base all'attività che intendi eseguire, puoi utilizzare una delle seguenti possibilità:

- Dall'interfaccia principale di Bitdefender:
  1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
  2. Seleziona il link **Vai a Bitdefender Central**.
  3. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
- Dal tuo browser web:
  1. Apri un browser web su un dispositivo con accesso a internet.

2. Vai a: https://central.bitdefender.com.
3. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.

6.2. I miei abbonamenti

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

6.2.1. Controllare gli abbonamenti disponibili

Per controllare gli abbonamenti disponibili:

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

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

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

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

6.2.2. Aggiungi un nuovo dispositivo

Se l'abbonamento copre più di un dispositivo, è possibile aggiungerne un altro e installare Bitdefender Internet Security 2018 su di esso, come segue:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **I miei dispositivi** e clicca su **INSTALLA PROTEZIONE LOCALE**.
3. Seleziona una delle due opzioni disponibili:
   - **SCARICA**

     Clicca sul pulsante e salva il file d'installazione.
   - **Su un altro dispositivo**

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

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

6.2.3. Rinnova abbonamento

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

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

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

6.2.4. Attiva abbonamento

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

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

Per attivare un abbonamento utilizzando un codice di attivazione:

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

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

6.3. I miei dispositivi

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

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

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

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

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

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

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

Per aggiornare Bitdefender in remoto su un dispositivo:

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

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

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

- **Interfaccia**. In questa finestra puoi visualizzare maggiori dettagli sul dispositivo selezionato, oltre a controllare il suo stato di protezione, lo stato di Bitdefender VPN e quante minacce sono state bloccate negli ultimi sette giorni. Lo stato di protezione può essere verde, quando nessun problema influenza il dispositivo, giallo quando il dispositivo richiede le tue attenzioni, e rosso, quando il dispositivo è a rischio. Quando ci sono eventuali problemi che influenzano il dispositivo, clicca sulla freccia a tendina nell'area di stato superiore per scoprire maggiori dettagli. Da qui puoi risolvere manualmente i problemi che influenzano la sicurezza del tuo dispositivo.
- **Protezione**. Da questa finestra, puoi eseguire in remoto una Scansione veloce o una Scansione di sistema sui tuoi dispositivi. Clicca sul pulsante **CONTROLLA** per avviare il processo. Puoi anche verificare quanto è stata eseguita l'ultima scansione sul dispositivo e visualizzare un rapporto della scansione più recente con tutte le informazioni più importanti.Per maggiori informazioni sui due processi di scansione, fai riferimento a «*Eseguire una scansione del sistema*» (p. 97) e «*Eseguire una Scansione veloce*» (p. 97).
- **Vulnerabilità**. Per verificare le vulnerabilità di un dispositivo, come l'assenza di aggiornamenti di Windows, applicazioni datate o password poco sicure, clicca sul pulsante **CONTROLLA** nella scheda Vulnerabilità. Le vulnerabilità non possono essere corrette in remoto. Nel caso venisse rilevata una vulnerabilità, devi eseguire una nuova scansione del dispositivo e intraprendere le azioni consigliate. Clicca su **Maggiori dettagli** per accedere

a un rapporto dettagliato sui problemi rilevati. Per maggiori dettagli su questa funzione, fai riferimento a «*Vulnerabilità*» (p. 134).

6.4. Il mio Account

Nella sezione **Il mio account**, hai la possibilità di personalizzare il tuo profilo, cambiare la password associata al tuo account, gestire le tue sessioni di accesso e i messaggi di aiuto di Bitdefender Central.

Cliccando sull'icona nel lato in alto a destra della schermata e seleziona **Il mio account**, otterrai le seguenti schede:

- **Profilo** - Qui puoi aggiungere e modificare le informazioni dell'account.
- **Cambia password** - Qui puoi modificare la password associata al tuo account.
- **Gestione sessione** - Qui puoi visualizzare e gestire le ultime sessioni di accesso inattive e attive in esecuzione sui dispositivi associati al tuo account.
- **Impostazioni** - Qui puoi attivare e disattivare i messaggi di aiuto di Bitdefender Central e decidere se essere informato o no, quando vengono scattate delle foto sui tuoi dispositivi Android.

6.5. Notifiche

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

7. MANTENERE AGGIORNATO BITDEFENDER

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

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

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

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

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

- Se il tuo computer si collega a Internet tramite un server proxy, devi configurare le impostazioni proxy come descritto nella sezione *«Come posso configurare Bitdefender per usare una connessione a Internet tramite proxy?»* (p. 83).
- 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. 205).
- Se sei connesso a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di Bitdefender su richiesta dell'utente. Per maggiori informazioni, fai riferimento a *«Eseguire un aggiornamento»* (p. 44).

7.1. Verificare se Bitdefender è aggiornato

Per verificare quando c'è stato l'ultimo aggiornamento di Bitdefender, controlla lo **Stato di sicurezza**, sul lato sinistro dell'area Stato.

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Nella scheda **Tutto**, seleziona la notifica relativa all'ultimo aggiornamento.

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

7.2. Eseguire un aggiornamento

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

Per avviare un aggiornamento, esegui una delle seguenti operazioni:

- Apri l'interfaccia di Bitdefender e clicca sul link **AGGIORNA ORA** localizzato sotto lo stato del tuo programma.
- Clicca con il pulsante destro sull'icona di Bitdefender nell'area di notifica e seleziona **Aggiorna ora**.

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

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

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

Per aggiornare Bitdefender in remoto su un dispositivo:

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

4. Seleziona **Aggiorna**.

7.3. Attivare o disattivare l'aggiornamento automatico

Per attivare o disattivare l'aggiornamento automatico:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **AGGIORNA**.
3. Clicca sull'interruttore ATTIVA/INATTIVA.
4. Comparirà una finestra di avviso. Devi confermare la tua scelta selezionando dal menu per quanto tempo desideri disattivare l'aggiornamento automatico. Puoi disattivare l'aggiornamento automatico per 5, 15 o 30 minuti, per un'ora, in modo permanente o fino a un riavvio del sistema.

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

7.4. Modificare le impostazioni di aggiornamento

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

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

Per regolare le impostazioni dell'aggiornamento:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **AGGIORNA** e regola le impostazioni in base alle tue preferenze.

Frequenza d'aggiornamento

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

Ubicazione aggiornamento

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

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

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

Regole di esecuzione dell'aggiornamento

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

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

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

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

7.5. Aggiornamenti costanti

Per assicurarsi che stai usando la versione più recente, Bitdefender cercherà automaticamente eventuali aggiornamenti del prodotto. Questi aggiornamenti potrebbero portare nuove funzionalità e miglioramenti, risolvere eventuali problemi del prodotto o fare l'upgrade automaticamente a una nuova versione. Quando la nuova versione di Bitdefender viene installata tramite un aggiornamento, le impostazioni personalizzate vengono salvate ed è possibile evitare le procedure di disinstallazione e reinstallazione.

Tali aggiornamenti richiedono un riavvio del sistema per avviare l'installazione di nuovi file. Quando l'aggiornamento di un prodotto viene completato, una finestra di pop-up ti informerà di riavviare il sistema. Se perdessi la notifica, puoi cliccare **RIAVVIA ORA** nella finestra Notifiche, dove viene indicato l'aggiornamento più recente o riavviare manualmente il sistema.

Nota

Gli aggiornamenti con nuove funzionalità e miglioramenti saranno consegnati solo agli utenti che hanno installato Bitdefender 2017.

COME FARE

8. INSTALLAZIONE

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

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

Per installare Bitdefender su un secondo computer:

1. Clicca sul link **INSTALLA SU UN ALTRO DISPOSITIVO** nell'angolo in basso a destra dell'interfaccia di Bitdefender.

   Sarai reindirizzato alla pagina web account Bitdefender. Assicurati di aver eseguito l'accesso con le tue credenziali.

2. Nella finestra che comparirà, seleziona il sistema operativo desiderato e poi clicca su **CONTINUA**.

3. Digita l'indirizzo e-mail a cui inviare il link di download per la piattaforma scelta.

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

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

8.2. Come posso reinstallare Bitdefender?

Alcune tipiche situazioni in cui dovresti reinstallare Bitdefender sono:

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

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

- In **Windows 7**:

  1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
  2. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
  3. Clicca su **REINSTALLA** nella finestra che comparirà.

4. Devi riavviare il computer per completare il processo.

- In **Windows 8 e Windows 8.1**:
  1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
  2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
  3. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
  4. Clicca su **REINSTALLA** nella finestra che comparirà.
  5. Devi riavviare il computer per completare il processo.
- In **Windows 10**:
  1. Clicca su **Start** e poi su Impostazioni.
  2. Clicca sull'icona **Sistema** nelle Impostazioni e seleziona **App e funzioni**.
  3. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
  4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
  5. Clicca su **REINSTALLA**.
  6. Devi riavviare il computer per completare il processo.

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

8.3. Dove posso scaricare il mio prodotto Bitdefender?

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

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

Per installare Bitdefender da Bitdefender Central:

1. Accedi a Bitdefender Central.

2. Seleziona il pannello **I miei dispositivi** e clicca su **INSTALLA PROTEZIONE LOCALE**.
3. Seleziona una delle due opzioni disponibili:
   - **SCARICA**

     Clicca sul pulsante e salva il file d'installazione.
   - **Su un altro dispositivo**

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

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

Se vuoi utilizzare Bitdefender in un'altra lingua, dovrai reinstallare il prodotto con la lingua desiderata.

Per utilizzare Bitdefender in un'altra lingua:

1. Rimuovi Bitdefender seguendo questi passaggi:
   - In **Windows 7**:
     a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
     b. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
     c. Clicca su **RIMUOVI** nella finestra che comparirà.
     d. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
   - In **Windows 8 e Windows 8.1**:
     a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
     b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
     c. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
     d. Clicca su **RIMUOVI** nella finestra che comparirà.

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

- In **Windows 10**:

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

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

  c. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.

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

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

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

2. Cambia la lingua di Bitdefender Central:

   a. Accedi a Bitdefender Central.

   b. Clicca sull'icona nell'angolo in basso a destra dello schermo.

   c. Clicca su **Il mio account** nel menu scorrevole.

   d. Seleziona la scheda **Profilo**.

   e. Seleziona la lingua dalla casella con elenco scorrevole **Lingua** e clicca su **SALVA**.

3. Scarica il file di installazione:

   a. Seleziona il pannello **I miei dispositivi** e clicca su **INSTALLA PROTEZIONE LOCALE**.

   b. Seleziona una delle due opzioni disponibili:

   - **SCARICA**

     Clicca sul pulsante e salva il file d'installazione.

   - **Su un altro dispositivo**

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

4. Esegui il prodotto Bitdefender che hai scaricato.

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

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

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

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

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

Può comparire in due occasioni:

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

  In questo caso, devi reinstallare il prodotto seguendo questi passaggi:

  - In **Windows 7**:

    1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
    2. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
    3. Clicca su **REINSTALLA** nella finestra che comparirà.
    4. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

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

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

1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
3. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
4. Clicca su **REINSTALLA** nella finestra che comparirà.
5. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

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

- In **Windows 10**:

1. Clicca su **Start** e poi su Impostazioni.
2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
3. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
5. Clicca su **REINSTALLA** nella finestra che comparirà.
6. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

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

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

- Hai cambiato sistema e vuoi continuare a utilizzare la protezione di Bitdefender. In questo caso, devi installare nuovamente il prodotto utilizzando la versione più recente.

  Per risolvere questa situazione:

1. Scarica il file di installazione:
   a. Accedi a Bitdefender Central.

b. Seleziona il pannello **I miei dispositivi** e clicca su **INSTALLA PROTEZIONE LOCALE**.

c. Seleziona una delle due opzioni disponibili:

- **SCARICA**

  Clicca sul pulsante e salva il file d'installazione.

- **Su un altro dispositivo**

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

2. Esegui il prodotto Bitdefender che hai scaricato.

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

8.6. Come posso fare l'upgrade alla versione più recente di Bitdefender?

A partire da Bitdefender 2018, l'upgrade alla versione più recente è possibile senza dover eseguire manualmente la procedura di disinstallazione e reinstallazione. Più precisamente, il nuovo prodotto, che include nuove funzionalità e importanti miglioramenti, viene fornito tramite l'aggiornamento del prodotto stesso e nel caso avessi già un abbonamento attivo di Bitdefender, viene attivato automaticamente.

Se stai giù usando la versione 2017, puoi fare l'upgrade alla versione più recente seguendo questi passaggi:

1. Clicca su **RIAVVIA ORA** nella notifica che ricevi con le informazioni dell'upgrade. Se non l'hai vista, accedi alla finestra Notifiche, cerca l'aggiornamento più recente e clicca sul pulsante **RIAVVIA ORA**. Attendi che il computer venga riavviato.

   Comparirà la finestra **Novità** con maggiori informazioni sulle nuove funzionalità e quelle migliorate.

2. Clicca sui link **Leggi altro** per essere reindirizzato alla nostra pagina dedicata con maggiori dettagli e articoli utili.

3. Chiudi la finestra **Novità** per accedere all'interfaccia della nuova versione installata.

Gli utenti che vogliono fare l'upgrade gratuitamente da Bitdefender 2016 o precedente alla versione di Bitdefender più recente, devono rimuovere la loro versione attuale dal Pannello di Controllo e scaricare il file di installazione più recente dal sito web di Bitdefender al seguente indirizzo: http://www.bitdefender.it/Downloads/. L'attivazione è possibile solo con un abbonamento valido.

9. ABBONAMENTI

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

Se hai un codice di licenza valido e vuoi utilizzarlo per attivare un abbonamento a Bitdefender Internet Security 2018, ci sono due possibilità:

- Sei passato da una versione precedente di Bitdefender a quella nuova:
  1. Una volta completato l'upgrade di Bitdefender Internet Security 2018, ti sarà chiesto di accedere al tuo account Bitdefender.
  2. Clicca su **Accedi** e inserisci il tuo indirizzo e-mail e la tua password di account Bitdefender.
  3. Clicca su **ACCEDI** per continuare.
  4. Nella schermata del tuo account comparirà una notifica che ti confermerà la creazione di un abbonamento. L'abbonamento così creato sarà valido per i giorni restanti nel tuo codice di licenza e per lo stesso numero di utenti.

     I dispositivi che stanno utilizzando versioni precedenti di Bitdefender e sono registrati con il codice di licenza che hai convertito in un abbonamento, dovranno attivare il prodotto con lo stesso account Bitdefender.
- Bitdefender non è stato precedentemente installato sul sistema:
  1. Una volta completata la fase di installazione, ti sarà chiesto di accedere al tuo account Bitdefender.
  2. Clicca su **Accedi** e inserisci il tuo indirizzo e-mail e la tua password di account Bitdefender.
  3. Clicca su **ACCEDI** per continuare e poi sul pulsante **FINE** per accedere all'interfaccia di Bitdefender Internet Security 2018.
  4. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
  5. Clicca sul link **Codice di attivazione**.

     Comparirà una nuova finestra.

6. Clicca sul link **Ottieni subito il tuo upgrade gratuito!**.
7. Inserisci il tuo codice di licenza nel campo corrispondente e clicca su **FAI L'UPGRADE DEL MIO PRODOTTO**. Un abbonamento con la stessa disponibilità e numero di utenti del tuo codice di licenza è stato associato al tuo account.

10. BITDEFENDER CENTRAL

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

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

Per utilizzare un altro account:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul pulsante **CAMBIA ACCOUNT** per cambiare l'account associato al computer.
3. Inserisci l'indirizzo e-mail e la password del tuo account nei campi corrispondenti e clicca su **ACCEDI**.

Nota
Il prodotto Bitdefender dal tuo dispositivo cambia automaticamente in base all'abbonamento associato al nuovo account Bitdefender.
Se non ci fosse alcun abbonamento disponibile associato al nuovo account Bitdefender o si volesse trasferirlo dall'account precedente, contattare il supporto tecnico di Bitdefender, come descritto nella sezione *«Chiedere aiuto»* (p. 230).

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

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

Se desideri disattivare questo tipo di messaggi:

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

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

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

- Dall'interfaccia di Bitdefender:

  1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
  2. Clicca sul pulsante **CAMBIA ACCOUNT**.

     Comparirà una nuova finestra.
  3. Clicca sul collegamento **Ho dimenticato password**.
  4. Inserisci l'indirizzo e-mail utilizzato per creare il tuo account Bitdefender e clicca sul pulsante **HO DIMENTICATO LA PASSWORD**.
  5. Controlla la tua casella di posta e clicca sul pulsante fornito.

     Si aprirà la finestra MODIFICA PASSWORD di Bitdefender.
  6. Inserisci l'indirizzo e-mail e la nuova password nel campo corrispondente. La password deve essere composta da almeno 8 caratteri e includere dei numeri.
  7. Clicca sul pulsante **CAMBIA PASSWORD**.

- Dal tuo browser web:

  1. Vai a: https://central.bitdefender.com.
  2. Clicca sul collegamento **Ho dimenticato password**.
  3. Inserisci il tuo indirizzo e-mail e clicca sul pulsante **HO DIMENTICATO LA PASSWORD**.
  4. Verifica il tuo account e-mail e segui le istruzioni fornite per impostare una nuova password per il tuo account Bitdefender.

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

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

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

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

11. SCANSIONE CON BITDEFENDER

11.1. Come posso controllare un file o una cartella?

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

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

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

Tipiche situazioni in cui si userebbe questo metodo includono:

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

11.2. Come posso eseguire una scansione del mio sistema?

Per eseguire una scansione completa del sistema:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTIVIRUS**, clicca su **Scansione sistema**.
4. Segui la procedura guidata della Scansione di sistema per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati.

   Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo. Per maggiori informazioni, fai riferimento a «*Procedura guidata scansione antivirus*» (p. 101).

11.3. Come posso programmare una scansione?

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

Per programmare una scansione:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTIVIRUS**, clicca su **Gestisci scansioni**.
4. Seleziona il tipo di scansione che vuoi programmare tra Scansione completa del sistema o Scansione veloce e poi clicca su **Opzioni di scansione**.

   In alternativa, puoi creare un tipo di scansione che si adatti alle tue necessità, cliccando su **Nuova attività personalizzata**.
5. Attiva l'interruttore **Programma**.

   Seleziona una delle opzioni corrispondenti per impostare un elenco:

   - All'avvio del sistema
   - Una volta
   - Periodicamente

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

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

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTIVIRUS**, clicca su **Gestisci scansioni**.

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

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

   Puoi anche scegliere di spegnere il computer al termine della scansione, se non venisse rilevata alcuna minaccia. Ricordati che questo sarà il comportamento predefinito ogni volta che esegui questa attività.
6. Clicca su **OK** per salvare le modifiche e chiudere la finestra.
7. Usa l'interruttore corrispondente se vuoi programmare la tua attività di scansione.
8. Clicca su **Esegui scansione** e segui la procedura guidata della scansione per completarla. Al termine della scansione, ti sarà chiesto di scegliere quali azioni intraprendere sui file rilevati, se presenti.
9. Se lo desideri, puoi eseguire nuovamente una scansione personale precedente cliccando sulla rispettiva voce nell'elenco disponibile.

11.5. Come posso escludere una cartella dalla scansione?

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

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

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

Per aggiungere una cartella alla lista delle eccezioni:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
4. Clicca sulla scheda **ECCEZIONI**.
5. Clicca sul menu accordion **Elenco di file e cartelle escluse dalla scansione** e poi sul pulsante **AGGIUNGI**.
6. Clicca su **Esplora**, seleziona la cartella che desideri escludere dalla scansione e quindi scegli il tipo di scansione da cui escluderla.
7. Clicca su **Aggiungi** per salvare le modifiche e chiudere la finestra.

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

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

1. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
   b. Clicca sul link **VEDI FUNZIONALITÀ**.
   c. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
   d. Nella finestra **PROTEZIONE**, clicca sull'interruttore ATTIVA/INATTIVA.

      Comparirà una finestra di avviso. Devi confermare la tua scelta selezionando dal menu per quanto tempo desideri disattivare la protezione in tempo reale. Puoi disattivare la protezione in tempo reale per 5, 15 o 30 minuti, un'ora, in modo permanente o fino a un riavvio del sistema.
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a *«Come posso visualizzare gli elementi nascosti in Windows?»* (p. 85).

3. Ripristina il file dalla quarantena:
   a. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
   b. Clicca sul link **VEDI FUNZIONALITÀ**.
   c. Nel pannello **ANTIVIRUS**, clicca su **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. 64).
5. Attiva la protezione antivirus in tempo reale di Bitdefender.
6. Contatta gli operatori del nostro supporto in modo da poter rimuovere la rilevazione dell'aggiornamento delle informazioni sulle minacce. Per scoprire come fare, fai riferimento a «*Chiedere aiuto*» (p. 230).

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

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

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

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Nella scheda **Tutto**, seleziona la notifica relativa all'ultima scansione.

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

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

12. PARENTAL ADVISOR

12.1. Come posso proteggere i bambini dalle minacce online?

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

Per configurare il Parental Advisor:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PARENTAL ADVISOR**, clicca su **Configura**.

   Sarai reindirizzato alla pagina web account Bitdefender. Assicurati di aver eseguito l'accesso con le tue credenziali.
4. Si aprirà l'interfaccia del Parental Advisor. Qui è dove puoi verificare e configurare le impostazioni del Parental Advisor.
5. Clicca su **AGGIUNGI PROFILO** nel lato destro della finestra **BAMBINI**.
6. Imposta le informazioni richieste nei campi corrispondenti, come nome e data di nascita. Per aggiungere una foto del profilo, clicca sul link **Scegli file**. Clicca su **CONTINUA** per continuare

   In base agli standard di sviluppo, impostando la data di nascita del bambino, il programma carica automaticamente alcune impostazioni di ricerca del web considerate appropriate per quella categoria d'età.
7. Se sul dispositivo del bambino è già stato installato Bitdefender Internet Security 2018, seleziona il suo dispositivo nell'elenco disponibile e seleziona l'account che vuoi monitorare. Clicca su **SALVA**.

   Se il bambino utilizza un dispositivo Android o iOS e la app Parental Advisor di Bitdefender non è stata installata, clicca su **AGGIUNGI DISPOSITIVO**. Se il bambino usa un dispositivo Mac e la app Bitdefender Antivirus for Mac non è installata, clicca sullo stesso pulsante. Seleziona il sistema operativo per la app che vuoi installare e poi clicca su **CONTINUA** per continuare.

8. Inserisci l'indirizzo e-mail a cui inviare il link di download dell'applicazione di Bitdefender e clicca su **INVIA LINK DI INSTALLAZIONE**.

Controlla le attività dei bambini e modifica le impostazioni del Parental Advisor utilizzando il tuo account Bitdefender da qualsiasi computer o dispositivo mobile connesso a Internet.

Importante
Sui dispositivi basati su Windows, il prodotto Bitdefender Internet Security 2018 incluso nel tuo abbonamento deve essere scaricato e installato.
Su dispositivi macOS, il prodotto Bitdefender Antivirus for Mac deve essere scaricato e installato.
Sui dispositivi Android e iOS, l'applicazione Parental Advisor di Bitdefender deve essere scaricata e installata.

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

Il Parental Advisor di Bitdefender ti consente di controllare i contenuti a cui il bambino accede tramite il proprio dispositivo e di bloccare eventualmente l'accesso a un sito web.

Per bloccare l'accesso a un sito web, devi aggiungerlo all'elenco delle eccezioni, in questo modo:

1. Vai a: https://central.bitdefender.com.
2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
3. Clicca su **Parental Advisor** per accedere all'interfaccia.
4. Seleziona il profilo del bambino dalla finestra **BAMBINI**.
5. Seleziona la scheda **Siti web**.
6. Clicca sul pulsante **GESTISCI**.
7. Inserisci la pagina web che vuoi bloccare nel campo corrispondente.
8. Seleziona **Consenti** o **Blocca**.
9. Clicca su **FINISH** per salvare le modifiche.

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

12.3. Come posso impedire ai bambini di usare un gioco?

Il Parental Advisor di Bitdefender ti consente di controllare i contenuti a cui il bambino accede tramite il computer.

Per bloccare l'accesso a un gioco:

1. Vai a: https://central.bitdefender.com.
2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
3. Clicca su **Parental Advisor** per accedere all'interfaccia.
4. Seleziona il profilo del bambino dalla finestra **BAMBINI**.
5. Seleziona la scheda **Applicazioni**.

   Verrà mostrato un elenco di carte. Le carte rappresentano le app usate dal bambino.
6. Seleziona la carta con la app di cui vuoi bloccare l'utilizzo da parte del bambino.

   Il simbolo di spunta che comparirà, indica che il bambino non potrà più utilizzare quella app.

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

Il Parental Advisor di Bitdefender ti consente di bloccare le chiamate da numeri sconosciuti o da determinati amici nella rubrica del bambino.

Per bloccare un determinato contatto su un dispositivo Android dotato della app Bitdefender Parental Advisor:

1. Vai a: https://central.bitdefender.com.
2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
3. Clicca su **Parental Advisor** per accedere all'interfaccia.
4. Seleziona il profilo del bambino per cui vuoi impostare le limitazioni.
5. Seleziona la scheda **Contatti telefonici**.

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

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

   Il simbolo di spunta che comparirà, indica che il bambino non potrà più essere raggiunto dal numero di telefono selezionato.

Per bloccare un determinato contatto su un dispositivo Android non dotato della app Bitdefender Parental Advisor:

1. Vai a: https://central.bitdefender.com.
2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
3. Clicca su **Parental Advisor** per accedere all'interfaccia.
4. Seleziona il profilo del bambino per cui vuoi impostare le limitazioni.
5. Clicca sul link **Installa Parental Advisor su un dispositivo** nella scheda desiderata.
6. Clicca su **AGGIUNGI DISPOSITIVO** nella finestra che comparirà.
7. Di norma, viene selezionata l'opzione **Bitdefender Parental Advisor per Android**. Clicca su **CONTINUA** per continuare e installa la app sul dispositivo desiderato.
8. Seleziona la scheda **Contatti telefonici**.

   Verrà mostrato un elenco di carte. Le tessere rappresentano i contatti dello smartphone Android del bambino.

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

   Il simbolo di spunta che comparirà, indica che il bambino non potrà più essere raggiunto dal numero di telefono selezionato.

Per bloccare i numeri di telefono sconosciuti, attivare l'interruttore **Blocca interazioni con chiamate non identificabili**.

Nota
Le restrizioni per le chiamate possono essere impostate solo per i dispositivi Android aggiunti al profilo del bambino.

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

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

Per impostare un luogo:

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

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

12.6. Come posso impedire al bambino di accedere ai dispositivi assegnati nei giorni di scuola?

Bitdefender Parental Advisor ti consente di limitare l'accesso ai dispositivi assegnati da parte del bambino durante le ore di scuola e quando dovrebbe fare i compiti.

Per impostare le limitazioni:

1. Accedi al pannello Parental Advisor da Bitdefender Central.
2. Dalla finestra **IL MIO BAMBINO**, seleziona il profilo del bambino per cui vuoi impostare le limitazioni.
3. Seleziona la scheda **Calendario**.
4. Nella sezione **LIMITI GIORNALIERI**, clicca su **SPECIFICI**
5. Seleziona la casella **Limiti giorni di scuola**.
6. Seleziona dalla griglia gli intervalli di tempo durante i quali deve essere bloccato l'accesso.

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

12.7. Come posso impedire al bambino di accedere ai dispositivi assegnati nelle serate dei giorni di scuola?

Bitdefender Parental Advisor ti consente di limitare l'accesso ai dispositivi assegnati da parte del bambino durante le serate dei giorni di scuola.

Per impostare le limitazioni:

1. Accedi al pannello Parental Advisor da Bitdefender Central.
2. Dalla finestra **IL MIO BAMBINO**, seleziona il profilo del bambino per cui vuoi impostare le limitazioni.
3. Seleziona la scheda **Calendario**.
4. Nella sezione **Ora di dormire**, seleziona la casella **Serate giorni di scuola**.
5. Usa i tasti freccia su e giù delle rispettive caselle per impostare gli intervalli di tempo durante i quali deve essere bloccato l'accesso.

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

12.8. Come posso impedire al bambino di accedere ai dispositivi assegnati nei fine settimana?

Bitdefender Parental Advisor ti consente di limitare l'accesso ai dispositivi assegnati da parte del bambino durante le giornate e le serate dei fine settimana.

Per impostare le limitazioni:

1. Accedi al pannello Parental Advisor da Bitdefender Central.
2. Dalla finestra **IL MIO BAMBINO**, seleziona il profilo del bambino per cui vuoi impostare le limitazioni.
3. Seleziona la scheda **Calendario**.
4. Nella sezione **ORA DI DORMIRE**, seleziona la casella **Serate fine settimana**.
5. Usa i tasti freccia su e giù delle rispettive caselle per impostare gli intervalli di tempo durante i quali deve essere bloccato l'accesso.
6. Nella sezione **LIMITI GIORNALIERI**, hai le seguenti opzioni:
   - **CUMULATIVI**
     a. Seleziona la casella **Limiti fine settimana**.
     b. Trascina i cursori per impostare l'intervallo di tempo consentito per l'accesso ai dispositivi.
   - **SPECIFICI**
     a. Seleziona la casella **Limiti fine settimana**.
     b. Seleziona dalla griglia gli intervalli di tempo durante i quali deve essere bloccato l'accesso.

   Nota che le impostazioni **CUMULATIVI** e **SPECIFICI** sono progettate per non funzionare insieme.

> **Nota**
> Le restrizioni possono essere impostate solo per i dispositivi Android e Windows.

12.9. Come rimuovere un profilo di un bambino

Se vuoi rimuovere un profilo di un bambino esistente:

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

2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
3. Clicca su **Parental Advisor** per accedere all'interfaccia.
4. Clicca sull'icona dal profilo del bambino che vuoi eliminare e poi seleziona **Rimuovi**.

13. PROTEZIONE DELLA PRIVACY

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

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

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

Per mantenere le tue attività online sempre sicure e private:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul pulsante azione **Safepay**.
3. Clicca sul pulsante per accedere alla **tastiera virtuale**.

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

13.2. Come posso usare i File Vault?

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

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

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

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

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

Comparirà una nuova finestra. Procedi come segue:

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

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

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

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

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

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

- **Mantieni il vault sempre bloccato.**

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

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

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

Per maggiori informazioni su come usare i File Vault, fai riferimento a «*Crittografia file*» (p. 148).

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

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

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

1. Clicca con il pulsante destro sul file o la cartella che vuoi eliminare in maniera definitiva, seleziona Bitdefender e poi **Distruttore di file**.
2. Apparirà una finestra di conferma. Clicca su **SÌ, ELIMINA** per avviare la procedura guidata del Distruttore di file.

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

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PROTEZIONE WEBCAM**, clicca su **Accesso a webcam**.

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

Per scoprire ciò che gli altri utenti di Bitdefender hanno scelto di fare con la app selezionata, clicca sull'icona . Sarai avvisato ogni volta che le applicazioni nell'elenco vengono bloccate dagli utenti di Bitdefender, indipendentemente dallo stato di Autopilot.

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

14. INFORMAZIONI UTILI

14.1. Come posso testare la mia soluzione di sicurezza?

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

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

Per testare la tua soluzione di sicurezza:

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

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

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

Se non ricevi alcun avviso da parte di Bitdefender, ti consigliamo di contattare il supporto tecnico di Bitdefender come descritto nella sezione «*Chiedere aiuto*» (p. 230).

14.2. Come posso rimuovere Bitdefender?

Se vuoi rimuovere il tuo Bitdefender Internet Security 2018:

- In **Windows 7**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
  2. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
  3. Clicca su **RIMUOVI** nella finestra che comparirà.

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

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

1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
3. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
4. Clicca su **RIMUOVI** nella finestra che comparirà.
5. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

- In **Windows 10**:

1. Clicca su **Start** e poi su Impostazioni.
2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
3. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
5. Clicca su **RIMUOVI** nella finestra che comparirà.
6. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

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

14.3. Come posso rimuovere Bitdefender VPN?

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

- In **Windows 7**:

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

Attendere che il processo di disinstallazione sia terminato.

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

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

     Attendere che il processo di disinstallazione sia terminato.

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

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

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

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.

2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTIVIRUS**, clicca su **Gestisci scansioni**.
4. Nella finestra **GESTISCI ATTIVITÀ DI SCANSIONE**, clicca su **Nuova attività personalizzata** per inserire un nome per la scansione e selezionare i percorsi da esaminare.
5. Se desideri configurare le opzioni di scansione in ogni dettaglio, seleziona la scheda **Avanzate**.
6. Scegli di spegnere il computer al termine della scansione, se non venisse rilevata alcuna minaccia.
7. Clicca su **OK** per salvare le modifiche e chiudere la finestra.
8. Clicca sul pulsante **Esegui scansione** per avviare la scansione del tuo sistema.

Se non vengono rilevate minacce, il computer si spegnerà.

Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo. Per maggiori informazioni, fai riferimento a «*Procedura guidata scansione antivirus*» (p. 101).

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

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

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

Per gestire le impostazioni del proxy:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **AVANZATE**.

3. Attiva l'uso del proxy cliccando l'interruttore corrispondente.
4. Clicca sul collegamento **Gestione proxy**.
5. Ci sono due opzioni per determinare le impostazioni proxy:
   - **Importa le impostazioni del proxy dal browser predefinito** - le impostazioni del proxy dell'utente attuale, estratte dal browser predefinito. Se il server proxy richiede un nome utente e una password, devi indicarli nei rispettivi campi.

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

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

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

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

Per scoprire se hai un sistema operativo a 32 o 64 bit:

- In **Windows 7**:
  1. Clicca su **Start**.
  2. Individua **Risorse del computer** nel menu **Start**.
  3. Clicca con il pulsante destro su **Computer** e seleziona **Proprietà**.
  4. Vai in **Sistema** per verificare le informazioni sul tuo sistema.

- Per **Windows 8**:

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

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

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

- In **Windows 10**:

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

14.7. Come posso visualizzare gli elementi nascosti in Windows?

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

Segui questi passaggi per mostrare gli elementi nascosti in Windows:

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

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

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

In **Windows 10**:

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

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

14.8. 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 2018 rileva automaticamente altri programmi di sicurezza e ti offre la possibilità di disinstallarli.

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

- In **Windows 7**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
  2. Attendi per qualche istante, finché non compare l'elenco del software installato.
  3. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
  4. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
- In **Windows 8 e Windows 8.1**:
  1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
  2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
  3. Attendi per qualche istante, finché non compare l'elenco del software installato.

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

- In **Windows 10**:

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

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

14.9. Come posso riavviare in modalità provvisoria?

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

Per avviare Windows in modalità provvisoria:

- In **Windows 7**:

1. Riavvia il computer.
2. Premi più volte il tasto **F8** prima del lancio di Windows per accedere al menu di avvio.
3. Seleziona **Modalità provvisoria** nel menu di avvio o **Modalità provvisoria con supporto di rete** se desideri avere l'accesso a Internet.

4. Premi **Invio** e attendi il caricamento di Windows in modalità provvisoria.
5. Questo processo termina con un messaggio di conferma. Clicca su **OK** per confermare.
6. Per avviare Windows normalmente, riavvia semplicemente il sistema.

- In **Windows 8, Windows 8.1 e Windows 10**:

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

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

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

GESTIRE LA PROPRIA SICUREZZA

15. PROTEZIONE ANTIVIRUS

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

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

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

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

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

Bitdefender controlla automaticamente ogni supporto rimovibile che è collegato al computer per assicurarti di accedervi in sicurezza. Per maggiori informazioni, fai riferimento a «*Scansione automatica di supporti rimovibili*» (p. 105).

Gli utenti più esperti possono configurare le eccezioni della scansione, se non desiderano controllare determinati file o estensioni. Per maggiori informazioni, fai riferimento a «*Configurare le eccezioni della scansione*» (p. 108).

Quando rileva una minaccia, Bitdefender tenterà automaticamente di rimuovere il codice dannoso dal file infetto, ricostruendo il file originale. Questa operazione è denominata disinfezione. I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione. Per maggiori informazioni, fai riferimento a «*Gestire i file in quarantena*» (p. 110).

Se il tuo computer è stato infettato da una minaccia, fai riferimento a «*Rimuovere le minacce dal sistema*» (p. 218). Per aiutarti a ripulire il tuo computer dalle minacce che non possono essere rimosse dal sistema operativo Windows, Bitdefender ti offre una «*Bitdefender Modalità di soccorso*

(Ambiente di soccorso in Windows 10)» (p. 218). Si tratta di un ambiente sicuro, realizzato specificatamente per la rimozione delle minacce, che ti consente di avviare il tuo computer in modo indipendente da Windows. Quando il computer parte in Modalità soccorso (Ambiente di soccorso in Windows 10), le minacce di Windows non sono attive, semplificando così la loro rimozione.

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

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

15.1.1. Attivare o disattivare la protezione in tempo reale

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
4. Nella finestra **PROTEZIONE**, clicca sull'interruttore ATTIVA/INATTIVA.
5. Se vuoi disattivare la protezione in tempo reale, comparirà una finestra di avviso. Devi confermare la tua scelta selezionando dal menu per quanto tempo desideri disattivare la protezione in tempo reale. Puoi disattivare la protezione in tempo reale per 5, 15 o 30 minuti, un'ora, in modo permanente o fino a un riavvio del sistema. La protezione in tempo reale si attiverà automaticamente allo scadere del tempo indicato.

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

15.1.2. Configurare le impostazioni avanzate della protezione in tempo reale

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

Per configurare le impostazioni avanzate della protezione in tempo reale:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
4. Nella finestra **PROTEZIONE**, clicca sul menu a fisarmonica **MOSTRA IMPOSTAZIONI AVANZATE**.

   Verrà mostrata una finestra a pannelli.
5. Scorri in basso sulla finestra per configurare le impostazioni di scansione in base alle tue esigenze.

Informazioni sulle opzioni di scansione

Questa informazione potrebbe esserti utile:

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

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

  I file delle applicazioni (o dei programmi) sono più vulnerabili agli attacchi delle minacce 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

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

  Se decidi di usare questa opzione, attivala e trascina il cursore lungo la scala per impostare un limite massimo di dimensione (in MB) degli archivi da esaminare all'accesso.

- **Esaminare email.** Per impedire il download di minacce sul tuo computer, Bitdefender esamina automaticamente le e-mail in entrata e uscita.

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

- **Scansiona i settori di avvio.** È possibile impostare Bitdefender per controllare i settori di boot del disco rigido. Questo settore del disco rigido contiene il codice necessario per inizializzare il processo di avvio del computer. Quando una minaccia infetta il settore di boot, il disco potrebbe non essere accessibile e potrebbe non essere possibile avviare il sistema e accedere ai dati.

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

- **Scansiona per keylogger.** Seleziona questa opzione per eseguire una scansione del sistema alla ricerca di applicazioni keylogger. I keylogger registrano ciò che digiti sulla tastiera per poi inviare queste informazioni tramite Internet a un hacker. L'hacker può trovare informazioni sensibili

nei dati rubati, come numeri e password di un conto corrente, e usarle per ottenere benefici personali.

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

Azioni intraprese sulle minacce rilevate

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
4. Nella finestra **PROTEZIONE**, clicca sul menu a fisarmonica **MOSTRA IMPOSTAZIONI AVANZATE**.

   Verrà mostrata una finestra a pannelli.
5. Scorri in basso nella finestra finché non trovi l'opzione **Azioni dopo il termine della scansione**.
6. Configura le impostazioni della scansione come necessario.

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

Esegui azioni appropriate

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

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

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

eseguiti né essere aperti, annullando il rischio d'infezione. Per maggiori informazioni, fai riferimento a «*Gestire i file in quarantena*» (p. 110).

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

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

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

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

Sposta i file in quarantena
Sposta i file infetti nella quarantena. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Per maggiori informazioni, fai riferimento a «*Gestire i file in quarantena*» (p. 110).

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

15.1.3. Ripristinare le impostazioni predefinite

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

Per ripristinare le impostazioni predefinite della protezione in tempo reale:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
4. Nella finestra **PROTEZIONE**, clicca sul menu a fisarmonica **MOSTRA IMPOSTAZIONI AVANZATE**.

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

15.2. Scansione a richiesta

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

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

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

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

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

15.2.2. Eseguire una Scansione veloce

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

Per eseguire una scansione veloce:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTIVIRUS**, clicca su **Scansione veloce**.
4. Segui la procedura guidata della scansione antivirus per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati. Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

O più rapidamente, clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender e poi clicca sul pulsante azione **Scansione veloce**.

15.2.3. Eseguire una scansione del sistema

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

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

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

- Assicurati che Bitdefender sia aggiornato con il suo database delle informazioni delle minacce. Eseguire la scansione con un database delle informazioni delle minacce obsoleto può impedire a Bitdefender di rilevare nuove minacce, trovate dopo l'ultimo aggiornamento. Per maggiori informazioni, fai riferimento a «*Mantenere aggiornato Bitdefender*» (p. 43).
- Chiudere tutti i programmi aperti.

Se desideri controllare ubicazioni particolari sul tuo computer o impostare le opzioni di scansione, configura ed esegui una scansione personale. Per maggiori informazioni, fai riferimento a «*Configurare una scansione personale*» (p. 98).

Per eseguire una scansione del sistema:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTIVIRUS**, clicca su **Scansione sistema**.
4. La prima volta che esegui una Scansione di sistema, ti sarà presentata questa funzionalità. Clicca su **OK, HO CAPITO** per continuare.
5. Segui la procedura guidata della scansione antivirus per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati. Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

15.2.4. Configurare una scansione personale

Per configurare una scansione personalizzata in ogni dettaglio e poi eseguirla:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTIVIRUS**, clicca su **Gestisci scansioni**.

4. Clicca sul pulsante **Nuova attività personalizzata**. Nella scheda **Base**, inserisci un nome per la scansione e seleziona i percorsi da controllare.
5. Se desideri configurare le opzioni di scansione in ogni dettaglio, seleziona la scheda **Avanzate**. Comparirà una nuova finestra. Attenersi alla seguente procedura:
   a. Puoi configurare facilmente le opzioni di scansione, impostando il livello della scansione. Trascina il cursore scorrevole lungo la barra per impostare il livello di scansione desiderato. Usa la descrizione sul lato destro della barra per identificare il livello di scansione che si adatta meglio alle tue necessità.

      Gli utenti avanzati possono trarre vantaggio dalle impostazioni di scansione offerte da Bitdefender. Per configurare in ogni dettaglio le opzioni della scansione, clicca su **Personalizzato**. Al termine di questa sezione trovi maggiori informazioni al riguardo.
   b. Puoi anche configurare queste opzioni generali:
      - **Esegui l'attività con bassa priorità .** Diminuisce la priorità del processo di scansione. Consentirai ad altri programmi di essere più veloci, incrementando il tempo necessario per terminare il processo di scansione.
      - **Minimizza la Procedura guidata di scansione nell'area di notifica .** Minimizza la finestra di scansione nell'area di notifica. Clicca due volte sull'icona di Bitdefender per riaprirlo.
      - Specifica l'azione da intraprendere se non venisse rilevata alcuna minaccia.
   c. Clicca su **OK** per salvare le modifiche e chiudere la finestra.
6. Se vuoi impostare un programma per le attività di scansione, usa l'interruttore **Programma** nella finestra **Base**. Seleziona una delle opzioni corrispondenti per impostare un elenco:
   - All'avvio del sistema
   - Una volta
   - Periodicamente
7. Clicca su **Esegui scansione** e segui la procedura guidata della scansione antivirus per completare la scansione. In base ai percorsi da controllare, la scansione potrebbe richiedere un po' di tempo. Al termine della

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

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

Informazioni sulle opzioni di scansione

Questa informazione potrebbe esserti utile:

- Se non conosci alcuni termini, verificali nel glossario. Puoi anche trovare informazioni utili cercando su Internet.
- **Scansiona 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.

  I file delle applicazioni (o dei programmi) sono più vulnerabili agli attacchi delle minacce 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 sistema. La minaccia può colpire il sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la protezione in tempo reale. Tuttavia, si consiglia di usare questa opzione per rilevare e rimuovere ogni minaccia potenziale, anche se non è immediata.

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

- **Scansiona i settori di avvio.** È possibile impostare Bitdefender per controllare i settori di boot del disco rigido. Questo settore del disco rigido contiene il codice necessario per inizializzare il processo di avvio del computer. Quando una minaccia infetta il settore di boot, il disco potrebbe non essere accessibile e potrebbe non essere possibile avviare il sistema e accedere ai dati.
- **Scansiona memoria.** Seleziona questa opzione per controllare i programmi in esecuzione nella memoria di sistema.
- **Registro della scansione.** Seleziona questa opzione per controllare le chiavi del registro. Il registro di Windows è un database che memorizza le impostazioni e le opzioni di configurazione delle componenti del sistema operativo Windows, oltre a quelle delle applicazioni installate.
- **Scansiona i cookie.** Seleziona questa opzione per controllare i cookie memorizzati dai browser sul tuo computer.
- **Scansiona solo file nuovi e modificati.** Controllando solo i file modificati o nuovi, potresti migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.
- **Ignora keylogger commerciali.** Seleziona questa opzione se hai installato e utilizzi un programma keylogger commerciale sul tuo computer. I keylogger commerciali sono programmi legittimi di monitoraggio del computer la cui funzione elementare è registrare tutto ciò che viene digitato sulla tastiera.
- **Scansiona alla ricerca di rootkit.** Seleziona questa opzione per eseguire una scansione alla ricerca di rootkit e oggetti nascosti usando tale software.

15.2.5. Procedura guidata scansione antivirus

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

Nota

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

Fase 1 - Eseguire la scansione

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

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

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

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

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

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

Fase 2 - Scegliere le azioni

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

Nota

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

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

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

Esegui azioni appropriate

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

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

  I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione. I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione. Per maggiori informazioni, fai riferimento a «*Gestire i file in quarantena*» (p. 110).

  ### Importante

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

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

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

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

Elimina

Rimuove i file rilevati dal disco.

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

Non fare nulla

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

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

Fase 3 - Sommario

Quando Bitdefender termina la risoluzione dei problemi, i risultati della scansione compariranno in una nuova finestra. Se desideri ricevere informazioni esaurienti sul processo di scansione, clicca su **REGISTRO** per visualizzare il registro della scansione. Il rapporto viene fornito in formato .xml e può essere salvato localmente, cliccando sul pulsante **Salva rapporto** e scegliendo una posizione.

Importante

Nella maggior parte dei casi Bitdefender disinfetta con successo i file infetti che rileva o isola l'infezione. Tuttavia, ci sono problemi che non possono

essere risolti automaticamente. Se richiesto, riavvia il sistema per completare il processo di pulizia. Per maggiori informazioni e istruzioni su come rimuovere una minaccia manualmente, fai riferimento a «*Rimuovere le minacce dal sistema*» (p. 218).

15.2.6. Controllare i registri di scansione

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

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Nella scheda **Tutto**, seleziona la notifica relativa all'ultima scansione.

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

15.3. Scansione automatica di supporti rimovibili

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

I dispositivi rilevati rientrano in una di queste categorie:

- CD/DVD
- 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.

15.3.1. Come funziona?

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

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

Se l'Autopilot è disattivato:

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

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

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 una minaccia, perché le minacce non possono essere rimosse dal disco (è un supporto di sola lettura). Assicurati che la protezione in tempo reale sia attivata per impedire la diffusione di minacce nel tuo sistema. Si consiglia di copiare tutti i dati importanti dal disco al proprio sistema e poi eliminare il disco.

- In alcuni casi, Bitdefender può non essere in grado di rimuovere le minacce da file specifici a causa di vincoli legali o tecnici. Un esempio sono i file archiviati con una tecnologia proprietaria (questo perché l'archivio non può essere ricreato correttamente).

  Per scoprire come comportarsi con le minacce, fai riferimento a «*Rimuovere le minacce dal sistema*» (p. 218).

15.3.2. Gestire la scansione di supporti rimovibili

Per gestire la scansione automatica di supporti rimovibili:

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
4. Seleziona la scheda **UNITÀ E DISPOSITIVI**.

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

15.4. Esamina file hosts

Il file hosts viene fornito di norma con l'installazione del sistema operativo ed è utilizzato per mappare gli hostname in indirizzi IP ogni volta che accedi a una nuova pagina web, ti connetti a un FTP o a un altro server Internet. Si tratta di un semplice file di testo e i programmi potenzialmente dannosi possono modificarlo. Gli utenti avanzati sanno come utilizzarlo per bloccare pubblicità, banner, cookie di terze parti o hijacker fastidiosi.

Per configurare la scansione del file hosts:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.

2. Seleziona la scheda **AVANZATE**.
3. Clicca sull'interruttore ATTIVA/INATTIVA.

15.5. Configurare le eccezioni della scansione

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

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

Nota

Le eccezioni NON saranno applicate per le scansioni contestuali e di sistema. La scansione di sistema è una scansione a richiesta che ti consente di esaminare l'intero sistema per trovare eventuali minacce che potrebbero compromettere la sicurezza dei tuoi dati. 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**.

15.5.1. Escludere file e cartelle dalla scansione

Per escludere determinati file e cartelle dalla scansione:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
4. Seleziona la scheda **ECCEZIONI**.
5. Clicca sul menu accordion **Elenco di file e cartelle escluse dalla scansione**. Nella finestra che compare, puoi gestire i file e le cartelle esclusi dalla scansione.
6. Aggiungi eccezioni seguendo questi passaggi:

a. Clicca sul pulsante **ADD**.

b. Clicca su **Sfoglia**, seleziona il file o la cartella che desideri escludere dalla scansione e quindi clicca su **OK**. In alternativa, puoi digitare (o copiare e incollare) il percorso del file o della cartella nello spazio apposito.

c. Di norma, il file o la cartella selezionati sono esclusi dalla scansione all'accesso e da quella su richiesta. Per cambiare quando applicare l'eccezione, seleziona una delle altre opzioni.

d. Clicca su **Aggiungi**.

15.5.2. Escludere estensioni di file dalla scansione

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

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

Per escludere delle estensioni dei file dalla scansione:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
4. Seleziona la scheda **ECCEZIONI**.
5. Clicca sul menu accordion **Elenco delle estensioni escluse dalla scansione**. Nella finestra che compare, puoi gestire le estensioni dei file escluse dalla scansione.
6. Aggiungi eccezioni seguendo questi passaggi:
   a. Clicca sul pulsante **ADD**.
   b. Inserisci le estensioni che vuoi escludere dalla scansione, separate da punto e virgola (;). Ecco un esempio:

      txt;avi;jpg

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

d. Clicca su **Aggiungi**.

15.5.3. Gestire le eccezioni della scansione

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

Per gestire le eccezioni di scansione:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
4. Seleziona la scheda **ECCEZIONI**.
5. Usa le opzioni nel menu accordion **Elenco di file e cartelle escluse dalla scansione** per gestire le eccezioni della scansione.
6. Per rimuovere o modificare le eccezioni della scansione, clicca su uno dei collegamenti disponibili. Procedi come segue:
   - Per rimuovere una voce dall'elenco, selezionala e clicca sul pulsante **RIMUOVI**.
   - Per modificare una voce dalla tabella, cliccaci sopra due volte (o selezionala e clicca sul pulsante **MODIFICA**). Apparirà una nuova finestra, dove potrai modificare l'estensione o il percorso da escludere e il tipo di scansione dal quale escluderlo, a seconda delle necessità. Esegui i cambiamenti necessari, poi clicca su **Modifica**.

15.6. Gestire i file in quarantena

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

Di norma, i file in quarantena sono inviati automaticamente ai laboratori di Bitdefender per essere analizzati dai ricercatori di Bitdefender. Se la presenza

di una minaccia viene confermata, viene rilasciato un aggiornamento delle informazioni per consentirne la rimozione.

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

Per controllare e gestire i file in quarantena:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTIVIRUS**, clicca su **Quarantena**.

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

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

   Clicca sugli interruttori per attivare o disattivare:

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

   Invia i file sospetti messi in quarantena per ulteriori analisi
   Tieni questa opzione attivata per inviare automaticamente i file in quarantena ai laboratori di Bitdefender. I file campioni saranno analizzati dai ricercatori di Bitdefender. Se la presenza di una minaccia viene confermata, viene rilasciato un aggiornamento nelle informazioni delle minacce per consentirne la rimozione.

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

Crea un'eccezione per i file ripristinati

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

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

16. DIFESA DA MINACCE AVANZATE

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

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

Come misura di sicurezza, sarai informato ogni volta che viene rilevato e bloccato un attacco ransomware, anche se è attivata la funzione Autopilot.

16.1. Attivare o disattivare Advanced Threat Defense

Per attivare o disattivare Advanced Threat Defense:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ADVANCED THREAT DEFENSE**, clicca sull'interruttore ATTIVA/INATTIVA.

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

16.2. Verificare gli attacchi ransomware rilevati

Per verificare gli attacchi ransomware rilevati da Advanced Threat Defense:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ADVANCED THREAT DEFENSE**, clicca su **Protezione da ransomware**.
4. La prima volta che accedi alla Protezione da ransomware, ti sarà presentata questa funzionalità. Clicca su **OK, HO CAPITO** per continuare.

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

16.3. Verificare le app sospette rilevate

Per verificare le app sospette rilevate da Advanced Threat Defense:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ADVANCED THREAT DEFENSE**, clicca su **Difesa minacce**.
4. La prima volta che accedi a Threat Defense, ti sarà presentata questa funzionalità. Clicca su **OK, HO CAPITO** per continuare.

   Vengono mostrate tutte le app rilevate come minacce e bloccate negli ultimi 90 giorni. Per scoprire dettagli su una app, il percorso del processo dannoso o se la disinfezone ha avuto successo, basta cliccarci sopra.

16.4. Aggiungere processi alle eccezioni

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **ADVANCED THREAT DEFENSE**.
4. Nella finestra **WHITELIST**, clicca su **Aggiungi applicazioni alla whitelist**.
5. Trova e seleziona l'applicazione che vuoi escludere, e clicca su **OK**.

   Per rimuovere una voce dall'elenco, clicca sul pulsante **Rimuovi** accanto ad essa.

17. PROTEZIONE WEB

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

Bitdefender fornisce protezione web in tempo reale per:

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

Per configurare le impostazioni della protezione web:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **PROTEZIONE WEB**.

Clicca sugli interruttori per attivare o disattivare:

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

  Non dovresti visitare questa pagina web.

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

  Questa è una pagina sicura da visitare.

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

- Baidu

  Ricerca sicura valuta i link pubblicati sui seguenti servizi di social network:
  - Facebook
  - 121

- Scansione SSL.

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

- Protezione dalle frodi.

- Protezione da phishing.

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

Per configurare e gestire siti web usando la protezione web fornita da Bitdefender:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PROTEZIONE WEB**, clicca su **Whitelist**.
4. Nella casella di testo **Aggiungi URL**, inserisci il nome del sito web che desideri aggiungere alla whitelist e 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.

17.1. Avvisi di Bitdefender nel browser

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

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

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

- Allontanati dalla pagina web, cliccando su **Per sicurezza torna indietro**.
- Procedi alla pagina web, malgrado l'avvertimento, cliccando su **Sono a conoscenza dei rischi, quindi prosegui**.

18. ANTISPAM

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

L'antispam di Bitdefender impiega notevoli innovazioni tecnologiche e filtri standard dell'industria antispam per eliminare lo spam prima che raggiunga la Posta in arrivo dell'utente. Per maggiori informazioni, fai riferimento a «*Approfondimenti antispam*» (p. 119).

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

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

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

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

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

18.1. Approfondimenti antispam

18.1.1. Filtri Antispam

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

Elenco amici / Elenco spammer

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

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

Filtro caratteri

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

18.1.2. 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 Spammer l'e-mail viene spostata direttamente nella **Posta in arrivo**.

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

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

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

18.1.3. Programmi e protocolli di posta elettronica supportati

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

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

18.2. Attivare o disattivare la protezione antispam

Di norma la protezione antispam è attivata.

Per attivare o disattivare la funzionalità Antispam:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTISPAM**, clicca sull'interruttore ATTIVA/INATTIVA.

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

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

> **Importante**
> Bitdefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo. Per un elenco completo delle applicazioni di posta supportate, fai riferimento a «*Programmi e protocolli di posta elettronica supportati*» (p. 120).

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

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

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

Aggiungi Spammer - aggiunge il mittente dell'e-mail selezionata all'elenco degli Spammer. Può essere necessario premere **OK** per confermare. I messaggi e-mail ricevuti dagli indirizzi nell'elenco Spammer sono contrassegnati automaticamente come [spam].
Aggiungi amico - aggiunge il mittente dell'e-mail selezionata all'elenco Amici. Può essere necessario premere **OK** per confermare. Riceverai sempre e-mail provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.
Spammer - Apre l'**elenco Spammer**, che contiene tutti gli indirizzi e-mail dai quali non vuoi ricevere messaggi, indipendentemente dal loro contenuto. Per maggiori informazioni, fai riferimento a *«Configurazione dell'elenco Spammer»* (p. 124).
Amici - Apre l'**elenco Amici** che contiene tutti gli indirizzi e-mail dai quali desideri ricevere sempre i messaggi, indipendentemente dal loro contenuto. Per maggiori informazioni, fai riferimento a *«Configurazione dell'elenco Amici»* (p. 123).

18.3.1. 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.

18.3.2. Indicare messaggi spam non rilevati

Se si utilizza un'applicazione di posta supportata si può facilmente indicare quali messaggi e-mail avrebbero dovuto essere rilevati come spam. Così facendo si migliorerà considerevolmente l'efficienza del filtro antispam. 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 (in genere localizzata nella parte superiore della finestra del client di posta). Vengono immediatamente contrassegnati come [spam] e verranno spostati alla cartella posta indesiderata.

18.3.3. 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**.

Hai le seguenti opzioni:

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

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

18.4. Configurazione dell'elenco Amici

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

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

Per configurare e gestire l'elenco Amici:

- Se stai usando Microsoft Outlook, clicca sul pulsante **Amici** nella barra degli strumenti antispam di Bitdefender.
- In alternativa:
  1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
  2. Clicca sul link **VEDI FUNZIONALITÀ**.
  3. Nel pannello **ANTISPAM**, clicca su **Gestisci amici**.

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

- com - Tutte le e-mail con il suffisso di dominio com saranno marcate come Spam;

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

Per eliminare un elemento dall'elenco, clicca sul collegamento **Rimuovi** corrispondente. Per eliminare tutti i dati dall'elenco, cliccare sul pulsante **Cancella lista**.

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

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

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

18.5. Configurazione dell'elenco Spammer

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

Per configurare e gestire l'elenco Spammer:

- Se stai usando Microsoft Outlook o Thunderbird, clicca sul pulsante **Spammer** nella barra degli strumenti antispam di Bitdefender integrata nel tuo client e-mail.
- In alternativa:
  1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
  2. Clicca sul link **VEDI FUNZIONALITÀ**.
  3. Nel pannello **ANTISPAM**, clicca su **Gestisci spammer**.

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

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

Avvertimento

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

Per eliminare un elemento dall'elenco, clicca sul collegamento **Rimuovi** corrispondente. Per eliminare tutti i dati dall'elenco, cliccare sul pulsante **Cancella lista**.

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

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

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

18.6. Configurare i filtri locali antispam

Come descritto in «*Approfondimenti antispam*» (p. 119), Bitdefender usa una combinazione di diversi filtri antispam per identificare lo spam. I filtri antispam sono pre-configurati per una protezione ottimale.

Importante

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

Per configurare i filtri locali antispam:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTISPAM**.
4. Clicca sugli interruttori ATTIVA/INATTIVA corrispondenti.

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

18.7. Configurare le impostazioni cloud

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

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

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTISPAM**.
4. Nella finestra **IMPOSTAZIONI**, seleziona le opzioni desiderate.

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

19. FIREWALL

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

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

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

Come misura di sicurezza sarai informato ogni volta che a un'applicazione potenzialmente dannosa viene impedito di accedere a Internet, persino quando l'Autopilot è attivato.

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

Per scoprire altre informazioni sulle impostazioni del firewall per ogni tipo di rete e come modificare le impostazioni della rete, fai riferimento a *«Gestire le impostazioni di connessione»* (p. 132).

19.1. Attivare o disattivare la protezione del firewall

Per attivare o disattivare la protezione del firewall:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **FIREWALL**, clicca sull'interruttore ATTIVA/INATTIVA.

Avvertimento

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

19.2. Gestire le regole delle app

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **FIREWALL**, clicca su **Accesso applicazione**.
4. La prima volta che accedi al Firewall, ti sarà presentata questa funzionalità. Clicca su **OK, HO CAPITO** per continuare.

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

Per ogni regola sono visualizzate le seguenti informazioni:

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

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

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

Aggiungere regole per le app

Per aggiungere una regola per una app:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **FIREWALL**.
4. Clicca sul link **Aggiungi regola** nella parte superiore della finestra **REGOLE**.

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

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

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

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

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

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

    Nota

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

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

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

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

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

Per rimuovere il set di regole attuale e ripristinare quelle predefinite, clicca sul link **Annulla regole** nella parte superiore della finestra **REGOLE**.

19.3. Gestire le impostazioni di connessione

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

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

Per configurare i tuoi adattori di rete:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **FIREWALL**.
4. Seleziona la tabella **TIPO DI RETE**.
5. Seleziona le impostaizoni che desideri applicare quando ti connetti ai seguenti adattatori:
   - Wi-Fi

- Ethernet

19.4. Configurare le impostazioni avanzate

Per configurare le impostazioni avanzate del firewall:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **FIREWALL**.
4. Seleziona la scheda **IMPOSTAZIONI**.

Possono essere configurate le seguenti funzionalità:

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

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

- **Modalità Paranoid** - Gli avvisi vengono mostrati ogni volta che un'applicazione tenta di connettersi a Internet. Seleziona **Consenti** o **Blocca**. Quando la modalità Paranoid è attivata, l'Autopilot e i Profili vengono disattivati automaticamente. La modalità Paranoid può essere utilizzata simultaneamente con la **Modalità Batteria**.

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

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

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

20. VULNERABILITÀ

Un passaggio importante nella protezione del computer contro azioni e applicazioni dannose è mantenere aggiornato il sistema operativo e le applicazioni che usi regolarmente. Inoltre, per prevenire l'accesso fisico non autorizzato al tuo computer, è necessario configurare password sicure (ovvero non facilmente indovinabili) per ogni account utente di Windows e per le reti Wi-Fi a cui ti connetti.

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

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

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

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

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

20.1. Controllare il sistema per rilevare vulnerabilità

Per risolvere le vulnerabilità del sistema utilizzando l'opzione Scansione vulnerabilità:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul pulsante azione **Scansione vulnerabilità**.
3. Attendi che Bitdefender controlli le vulnerabilità del sistema. Per fermare il processo di scansione, clicca sul pulsante **Ignora** nella parte superiore della finestra.

   - **Aggiornamenti critici di Windows**

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

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

- **Aggiornamenti applicazioni**

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

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

- **Password account Windows deboli**

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

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

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

- **Reti Wi-Fi vulnerabili**

  Clicca su **Mostra dettagli** per scoprire maggiori informazioni sulla rete wireless a cui sei connesso. Se ti viene suggerito di impostare una password più sicura per la tua rete di casa, clicca sul link corrispondente.

  Quando sono disponibili altri suggerimenti, segui le istruzioni fornite per assicurarti che la tua rete di casa sia sempre protetta dagli occhi indiscreti dei pirati informatici.

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

20.2. Usare il controllo automatico delle vulnerabilità

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

Per controllare e correggere i problemi rilevati:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Nella scheda **Tutto**, seleziona la notifica relativa alla scansione vulnerabilità.
3. Puoi visualizzare informazioni dettagliate sulle vulnerabilità del sistema rilevate. In base al problema, per risolvere una vulnerabilità specifica procedi come segue:
   - Se sono disponibili aggiornamenti di Windows, clicca su **INSTALLA**.
   - Se gli aggiornamenti automatici di Windows sono disattivati, clicca su **ATTIVA**.
   - Se un'applicazione non è aggiornata, clicca su **AGGIORNA ORA** per trovare un link alla pagina web del distributore, da dove poter installare la versione più recente dell'applicazione.
   - Se un account utente Windows ha una password poco sicura, clicca su **CAMBIA PASSWORD** per costringere l'utente a modificare la password al prossimo accesso, oppure cambiala direttamente. Per avere una password sicura, utilizza una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).
   - Se la funzione di esecuzione automatica di Windows è attivata, clicca su **RISOLVI** per disattivarla.
   - Se il router che hai configurato ha una password poco sicura, clicca su **CAMBIA PASSWORD** per accedere alla sua interfaccia da dove potrai impostarne una migliore.
   - Se la rete a cui ti connetti ha alcune vulnerabilità che potrebbero esporre il tuo sistema a eventuali rischi, clicca su **CAMBIA IMPOSTAZIONI WI-FI**.

Per configurare le impostazioni del monitoraggio vulnerabilità:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.

2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **VULNERABILITÀ**, clicca sull'interruttore ATTIVA/INATTIVA.

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

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

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

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

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

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

   Notifiche Wi-Fi Security Advisor
   Verifica se la rete wireless di casa a cui sei connesso è sicura oppure no, e se ha eventuali vulnerabilità. Inoltre, verifica se la password del router domestico sia abbastanza sicura e ti consiglia come potenziarla.

La maggior parte delle reti wireless non cifrate sono poco sicure, cosa che consente agli occhi indiscreti dei pirati informatici di accedere alle tue attività personali.

Nota
Disattivando il monitoraggio di una determinata vulnerabilità, i relativi problemi non saranno più registrati nella finestra Notifiche.

20.3. Wi-Fi Security Advisor

Mentre sei in viaggio, lavorando in un bar o aspettando all'aeroporto, connettersi a una rete wireless pubblica per effettuare pagamenti, controllare le e-mail o gli account dei social network può essere la soluzione più rapida. Ma potrebbero esserci alcuni occhi indiscreti che cercheranno di ottenere i tuoi dati personali, sfruttando ogni falla nella rete per sottrarre informazioni.

E i dati personali sono password e nomi utenti che utilizzi per accedere ai tuoi account online, come e-mail, conti bancari, social network, ma anche i messaggi che invii.

In genere, le reti wireless pubbliche possono essere più pericolose in quando non richiedono una password per accedervi, e se lo fanno, la password potrebbe essere comunque disponibile per chiunque voglia connettersi. Inoltre, potrebbero esserci reti pericolose o honeypot, che rappresentano un bersaglio per i pirati informatici.

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

Bitdefender Wi-Fi Security Advisor ti fornisce informazioni su:

- Reti Wi-Fi di casa
- Reti Wi-Fi pubbliche

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.

2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona ⚙ nell'angolo in basso a destra del pannello **VULNERABILITÀ**.
4. Nella finestra **IMPOSTAZIONI**, clicca sull'interruttore ATTIVA/INATTIVA corrispondente.

20.3.2. Configurare la rete Wi-Fi di casa

Per iniziare a configurare la tua rete di casa:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **VULNERABILITÀ**, clicca su **Wi-Fi Security Advisor**.
4. Nella scheda **WI-FI DI CASA**, clicca sul pulsante **SELEZIONA WI-FI DI CASA**.

   Viene mostrato un elenco con tutte le reti wireless a cui ti sei connesso finora.
5. Individua la tua rete di casa e clicca su **SELEZIONA**.

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

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

20.3.3. Wi-Fi pubblica

Mentre sei connesso a una rete wireless non sicura o poco protetta, viene attivato il profilo Wi-Fi pubblica. Mentre esegui questo profilo, Bitdefender Internet Security 2018 viene configurato per eseguire automaticamente le seguenti impostazioni del programma:

- Advanced Threat Defense è attivato
- Il Firewall di Bitdefender è stato attivato e al tuo adattatore wireless verranno applicate le seguenti impostazioni:
  - Modalità invisibile - ATTIVATA
  - Tipo di rete - Pubblica

- Le seguenti impostazioni della Protezione web vengono attivate:
  - Controlla SSL
  - Protezione dalle frodi
  - Protezione da phishing
- È disponibile un pulsante per aprire Bitdefender Safepay™. In questo caso, la Protezione hotspot per le reti non sicure viene attivata di default.

20.3.4. Controllare le informazioni sulle reti Wi-Fi

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **VULNERABILITÀ**, clicca su **Wi-Fi Security Advisor**.
4. In base alle informazioni che ti servono, seleziona una delle due schede, **WI-FI DI CASA** o **WI-FI PUBBLICA**.
5. Clicca su **Mostra dettagli** accanto alla tua rete per trovare maggiori informazioni al riguardo.

Ci sono tre tipi di reti wireless filtrate per la loro importanza, ognuna indicata da un'icona specifica:

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

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

Rete Wi-Fi sicura - Indica che la rete che stai utilizzando è sicura. In questo caso, puoi usare dati sensibili per effettuare operazioni online.

Cliccando sul link **Mostra dettagli** nell'area di ciascuna rete, vengono mostrati i seguenti dettagli:

- **Protetto** - Qui puoi visualizzare se la rete selezionata è protetta oppure no. Reti non cifrate possono lasciare esposti i dati che utilizzi.
- **Tipo di cifratura** - Qui puoi visualizzare il tipo di cifratura utilizzato dalla rete selezionata. Alcuni tipi di cifratura potrebbero non essere sicuri. Inoltre, consigliamo vivamente di controllare le informazioni sul tipo di cifratura indicato, per assicurarsi di essere protetti durante la navigazione.
- **Canale/Frequenza** - Qui puoi visualizzare la frequenza del canale utilizzata dalla rete selezionata.
- **Complessità password** - Qui puoi visualizzare il livello di sicurezza della password. Ricordati che le reti dotate di password poco sicure rappresentano un facile bersaglio per i pirati informatici.
- **Tipo di accesso** - Qui puoi visualizzare se la rete selezionata è protetta da una password oppure no. Si consiglia vivamente di connettersi solo a reti dotate di password sicure.
- **Tipo di autenticazione** - Qui puoi visualizzare il tipo di autenticazione utilizzato dalla rete selezionata.

Tieni attivata l'opzione **Notifica** per ricevere notifiche ogni volta che il tuo sistema si connette a questa rete.

21. PROTEZIONE WEBCAM

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

Come misura di sicurezza, sarai avvisato ogni volta che una app non affidabile tenterà di accedere alla tua videocamera, anche quando è stata attivata la funzione Autopilot.

21.1. Attivare o disattivare la Protezione webcam

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PROTEZIONE WEBCAM**, clicca sull'interruttore ATTIVA/INATTIVA.

21.2. Configurare la Protezione webcam

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **PROTEZIONE WEBCAM**.

Regole di blocco delle applicazioni

- **Blocca ogni accesso alla webcam** - Nessuna applicazione potrà accedere alla tua webcam.
- **Blocca l'accesso dei browser alla webcam** - A nessun browser web, tranne Internet Explorer e Microsoft Edge, sarà consentito di accedere alla tua

webcam. Siccome le app di Windows Store vengono eseguite in un singolo processo, Internet Explorer e Microsoft Edge non possono essere rilevati da Bitdefender come browser web e quindi sono esclusi da questa impostazione.

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

  Sarai avvisato ogni volta che una delle app installate sarà indicata come "bloccata" dalla maggior parte degli utenti di Bitdefender, anche quando la funzione Autopilot è attivata.

Notifiche

- **Notifica quando applicazioni consentite si connettono alla webcam** - Sarai avvisato ogni volta che una app consentita tenterà di accedere alla webcam, anche quando la funzione Autopilot è attiva.

21.3. Aggiungere app all'elenco della Protezione webcam

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PROTEZIONE WEBCAM**, clicca su **Accesso a webcam**.
4. La prima volta che accedi alla Protezione webcam, ti sarà presentata questa funzionalità.
5. Clicca sul link desiderato:
   - **Seleziona le app di Windows Store da aggiungere all'elenco di quelle autorizzate** - Viene mostrato un elenco con le app di Windows Store

rilevate. Attiva gli interruttori accanto alle app che vuoi aggiungere all'elenco.

- **Inizia ad aggiungere applicazioni all'elenco di accesso alla webcam** - Vai al file .exe che desideri aggiungere all'elenco e clicca su **OK**.

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

Clicca sull'interruttore Accesso consentito/Accesso bloccato.

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

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

Sarai avvisato ogni volta che le applicazioni consentite vengono bloccate dagli utenti di Bitdefender, indipendentemente dallo stato di Autopilot.

22. SAFE FILES

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

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

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

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

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

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

22.1. Attivare o disattivare Safe files

Per attivare o disattivare la funzionalità Safe files:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **SAFE FILES**, clicca sull'interruttore ATTIVA/INATTIVA.

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

Nota
La funzionalità Safe files non viene attivata automaticamente.

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **SAFE FILES**, clicca su **Cartelle protette**.
4. La prima volta che accedi a Cartelle protette, ti sarà presentata questa funzionalità. Clicca su **PROTEGGI ALTRE CARTELLE** per continuare.
5. Seleziona la cartella che vuoi proteggere e clicca su **OK**.

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

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

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

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

22.3. Configurare l'accesso alle app

Le applicazioni che cercano di modificare o eliminare file protetti potrebbero essere segnalate come potenzialmente pericolose e aggiunte all'elenco delle

"applicazioni bloccate". Se un'applicazione venisse bloccata ma hai la certezza che il suo comportamento sia assolutamente normale, puoi autorizzarla seguendo questi passaggi:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **SAFE FILES**, clicca su **Accesso applicazione**.
4. Verranno elencate le app che hanno richiesto di modificare i file nelle tue cartelle protette. Clicca sull'interruttore Consenti accanto all'applicazione che ritieni sicura.

Nella stessa finestra, puoi disattivare la protezione dai ransomware per determinate applicazioni, cliccando sull'interruttore Blocca.

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

22.4. Protezione all'avvio

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

Per disattivare la protezione all'avvio:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **SAFE FILES**.
4. Clicca sull'interruttore ATTIVA/INATTIVA.

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

23. CRITTOGRAFIA FILE

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

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

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

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

23.1. Gestire i File Vault

Per gestire i tuoi File Vault da Bitdefender, clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.

I File Vault esistenti compaiono nel pannello **File Vault**.

23.2. Creare i File Vault

Per creare un nuovo Vault:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **CRITTOGRAFIA FILE**, clicca su **Crea nuovo File Vault**.
4. Specifica il nome e la posizione del File Vault.
   - Inserisci il nome del File Vault nel campo corrispondente.
   - Clicca su **Sfoglia**, seleziona la posizione del vault e salva il file sotto il nome desiderato.

5. Scegli una lettera dell'unità dal menu corrispondente. Aprendo il Vault, un disco virtuale con la lettera selezionata comparirà su Risorse del Computer.
6. Se desideri cambiare la dimensione predefinita del Vault (100 MB), usa i tasti freccia su e giù nella casella numerica **Dimensione Vault (MB)**.
7. Digita la password desiderata per il Vault nei campi **Password** e **Conferma password**. La password deve essere composta da almeno 8 caratteri. Qualsiasi persona che tenti di aprire il vault e accedere ai suoi file, dovrà fornire la password.
8. Clicca su **Crea**.

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

Per creare più rapidamente un nuovo Vault, clicca con il pulsante destro sul desktop o in una cartella del tuo computer, vai a **Bitdefender** e **File Vault di Bitdefender**, e seleziona **Crea file Vault**.

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

23.3. Importare un File Vault

Per importare un File Vault memorizzato in locale:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **CRITTOGRAFIA FILE**, clicca su **Importa Vault**.
4. Cerca il percorso del tuo Vault e selezionalo (il file .bvd).
5. Clicca su **Apri**.

23.4. Aprire i File Vault

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

Per aprire un Vault:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.

   I File Vault esistenti compaiono nel pannello **File Vault**.

2. Clicca sul link **Vedi Vault** e seleziona il Vault che vuoi aprire.
3. Clicca sul pulsante **Sblocca** e digita la password richiesta.
4. Clicca su **OK** e poi sul pulsante **Apri** per aprire il tuo Vault.

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

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

23.5. Aggiungere file ai Vault

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

Per aggiungere nuovi file al tuo Vault:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **CRITTOGRAFIA FILE**.
4. Nella finestra **I MIEI VAULT**, seleziona il Vault che vuoi aprire.
5. Clicca sul pulsante **Sblocca** e digita la password richiesta.
6. Clicca sul pulsante **Apri** per aprire il tuo Vault.
7. Aggiungi file o cartelle come faresti normalmente in Windows (per esempio, puoi utilizzare il classico metodo "copia e incolla").

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

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

23.6. Bloccare i Vault

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

Per bloccare un Vault:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Nel pannello **File Vault**, clicca su **Visualizza Vault**.
3. Nella finestra **I MIEI VAULT**, seleziona il Vault che vuoi bloccare.
4. Clicca sul pulsante **Blocca**.

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

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

23.7. Rimuovere file dai Vault

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **CRITTOGRAFIA FILE**.
4. Nella finestra **I MIEI VAULT**, seleziona il Vault da cui vuoi rimuovere i file.

5. Clicca sul pulsante **Sblocca**, nel caso fosse bloccato.
6. Clicca sul pulsante **Apri**.

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

23.8. Cambiare la password del Vault

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **CRITTOGRAFIA FILE**.
4. Nella finestra **I MIEI VAULT**, seleziona il Vault per cui vuoi cambiare la password.
5. Clicca sul pulsante **Impostazioni**.
6. Digita la password corrente del vault nel campo **Vecchia password**.
7. Digita la nuova password del vault nei campi **Nuova password** e **Conferma nuova password**.

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

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

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

24. PROTEZIONE DI PASSWORD MANAGER PER LE TUE CREDENZIALI

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

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

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

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

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

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

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

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

Password Manager protegge le seguenti informazioni private:

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

24.1. Crea un nuovo database del Portafoglio

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PORTAFOGLIO**, clicca su **Crea nuovo Portafoglio**.
4. Clicca sul pulsante **Crea nuovo**.
5. Digita le informazioni richieste nei campi corrispondenti.
   - Etichetta Portafoglio - Imposta un nome unico per il database del tuo Portafoglio.
   - Password principale - Inserisci una password per il tuo Portafoglio.
   - Ridigita la password - Ridigita la password impostata.
   - Suggerimento - Inserisci un suggerimento per ricordarti la password.
6. Clicca su **Continua**.
7. In questa fase, puoi scegliere di archiviare i tuoi dati nel cloud. Selezionando Sì, le informazioni bancarie resteranno comunque memorizzate a livello locale sul tuo dispositivo. Scegli l'opzione che desideri e poi clicca su **Continua**.
8. Seleziona il browser web da cui vuoi importare le credenziali.
9. Clicca su **Termina**.

24.2. Importa un database esistente

Per importare un database del Portafoglio memorizzato in locale:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PORTAFOGLIO**, clicca su **Crea nuovo Portafoglio**.
4. Clicca sul pulsante **Percorso**.

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

24.3. Esporta il database del Portafoglio

Per esportare il database del tuo Portafoglio:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PORTAFOGLIO**, clicca su **I miei Portafogli**.
4. Clicca sull'icona nel Portafoglio desiderato e seleziona **Esporta**.
5. Cerca il percorso del tuo database del Portafoglio e selezionalo (il file .db).
6. Clicca su **Salva**.

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

24.4. Sincronizzare i tuoi Portafogli nel cloud

Per attivare o disattivare la sincronizzazione dei Portafogli nel cloud:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PORTAFOGLIO**, clicca su **I miei Portafogli**.
4. Clicca sull'icona nel Portafoglio desiderato e seleziona **Impostazioni**.

5. Scegli l'opzione che desideri nella finestra che comparirà e poi clicca su **Salva**.

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

24.5. Gestisci le tue credenziali del Portafoglio

Per gestire le tue password:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PORTAFOGLIO**, clicca su **I miei Portafogli**.
4. Seleziona il database del Portafoglio desiderato dalla finestra **I MIEI PORTAFOGLI** e poi clicca sul pulsante **ATTIVA IL PORTAFOGLIO**.
5. Digita la password principale e clicca su **OK**.

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

- Identità
- Siti web
- Online banking
- E-mail
- App
- Reti Wi-Fi

Aggiungere/modificare le credenziali

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

- Per eliminare una voce, selezionala e clicca sul pulsante **Elimina**.

24.6. Attivare o disattivare la protezione del Password Manager

Per attivare o disattivare la protezione del Gestore Password:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PORTAFOGLIO**, clicca sull'interruttore ATTIVA/DISATTIVA.

24.7. Gestire le impostazioni del Password Manager

Per configurare la password principale in ogni dettaglio:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **PORTAFOGLIO**.
4. Seleziona la scheda **IMPOSTAZIONI DI SICUREZZA**.

Sono disponibili le seguenti opzioni:

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

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

Migliora la tua esperienza

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **PORTAFOGLIO**.
4. Seleziona la scheda **PLUGIN**.

   Controlla se un'applicazione utilizza Password Manager e migliora la tua esperienza:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Configurare l'opzione Compila automaticamente

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **PORTAFOGLIO**.

4. Seleziona la scheda **IMP. COMP. AUTOMATICA**.
5. Puoi configurare le seguenti opzioni:
   - **Configura la protezione delle credenziali da parte del Portafoglio.**:
     - **Salva automaticamente le credenziali nel Portafoglio** - Le credenziali di accesso e altri informazioni identificabili, come dati personali o il numero della carta di credito, vengono salvati e aggiornati automaticamente nel Portafoglio.
     - **Chiedi sempre** - Ti sarà chiesto ogni volta se desideri aggiungere le credenziali al Portafoglio.
     - **Non salvare, aggiornerò le informazioni manualmente** - Le credenziali possono essere aggiunte nel Portafoglio solo manualmente.
   - **Compila automaticamente le credenziali di accesso**:
     - **Compila automaticamente le credenziali di accesso ogni volta** - Le credenziali vengono inserite automaticamente nel browser.
   - **Comp. automaticamente moduli**:
     - **Inserisci direttamente i miei dati quando visito una pagina con dei moduli** - Ogni volta che Bitdefender rileva la tua intenzione di eseguire un pagamento o una registrazione online, comparirà una finestra di pop-up con le opzioni già compilate.

Gestisci le informazioni del Password Manager dal browser

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

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

Il Portafoglio di Bitdefender include le seguenti opzioni:

- Apri Portafoglio - Apri il Portafoglio.
- Blocca Portafoglio - Blocca il portafoglio.

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

25. VPN

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

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

25.1. Installare VPN

La app VPN può essere installata dallla tua interfaccia di Bitdefender come segue:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **VPN**, clicca su **Attiva VPN**.
4. Nella finestra con la descrizione della app VPN, leggi l'**Accordo di abbonamento** e clicca su **ATTIVA Bitdefender VPN**.

   Attendi qualche istante per il download e l'installazione dei file.
5. Clicca su **APRI BITDEFENDER VPN** per completare la fase di installazione.

Nota
Bitdefender VPN richiede .Net Framework 4.5.2 o superiore per essere installato. Nel caso non avessi tale pacchetto installato, comparirà una finestra

di notifica. Clicca su **installa .Net Framework** per essere reindirizzato a una pagina da cui puoi scaricare la versione più recente di questo software.

25.2. Aprire VPN

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

- Dall'area di notifica
  1. Clicca con il pulsante destro del mouse sull'icona nella barra delle applicazioni e poi clicca su **Mostra**.
- Dall'interfaccia di Bitdefender:
  1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
  2. Clicca sul pulsante azione **VPN**.

25.3. Interfaccia di VPN

L'interfaccia di VPN mostra lo stato della app, connessa o disconnessa. L'ubicazione del server per gli utenti con la versione gratuita viene impostata automaticamente da Bitdefender sul server più appropriato, mentre gli utenti premium hanno la possibilità di modificare la posizione del server a cui desiderano connettersi. Per maggiori informazioni sugli abbonamenti di VPN, fai riferimento a «*Abbonamenti*» (p. 163).

Per connetterti o disconnetterti, clicca semplicemente sullo stato mostrato nella parte superiore della schermata, oppure clicca con il pulsante destro del mouse sull'icona nella barra delle applicazioni. L'icona nella barra delle applicazioni mostra un segno di spunta verde quando VPN è connesso e un segno di spunta rosso quando è disconnesso.

Mentre sei connesso, il tempo trascorso e l'indirizzo IP assegnato automaticamente al tuo dispositivo vengono mostrati nella parte inferiore dell'interfaccia.

Per avere più opzioni, accedi all'area **Menu**, cliccando sull'icona nella lato superiore a sinistra. Hai le seguenti opzioni:

- **Il mio account** - Mostra informazioni sull'account di Bitdefender e l'abbonamento a VPN. Clicca su **Cambia account**, se vuoi accedere con un altro account.

- **Impostazioni** – In base alle tue necessità, puoi personalizzare il comportamento del tuo prodotto:
  - Ricevi notifiche quando VPN si connette o disconnette automaticamente
  - Esegui automaticamente la app VPN all'avvio di Windows
  - Lancia automaticamente la app VPN quando il dispositivo si connette a reti wireless non sicure
- **Passa a premium** - Se stai utilizzando la versione gratuita, qui puoi fare l'upgrade al piano premium.
- **Supporto** - Sarai reindirizzato alla piattaforma del nostro Centro di supporto, da cui potrai leggere un articolo molto utile su come utilizzare Bitdefender VPN.
- **Info** - Vengono mostrate alcune informazioni sulla versione installata.

25.4. Abbonamenti

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

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

Puoi fare l'upgrade alla versione premium di Bitdefender VPN in qualsiasi momento, cliccando sul pulsante **OTTIENI TRAFFICO ILLIMITATO** disponibile nell'interfaccia del prodotto.

L'abbonamento a Bitdefender Premium VPN è indipendente dall'abbonamento a Bitdefender Internet Security 2018, il che significa che potrai usarlo per la sua intera disponibilità, indipendentemente dallo stato dell'abbonamento della soluzione di sicurezza. Se l'abbonamento Bitdefender premium a VPN scadesse, ma quello a Bitdefender Internet Security 2018 fosse ancora attivo, sarà riconvertito al piano gratuito.

Bitdefender VPN è un prodotto multipiattaforma, disponibile nei prodotti Bitdefender compatibili con Windows, macOS, Android e iOS. Una volta fatto l'upgrade al piano premium, potrai utilizzare il tuo abbonamento su tutti i prodotti, a patto di eseguire l'accesso allo stesso account di Bitdefender.

26. SAFEPAY: SICUREZZA PER LE TRANSAZIONI ONLINE

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

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

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

Per assicurare una migliore protezione della privacy, Bitdefender Password Manager è stato integrato in Bitdefender Safepay™ per proteggere le proprie credenziali ogni volta che si desidera accedere a indirizzi privati online. Per maggiori informazioni, fai riferimento a «*Protezione di Password Manager per le tue credenziali*» (p. 153).

Bitdefender Safepay™ offre le seguenti funzioni:

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

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

26.1. Utilizzare Bitdefender Safepay™

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

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

- Dall'interfaccia di Bitdefender:
  1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
  2. Clicca sul pulsante azione **Safepay**.
- Da Windows:
  - In **Windows 7**:
    1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
    2. Clicca su **Bitdefender**.
    3. Clicca su **Bitdefender Safepay™**.
  - In **Windows 8 e Windows 8.1**:

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

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

Nota

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

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

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

Nota
Per passare da Bitdefender Safepay™ al desktop di Windows e vice versa, premi i tasti **Alt+Tab** o clicca sul pulsante **Minimizza**.

26.2. Configurare le impostazioni

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

- Nelle **Impostazioni generali** puoi impostare le seguenti opzioni:

  Comportamento di Bitdefender Safepay™
  Scegli cosa succede quando accedi a un negozio online a un sito di online banking nel tuo browser standard:
  - Apri automaticamente siti web in Safepay.
  - Suggeriscimi di usare Safepay.
  - Non suggerirmi di usare Safepay.

Elenco domini

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

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

Bloccare le finestre pop-up

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

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

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

Per rimuovere un sito web dall'elenco, seleziona la X corrispondente alla voce desiderata.

- Nella sezione **Impostazioni avanzate**, sono disponibili le seguenti opzioni:

Gestione Plug-in

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

Gestisci i certificati

Puoi importare i certificati dal sistema a un archivio di certificati.

Seleziona **Importa i certificati** e segui la procedura guidata per utilizzare i certificati in Bitdefender Safepay™.

Apre automaticamente la tastiera virtuale nei campi in cui va inserita la password

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

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

Chiedi conferma prima di stampare

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

26.3. Gestire i segnalibri

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

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

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

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

2. Clicca sul pulsante **+** per aggiungere un nuovo segnalibro.
3. Inserisci l'URL e il nome del segnalibro, poi clicca su **Crea**. Seleziona l'opzione **Apri automaticamente in Safepay**, se desideri che la pagina salvata nei segnalibri si apra in Bitdefender Safepay™ ogni volta che vi accedi. L'URL viene aggiunto anche nell'elenco dei domini alla pagina delle impostazioni.

27. PROTEZIONE DATI

27.1. Eliminare i file in modo permanente

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

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

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

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

In alternativa, puoi distruggere i file dall'interfaccia di Bitdefender, nel seguente modo:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PROTEZIONE DATI**, clicca su **Distruttore di file**.
4. Segui la procedura guidata del Distruttore di file:
   a. Clicca sul pulsante **AGGIUNGI CARTELLE** per aggiungere file o cartelle che vuoi rimuovere in modo permanente.

      In alternativa, trascina i file o le cartelle in questa finestra.

   b. Clicca su **ELIMINA DEFINITIVAMENTE** e conferma la tua volontà di continuare.

      Attendi che Bitdefender termini la distruzione dei file.

c. **Riepilogo risultati**

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

28. PARENTAL ADVISOR

La funzione Parental Advisor ti consente di controllare l'accesso a Internet e a determinate applicazioni per ogni dispositivo su cui è installata. Una volta configurato il Parental Advisor, puoi scoprire facilmente cosa sta facendo il bambino sul dispositivo che utilizza e dove è stato nelle ultime 24 ore. Inoltre, per aiutarti a sapere meglio cosa fa il bambino, l'applicazione ti fornisce alcune statistiche sulle sue attività e i suoi interessi.

Tutto ciò che ti serve è un computer con accesso a Internet e un browser web.

Puoi configurare il Parental Advisor per bloccare:

- pagine web inappropriate.
- applicazioni come giochi, chat, programmi di condivisione di file e altri.
- determinati contatti a cui non è permesso entrare in contatto con il bambino tramite il telefono.

Controlla le attività dei bambini e modifica le impostazioni del Parental Advisor utilizzando il tuo account Bitdefender da qualsiasi computer o dispositivo mobile connesso a Internet.

28.1. Accedere a Parental Advisor - BAMBINI

Una volta aperta la sezione Parental Advisor, è disponibile la finestra **BAMBINI**. Qui puoi visualizzare e modificare tutti i profili che hai creato per il bambino. I profili vengono mostrati come schede, consentendoti di gestirli rapidamente e verificare subito il proprio stato.

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

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

Accedi al tuo account Bitdefender:

- Da qualsiasi dispositivo con accesso a Internet:
  1. Accedi a Bitdefender Central.
  2. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.

3. Seleziona la funzionalità **Parental Advisor**.
4. Nella finestra **BAMBINI** che comparirà, potrai gestire e configurare i profili del Parental Advisor per ogni dispositivo.

- Dall'interfaccia di Bitdefender:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PARENTAL ADVISOR**, clicca su **Configura**.

   Sarai reindirizzato alla pagina web account Bitdefender. Assicurati di aver eseguito l'accesso con le tue credenziali.
4. Seleziona la funzionalità **Parental Advisor**.
5. Nella finestra **BAMBINI** che comparirà, potrai gestire e configurare i profili del Parental Advisor per ogni dispositivo.

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

28.2. Aggiungere il profilo dei propri bambini

Per avviare il monitoraggio delle attività del bambino, devi configurare un profilo e installare il Parental Advisor di Bitdefender sui dispositivi che utilizza.

Per aggiungere il profilo di un bambino al Parental Advisor:

1. Accedi al pannello Parental Advisor da Bitdefender Central.
2. Clicca su **AGGIUNGI PROFILO** nel lato destro della finestra **BAMBINI**.
3. Imposta le informazioni richieste nei campi corrispondenti, come nome e data di nascita. Per aggiungere una foto del profilo, clicca sul link **Scegli file**. Clicca su **CONTINUA** per continuare

   In base agli standard di sviluppo, impostando la data di nascita del bambino, il programma carica automaticamente alcune impostazioni di ricerca del web considerate appropriate per quella categoria d'età.

4. Se sul dispositivo del bambino è già stato installato Bitdefender Internet Security 2018, seleziona il suo dispositivo nell'elenco disponibile e seleziona l'account che vuoi monitorare. Clicca su **SALVA**.

   Se il bambino utilizza un dispositivo Android o iOS e la app Parental Advisor di Bitdefender non è stata installata, clicca su **AGGIUNGI DISPOSITIVO**. Se il bambino usa un dispositivo Mac e la app Bitdefender Antivirus for Mac non è installata, clicca sullo stesso pulsante. Seleziona il sistema operativo per la app che vuoi installare e poi clicca su **CONTINUA** per continuare.

5. Inserisci l'indirizzo e-mail a cui inviare il link di download dell'applicazione di Bitdefender e clicca su **INVIA LINK DI INSTALLAZIONE**.

Importante
Sui dispositivi basati su Windows, il prodotto Bitdefender Internet Security 2018 incluso nel tuo abbonamento deve essere scaricato e installato.
Su dispositivi macOS, il prodotto Bitdefender Antivirus for Mac deve essere scaricato e installato.
Sui dispositivi Android e iOS, l'applicazione Parental Advisor di Bitdefender deve essere scaricata e installata.

28.2.1. Assegnare più dispositivi allo stesso profilo

Puoi assegnare più dispositivi allo stesso profilo, in modo da applicare le stesse restrizioni, come segue:

1. Accedi a Bitdefender Central.
2. Seleziona la funzionalità Parental Advisor.
3. Clicca sull'icona ⋮ nella scheda del profilo desiderata e seleziona **Dispositivi**.
4. Seleziona dall'elenco i dispositivi disponibile che vuoi assegnare al profilo.

   Se il bambino utilizza un dispositivo Android o iOS e la app Parental Advisor di Bitdefender non è stata installata, clicca su **AGGIUNGI DISPOSITIVO**. Se il bambino usa un dispositivo Mac e la app Bitdefender Antivirus for Mac non è installata, clicca sullo stesso pulsante. Seleziona il sistema operativo per la app che vuoi installare e poi clicca su **CONTINUA** per continuare.

   Inserisci l'indirizzo e-mail a cui inviare il link di download dell'applicazione di Bitdefender e clicca su **INVIA LINK DI INSTALLAZIONE**.

5. Dopo aver completato il processo d'installazione sul nuovo dispositivo, selezionalo dall'elenco per assegnare il profilo.
6. Seleziona **SALVA**.

28.2.2. Associare il Parental Advisor a Bitdefender Central

Per monitorare le attività online del bambino su Android e iOS, devi associare il suo dispositivo con il tuo account Bitdefender, accedendo all'account dall'applicazione.

Per collegare un dispositivo al tuo account di Bitdefender:

- Su **Android**:
  1. Seleziona il pulsante che compare nell'e-mail inviata dal nostro server. Sarai reindirizzato a Google Play Store.

     Se nel tuo account di Bitdefender non hai scelto di inviare un link di download all'indirizzo e-mail del bambino, vai in Google Play e cerca la app Bitdefender Parental Advisor.
  2. Tocca **INSTALLA** nella finestra Bitdefender Parental Advisor e tocca **ACCETTA** se ti viene chiesto di autorizzare il permesso. Bitdefender richiede i permessi per tenerti informato sulle attività del bambino. Se non vengono accettati, la app non sarà installata.
  3. Apri l'applicazione del Parental Advisor.
  4. Leggi l'**Accordo di Abbonamento** e tocca **CONTINUA**.
  5. Accedi al tuo account Bitdefender esistente o a un account Google.

     Se non hai un account Bitdefender, puoi scegliere di crearne uno utilizzando l'opzione corrispondente.
  6. Tocca **VAI A IMPOSTAZIONI** per essere reindirizzato alla schermata da cui potrai attivare l'opzione Accessibilità per la app. Segui le istruzioni sullo schermo per configurare correttamente la app.
  7. Tocca **VAI A IMPOSTAZIONI** per essere reindirizzato alla schermata da cui potrai attivare l'opzione Attiva accesso utilizzo per la app. Segui le istruzioni sullo schermo per configurare correttamente la app.
  8. Tocca **VAI A IMPOSTAZIONI** per essere reindirizzato alla schermata da cui potrai attivare l'opzione Attiva diritti amministratore dispositivo per la app. Segui le istruzioni sullo schermo per configurare correttamente la app.

Ciò impedirà al bambino di disinstallare l'Agente del Parental Advisor.

9. Tocca **FATTO** per terminare il processo di installazione.

> **Nota**
> In Android 4.4 e versioni più recenti, per attivare il monitoraggio dei messaggi SMS del bambino, Bitdefender richiede che le impostazioni predefinite della app Messaggi di Android vengano modificate. Ti consigliamo di scegliere **Sì** nella finestra pop-up che comparirà dopo aver toccato **FATTO** nella app.

- Su **iOS**:
  1. Seleziona il pulsante che compare nell'e-mail inviata dal nostro server e poi installa la app.
  2. Apri l'applicazione del Parental Advisor.
  3. Viene mostrata una procedura guidata d'interruzione contenente alcuni dettagli sulle funzionalità del prodotto. Tocca **Avanti** per continuare.
  4. Accedi al tuo account di Bitdefender utilizzando il tuo indirizzo e-mail e password.
  5. Consenti l'accesso alla posizione del dispositivo in modo che Bitdefender possa localizzarlo.
  6. Consenti alla app di inviare delle notifiche.
  7. Assegna il dispositivo al profilo del bambino.

28.2.3. Monitorare le attività dei bambini

Bitdefender ti aiuta a monitorare le attività online dei bambini.

In questo modo, puoi sempre scoprire esattamente quali siti web hanno visitato, quali applicazioni hanno usato o quali attività sono state bloccate dal Parental Advisor.

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

- Lo stato dell'evento.
- L'intensità delle notifiche.
- Il nome del dispositivo.

- La data e l'ora in cui si è verificato l'evento.

Per monitorare il traffico Internet, le applicazioni utilizzate o le attività Facebook dei bambini:

1. Accedi al pannello Parental Advisor da Bitdefender Central.
2. Seleziona la scheda del dispositivo desiderato.

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

28.2.4. Configurazione delle Impostazioni Generali

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

Per ricevere le notifiche via e-mail:

1. Accedi al pannello Parental Advisor da Bitdefender Central.
2. Seleziona la scheda **Impostazioni** nell'angolo in alto a destra.
3. Attiva l'opzione corrispondente per ricevere rapporti sulle attività.
4. Inserisci l'indirizzo e-mail in cui vuoi ricevere le notifiche e-mail.
5. Riceverai le notifiche via e-mail per le seguenti informazioni:
   - Siti web bloccati
   - App bloccate
   - Aree vietate
   - Chiamata o SMS ricevuto da un numero di telefono bloccato
   - Rimozione dell'applicazione Facebook Parental Advisor
6. Clicca su **SALVA**.

28.2.5. Modificare un profilo

Per modificare un profilo esistente:

1. Accedi a Bitdefender Central.
2. Seleziona il pannello **Parental Advisor**.

3. Clicca sull'icona ⋮ sulla scheda del profilo desiderato e seleziona **Modifica**.
4. Dopo aver personalizzato le impostazioni desiderate, seleziona **SALVA**.

28.2.6. Rimuovere un profilo

Per rimuovere un profilo esistente:

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

28.3. Configurare i profili del Parental Advisor

Per iniziare a monitorare il bambino, un profilo deve essere assegnato al dispositivo su cui è stato installato l'Agente del Parental Advisor di Bitdefender.

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

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

Clicca su una scheda per configurare la caratteristica corrispondente del Parental Advisor per il dispositivo:

- Attività - Mostra tutte le attività, gli interessi, i luoghi e le interazioni con amici, dal giorno attuale.
- Applicazioni - Ti consente di bloccare l'accesso a determinate applicazioni, come giochi, programmi di chat, film, ecc.
- Siti web - Ti consente di filtrare la navigazione web.
- Contatti telefonici - Qui puoi indicare quali contatti nella rubrica del bambino possono entrare in contatto con lui tramite il telefono.
- Posizione del bambino - Qui puoi impostare i luoghi che sono sicuri o vietati per il bambino.

- Social network - Ti consente di bloccare l'accesso ai social network.
- Calendario - Ti consente di bloccare l'accesso ai dispositivi indicati da parte del profilo del bambino.

28.3.1. Attività

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

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

- **Luoghi** - Qui puoi visualizzare i luoghi in cui il bambino è stato durante la giornata.
- **Interessi** - Qui puoi visualizzare informazioni sulle categorie dei siti web che il bambino ha visitato. Clicca sul link **Verifica contenuto inappropriato** per consentire o negare l'accesso a determinati interessi.
- **Interazioni sociali** - Qui puoi controllare i contatti con cui il bambino interagisce. Clicca sul link **Gestisci i contatti** per selezionare i contatti con cui il bambino può o meno interagire.
- **Applicazioni** - Qui puoi visualizzare le app usate dal bambino. Clicca sul link **Rivedi limitazioni app** per bloccare o consentire l'accesso a determinate applicazioni.
- **Attività quotidiane** - Qui puoi visualizzare il tempo trascorso online su tutti i dispositivi assegnati al bambino, oltre ai luoghi in cui si è recato. Le informazioni raccolte sono della giornata odierna.

28.3.2. Applicazioni

La finestra Applicazioni ti aiuta a bloccare l'esecuzione di qualsiasi applicazione. In questo modo è possibile bloccare giochi, altri media, programmi di chat e altre categorie di applicazioni.

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

Per configurare il Controllo applicazioni per un account utente specifico:

1. Verrà mostrato un elenco di carte. Le carte rappresentano le app usate dal bambino.

2. Seleziona la carta con la app di cui vuoi bloccare l'utilizzo da parte del bambino.

   Il simbolo di spunta che comparirà, indica che il bambino non potrà più utilizzare quella app.

28.3.3. Siti web

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

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

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

Il simbolo di spunta che comparirà, indica che il bambino non potrà accedere ai contenuti di quella determinata categoria.

Consentire o bloccare un sito web

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

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

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

28.3.4. Contatti telefono

La finestra Contatti telefonici ti consente di specificare quali amici nella rubrica del bambino possano o non possano entrare in contatto con lui tramite il telefono.

Per limitare un determinato numero di telefono di un contatto, per prima cosa devi aggiungere al profilo del bambino il dispositivo Android che sta utilizzando seguendo questi passaggi:

1. Seleziona il pannello **Parental Advisor** in Bitdefender Central.
2. Clicca sul link **Installa Parental Advisor su un dispositivo** nella scheda desiderata.
3. Clicca su **AGGIUNGI DISPOSITIVO** nella finestra che comparirà.
4. Di norma, viene selezionata l'opzione **Bitdefender Parental Advisor per Android**. Clicca su **CONTINUA** per continuare
5. Seleziona il profilo del bambino per cui vuoi impostare le limitazioni.
6. Seleziona la scheda **Contatti telefonici**.

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

   Il simbolo di spunta che comparirà, indica che il bambino non potrà più essere raggiunto dal numero di telefono selezionato.

Per bloccare i numeri di telefono sconosciuti, attivare l'interruttore **Blocca interazioni con chiamate non identificabili**.

> **Nota**
> Le restrizioni per le chiamate possono essere impostate solo per i dispositivi Android aggiunti al profilo del bambino.

28.3.5. Posizione bambino

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

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

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

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

Configurare la posizione del controllo

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

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

Per configurare un luogo:

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

> **Nota**
> Il localizzatore può essere usato per monitorare i dispositivi Android e iOS su cui è stata installata la app Bitdefender Parental Advisor.

28.3.6. Social network

Il Parental Advisor monitora l'account Facebook del bambino e segnala tutte le sue attività principali.

Queste attività online sono state verificate e sarai avvisato, se dovessero essere una minaccia per la privacy del bambino.

Gli elementi monitorati dell'account online includono:

- Informazioni account
- Pagine seguite
- Immagini caricate

Per configurare la protezione di Facebook per un determinato account, inserisci l'e-mail dell'account del bambino controllato e clicca su **INVIA**.

Informa il bambino delle tue intenzioni e chiedigli di cliccare sul pulsante **PROTEGGI ACCOUNT** che ha ricevuto da parte nostra nella sua casella di posta.

Per accedere all'account Facebook monitorato, clicca sul link **Vedi su Facebook**.

Per smettere di monitorare l'account, utilizza il pulsante **SCOLLEGA ACCOUNT** in alto.

Per essere avvisato via e-mail quando il bambino rimuove la app Parental Control dal proprio dispositivo, seleziona la casella corrispondente.

28.3.7. Calendario

La finestra Calendario ti consente di bloccare l'accesso ai dispositivi indicati da parte del profilo del bambino. Le restrizioni possono essere impostate a qualsiasi ora durante le ore scolastiche e nei weekend solo per i dispositivi Windows e Android.

Per iniziare a configurare le limitazioni temporali durante le serate:

1. Nella sezione **ORA DI DORMIRE**, seleziona le caselle **Serate giorni di scuola** e **Serate fine settimana**.
2. Clicca sull'icona ⊗ nelle caselle corrispondenti e usa i tasti freccia su e giù per impostare gli intervalli di tempo durante i quali dev'essere bloccato l'accesso.

Per iniziare a configurare le limitazioni temporali durante le giornate:

1. Nella sezione **LIMITI GIORNALIERI**, hai le seguenti opzioni:
   - **CUMULATIVI**

a. Seleziona le caselle **Limiti giorni di scuola** e **Limiti fine settimana**.

b. Trascina i cursori per impostare l'intervallo di tempo consentito per l'accesso ai dispositivi.

- **SPECIFICI**

a. Seleziona le caselle **Limiti giorni di scuola** e **Limiti fine settimana**.

b. Seleziona dalla griglia gli intervalli di tempo durante i quali deve essere bloccato l'accesso.

Nota
Le impostazioni **CUMULATIVI** e **SPECIFICI** sono progettate per funzionare in modo indipendente.

29. BITDEFENDER USB IMMUNIZER

La funzione di esecuzione automatica inclusa nei sistemi operativi Windows è uno strumento molto utile che consente ai computer di eseguire automaticamente un file da un qualsiasi supporto a esso collegato. Per esempio, l'installazione di un software si avvia automaticamente, inserendo un CD nel lettore ottico.

Sfortunatamente, questa funzione può essere utilizzata anche dalle minacce per avviarsi automaticamente e infiltrarsi nel tuo computer da supporti riscrivibili, come unità USB e schede di memoria, collegate tramite lettori di schede. Negli ultimi anni, sono stati rilevati moltissimi attacchi basati sull'esecuzione automatica.

Con USB Immunizer puoi impedire a qualsiasi unità flash formattata in NTFS, FAT32 o FAT dall'eseguire automaticamente ogni minaccia. Una volta che un dispositivo USB è immunizzato, le minacce non possono più configurarlo per eseguire una determinata applicazione quando il dispositivo viene collegato a un computer con Windows.

Per immunizzare un dispositivo USB:

1. Collega l'unità flash al tuo computer.
2. Esegui una ricerca nel computer per localizzare il dispositivo di archiviazione rimovibile e clicca con il pulsante destro sulla sua icona.
3. Nel menu contestuale, seleziona **Bitdefender** e poi l'opzione **Immunizza questa unità**.

> **Nota**
> Se l'unità è già stata immunizzata, al posto dell'opzione Immunizza, comparirà il messaggio **L'unità USB è protetta da ogni minaccia basata sull'esecuzione automatica**.

Per impedire al computer di eseguire minacce da dispositivi USB non immunizzati, disattiva la funzione di esecuzione automatica. Per maggiori informazioni, fai riferimento a «*Usare il controllo automatico delle vulnerabilità*» (p. 136).

OTTIMIZZAZIONE SISTEMA

30. PROFILI

Le attività quotidiane, guardare un film o usare un videogioco, possono causare rallentamenti al sistema, in particolare se sono eseguite contemporaneamente ai processi di aggiornamento di Windows o alle attività di manutenzione. Con Bitdefender, ora puoi scegliere e applicare il tuo profilo preferito, che adatta le impostazioni del sistema in modo da incrementare le prestazioni di determinate applicazioni installate.

Bitdefender offre i seguenti profili:

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

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

In base alle tue attività, vengono applicate le seguenti impostazioni del prodotto quando si attivano i profili Lavoro, Film o Gioco:

- Tutti gli allarmi e pop-up Bitdefender sono disabilitati.
- L'Aggiornamento automatico è stato ritardato.
- Le scansioni programmate sono rinviate.
- La Ricerca sicura è stata disattivata.
- Le notifiche sulle offerte speciali sono disattivate.

In base alle tue attività, vengono applicate le seguenti impostazioni di sistema quando si attivano i profili Lavoro, Film o Gioco:

- Gli Aggiornamenti automatici di Windows sono stati ritardati.
- Gli avvisi e le finestre pop-up di Windows sono state disattivate.
- I programmi in background non necessari sono stati sospesi.
- Gli effetti visivi sono stati regolati per ottenere le migliori prestazioni.
- Le attività di manutenzione sono state ritardate.

- Le impostazioni di alimentazione sono state regolate.

Mentre è in esecuzione nel profilo Rete Wi-Fi pubblica, Bitdefender Internet Security 2018 viene impostato automaticamente per applicare le seguenti impostazioni del programma:

- Advanced Threat Defense è attivato
- Il Firewall di Bitdefender è stato attivato e al tuo adattatore wireless verranno applicate le seguenti impostazioni:
  - Modalità invisibile - ATTIVATA
  - Tipo di rete - Pubblica
- Le seguenti impostazioni della Protezione web vengono attivate:
  - Controlla SSL
  - Protezione dalle frodi
  - Protezione da phishing

30.1. Profilo Lavoro

Eseguire più attività, come inviare e-mail, tenere una comunicazione video con alcuni colleghi in remoto o lavorare con applicazioni grafiche può influenzare notevolmente le prestazioni del sistema. Il profilo Lavoro è stato progettato per aiutarti a migliorare la tua efficienza lavorativa, disattivando alcuni servizi e attività di manutenzione in background.

Configurare il profilo Lavoro

Per configurare le azioni da intraprendere quando sei nel profilo Lavoro:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **PROFILI**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Lavoro.
4. Seleziona le regolazioni del sistema da applicare, spuntando le seguenti opzioni:
   - Aumenta le prestazioni delle applicazioni
   - Ottimizza le impostazioni del prodotto per il profilo Lavoro

- Rimanda i programmi in background e le attività di manutenzione
- Posticipa gli aggiornamenti automatici di Windows

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

Aggiungere manualmente le applicazioni all'elenco del profilo Lavoro

Se lanciando una determinata applicazione, Bitdefender non attiva automaticamente il profilo Lavoro, puoi aggiungere manualmente l'applicazione nell'**Elenco applicazioni**.

Per aggiungere manualmente le applicazioni all'Elenco applicazioni nel profilo Lavoro:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **PROFILI**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Lavoro.
4. Nella finestra **PROFILO LAVORO**, clicca sul link **Elenco applicazioni**.
5. Clicca su **Aggiungi** per aggiungere una nuova applicazione all'**Elenco applicazioni**.

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

30.2. Profilo Film

Visualizzare contenuti video di alta qualità, come film in alta definizione, richiede molte risorse di sistema. Il profilo Film regola le impostazioni del sistema e del prodotto, per consentirti di visualizzare il film senza interruzioni e rallentamenti.

Configurare il profilo Film

Per configurare le azioni da intraprendere quando sei nel profilo Film:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **PROFILI**.

3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Film.
4. Seleziona le regolazioni del sistema da applicare, spuntando le seguenti opzioni:
   - Aumenta le prestazioni dei lettori multimediali
   - Ottimizza le impostazioni del prodotto per il profilo Film
   - Rimanda i programmi in background e le attività di manutenzione
   - Posticipa gli aggiornamenti automatici di Windows
   - Modifica le impostazioni dei consumi energetici per i film
5. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

Aggiungere manualmente i lettori multimediali all'elenco del profilo Film

Se lanciando un determinato lettore multimediale, Bitdefender non attiva automaticamente il profilo Film, puoi aggiungere manualmente l'applicazione nell'**Elenco lettori**.

Per aggiungere manualmente i lettori multimediali all'Elenco lettori nel profilo Film:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **PROFILI**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Film.
4. Nella finestra **PROFILO FILM**, clicca sul link **Elenco lettori**.
5. Clicca su **Aggiungi** per aggiungere una nuova applicazione all'**Elenco lettori**.

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

30.3. Profilo Gioco

Per usufruire di un'esperienza di gioco senza interruzioni, bisogna ridurre i caricamenti del sistema e diminuire i rallentamenti. Utilizzando euristiche comportamentali con un elenco di giochi conosciuti, Bitdefender è in grado

di rilevare automaticamente i giochi in esecuzione e ottimizzare le risorse del sistema, in modo da usufruire di una perfetta esperienza di gioco.

Configurare il profilo Gioco

Per configurare le azioni da intraprendere quando sei nel profilo Gioco:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **PROFILI**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Gioco.
4. Seleziona le regolazioni del sistema da applicare, spuntando le seguenti opzioni:
   - Aumenta le prestazioni con i giochi
   - Ottimizza le impostazioni del prodotto per il profilo Gioco
   - Rimanda i programmi in background e le attività di manutenzione
   - Posticipa gli aggiornamenti automatici di Windows
   - Modifica le impostazioni dei consumi energetici per i giochi
5. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

Aggiungere manualmente giochi all'Elenco dei giochi

Se lanciando una determinata applicazione o un videogioco, Bitdefender non attiva automaticamente il profilo Gioco, puoi aggiungere manualmente l'applicazione nell'**Elenco giochi**.

Per aggiungere manualmente i giochi all'Elenco giochi nel profilo Gioco:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **PROFILI**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Gioco.
4. Nella finestra **PROFILO GIOCO**, clicca sul link **Elenco giochi**.
5. Clicca su **Aggiungi** per aggiungere un nuovo gioco all'**Elenco giochi**.

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

30.4. Profilo rete Wi-Fi pubblica

Inviare e-mail, inserire credenziali riservate o fare shopping online mentre si è connessi a reti wireless non sicure potrebbe mettere a rischio i tuoi dati personali. Il profilo Rete Wi-Fi pubblica regola le impostazioni del prodotto per darti la possibilità di effettuare i pagamenti online e utilizzare ogni informazione riservata in un ambiente protetto.

Configurare il profilo Rete Wi-Fi pubblica

Per configurare Bitdefender per applicare le impostazioni del prodotto mentre si è connessi a una rete wireless non sicura:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **PROFILI**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del Profilo Rete Wi-Fi pubblica.
4. Mantieni attivata l'opzione **Modifica le impostazioni del prodotto per incrementare la protezione quando ci si connette a una rete Wi-Fi pubblica poco sicura**.
5. Clicca su **Salva**.

30.5. Profilo Modalità Batteria

Il profilo Modalità Batteria è stato progettato appositamente per gli utenti di computer portatili e tablet. Il suo scopo è ridurre al minimo l'impatto del sistema e di Bitdefender sul consumo energetico, quando il livello di carica della batteria è inferiore a quello predefinito o selezionato.

Configurare il profilo Modalità Batteria

Per configurare il profilo Modalità Batteria:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.

2. Seleziona la scheda **PROFILI**.
3. Clicca sul pulsante **CONFIGURA** nella sezione del profilo Modalità Batteria.
4. Seleziona le regolazioni del sistema da applicare, spuntando le seguenti opzioni:
   - Ottimizza le impostazioni del prodotto per la modalità Batteria.
   - Rimanda i programmi in background e le attività di manutenzione.
   - Posticipa aggiornamenti automatici di Windows.
   - Modifica le impostazioni dei consumi energetici per la modalità Batteria.
   - Disattiva i dispositivi esterni e le porte di rete.
5. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

Digita un valore valido nella casella numerica o selezionane uno usando le frecce su e giù per specificare quando il sistema deve iniziare a operare in modalità Batteria. Di norma, la modalità si attiva quando il livello di carica della batteria è inferiore al 30%.

Quando Bitdefender funziona con il profilo Modalità Batteria, vengono applicate le seguenti impostazioni del prodotto:

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

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

30.6. Ottimizzazione in tempo reale

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

Per attivare o disattivare l'Ottimizzazione in tempo reale:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **PROFILI**.
3. Scorri verso il basso finché non trovi l'opzione dell'ottimizzazione in tempo reale e usa l'interruttore corrispondente per attivarla o disattivarla.

RISOLUZIONE DEI PROBLEMI

31. RISOLVERE I PROBLEMI PIÙ COMUNI

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

- «*Il mio sistema sembra lento*» (p. 195)
- «*La scansione non parte*» (p. 197)
- «*Non posso più usare una app*» (p. 199)
- «*Cosa fare quando Bitdefender blocca un sito web o un'applicazione online sicuri*» (p. 200)
- «*Cosa fare se Bitdefender rilevasse un'applicazione sicura come ransomware*» (p. 201)
- «*Come aggiornare Bitdefender con una connessione a Internet lenta*» (p. 205)
- «*I servizi Bitdefender non rispondono*» (p. 206)
- «*Il filtro antispam non funziona correttamente*» (p. 206)
- «*L'opzione Compila automaticamente nel mio Portafoglio non funziona*» (p. 212)
- «*Rimozione di Bitdefender non riuscita*» (p. 213)
- «*Il sistema non si riavvia dopo aver installato Bitdefender*» (p. 214)

Se non riesci a trovare il problema qui, o se la soluzione fornita non lo risolve, puoi contattare un operatore del supporto tecnico di Bitdefender come indicato nel capitolo «*Chiedere aiuto*» (p. 230).

31.1. Il mio sistema sembra lento

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

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

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

  Sebbene Bitdefender cerchi e rimuova i programmi di sicurezza trovati durante l'installazione, si consiglia di rimuovere ogni altra soluzione di

sicurezza in uso prima dell'installazione di Bitdefender. Per maggiori informazioni, fai riferimento a «*Come posso rimuovere le altre soluzioni di sicurezza?*» (p. 86).

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

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

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

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

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

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

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

  Per avviare la scansione del sistema:

  1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
  2. Clicca sul link **VEDI FUNZIONALITÀ**.
  3. Nel pannello **ANTIVIRUS**, clicca su **Scansione sistema**.
  4. Segui i passaggi della procedura guidata.

31.2. La scansione non parte

Questo tipo di problema può avere due cause principali:

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

  In questo caso, reinstalla Bitdefender:

  - In **Windows 7**:

    1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
    2. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
    3. Clicca su **REINSTALLA** nella finestra che comparirà.
    4. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.

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

    1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
    2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
    3. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
    4. Clicca su **REINSTALLA** nella finestra che comparirà.
    5. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.

  - In **Windows 10**:

    1. Clicca su **Start** e poi su Impostazioni.
    2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
    3. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
    4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
    5. Clicca su **REINSTALLA** nella finestra che comparirà.
    6. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.

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

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

  In questo caso:

  1. Rimuovi l'altra soluzione di sicurezza. Per maggiori informazioni, fai riferimento a «*Come posso rimuovere le altre soluzioni di sicurezza?*» (p. 86).
  2. Reinstalla Bitdefender:
     - In **Windows 7**:
       a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
       b. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
       c. Clicca su **REINSTALLA** nella finestra che comparirà.
       d. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.
     - In **Windows 8 e Windows 8.1**:
       a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
       b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
       c. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
       d. Clicca su **REINSTALLA** nella finestra che comparirà.
       e. Attendi che il processo di reinstallazione sia completo e riavvia il sistema.
     - In **Windows 10**:
       a. Clicca su **Start** e poi su Impostazioni.
       b. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.
       c. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.

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

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

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

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 230).

31.3. Non posso più usare una app

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

Dopo aver installato Bitdefender potrebbe verificarsi una di queste situazioni:

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

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

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

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

Per aggiungere il programma all'elenco delle eccezioni:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.

2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona ⚙ nell'angolo in basso a destra del pannello **ADVANCED THREAT DEFENSE**.
4. Nella finestra **WHITELIST**, clicca su **Aggiungi applicazioni alla whitelist**.
5. Trova e seleziona l'applicazione che vuoi escludere, e clicca su **OK**.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 230).

31.4. Cosa fare quando Bitdefender blocca un sito web o un'applicazione online sicuri

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

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

Per aggiungere un sito web alla **Whitelist**:

1. Clicca sull'icona Ⓑ nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **PROTEZIONE WEB**, clicca su **Whitelist**.
4. Inserisci l'indirizzo del sito web o dell'applicazione online bloccata nel campo corrispondente e clicca su **Aggiungi**.
5. Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

A questo elenco andrebbero aggiunti solo siti web e applicazioni assolutamente affidabili. Saranno esclusi dalle scansioni eseguite dai seguenti motori: minacce, phishing e frodi.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 230).

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

Un Ransomware è un programma dannoso che cerca di sottrarre denaro agli utenti, bloccando i loro sistemi vulnerabili. Per mantenere sempre sicuro il sistema da ogni situazione spiacevole, Bitdefender ti dà la possibilità di proteggere i file personali.

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **SAFE FILES**, clicca su **Accesso applicazione**.
4. Verranno elencate le app che hanno richiesto di modificare i file nelle tue cartelle protette. Clicca sull'interruttore Consenti accanto all'applicazione che ritieni sicura.

31.6. Non riesco a connettermi a Internet

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **FIREWALL**.
4. Seleziona la scheda **REGOLE**.
5. Per aggiungere una regola per l'applicazione, clicca sul link **Aggiungi regola**.

6. Apparirà una nuova finestra, dove potrai aggiungere i dettagli. Assicurati di selezionare tutti i tipi di rete disponibili e nella sezione **Autorizzazione** seleziona **Consenti**.

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 230).

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

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Clicca sull'icona nell'angolo in basso a destra del pannello **FIREWALL**.
4. Clicca sul link **Aggiungi regola** nella parte superiore della finestra **REGOLE**.
5. Nella finestra **IMPOSTAZIONI**, attiva l'opzione **Applica questa regola a tutte le applicazioni.**.
6. Clicca sulla scheda **AVANZATE**.
7. Nella casella **Indirizzo remoto personale**, digita l'indirizzo IP del computer o della stampante a cui vuoi accedere senza restrizioni.

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

Controllare altre potenziali cause, ad esempio le seguenti:

- Il firewall su un altro computer potrebbe bloccare la condivisione di file e stampante con il tuo computer.
  - Se viene utilizzato il firewall di Windows, è possibile configurarlo per permettere la condivisione di file e stampanti nel modo seguente:

- In **Windows 7**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e seleziona **Sistema e sicurezza**.
  2. Vai a **Windows Firewall** e clicca su **Consenti un programma con Windows Firewall**.
  3. Seleziona la casella **Condivisione file e stampanti**.
- In **Windows 8 e Windows 8.1**:
  1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
  2. Clicca su **Sistema e sicurezza**, vai a **Windows Firewall** e seleziona **Consenti una app con Windows Firewall**.
  3. Seleziona la casella **Condivisione file e stampanti** e clicca su **OK**.
- In **Windows 10**:
  1. Digita "Consenti app attraverso Windows Firewall" nella casella di ricerca della barra delle applicazioni e clicca sulla sua icona.
  2. Clicca su **Cambia impostazioni**.
  3. Nell'elenco **App e funzionalità consentite**, metti la spunta a **Condivisione file e stampanti** e clicca su **OK**.
- Se viene utilizzato un altro programma firewall, fai riferimento alla sua documentazione o al file della guida.

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

- La stampante collegata al proprio computer o all'altro computer non è condivisa.
- La stampante condivisa non è stata aggiunta al computer.

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

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 230).

31.8. Internet è lento

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

Per risolvere questa situazione:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **FIREWALL**, clicca sull'interruttore ATTIVA/INATTIVA per disattivare la funzionalità.
4. 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. 230).

- Se la connessione a Internet è migliorata dopo aver disattivato il firewall di Bitdefender:

  a. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.

  b. Clicca sul link **VEDI FUNZIONALITÀ**.

  c. Clicca sull'icona nell'angolo in basso a destra del pannello **FIREWALL**.

  d. Vai alla scheda **ADATTATORI DI RETE** e imposta la tua connessione a Internet come **Casa/Ufficio**.

  e. Nella scheda **IMPOSTAZIONI AVANZATE**, clicca sull'interruttore per disattivare **Blocca port scan nella rete**.

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

  f. 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. 230).

31.9. Come aggiornare Bitdefender con una connessione a Internet lenta

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

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Seleziona la scheda **AGGIORNA**.
3. Accanto a **Regole di esecuzione dell'aggiornamento**, seleziona **Chiedi prima di scaricare** dal menu a tendina.
4. Torna alla finestra principale e clicca sul link **AGGIORNA**.
5. Seleziona solo **Aggiornamento firme** e poi clicca su **OK**.

6. Bitdefender scaricherà e installerà solo il database delle informazioni sulle minacce.

31.10. I servizi Bitdefender non rispondono

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

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

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

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

Per risolvere questo errore, provare queste soluzioni:

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

   Per maggiori informazioni, fai riferimento a «*Come posso rimuovere le altre soluzioni di sicurezza?*» (p. 86).

Se l'errore persiste, contatta i nostri operatori del supporto tecnico per ricevere assistenza, come indicato nella sezione «*Chiedere aiuto*» (p. 230).

31.11. Il filtro antispam non funziona correttamente

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

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

31.11.1. 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 degli Amici sono considerati legittimi. Non vengono verificati dal filtro antispam e di conseguenza non vengono mai contrassegnati come [spam].

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

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

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

> **Nota**
> Bitdefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo. Per un elenco completo delle applicazioni di posta supportate, fai riferimento a «*Programmi e protocolli di posta elettronica supportati*» (p. 120).

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. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTISPAM**, clicca su **Gestisci amici**.

   Apparirà una 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.

31.11.2. 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 delle applicazioni di posta supportate, fai riferimento a «*Programmi e protocolli di posta elettronica supportati*» (p. 120).

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

Indica messaggi spam non rilevati

Se si utilizza un'applicazione di posta supportata si può facilmente indicare quali messaggi e-mail avrebbero dovuto essere rilevati come spam. Così facendo si migliorerà considerevolmente l'efficienza del filtro antispam. 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 (in genere localizzata nella parte superiore della finestra del client di posta). Vengono immediatamente contrassegnati come [spam] e verranno spostati alla cartella posta indesiderata.

Aggiungi spammer a elenco Spammer

Se stai utilizzando un'applicazione di posta supportata, puoi facilmente aggiungere i mittenti dei messaggi di spam all'elenco Spammer. 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 utilizzi un client di posta diverso, puoi aggiungere manualmente nuovi contatti all'elenco Spammer dall'interfaccia di Bitdefender. Si tratta di un metodo conveniente solo quando si ricevono diversi messaggi spam dallo stesso indirizzo e-mail. Attenersi alla seguente procedura:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTISPAM**, clicca su **Gestisci spammer**.

   Apparirà una 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.

31.11.3. 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 seguenti condizioni:

- La protezione antispam potrebbe essere disattivata. Per verificare lo stato della protezione antispam, clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender e seleziona il link **VEDI FUNZIONALITÀ**. Clicca sulla ruota del pannello **ANTISPAM** e verifica nella parte superiore della finestra se la funzionalità è attivata.

  Se l'antispam è disattivato, questa è la causa dei problemi. Clicca sull'interruttore corrispondente per attivare la protezione antispam.

- La protezione antispam di Bitdefender è disponibile solo per client e-mail configurati per ricevere messaggi e-mail tramite il protocollo POP3. Questo vuol dire che:

  - I messaggi e-mail ricevuti tramite servizi e-mail web (ad esempio Yahoo, Gmail, Hotmail o altri) non sono filtrati per spam da Bitdefender.
  - Se il tuo client e-mail è configurato per ricevere messaggi e-mail usando un protocollo diverso da POP3 (per esempio, IMAP4), il filtro antispam di Bitdefender non verifica se siano spam.

  Nota

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

- Bitdefender Internet Security 2018 non esegue la scansione del traffico POP3 di Lotus Notes.

Una possibile soluzione consiste nel riparare o reinstallare il prodotto. Tuttavia puoi contattare Bitdefender per ricevere supporto, come descritto nella sezione «*Chiedere aiuto*» (p. 230).

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

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

Per risolvere il problema, segui questi passaggi:

- In **Internet Explorer:**
  1. Apri Internet Explorer.
  2. Clicca su Strumenti.
  3. Clicca su Gestisci Add-on.
  4. Clicca su Barre degli strumenti ed Estensioni.
  5. Seleziona **Portafoglio di Bitdefender** e clicca su **Attiva**.
- In **Mozilla Firefox:**
  1. Apri Mozilla Firefox.
  2. Clicca su Strumenti.
  3. Clicca su Add-on.
  4. Clicca su Estensioni.
  5. Seleziona **Portafoglio di Bitdefender** e clicca su **Attiva**.
- In **Google Chrome:**
  1. Apri Google Chrome.
  2. Vai all'icona del menu.
  3. Clicca su Altri strumenti.
  4. Clicca su Estensioni.
  5. Seleziona **Portafoglio di Bitdefender** e clicca su **Attiva**.

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

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 230).

31.13. Rimozione di Bitdefender non riuscita

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

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

Per rimuovere completamente Bitdefender dal sistema:

- In **Windows 7**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
  2. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
  3. Clicca su **RIMUOVI** nella finestra che comparirà.
  4. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
- In **Windows 8 e Windows 8.1**:
  1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
  2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
  3. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
  4. Clicca su **RIMUOVI** nella finestra che comparirà.
  5. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
- In **Windows 10**:
  1. Clicca su **Start** e poi su Impostazioni.
  2. Clicca sull'icona **Sistema** nelle Impostazioni e poi seleziona **Applicazioni installate**.

3. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
5. Clicca su **RIMUOVI** nella finestra che comparirà.
6. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.

31.14. Il sistema non si riavvia dopo aver installato Bitdefender

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

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

Ecco come affrontare ogni situazione:

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

  Per risolvere:

  1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a «*Come posso riavviare in modalità provvisoria?*» (p. 87).
  2. Rimuovi Bitdefender dal tuo sistema:
     - In **Windows 7**:
       a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
       b. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.
       c. Clicca su **RIMUOVI** nella finestra che comparirà.
       d. Attendi che il processo di disinstallazione sia completo e riavvia il sistema.
       e. Riavvia il sistema in modalità normale.
     - In **Windows 8 e Windows 8.1**:

a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.

b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.

c. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.

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

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

f. Riavvia il sistema in modalità normale.

- In **Windows 10**:

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

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

c. Trova **Bitdefender Internet Security 2018** e seleziona **Disinstalla**.

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

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

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

g. Riavvia il sistema in modalità normale.

3. Reinstalla il tuo prodotto Bitdefender.

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

Per risolvere:

1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a «*Come posso riavviare in modalità provvisoria?*» (p. 87).
2. Rimuovi l'altra soluzione di sicurezza dal sistema:

- In **Windows 7**:

a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.

b. Trova il nome del programma che desideri rimuovere e seleziona **Rimuovi**.

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

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

a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.

b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.

c. Trova il nome del programma che desideri rimuovere e seleziona **Rimuovi**.

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

- In **Windows 10**:

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

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

c. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.

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

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

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

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

Per risolvere:

1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a «*Come posso riavviare in modalità provvisoria?*» (p. 87).
2. Usa l'opzione Ripristino configurazione di sistema di Windows per ripristinare il computer a uno stato precedente all'installazione del prodotto Bitdefender.

3. Riavvia il sistema in modalità normale e contatta i nostri operatori del supporto per assistenza, come indicato nella sezione «*Chiedere aiuto*» (p. 230).

32. RIMUOVERE LE MINACCE DAL SISTEMA

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

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

- «*Bitdefender Modalità di soccorso (Ambiente di soccorso in Windows 10)*» (p. 218)
- «*Cosa fare quando Bitdefender trova delle minacce sul computer?*» (p. 222)
- «*Come posso rimuovere una minaccia in un archivio?*» (p. 224)
- «*Come posso rimuovere una minaccia in un archivio di e-mail?*» (p. 225)
- «*Cosa fare se sospetti che un file possa essere pericoloso?*» (p. 226)
- «*Quali sono i file protetti da password nel registro della scansione?*» (p. 226)
- «*Quali sono gli elementi ignorati nel registro della scansione?*» (p. 227)
- «*Quali sono i file supercompressi nel registro della scansione?*» (p. 227)
- «*Perché Bitdefender ha eliminato automaticamente un file infetto?*» (p. 228)

Se non riesci a trovare il problema qui, o se la soluzione fornita non lo risolve, puoi contattare un operatore del supporto tecnico di Bitdefender come indicato nel capitolo «*Chiedere aiuto*» (p. 230).

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

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

Una volta installato Bitdefender Internet Security 2018 s **Windows 7, Windows 8 e Windows 8.1** e scaricato il file dell'immagine della modalità Soccorso di Bitdefender, la modalità Soccorso può essere utilizzata anche se non sei più in grado di avviare Windows.

In Windows 10, l'ambiente di Soccorso di Bitdefender è integrato con Windows RE, il che significa che non sarà necessario scaricare alcuna immagine della modalità Soccorso in questo sistema operativo, e la funzione non potrà essere usata se ci sono problemi in avvio. Per pulire il sistema prima che vengano caricati i servizi di Windows, ti consigliamo di usare il CD di soccorso di Bitdefender.

Il CD di soccorso di Bitdefender è uno strumento gratuito che esamina e pulisce il computer ogni volta che sospetti che una minaccia possa influenzarne il funzionamento. Una serie di articoli utili contenenti dettagli su come crearlo e utilizzarlo sono disponibili nella piattaforma del Centro di supporto di Bitdefender: http://www.bitdefender.it/support/consumer.html.

Scaricare l'immagine della modalità di Soccorso di Bitdefender

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

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTIVIRUS**, clicca su **Modalità Soccorso**.
4. Clicca su **SÌ** nella finestra di conferma che compare per riavviare il computer.

   Attendi che il file dell'immagine della modalità Soccorso di Bitdefender sia stato scaricato dai server di Bitdefender. Non appena termina il processo di download, il computer sarà riavviato.

   Comparirà un menu per avvisarti di selezionare un sistema operativo. In questo passaggio, puoi scegliere di avviare il tuo sistema in modalità soccorso o normale.

Nota
A causa dell'integrazione con l'ambiente di ripristino di Windows in **Windows 10**, non è necessario scaricare alcuna immagine della modalità di soccorso su questo sistema operativo.

Avviare il sistema in modalità soccorso in Windows 7, Windows 8 e Windows 8.1

Puoi accedere alla Modalità soccorso in uno dei due modi:

Dall'interfaccia di Bitdefender

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTIVIRUS**, clicca su **Modalità Soccorso**.
4. Clicca su **SÌ** nella finestra di conferma che compare per riavviare il computer.
5. Dopo il riavvio del computer, compare un menu che ti avvisa di selezionare un sistema operativo. Seleziona **Modalità soccorso di Bitdefender** per avviare un ambiente di Bitdefender da cui poter pulire la tua partizione Windows.
6. Se richiesto, premi **Invio** e seleziona la risoluzione dello schermo più vicina a quella che usi normalmente. Poi premi di nuovo **Invio**.

   La modalità soccorso di Bitdefender sarà pronta tra pochi istanti.

Avvia il computer direttamente in Modalità soccorso

Se Windows non parte più, puoi avviare il tuo computer direttamente nella Modalità soccorso di Bitdefender seguendo i passaggi sottostanti:

- In **Windows 7**:
  1. Premi il tasto **F8** finché non compaiono sullo schermo le **Opzioni avanzate di avvio**.
  2. Usa i tasti freccia per selezionare la modalità di soccorso di Bitdefender e premi **Invio**.

     Tra pochi istanti la Modalità soccorso di Bitdefender si caricherà.
- In **Windows 8 e Windows 8.1**:
  1. Premi il tasto **Shift** finché non compaiono sullo schermo le **Opzioni avanzate di avvio**.
  2. Seleziona l'opzione **Usa un altro sistema operativo** e poi Modalità soccorso di Bitdefender.

Tra pochi istanti la Modalità soccorso di Bitdefender si caricherà.

Nota
È possibile caricare il tuo computer in modalità soccorso solo se il file dell'immagine della modalità soccorso in precedenza è stato scaricat, come descritto in «Scaricare l'immagine della modalità di Soccorso di Bitdefender» (p. 219).

Avviare il tuo sistema con l'ambiente di soccorso in Windows 10

Puoi accedere all'ambiente di soccorso solo dal tuo prodotto Bitdefender, come segue:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Clicca sul link **VEDI FUNZIONALITÀ**.
3. Nel pannello **ANTIVIRUS**, clicca su **Ambiente di soccorso**.
4. Clicca su **Riavvia** nella finestra che comparirà.

   L'ambiente di soccorso di Bitdefender sarà pronto tra pochi istanti.

Esaminare il tuo sistema nella modalità di soccorso (Ambiente di soccorso in Windows 10)

Per esaminare il tuo sistema nella modalità di soccorso (Ambiente di soccorso):

- In **Windows 7, Windows 8 e Windows 8.1**:
  1. Entra in Modalità soccorso, come descritto in «Avviare il sistema in modalità soccorso in Windows 7, Windows 8 e Windows 8.1» (p. 220).
  2. Comparirà il logo di Bitdefender e i motori della soluzione di sicurezza inizieranno a essere copiati.
  3. Comparirà una finestra di benvenuto. Clicca su **Continua**.
  4. Viene avviato un aggiornamento del database delle informazioni sulle minacce.
  5. Una volta completato l'aggiornamento, compare la finestra della scansione antivirus su richiesta di Bitdefender.

6. Clicca su **Controlla ora**, seleziona l'obiettivo della scansione nella finestra che compare e clicca su **Apri** per avviare la scansione.

   Si consiglia di controllare la tua intera partizione di Windows.

   > **Nota**
   > Quando si lavora in Modalità soccorso, avrai a che fare con nomi di partizioni tipo Linux. Le partizioni del disco compariranno come sda1 che corrisponde alla partizione di Windows (C:), sda2 che corrisponde a (D:) e così via.

7. Attendi il completamento della scansione. Se viene rilevata una minaccia, segui le istruzioni per rimuoverla.
8. Per uscire dalla modalità soccorso, clicca con il pulsante destro in un'area libera del desktop, seleziona **Esci** nel menu che comparirà e poi seleziona se riavviare o spegnere il computer.

- In **Windows 10**:

  1. Accedi all'ambiente di soccorso, come descritto in «Avviare il tuo sistema con l'ambiente di soccorso in Windows 10» (p. 221).
  2. Il processo di scansione di Bitdefender parte automaticamente non appena il sistema viene caricato nell'ambiente di soccorso.
  3. Attendi il completamento della scansione. Se viene rilevata una minaccia, segui le istruzioni per rimuoverla.
  4. Per uscire dall'ambiente di soccorso, clicca sul pulsante **CHIUDI** nella finestra con i risultati della scansione.

32.2. Cosa fare quando Bitdefender trova delle minacce sul computer?

Puoi scoprire la presenza di una minaccia sul computer in uno dei seguenti modi:

- Hai controllato il tuo computer e Bitdefender ha trovato alcuni elementi infetti.
- Un avviso di minaccia ti informa che Bitdefender ha bloccato una o più minacce sul tuo computer.

In tali situazioni, aggiorna Bitdefender per assicurarti di avere il più recente database dele informazioni sulle minacce e avvia una Scansione del sistema per analizzarlo.

Al termine della scansione del sistema, seleziona l'azione desiderata per gli elementi infetti (Disinfetta, Elimina, Sposta in quarantena).

Avvertimento
Se sospetti che il file sia parte del sistema operativo Windows o che non sia un file infetto, non seguire questi passaggi e contatta il Servizio clienti di Bitdefender il prima possibile.

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

Il primo metodo può essere usato in modalità normale:

1. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
   b. Clicca sul link **VEDI FUNZIONALITÀ**.
   c. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
   d. Nella finestra **PROTEZIONE**, clicca sull'interruttore ATTIVA/INATTIVA.
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a *«Come posso visualizzare gli elementi nascosti in Windows?»* (p. 85).
3. Trova l'ubicazione del file infetto (controlla il registro della scansione) ed eliminalo.
4. Attiva la protezione antivirus in tempo reale di Bitdefender.

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

1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a *«Come posso riavviare in modalità provvisoria?»* (p. 87).
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a *«Come posso visualizzare gli elementi nascosti in Windows?»* (p. 85).

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. 230).

32.3. Come posso rimuovere una minaccia in un archivio?

Un archivio è un file o una raccolta di file compressi in un formato speciale per ridurre lo spazio su disco necessario alla loro archiviazione.

Alcuni di questi formati sono aperti, offrendo così a Bitdefender l'opportunità per controllarli all'interno e intraprendere le azioni adeguate per rimuoverli.

Altri formati dell'archivio sono chiusi parzialmente o interamente, e Bitdefender può solo rilevare la presenza di minacce al loro interno, senza poter intraprendere alcuna azione.

Se Bitdefender ti avvisa di aver rilevato una minaccia in un archivio e di non poter attuare alcuna azione, significa che non puoi rimuovere la minaccia a causa delle restrizioni sulle impostazioni di permesso dell'archivio.

Ecco come rimuovere una minaccia in un archivio:

1. Identifica l'archivio che include la minaccia, eseguendo una scansione del sistema.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
   b. Clicca sul link **VEDI FUNZIONALITÀ**.
   c. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
   d. Nella finestra **PROTEZIONE**, clicca sull'interruttore ATTIVA/INATTIVA.
3. Vai all'ubicazione dell'archivio e decomprimilo usando un programma di compressione, come WinZip.
4. Identifica il file infetto e lo elimina.

5. Elimina l'archivio originale per assicurarti che l'infezione sia stata rimossa completamente.
6. Ricomprimi i file in un nuovo archivio usando un'applicazione di archiviazione, come WinZip.
7. Attiva la protezione antivirus in tempo reale di Bitdefender ed esegui una scansione del sistema per assicurarti che non ci siano altre infezioni.

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

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 230).

32.4. Come posso rimuovere una minaccia in un archivio di e-mail?

Bitdefender può anche identificare le minacce nei database e-mail e negli archivi e-mail presenti sul disco rigido.

A volte devi identificare il messaggio infetto usando le informazioni fornite nel rapporto della scansione ed eliminarlo manualmente.

Ecco come rimuovere una minaccia presente in un archivio e-mail:

1. Controlla il database e-mail con Bitdefender.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
   b. Clicca sul link **VEDI FUNZIONALITÀ**.
   c. Clicca sull'icona nell'angolo in basso a destra del pannello **ANTIVIRUS**.
   d. Nella finestra **PROTEZIONE**, clicca sull'interruttore ATTIVA/INATTIVA.
3. Apri il rapporto della scansione e usa le informazioni d'identificazione (oggetto, da, a) dei messaggi infettati per localizzarli nel client e-mail.

4. Elimina i messaggi infetti. La maggior parte dei client e-mail spostano il messaggio eliminato in una cartella di recupero, dalla quale può essere recuperato. Dovresti assicurarti che il messaggio sia eliminato anche da questa cartella di ripristino.
5. Compatta la cartella di memorizzazione del messaggio infetto.
   - Per Microsoft Outlook 2007: Nel menu File, clicca su Gestione file dati. Seleziona i file delle cartelle personali (.pst) che desideri compattare e clicca su Impostazioni. Clicca su Compatta.
   - Per Microsoft Outlook 2007 / 2013/ 2016: Nel menu File, clicca su Info e poi su Impostazioni account (Consente di aggiungere e rimuovere account o di modificare le impostazioni di connessione esistenti). Poi clicca su File di dati, seleziona i file delle cartelle personali (.pst) che desideri compattare e clicca su Impostazioni. Clicca su Compatta.
6. Attiva la protezione antivirus in tempo reale di Bitdefender.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 230).

32.5. Cosa fare se sospetti che un file possa essere pericoloso?

Puoi sospettare che un file del tuo sistema sia pericoloso, anche se il prodotto Bitdefender non l'ha rilevato.

Per assicurarti che il tuo sistema sia protetto:

1. Esegui una **Scansione del sistema** con Bitdefender. Per scoprire come fare, fai riferimento a «*Come posso eseguire una scansione del mio sistema?*» (p. 62).
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. 230).

32.6. Quali sono i file protetti da password nel registro della scansione?

Questa è solo una notifica per indicare che Bitdefender ha rilevato che questi file sono protetti da una password o da una qualche forma di crittografia.

In genere gli elementi protetti da password sono:

- File che appartengono a un'altra soluzione di sicurezza.
- File che appartengono al sistema operativo.

Per poter controllare i contenuti, devi estrarre o quantomeno decriptare questi file.

Qualora tali contenuti venissero estratti, la scansione in tempo reale di Bitdefender li controllerebbe automaticamente per proteggere il tuo computer. Se desideri controllare quei file con Bitdefender, devi contattare il produttore per ottenere maggiori informazioni sui file.

Ti consigliamo di ignorare quei file perché non sono una minaccia per il sistema.

32.7. Quali sono gli elementi ignorati nel registro della scansione?

Tutti i file che compaiono come Ignorati nel rapporto della scansione sono puliti.

Per prestazioni superiori, Bitdefender non controlla file che non sono stati modificati dall'ultima scansione.

32.8. Quali sono i file supercompressi nel registro della scansione?

Gli oggetti supercompressi sono elementi che non possono essere estratti dal motore di scansione o elementi per i quali la crittografia avrebbe impiegato troppo tempo, rendendo il sistema instabile.

Supercompresso significa che Bitdefender ha saltato la scansione di quell'archivio perché scompattarlo avrebbe richiesto troppe risorse di sistema. Se necessario, il contenuto sarà controllato solo durante l'accesso in tempo reale.

32.9. Perché Bitdefender ha eliminato automaticamente un file infetto?

Se viene rilevato un file infetto, Bitdefender tenterà di disinfettarlo automaticamente. Se la disinfezione dovesse fallire, il file sarà messo in quarantena per contenere l'infezione.

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

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

CONTATTACI

33. CHIEDERE AIUTO

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

La sezione «*Risolvere i problemi più comuni*» (p. 195) 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. 230)
- «Contattaci tramite il nostro Centro di supporto online» (p. 231)

Contattaci direttamente dal tuo prodotto Bitdefender

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

Attenersi alla seguente procedura:

1. Clicca sull'icona nella barra laterale sinistra dell'interfaccia di Bitdefender.
2. Hai le seguenti opzioni:
   - **MANUALE D'USO**

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

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

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

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

i. Seleziona il tipo di problema che hai riscontrato.

ii. Inserisci una descrizione del problema riscontrato.

iii. Clicca su **PROVA A RIPRODURRE IL PROBLEMA** nel caso riscontrassi un problema con il prodotto. Continua con i passaggi richiesti.

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

iv. Clicca su **CONFERMA TICKET**.

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

i. Inserisci il tuo nome completo.

ii. Inserisci il tuo indirizzo e-mail.

iii. Seleziona la casella di accettazione.

iv. Clicca su **INVIA TICKET**.

Attendi qualche istante in cui il tuo ticket sarà creato e le informazioni raccolte saranno inviate al Supporto tecnico di Bitdefender.

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

Contattaci tramite il nostro Centro di supporto online

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

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

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

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

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

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

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

34. RISORSE ONLINE

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

- Centro di supporto di Bitdefender:

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

- Forum del supporto di Bitdefender:

  http://forum.bitdefender.com

- Il portale di sicurezza informatica HOTforSecurity:

  http://www.hotforsecurity.com

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

34.1. Centro di supporto di Bitdefender

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

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

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

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

34.2. Forum supporto di Bitdefender

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

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

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

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

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

34.3. Portale HOTforSecurity

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

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

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

35. CONTATTI

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

35.1. Indirizzi web

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

35.2. Distributori locali

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

Per trovare un distributore di Bitdefender nel tuo paese:

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

35.3. Uffici di Bitdefender

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

USA

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

Regno Unito e Irlanda

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
E-mail: info@bitdefender.co.uk
Telefono: (+44) 2036 080 456
Vendite: sales@bitdefender.co.uk
Supporto tecnico: https://www.bitdefender.co.uk/support/
Web: https://www.bitdefender.co.uk

Germania

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Ufficio: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Vendite: vertrieb@bitdefender.de
Supporto tecnico: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

Danimarca

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Ufficio: +45 7020 2282
Supporto tecnico: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

Spagna

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Telefono: +34 902 19 07 65
Vendite: comercial@bitdefender.es
Supporto tecnico: https://www.bitdefender.es/support/consumer.html
Sito web: https://www.bitdefender.es

Romania

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Telefono vendite: +40 21 2063470
E-mail vendite: sales@bitdefender.ro
Supporto tecnico: https://www.bitdefender.ro/support/consumer.html
Sito web: https://www.bitdefender.ro

Emirati Arabi Uniti

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefono vendite: 00971-4-4588935 / 00971-4-4589186
E-mail vendite: mena-sales@bitdefender.com
Supporto tecnico: https://www.bitdefender.com/support/consumer.html
Sito web: https://www.bitdefender.com

Glossario

Abbonamento

Un accordo di acquisto che offre all'utente il diritto di utilizzare un particolare prodotto o servizio su un numero specifico di dispositivi e per un certo periodo di tempo. Un abbonamento scaduto può essere rinnovato automaticamente, utilizzando le informazioni fornite dall'utente con il primo acquisto.

ActiveX

ActiveX è una tecnologia per lo sviluppo di programmi che possano essere richiamati da altri programmi e sistemi operativi. La tecnologia ActiveX è utilizzata in Microsoft Internet Explorer per generare pagine web interattive che appaiano e si comportino come applicazioni invece che come pagine statiche. Con ActiveX, gli utenti possono chiedere o rispondere a domande, adoperare pulsanti e interagire in altri modi con la pagina web. I controlli ActiveX sono spesso scritti utilizzando il linguaggio Visual Basic.

Gli ActiveX sono noti per una totale mancanza di controlli di sicurezza; gli esperti di sicurezza dei computer scoraggiano il loro utilizzo attraverso Internet.

Adware

La modalità adware è spesso combinata con un'applicazione che viene fornita gratuitamente se l'utente accetta l'adware. Considerando che le applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove viene spiegato il proposito dell'applicazione, non viene commessa alcuna infrazione.

Comunque, le finestre pop-up di avvertimento possono essere fastidiose e in alcuni casi ridurre le prestazioni del sistema. Inoltre, le informazioni che vengono raccolte da alcune di queste applicazioni possono causare inconvenienti riguardo la privacy degli utenti, non sempre completamente informati sui termini dell'accordo di licenza.

Aggiornamento

Una nuova versione di un prodotto software o hardware creato per sostituire la versione precedente. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già

installata una versione precedente sul computer, diversamente non sarà possibile installare l'aggiornamento.

Bitdefender dispone della propria funzionalità di aggiornamento, che consente la verifica manuale degli aggiornamenti, oppure l'aggiornamento automatico del prodotto.

Aggiornamento informazioni minacce
Lo schema binario di una minaccia, usato dalla soluzione di sicurezza per rilevare ed eliminare la minaccia.

Applet Java
Un programma Java concepito per funzionare solo su pagine web. Per utilizzare un applet su una pagina web, bisogna specificare il nome dell'applet e la dimensione (lunghezza e larghezza in pixel) che può utilizzare. Quando si accede alla pagina web, il browser scarica l'applet dal server e lo esegue sulla macchina dell'utente (il client). Gli applet differiscono dalle applicazioni in quanto sono governati da un rigido protocollo di sicurezza.

Ad esempio, anche se gli applet vengono lanciati sul client, non possono leggere o scrivere dati nella macchina dell'utente. Inoltre, gli applet sono ulteriormente limitati in modo che possano leggere e scrivere dati solo dallo stesso dominio dai quali provengono.

Archivio
Un Disco, un nastro o una cartella che contiene file memorizzati.

Un file che contiene uno o più file in forma compressa.

Area di notifica
Introdotta con Windows 95, l'area di notifica è situata nella barra delle applicazioni di Windows (in genere in basso vicino all'orologio) e contiene icone miniaturizzate per un accesso veloce a funzioni di sistema come fax, stampante, modem, volume e molto altro. Clicca due volte o clicca con il pulsante destro su un'icona per visualizzare e accedere ai dettagli e i controlli.

Backdoor
Una breccia nella sicurezza di un sistema deliberatamente lasciata dal programmatore o dal manutentore. La presenza di tali "brecce" non sempre è dolosa: su alcuni sistemi operativi, ad esempio, vengono

utilizzate per l'accesso con utenze privilegiate per servizi tecnici o per i programmatori del produttore a scopo di manutenzione.

Botnet

Il termine "botnet" è composto dalle parole "robot" e "network". I botnet sono dispositivi connessi a Internet e infettati con minacce, che possono essere utilizzati per inviare e-mail spam, sottrarre dati, controllare in remoto dispositivi vulnerabili o diffondere spyware, ransomware e altri tipi di minacce. Il loro obiettivo è infettare il maggior numero di dispositivi connessi possibile, come PC, server, dispositivi mobile o IoT che appartengono a grandi organizzazioni o aziende.

Browser

Abbreviazione di browser web, un'applicazione software utilizzata per localizzare e visualizzare pagine web. I browser più diffusi sono Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Questi sono browser grafici, ovvero in grado di visualizzare sia elementi grafici che il testo. Inoltre, i browser più moderni possono presentare informazioni multimediali, inclusi suoni e animazioni, anche se per alcuni formati, richiedono dei plug-in.

Client mail

Un client e-mail è un'applicazione che ti consente di inviare e ricevere e-mail.

Codice di attivazione

È una chiave unica che può essere acquistata dal rivenditore e usata per attivare un servizio o un prodotto specifico. Un codice di attivazione consente l'attivazione di un abbonamento valido per un determinato periodo di tempo e un certo numero di dispositivi. Inoltre, può anche essere utilizzato per estendere un abbonamento, a condizione che venga generato per lo stesso prodotto o servizio.

Cookie

Nell'industria di Internet, i cookie vengono descritti come piccoli file contenenti informazioni relative ai computer individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia di interessi e gusti online degli utenti. In questo settore, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire offerte pubblicitarie personalizzate in base agli interessi degli utenti. Per molte

persone è una lama a doppio taglio, poiché da una parte è efficace e consente di far vedere solo ciò che viene dichiarato interessante. Ma dall'altra, implica in effetti un "tracciamento" di dove si va e di cosa si seleziona. In considerazione di questo è in atto un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come un "codice SKU" (il codice a barre sul retro delle confezioni che viene letto dalle casse). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

Download

Per copiare dati (solitamente un file intero) da una fonte principale su un dispositivo periferico. Il termine viene spesso utilizzato per descrivere un processo di copia di un documento da un servizio online al computer di un utente. Si può inoltre riferire al processo di copiatura di un file da un file server di rete a un computer della rete.

E-mail

Posta elettronica. Un servizio che invia messaggi ai computer attraverso reti locali o globali.

Elementi di avvio

Qualsiasi file posizionato in questa cartella si aprirà all'avvio del computer. Ad esempio, una schermata di avvio, un file audio da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure app che possono essere elementi di avvio. Normalmente in questa cartella viene posizionato un alias di un file, al posto del file stesso.

Estensione del nome di un file

Porzione del nome di un file che segue il punto finale e che indica il tipo di dati inclusi nel file.

Molti sistemi operativi utilizzano estensioni di file, come Unix, VMS e MS-DOS. Sono normalmente composti da una a tre lettere (alcuni vecchi sistemi operativi non ne supportano più di tre). Esempi: "c" per codici sorgente C, "ps" per PostScript, "txt" per testi semplici.

Euristico

Un metodo basato su regole per l'identificazione di nuove minacce. Questo metodo di scansione non si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione euristica è di non essere ingannata dalle nuove varianti di minacce esistenti. Tuttavia,

può occasionalmente segnalare una parte di codice sospetto in programmi normali, generando i cosiddetti "falsi positivi".

Eventi

Un'azione oppure un evento segnalato da un programma. Gli eventi possono essere azioni dell'utente, come cliccare con il mouse o premere un tasto sulla tastiera, oppure del sistema, come l'esaurimento della memoria.

Falso positivo

Appare quando un prodotto di analisi antivirus individua un documento come infettato quando di fatto non lo è.

File di rapporto

Un file che elenca le azioni avvenute. Bitdefender crea un rapporto che elenca i percorsi controllati, le cartelle, il numero di archivi e file esaminati, oltre a quanti file infetti e sospetti sono stati trovati.

Honeypot

Un sistema trappola usato per attirare i pirati informatici in modo da studiare come agiscono e identificare i metodi che utilizzano per ottenere informazioni sul sistema. Aziende e organizzazioni sono sempre più interessate a implementare e utilizzare gli honeypot per migliorare il loro stato di sicurezza generale.

IP

Internet Protocol – protocollo di instradamento nella suite di protocollo TCP/IP, responsabile dell'indirizzamento IP, dell'instradamento, della frammentazione e della ricomposizione dei pacchetti IP.

Keylogger

Un keylogger è una app che registra ogni cosa che digiti.

I keylogger non sono dannosi di natura. Possono essere usati anche per scopi legittimi, come monitorare le attività di dipendenti o bambini. Tuttavia, sono utilizzati anche dai criminali informatici per scopi dannosi (per esempio, ottenere dati personali, come credenziali o codici di accesso).

Linea di comando

In un'interfaccia a linea di comando, l'utente digita i comandi nello spazio previsto direttamente sullo schermo, utilizzando il linguaggio di comando.

Macro virus

Un tipo di minaccia informatica, codificata come macro all'interno di un documento. Molte applicazioni, come ad esempio Microsoft Word ed Excel, supportano potenti linguaggi macro.

Queste applicazioni consentono di codificare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Memoria

Aree di archiviazione interne al computer. Il termine memoria identifica la memorizzazione dei dati sotto forma di chip, mentre la parola archiviazione viene utilizzata per la memoria su nastri o dischi. Ogni computer dispone di un certo quantitativo di memoria fisica, solitamente chiamata memoria principale oppure RAM.

Minaccia

Un programma o parte di codice caricato sul computer a propria insaputa e che viene eseguito contro la propria volontà. La maggior parte delle minacce è anche in grado di auto replicarsi. Tutte le minacce informatiche sono state create dall'uomo. È relativamente facile produrre una semplice minaccia in grado di copiare sé stessa innumerevoli volte. Persino una minaccia così semplice è pericolosa in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di minaccia ancora più pericolosa è quella in grado di trasmettere sé stessa attraverso le reti superando i sistemi di sicurezza.

Minaccia avanzata persistente

Una minaccia avanzata persistente (in inglese, Advanced Persistent Threat o APT) sfrutta le vulnerabilità dei sistemi per sottrarre informazioni importanti e inviarle alla fonte. Questa minaccia prende di mira alcuni grandi gruppi, come organizzazioni, società o governi.

L'obiettivo di una minaccia persistente avanzata è restare nascosta per molto tempo, in modo da monitorare e raccogliere informazioni importanti, senza danneggiare i computer colpiti. Il metodo utilizzato per inserire la minaccia nella rete è tramite un file PDF o un documento

Office, in apparenza innocuo, in modo che ogni utente lo utilizzi senza problemi.

Non euristico

Questo metodo di scansione si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione non-euristica è di non essere ingannata da ciò che potrebbe sembrare una minaccia, e quindi non genera falsi allarmi.

Pacchetti di programmi

Un file in un formato compresso. Molti sistemi operativi e molte applicazioni contengono comandi che vi consentono di compattare un file in modo da occupare meno memoria. Ad esempio, supponiamo di avere un file di testo che contenga dieci caratteri spazio consecutivi. Normalmente occuperebbe dieci byte di memoria.

Un programma che compatta i file potrebbe sostituire gli spazi dei caratteri con un carattere speciale seguito dal numero di spazi sostituiti. In questo caso i dieci spazi occuperebbero solo due byte. Questa è solo una tecnica di compattazione, ma ce ne sono molte altre.

Percorso

I percorsi esatti per raggiungere un file su un computer. Questi percorsi vengono solitamente descritti attraverso il file system gerarchico dall'alto verso il basso.

La strada tra due punti qualsiasi, come ad esempio il canale di comunicazioni tra due computer.

Phishing

L'atto d'inviare un'e-mail a un utente fingendo di essere una società legittima e affermata, nel tentativo di truffarlo, facendogli cedere informazioni private che saranno usate per furti d'identità. L'e-mail invita gli utenti a visitare una pagina web, dove gli sarà chiesto di aggiornare determinate informazioni personali, come password e numero di carta di credito, codice fiscale o coordinate bancarie. In ogni caso, la pagina web è falsa e creata solo per rubare i dati personali dell'utente.

Photon

Photon è una tecnologia di Bitdefender innovativa e discreta, progettata per minimizzare l'impatto della tua soluzione di sicurezza sulle prestazioni del sistema. Monitorando in background l'attività del PC,

crea degli schemi di utilizzo, per ottimizzare i processi di avvio e scansione.

Porta

Un'interfaccia su un computer dalla quale è possibile connettere un dispositivo. I personal computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, monitor e tastiere. Esternamente i personal computer hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

Nelle reti TCP/IP e UDP, un endpoint per una connessione logica. Il numero della porta ne identifica il tipo. Ad esempio, la porta 80 viene usata per il traffico HTTP.

Ransomware

Un Ransomware è un programma dannoso che cerca di sottrarre denaro agli utenti, bloccando i loro sistemi vulnerabili. CryptoLocker, CryptoWall e TeslaWall sono solo alcune delle varianti in grado di violare i sistemi personali degli utenti.

L'infezione può partire, aprendo e-mail di spam, scaricando gli allegati di un messaggio o installando determinate applicazioni, il tutto lasciando l'utente ignaro di ciò che sta accadendo sul suo sistema. Gli autori di ransomware puntano a colpire soprattutto gli utenti normali e le aziende.

Rete privata virtuale (VPN)

È una tecnologia che consente una connessione diretta temporanea e cifrata a una determinata rete su una rete meno sicura. In questo modo, la ricezione e l'invio dei dati sono sempre sicuri e cifrati, ma soprattutto più difficili da intercettare dai pirati informatici. Una prova di sicurezza è l'autenticazione, che può essere fatta solo usando un nome utente e una password.

Rootkit

Un rootkit è una serie di strumenti software che consente di accedere a un sistema come amministratore. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la propria presenza, in modo da non essere visti dagli amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, gli accessi e i registri. Se incorporano il software adeguato, possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche.

I rootkit non sono dannosi per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando i rootkit. Comunque, vengono principalmente utilizzati per nascondere minacce o per celare la presenza di un intruso nel sistema. Se combinati alle minacce, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e registri, ed evitare il rilevamento.

Script

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Settore di avvio:

Un settore all'inizio di ogni disco che ne identifica l'architettura (dimensione del settore, dimensione del cluster, ecc.). Nei dischi di avvio, il settore di boot contiene anche un programma che carica il sistema operativo.

Spam

Messaggi di posta elettronica o newsgroup indesiderati. Generalmente conosciuto come e-mail non desiderate.

Spyware

Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessone a Internet, senza che questo se ne accorga, di solito per scopi pubblicitari. Le applicazioni spyware in genere sono incluse come componente nascosta di programmi freeware o shareware, che possono essere scaricati da Internet. Tuttavia, occorre segnalare che la maggioranza delle applicazioni shareware o freeware non includono alcun programma spyware. Una volta installato, uno spyware monitora le attività dell'utente su Internet e trasmette di nascosto tali informazioni a qualcun altro. Gli spyware possono anche raccogliere informazioni su indirizzi e-mail o addirittura password e numeri di carta di credito.

Gli spyware sono simili a un Trojan che gli utenti installano inconsapevolmente installando altre applicazioni. Un modo comune per

diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli spyware utilizzano memoria e risorse del sistema, le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di rete largamente utilizzati su Internet, che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il relativo traffico.

Trojan

Un programma distruttivo che si maschera da applicazione benevola. A differenza di programmi software dannosi e worm, i trojan non si replicano ma possono essere altrettanto distruttivi. Un tipo di minaccia Trojan particolarmente insidiosa è un programma che dichiara di pulire le minacce dal computer, ma al contrario le introduce.

Il termine deriva da una storia dell'Iliade di Omero, in cui i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

Unità disco

È un dispositivo che legge e scrive dei dati su un disco.

Un drive di disco rigido legge e scrive dischi rigidi.

Un drive di floppy accede i dischi floppy.

Le unità disco possono essere interne (incorporate all'interno di un computer) oppure esterne (collocate in un meccanismo separato e connesso al computer).

Virus di boot

Una minaccia che infetta il settore di avvio di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infettato con un virus di boot, farà sì che la minaccia venga attivata nella memoria. Da quel momento in poi, ogni volta che si esegue il boot del sistema, la minaccia sarà attiva nella memoria.

Virus polimorfico

Una minaccia che modifica la propria forma con ogni file che infetta. Non avendo caratteristiche binarie costanti, queste minacce sono difficili da identificare.

Worm

Un programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.