bitdefender 9

Professional Plus

Manuale dell'utente

- Antivirus
- Antispam
- Firewall
- Antispyware

BitDefender 9 Professional Plus
Manuale dell'utente

SOFTWIN

Pubblicato 2006.05.22
Version 9.5

Avvertimenti Legali


bitdefender
secure your every bit

Sommario

Licenza e garanzia

Questo accordo di Licenza è un contratto legale tra te (utente finale o individuale o entità singola) e SOFTWIN, per l'uso dei prodotti Software SOFTWIN identificati sopra, il quale include il software e può includere mezzi associati, materiale stampato, e documentazione "online" o elettronica ("BitDefender"), essi tutti protetti dalle leggi degli Stati Uniti ed internazionali su copyright, e trattati di protezione internazionali. Mediante l'installazione, copia, o qualsiasi uso di BitDefender, accetti di essere legato dai termini di questo accordo. Se non accetti i termini di questo accordo, non installare ne usare BitDefender; puoi, in ogni caso, riportarlo al tuo punto vendita per il rimborso completo dell'importo, entro 30 giorni dopo l'acquisto. Potrà essere chiesta una prova d'acquisto.

BitDefender è protetto da leggi e trattati internazionali su copyright, così come da altre leggi e trattati sulla proprietà intellettuale. BitDefender è autorizzato, non venduto.

CONCESSIONE DI LICENZA. Con questa, SOFTWIN ti concede, e soltanto a te, la seguente licenza non esclusiva per usare BitDefender:

SOFTWARE DELL' APPLICAZIONE. Puoi installare ed usare una copia di BitDefender, o qualsiasi versione precedente per lo stesso sistema operativo, su un singolo computer (terminale). L'utente primario del computer sul quale è installato BitDefender, può fare una copia addizionale per il suo uso esclusivo su un computer portatile.

UTILIZZO IN RETE. Puoi anche memorizzare o installare una copia di BitDefender su un dispositivo di memoria, come un server di rete, usato solo per installare o eseguire il BitDefender sui tuoi altri computers in una rete interna; comunque, devi acquistare e dedicare una licenza separata per ogni singolo terminale nel quale venga installato o eseguito dal dispositivo di memoria. Una licenza di BitDefender non può essere condivisa ne usata contemporaneamente su diversi computer o terminali. Dovresti acquistare un pacchetto di licenze se hai necessità di diverse licenze da usare su diversi computer o terminali.

PACCHETTO DI LICENZE. Se acquisti un Pacchetto di Licenze e hai acquisito questo Contratto di Licenza per multiple licenze di BitDefender, puoi fare il numero di copie addizionali delle parti di software di BitDefender specificate sopra come "copie accreditate". Sei anche autorizzato a fare il corrispondente numero di copie secondarie per uso sui computer portatili, come specificato sopra, nella sezione intitolata "Software della applicazione".

PERIODO DI LICENZA. La licenza qui concessa avrà inizio nella data in cui installi, copi, o in qualche modo usi per la prima volta BitDefender, e continuerà solo sul computer sul quale è stato installato per la prima volta.

UPGRADE (MIGLIORAMENTI). Se BitDefender è identificato come un upgrade, per usarlo devi essere autorizzato ad usare un prodotto classificato da SOFTWIN come idoneo per l'upgrade.Un BitDefender classificato come un upgrade sostituisce o complementa il prodotto che serve di base idonea per l'upgrade. Puoi usare il prodotto risultante dell'upgrade solo in conformità con i termini di questo Accordo di Licenza. Se BitDefender è un upgrade di una componente di un pacchetto di programmi software, dato in licenza come un solo prodotto, BitDefender può essere utilizzato e trasferito soltanto come parte di questo pacchetto e non può essere separato per l'utilizzo su più di un computer.

COPYRIGHT. Diritto, titolo, interesse in o verso BitDefender e tutti i diritti di copyright in o verso BitDefender (includendo ma non limitando qualsiasi immagine, fotografia, logo, animazione, video, audio, musica, testo e "applets" incorporati nel BitDefender) il materiale stampato accompagnatorio e qualsiasi copia di BitDefender sono proprietà della SOFTWIN. BitDefender è protetto dalle leggi di copyright e da quanto previsto dai trattati internazionali. Di conseguenza, tu devi considerare bd come qualunque altro materiale protetto da copyright ad eccezione del fatto che tu puoi installare bd su un singolo computer a patto che tu tenga l'originale solamente per scopi di backup o archiviazione. Non puoi copiare il materiale stampato che accompagna BitDefender. In tutte le copie create indipendentemente dal supporto o formato in cui esista BitDefender, devi riprodurre ed includere tutte le note copyright in formato originale. Non puoi dare a tua volta in licenza, noleggiare, vendere, dare in leasing BitDefender. Non puoi smontare, raggruppare, disassemblare, creare lavori derivati, modificare, tradurre né fare alcun tentativo per scoprire il codice fonte di BitDefender.

GARANZIA LIMITATA. SOFTWIN garantisce che il supporto sul quale viene distribuito BitDefender non ha difetti per un periodo per un periodo di trenta giorni dalla data in cui ti viene consegnato. L'unico rimedio per l'infrazione di questa garanzia sarà che SOFTWIN, a sua discrezione, può sostituire il supporto difettoso presentata la ricevuta, o rimborsare il denaro pagato per BitDefender. SOFTWIN non garantisce che BitDefender sia ininterrottamente o assolutamente privo di errori o che gli errori verranno corretti. SOFTWIN non garantisce che BitDefender copra le tue necessità. SOFTWIN CON LA PRESENTE NEGA QUALSIASI ALTRA GARANZIA PER BITDEFENDER, SIA ESPLICITA O IMPLICITA. LA GARANZIA SUDDETTA è ESCLKUSIVA E SOSTITUISCE TUTTE LE ALTRE GARANZIE, SIA ESPLICITE O IMPLICITE, INCLUDENDO LE GARANZIE DI COMMERCIABILITA', DI ADEGUAMENTO AD UN PROPOSITO PARTICOLARE, O DI NON INFRAZIONE. QUESTA GARANZIA TI CONCEDE DIRITTI LEGALI SPECIFICI. PUOI AVERE ALTRI DIRITTI, I QUALI VARIANO DA STATO A STATO.

RETTIFICAZIONE DI DANNI. Qualunque persona usando, provando o valutando BitDefender, si assume tutto il rischio della qualità e prestazioni di BitDefender. In nessun caso SOFTWIN sarà responsabile di qualunque danno di qualsiasi tipo, includendo senza limitazioni danni diretti o indiretti che provengano da fuori dell'uso, disimpegno, o consegna di BitDefender, per fino nel caso in cui SOFTWIN abbia avvertito dell'esistenza o possibilità di tali danni.

ALCUNI STATI NON PERMETTONO LA LIMITAZIONE O ESCLUSIONE DI RESPONSABILITA' PER DANNI ACCIDENTALI O CONSEGUENTI, IN QUEL CASO LA LIMITAZIONE O ESCLUSIONE SOPRA INDICATA NON POTRA' ESSERE APPLICATA. IN NESSUN CASO LA RESPONSABILITA' DI SOFTWIN POTRA' ECCEDERE IL PREZZO CHE HAI PAGATO PER BITDEFENDER. Le restrizioni e limitazioni fissate sopraverranno applicate indipendentemente dal modo in cui accetti di usare, valutare o provare BitDefender.

AVVISO IMPORTANTE AGLI UTENTI. QUESTO SOFTWARE NON E' "RESISTENTE AI GUASTI" E NON E' STATO DISEGNATO NE' DESTINATO ALL'USO IN AMBIENTI PERICOLOSI CHE RICHIEDANO OPERAZIONI O ATTUAZIONI IN MANCATA SICUREZZA. QUESTO SOFTWARE MNON E' ADATTO ALL'USO NELL'OPERAZIONE DI NAVIGAZIONE AEREA, NELLE ISTALLAZIONI NUCLEARI, NEI SISTEMI DI COMUNICAZIONE, SISTEMI DI ARMAMENTO, NEI SISTEMI DI RESPIRAZIONE ASSISTITA DIRETTA O INDIRETTA, CONTROLLO DEL TRAFFICO AEREO O QUALUNQUE APPLICAZIONE ISTALLAZIONE DOVE L'ERRORE POSSA RISULTARE IN MORTE, FERITE FISICHE GRAVI, O DANNI ALLA PROPRIETA'.

DIRITTI RISERVATI DEL GOVERNO /. L'uso, duplicazione o rivelazione da parte del governo saranno soggetti alle restrizioni fissate nel sottoparagrafo (C) (1)(ii) della clausola sui Diritti sui dati tecnici e software di computer nella DFARS252.227-7013 o sottoparagrafi (C) (1) e (2) della clausola sui Diritti Riservati del Software Commerciale nella 48 CFR 52.227-19. Contatta SOFTWIN al: 5, F-ca de Glucoza str., 72322-Sect.2, Bucarest, Romania, Tel: 40-21-2330780 o fax 40-21-2330763

GENERALE. Questo accordo sarà regolato dalle leggi della Romania e dai regolamenti e trattati internazionali sul copyright. Questo accordo potrà esser modificato mediante un addendum della licenza, il quale accompagnerà questo accordo o mediante un documento scritto che sia sto firmato da entrambe le parti. Questo contratto è stato scritto solo in lingua inglese e non è da tradurre né interpretare in qualunque altra lingua. Prezzi costi e tariffe di uso di BitDefender sono soggetti a cambi senza previa notifica. Nel caso di invalidità di qualunque parte di questo contratto, questa invalidità non avrà effetto sulla validità delle parti restanti di questo accordo. Bitdefender e il logo di BitDefender sono marchi registrati della SOFTWIN. Microsoft, Windows, Excel, Word, il logo di Windows, Windows NT, Windows 2000 sono marchi registrati della Microsoft Corporations. Tutti gli altri marchi registrati sono di proprietà dei loro rispettivi proprietari.

Prefazione

Questa Guida dell'utente è destinata a tutti gli utenti che hanno scelto **BitDefender 9 Professional Plus** come la soluzione di sicurezza per i loro personal computer. L'informazione presentata in questo libro è indicata non solo per intenditori di computer, è accessibile per tutti quelli che siano capaci di lavorare con Windows.

Questo libro descriverà per te **BitDefender 9 Professional Plus**, l'azienda e il team che l'ha costruito, ti guiderà attraverso il processo di installazione e ti insegnerà come configurarlo. Troverai come usare **BitDefender 9 Professional Plus**, come aggiornarlo, provarlo e personalizzarlo. Imparerai a cogliere il meglio di BitDefender.

Ti auguriamo una lettura gradevole e utile.

1. Convenzioni usate in questo libro

1.1. Convenzioni tipografiche

Nel libro vengono usati diversi stili di testo per una leggibilità migliorata. Il loro aspetto e significato vengono presentati nella tabella sottostante.

Aspetto	Descrizione
`Esempio sintattico`	Gli esempi sintattici vengono scritte con caratteri `monospazio`.
http://www.bitdefender.com	I link URL puntano su alcuna ubicazione esterna, su server http o ftp.
<support@bitdefender.com>	Gli indirizzi e-mail vengono inseriti nel testo per informazione sui contatti.
«Prefazione» (p. xiii)	Questo è un link interno, verso qualche ubicazione nel documento.
`Nome file`	File e directory (cartelle) vengono scritte con fonti `monospazio`.
Opzione	Tutte le opzioni del prodotto vengono scritte usando caratteri in **grassetto**.

Aspetto	Descrizione
`Esempio listato codice`	Il listato codici è scritto con caratteri `monospazio`.

1.2. Avvertenze

Le avvertenze appaiono in note di testo, segnalate graficamente, offrendo alla tua attenzione informazione addizionale relativa al paragrafo corrente.

Nota

La nota è solo una piccola osservazione. Anche se la puoi omettere, la nota può provvedere informazione di valore come una caratteristica specifica o un link verso temi relazionati.

Importante

Questa richiede la tua attenzione e non è consigliato saltarla. Solitamente facilita informazione non critica ma significante.

Avvertimento

Questa è un'informazione critica che dovresti trattare con crescente cautela. Niente di male accadrà se segui le istruzioni. Dovresti leggerlo e capirlo, perché descrive qualcosa di estremamente rischioso.

2. Struttura del manuale

Il libro consta di sei parti, contenendo i principali temi: Installazione del prodotto, Descrizione e caratteristiche, Console di gestione, Pratiche consigliate, CD di soccorso BitDefender e Ottenere aiuto. Inoltre un glossario ed appendici vengono forniti per chiarificare diversi aspetti BitDefender, che potrebbero derivare in problemi tecnici.

Installazione del prodotto. Istruzioni passo a passo per installare BitDefender su una postazione di lavoro (workstation) IBM. Questa parte è una guida esaustiva sull'installazione di **BitDefender 9 Professional Plus**. Iniziando con i prerequisiti per una installazione con successo, sarai guidato attraverso tutto il processo di installazione. Finalmente, la procedura di disinstallazione è descritta per il caso in cui tu abbia bisogna di disinstallare BitDefender.

Descrizione e caratteristiche. Una breve introduzione a BitDefender. Esplica chi è BitDefender, chi è SOFTWIN e la Divisione Sicurezza Dati(Data Security Division). Ti viene presentato **BitDefender 9 Professional Plus**, le sue caratteristiche e i moduli del prodotto.

Console di gestione. Descrizione dell'amministrazione basilare ed il mantenimento di BitDefender. I capitoli ti spiegano in dettaglio tutte le opzioni del **BitDefender 9 Professional Plus**, come registrare il prodotto, come eseguire la scansione del computer, come configurare il modulo Antispam, come configurare il modulo Firewall e come eseguire gli aggiornamenti.

Pratiche consigliate. Segui le fasi qui descritte per assicurarti un computer libero da virus, spam e spyware.

CD di soccorso BitDefender. Descrizione del CD di soccorso BitDefender. Consente di comprendere e utilizzare le funzioni offerte da questo CD di avvio.

Ottenere aiuto. Dove cercare e dove chiedere aiuto se qualcosa non va tanto bene. Include anche una sezione FAQ (Domande frequenti).

Glossario. Il glossario cerca di spiegare alcuni termini tecnici e poco comuni che troverai tra le pagine di questo documento.

3. Richiesta di commenti

Ti invitiamo ad aiutarci a migliorare questo manuale. Abbiamo provato e verificato tutta l'informazione con la nostra massima capacità, ma potresti trovare che le caratteristiche siano cambiate (o persino che abbiamo commesso degli errori). Per favore scrivi per parlarci su qualsiasi errore trovi in questo libro o come credi che possa essere migliorato, per aiutarci a fornirti la migliore documentazione possibile.

Facci sapere inviando una e-mail a <documentation@bitdefender.com>.

Installazione del prodotto

1. Installazione di BitDefender 9 Professional Plus

La sezione **Installazione di BitDefender 9 Professional Plus** di questa guida dell'utente contiene i seguenti punti:

- Requisiti di sistema
- Fasi dell'installazione
- Upgrade
- Rimozione, riparazione e modifica delle caratteristiche di BitDefender

1.1. Requisiti del sistema

Per assicurare un funzionamento appropriato del prodotto, verificare, prima dell'installazione, che ci siano i seguenti requisiti del sistema:

- **Processore minimo** - Pentium MMX 200 MHz
- **Minimo spazio in hard disk disponibile** - 40MB
- **Memoria RAM minima** - 64MB (128MB consigliato)
- **Sistema operativo** - Windows 98/NT-SP6/ME/2000/XP; Internet Explorer 5.5 (+)

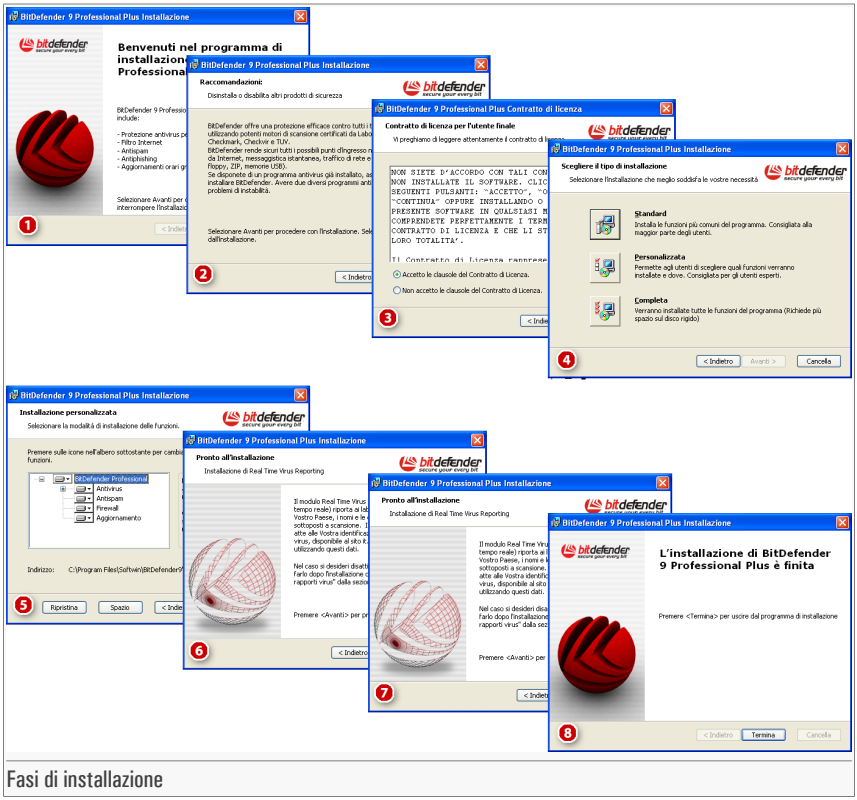
Avvertimento

BitDefender 9 Professional Plus non può essere istallato su Windows NT 4.0 Server, Windows 2000 Server o Windows 2003 Server. Per queste piattaforme consigliamo i prodotti aziendali per server di archiviazione, gateway e posta elettronica.

1.2. Fasi per l'installazione

Individuare il file di setup e fare click due volte con il mouse. Verrà lanciata la finestra di setup, che vi condurrà attraverso il processo di setup:

Fasi di installazione:



Fasi di installazione

1. Selezionare **Avanti** per continuare oppure **Cancella** se si desidera interrompere l'installazione.

2. Selezionare **Avanti** per continuare oppure **Indietro** per tornare al primo passaggio.

3. Vi preghiamo di leggere il Contratto di Licenza, di selezionare **Accetto le clausole del Contratto di Licenza** e di selezionare **Avanti**. Se non siete d'accordo con tali condizioni, selezionare **Cancella**. Abbandonerete in questo modo il processo di installazione e uscirete dal setup.

4. Si può scegliere il tipo di installazione che si desidera: standard, personalizzata oppure completa.

- **Standard** - Il programma verrà installato con le opzioni più comuni. Questa opzione è consigliata alla maggior parte degli utenti.
- **Personalizzata** - Si possono scegliere le componenti che si desiderano installare. Consigliato solo agli utenti più esperti.
- **Completa** - Per l'installazione completa del prodotto. Verranno installati tutti i moduli BitDefender.

  Se sceglierete l'installazione **Standard** o **Completa** dovrete saltare la fase 5.

5. Se avete selezionato l'installazione **Personalizzata** apparirà una nuova finestra che contiene tutte le componenti BitDefender disponibili, in modo da poter selezionare quelle che desiderate installare.

   Se si seleziona una qualsiasi componente, apparirà sulla destra una breve descrizione (incluso lo spazio minimo richiesto sul disco fisso). Se clicchi qualsiasi icona componente, una finestra appariràdove puoi scegliere di installare o no il modulo selezionato.

   Si può selezionare la cartella dove volete installare il prodotto. La cartella di default è `C:\Program Files\Softwin\BitDefender 9`.

   Se si desidera selezionare un'altra cartella, fare click su **Visualizza** e selezionare la cartella nella finestra che aprirà. Selezionare **Avanti**.

6. Selezionare **Avanti**.

7. Verranno selezionate quattro opzioni di default:

   - **Aggiornamento BitDefender** - per aggiornare BitDefender al termine dell'installazione. Per l'aggiornamento è necessario che il vostro sistema sia connesso ad Internet.
   - **Esamina la cartella di sistema Windows** - per eseguire la scansione della cartella del sistema Windows alla fine dell'installazione.
   - **Apri il file readme** - per aprire il file leggimi al termine dell'installazione.
   - **Metti un collegamento sul desktop** - per inserire un collegamento sul desktop al termine dell'installazione.

   Selezionare **Installa** per iniziare l'installazione del prodotto.

8. Selezionare **Termina** per completare l'installazione del prodotto. Se avete accettato le impostazioni di default per il percorso di installazione, verrà creata una nuova cartella chiamata `Softwin` in `Program Files` che contiene la sottocartella `BitDefender 9`.

Nota

Ti potrebbe essere chiesto di riavviare il tuo sistema in modo che il setup del wizard può completare il processo di installazione.

1.3. Upgrade

Per eseguire l'Upgrade ci sono due possibilità:

- **Installare senza rimuovere la versione precedente – solo da V8 a V9**

  Clicca 2 volte sul file di setup e segui il processo descritto nella sezione «*Fasi per l'installazione*» (p. 19).

  Importante

  Durante il processo di installazione apparirà un messaggio di errore causato da `servizio Filespy`. Clicca **OK** per continuare con l'istallazione.

- **Disinstallare la tua versione precedente ed installare la nuova – per tutte le versioni BitDefender**

  Prima di tutto devi rimuovere la tua versione precedente, riavviare il computer ed installare la nuova come descritto nella sezione «*Fasi per l'installazione*» (p. 19).

  Importante

  Se esegui l'Upgrade da V8 a V9 ti consigliamo di salvare le impostazioni di BitDefender, l'elenco Amici, l'elenco Spammers e le regole del Firewall. Una volta completato il processo di Upgrade potrai ripristinarli.

1.4. Rimozione, riparazione e modifica delle caratteristiche di BitDefender

Se si desidera modificare, riparare o disinstallare **BitDefender 9 Professional Plus** selezionare dal menu di avvio di Windows: **Start** -> **Programs** -> **BitDefender 9** -> **Modifica, Ripara o Disinstalla**.

Vi verrà richiesto di confermare la vostra scelta selezionando **Avanti**. Apparirà una nuova finestra dove potrete selezionare:

- **Modifica** - per selezionare le nuove componenti del programma da aggiungere o selezionare le componenti attualmente installate da rimuovere;
- **Ripara** - per installare nuovamente tutte le componenti del programma installate dal precedente setup;

Importante

Prima di riparare il prodotto, consigliamo di esportare gli elenchi Amici e Spammer e le regole del Firewall. E' possible anche salvare le Impostazioni del BitDefender e l'archivio Bayesiano. Dopo che il processo di riparazione è terminato, puoi salvarli.

- **Rimuovi** - per rimuovere tutte le componenti installate.

Per continuare il processo di installazione, selezionare una delle tre opzioni elencate. Consigliamo **Rimuovi** per un'installazione pulita. Al termine del processo di installazione, consigliamo di cancellare la cartella `Softwin` dalla cartella dei `Program Files`.

Descrizione e caratteristiche

2. Vista principale

BitDefender fornisce soluzioni di sicurezza per soddisfare la necessita di protezione dell'ambiente informatico di oggi, consegnando una gestione una effettiva gestione delle minacce ad oltre 41 milioni di utenti individuali ed aziendali in più di 100 paesi.

Disegnato per fornire protezione completa a sistemi e reti aziendali, il rango della soluzione BitDefender comprende, assieme alla protezione antivirus, antispam, firewall personale e soluzioni di gestione della sicurezza. BitDefender si specializza anche nel provvedere assistenza, disegnando e stabilendo i contenuti della politica di sicurezza per le reti aziendali.

BitDefender Professional è stato il terzo prodotto del suo tipo nel mondo a ricevere la certificazione ICSA per Windows XP ed il primo ad essere premiato per innovazione all'avanguardia dalla Commissione Europea e Accademie. L'antivirus BitDefender è certificato dai principali critici nel campo degli antivirus – ICSA LABS, CheckMark, CheckVir, TÜV e Virus Bulletin.

BitDefender ha la sua sede principale a Bucarest, Romania e ha succursali a Tettnang (Germania), Barcellona (Spagna) e Florida (USA). Sito Web: http://www.bitdefender.com

2.1. Perché BitDefender?

Provato. Produttore antivirus più reattivo. La veloce reattività di BitDefender nel caso di virus epidemici è stata confermata, a cominciare dalle ultime ondate di CodeRed, Nimda e Sircam, così come Badtrans.B o altri codici maligni, pericolosi e di rapida propagazione. BitDefender è stato il primo a fornire antidoti contro questi codici ed a renderli gratuitamente disponibili su Internet per tutti i colpiti. Adesso, con la continua espansione del virus Klez – nelle diverse versioni, la protezione antivirus è diventata un'altra volta una necessità critica per qualsiasi sistema.

Innovativo. Premiato per innovazione dalla Commissione Europea ed EuroCase. BitDefender è stato proclamato un vincitore del premio European IST, premiato dalla Commissione Europea e da rappresentanti di 18 Accademie in Europa. Adesso, nel suo ottavo anno, il Premio Europeo IST è una ricompensa per prodotti all'avanguardia che rappresentano il meglio della Innovazione europea e tecnologia dell'informazione.

Esaustivo. Copre ogni singolo punto della tua rete, fornendo una sicurezza completa. Le soluzioni di sicurezza di BitDefender per l'ambiente aziendale soddisfano le necessità di protezione del mondo commerciale attuale, permettendo la gestione di tutte le complesse

minacce che mettono in pericolo la rete, dalla piccola area locale fino a enormi WAN multi-server e multi-piattaforme.

La tua protezione finale. La frontiera finale per ogni possibile pericolo per il sistema del tuo computer. Se come il rilevamento dei virus basato nell'analisi dei codici non ha sempre offerto buoni risultati, BitDefender ha implementato la protezione basata sul comportamento, offrendo sicurezza contro malware (software maligno) appena nato.

Questi sono **i costi** che le organizzazioni vogliono evitare e per la cui prevenzione vengono disegnati i prodotti di sicurezza:

- Attacchi Worm
- Perdita di comunicazioni per via di mail infette
- Interruzione o guasto mail
- Pulizia e recupero dei sistemi
- Perdita di produttività degli utenti finali perché i sistemi non sono disponibili
- Pirateria informatica, ed accessi non autorizzati che causano danni

Mediante l'uso del set di sicurezza BitDefender, si possono conseguire simultaneamente **sviluppi e benefici**:

- Incrementare la disponibilità della rete, fermando la diffusione di attacchi di codici maligni (Nimda, cavalli di Troia, DdoS).
- Proteggere utenti remoti dagli attacchi.
- Ridurre i costi amministrativi ed incrementare la rapidità, con le capacità gestionali di BitDefender Enterprise.
- Fermare la diffusione di malware tramite e-mail, usando una protezione di posta BitDefender sul gateway dell'azienda. Blocco temporaneo o permanente di connessioni ad applicazioni non autorizzate, vulnerabili o care.

2.2. Data Security Division - Divisione Sicurezza Dati

Già dall'inizio, la Divisione Sicurezza Dati della SOFTWIN ebbe un approccio alla protezione dei dati in un modo specifico, con il primo aggiornamento intelligente, che non richiedeva l'intervento dell'utente, la prima gestione remota di antivirus tramite tecnologia WAP, o il primo Firewall Personale da integrare all'interno dei motori antivirus, per offrire una risposta completa alle complesse minacce attuali per la sicurezza.

Nata per fornire la sicurezza piena dei dati a tutti i livelli critici nell'ambiente commerciale di oggi, la Divisione Sicurezza Dati mira ad assicurare la protezione dei sistemi contro virus informatici, alla ricerca su gli antivirus, a sviluppare nuove tecnologie per il monitoraggio di

tutti i possibili modi d'infettare un sistema, ed ultimo ma non meno importante, a educare il pubblico IT&C sul pericolo dei virus informatici.

Le soluzioni di sicurezza di BitDefender soddisfano le necessità di protezione del mondo commerciale attuale, permettendo la gestione di tutte le complesse minacce che mettono in pericolo la rete, dalla piccola area locale fino a enormi WAN multi-server e multi-piattaforme.

2.3. SOFTWIN

SOFTWIN, con base a Bucarest, è il fornitore leader di servizi e soluzioni di software complesso in Romania.

SOFTWIN è focalizzata nella fornitura di servizi e soluzioni di software che permettono alle aziende in rapida crescita, di risolvere sfide commerciali critiche e di capitalizzare le nuove opportunità di business.

SOFTWIN permette alle aziende di focalizzarsi sulle loro attività essenziali ed espandersi verso nuovi mercati, mediante la delocalizzazione delle attività non essenziali.

SOFTWIN impiega più di 500 professionisti altamente qualificati e con esperienza nello sviluppo di soluzioni e servizi personalizzati.

Dalla sua fondazione in 1990, l'entrata media annuale di SOFTWIN si è incrementata in + 30%.

SOFTWIN ha 4 divisioni, le quali definiscono anche le linee principali di attività dell'azienda:

- CRM
- Business Information Solutions
- eContent Solutions
- Data Security Solutions

SOFTWIN fornisce servizi e soluzioni a clienti in tutto il mondo. Più del 90% del fatturato dell'azienda viene ottenuto dall'esportazioni agli USA ed all'Unione Europea.

Usando tecnologie all'avanguardia, SOFTWIN ha sviluppato con successo più di 500 progetti di sviluppo di software, più di 3500 progetti di strutturazione di contenuti per partner internazionali, raggiungendo più di 43 ml. di utenti di soluzioni di sicurezza dati in 80 paesi in tutto il mondo e più di 1,5 ml di chiamate da clienti per servizi CRM all'anno.

3. BitDefender 9 Professional Plus

BitDefender 9 Professional Plus integra i moduli antivirus, antispam e firewall in un unico pacchetto di sicurezza, appositamente creato per soddisfare le richieste degli utenti privati e aziendali di tutto il mondo.

3.1. Antivirus

La missione del modulo Antivirus è assicurare il rilevamento e la rimozione di tutti i virus. L'antivirus BitDefender utilizza un potente motore di scansione, certificato dai Laboratori ICSA, Virus Bulletin, Checkmark, CheckVir e TÜV.

B-HAVE. B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments) emula un computer virtuale dentro ad un altro nel quale diversi software vengono eseguiti per il controllo di potenziali comportamenti anomali. Questa tecnologia rappresenta un nuovo livello di sicurezza che mantiene il sistema operativo al sicuro da virus sconosciuti rilevando codici maligni, le cui firme non sono state ancora rilasciate.

Protezione antivirus ed antispyware permanente. I nuovi e migliorati motori di scansione BitDefender effettueranno la scansione e puliranno i file infetti nel momento dell'accesso, minimizzando la perdita di dati. I documenti infetti possono essere recuperati invece di essere cancellati.

Protezione applicazioni Peer-2-Peer. Filtri contro virus diffusi via messaggeria istantanea (instant messaging) e applicazioni con condivisione di file & software.

Scansione e pulizia di Spyware. BitDefender può fare la scansione di tutto il tuo sistema, o solo di una parte, per rilevare le minacce di spyware. La scansione utilizza un database di firme spyware costantemente aggiornato.

Protezione completa E-mail (posta elettronica). BitDefender esegue a livello protocollo POP3/SMTP il filtraggio dei messaggi in entrata ed uscita, indipendentemente dal Client utilizzato (MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Pegasus, The Bat, etc.) senza alcuna configurazione addizionale.

3.2. Antispam

Situazione abbastanza semplice: il modulo Antispam gestisce il problema dello spam, quindi tu non devi farlo.

Anti-Phishing. Tieniti pulito da e-mail maligni che cercano la truffa facendoti dare informazione sul tuo conto bancario con il nuovo rilevatore Phishing di BitDefender.

Filtro autodidatta Bayesiano. L'avanzzato filtro autodidatta bayesiano ti permette di classificare i messagi come "Spam" o "Ham" con un semplice click sulla barra degli strumenti del antispam BitDefender. Il filtro imparerà dopo qualche iterazione e così ti troverai a dover prendere sempre meno decisioni col passare del tempo. Ogni etichetta che tu assegni migliorerà l'accuratezza del filtro. Le inpostazioni della sensibilità del tuo filtro possono essere tanto alte o tante basse come tu preferisci.

Euristica, URL, Lista bianca / Lista nera, filtro Charset e immagini. Cinque tipi di filtro raffineranno ancora di più il tuo controllo sulla posta elettronica. Il filtro euristico verifica la posta con caratteristiche di spam. Il filtro Lista bianca/Lista nera rifiuterà le mail da indirizzi conosciuti come spammers e ammetterà quelle dei tuoi amici. Il filtro URL blocca le mail che contengono links maligni, mentre il filtro charset blocca le mail scritte con caratteri "strani". Il filtro immagini può decidere se immagini contenute nelle mail sono specifiche di spam.

Senza disturbi. Sarai avvertito soltanto all'arrivo di messaggi legittimi. Lo Spam verrà raccolto silenziosamente nella tu cartella "Junk" ("Cestino") per essere esaminata o cestinata a tuo discrezione.

Compatibilità ed integrazione in Outlook (tm). L'antispam BitDefender è compatibile con tutti i clients di posta. La barra di menù dell'antispam BitDefender in Microsoft Outlook ed Outlook Express permette agli utenti di filtrare mail e contatti senza uscire da Outlook.

3.3. Firewall

Il modulo Firewall protegge i tuoi dati e la tua privacy mediante il filtraggio del traffico in entrata ed uscita, controllando cookies, bloccando scripts maligni e programmi del tipo "XXX-dialer".

Controllo traffico Internet. Definisce esattamente quali connessioni in entrata o in uscita permettere o negare. Definisce regole riguardo a protocolli specifici, porte, applicazioni e/o indirizzi remoti.

Controllo intensificato delle applicazioni Internet. Allerta gli utenti su qualsiasi applicazione che cerca the accedere ad Internet. Sarai avvertito se le applicazioni che domandano accesso alla rete sono affidabili, in modo di poter prendere decisioni informate.

Controllo esaustivo della privacy. Il Firewall filtra i file in entrata ed uscita del tipo cookie, mantenendo la tua identità e preferenze confidenziali quando navighi in Internet.

Controllo dei Contenuti Attivi. Blocca in maniera proattiva qualsiasi applicazione potenzialmente pericolosa come: ActiveX, Java Applet o codici di tipo Java Script.

Controllo delle chiamate. Un anti-dialer configurabile impedisce alle applicazioni pericolose di farvi incorrere, vostro malgrado, in elevate bollette telefoniche.

3.4. Altre caratteristiche

Aggiornamenti orari. La tua copia di BitDefender sarà aggiornata 24 volte al giorno su internet, direttamente o tramite un server Proxy. Il prodotto è capace di autoripararsi, se fosse necessario, mediante il download dai server di BitDefender dei file danneggiati o persi. I proprietari delle licenze BitDefender beneficeranno gratuitamente di aggiornamenti di definizioni di virus e miglioramenti del prodotto.

Supporto 24/7. Offerto on-line da personale qualificato di supporto e da un database on-line con le risposte alle FAQs (domande frequenti).

Disco di soccorso (Rescue disk). BitDefender 9 Professional Plus è consegnato su un CD avviabile (basato su LinuxDefender) che può essere usato per disinfettare il sistema senza dover inizializzarlo.

4. Moduli BitDefender

BitDefender 9 Professional Plus contiene i moduli: **Generale**, **Antivirus**, **Antispam**, **Firewall** ed **Update**.

4.1. Modulo Generale

BitDefender arriva completamente configurato per la massima sicurezza.

Nel Modulo Generale viene presentata l'informazione essenziale sullo stato di tutti i moduli di BitDefender. Qui puoi registrare il tuo prodotto e puoi impostare il comportamento generale di BitDefender.

4.2. Modulo Antivirus

BitDefender vi protegge dai virus in ingresso nel vostro sistema esaminando i vostri file, i messaggi e-mail, i download e tutti gli altri contenuti nel momento in cui entrano nel vostro sistema. Dal modulo antivirus è possibile accedere a tutte le impostazioni e le funzionalità dell'antivirus Bitdefender.

La protezione dai virus è divisa in due categorie:

- Scansione all'accesso - impedisce l'ingresso di nuovi virus nel vostro sistema. Ciò viene anche chiamato virus shield – I file vengono esaminati nel momento in cui l'utente gli accede. BitDefender, ad esempio, esaminerà un documento word alla ricerca di virus nel momento in cui verrà aperto quel documento e un messaggio e-mail quando ne verrà ricevuto uno. BitDefender interviene con la scansione "nel momento in cui usate i vostri file" - all'accesso.

- Scansione a richiesta - rileva virus già esistenti nel vostro sistema. Si tratta della classica scansione dei virus avviata dall'utente – si sceglie quale drive, cartella o file BitDefender deve esaminare e BitDefender li esamina – a richiesta.

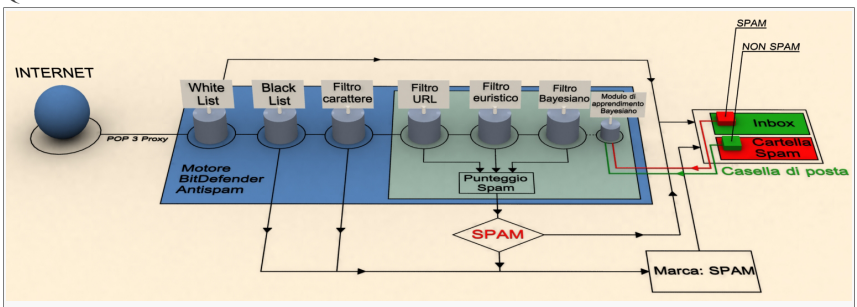
4.3. Modulo Antispam

Lo Spam rappresenta un problema in continua crescita, sia per i privati che per le aziende. Non è piacevole, non vorreste che i vostri figli lo vedessero, potrebbe penalizzarvi (per aver sprecato

troppo tempo o per aver ricevuto mail pornografiche in ufficio) e non potete impedire alla gente di inviarlo. La miglior cosa da fare, ovviamente, e di fermarne la ricezione. Sfortunatamente lo Spam si presenta sotto molte forme e dimensioni e ce n'è veramente tanto in giro.

4.3.1. Schema di lavoro

Questo schema mostra come funziona BitDefender.



Filtri Antispam

Il filtro Antispam dallo schema sopra (White list, Black list, filtro Carattere, Filtro Immagine, filtro URL, filtro Euristico e filtro Bayesiano) vengono utilizzati congiuntamente dal modulo Antispam di BitDefender per determinare se una determinata parte di mail vada inoltrata o no alla vostra **Inbox**.

Ogni e-mail che arriva da Internet viene prima verificata dal filtro White list/Black list. Se l'indirizzo del mittente viene trovato nella White list, l'e-mail viene spostata direttamente nella vostra **Inbox**.

Diversamente, il filtro Black list prenderà in carico l'e-mail per verificare se l'indirizzo del mittente è contenuto nel suo elenco. L'e-mail verrà marcata come SPAM e spostata nella cartella **Spam** (situata in Microsoft Outlook) qualora il confronto con la lista abbia dato esito positivo.

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

Qualora l'e-mail non fosse scritta con caratteri asiatici o cirillici, la stessa verrà passata al filtro Filtro Immagine. Il **Filtro Immagine** cntrollerà tutti I messaggi e-mail contenenti allegati con immagini con contenuti di spam.

Il filtro URL cercherà i link e li comparerà con i link del database di BitDefender. In caso di corrispondenza, il filtro aggiungerà un punteggio Spam alla e-mail.

Il filtro Euristico prenderà in carico l'e-mail ed eseguirà una serie di test su tutte le componenti del messaggio, alla ricerca di parole, frasi, collegamenti o caratteristiche dello Spam. Il risultato sarà quello di aggiungere un altro punteggio Spam alla e-mail.

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

Il modulo del filtro Bayesiano analizzerà ulteriormente il messaggio, basandosi su informazioni statistiche relative all'incidenza con cui determinate parole appaiono nei messaggi classificati come Spam in paragone a quelli dichiarati come non-Spam (da voi o dal filtro euristico). Verrà aggiunto un punteggio Spam alla e-mail.

Se la risultanza del punteggio (punteggio URL + punteggio Euristico + punteggio Bayesiano) eccede il punteggio Spam per un messaggio (impostato dall'utente nella sezione Antispam come livello di tolleranza), il messaggio viene considerato come SPAM.

Importante
Se utilizzate un client di e-mail diverso da Microsoft Outlook o Microsoft Outlook Express, dovrete create una regola per spostare i messaggi e-mail contrassegnati come Spam da BitDefender in una cartella personalizzata di quarantina. BitDefender allega il prefisso [SPAM] al soggetto dei messaggi considerati come Spam.

4.3.2. Filtri Antispam

Il Motore Antispam BitDefender incorpora sei diversi filtri che garantiscono l'assenza di Spam nella vostra : White list, Black list, filtro Carattere, Filtro Immagine, filtro URL, filtro Euristico e filtro Bayesiano.

Nota
E' possibile abilitare/disabilitare ognuno di questi filtri nel modulo **Antispam**, sezione Impostazioni.

White list / Black list

La maggior parte delle persone comunica regolarmente con un gruppo di persone o riceve persino messaggi da organizzazioni o società nello stesso dominio. Utilizzando l'**elenco amici o spammer**, potrete facilmente classificare da quali persone volete ricevere e-mail (amici)

indifferentemente dal contenuto del messaggio, o da quali persone non volete più ricevere nulla (spammer).

Nota

White list / Black list sono anche chiamati **Elenco Amici / Elenco Spammer**.

E' possibile gestire l'**elenco amici/spammer** dalla Console di Gestione BitDefender oppure dalla barra strumenti BitDefender.

Nota

Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all'**elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell'elenco; aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

Filtro Carattere

La maggior parte dei messaggi Spam sono scritti in caratteri cirillici e/o asiatici. Consigliamo di configurare questo filtro se si desiderano rifiutare tutti i messaggi scritti con questi caratteri.

Filtro Immagine

Da quando l'eliminazione della scansione con il Filtro Euristico è diventata una scoperta, oggigiorno le cartelle di posta in arrivo sono piene di molti messaggi contenenti solo un imagine con contenuti insoliti. Per contrastare questo crescente problema, BitDefender ha introdotto il **Filtro Immagine** che confronta le firme delle immagine delle e-mail con il database del BitDefender. In caso di riconoscimento, la e-mail verrà etichettata come Spam.

Filtro URL

La maggior parte dei messaggi Spam contengono link a vari siti web (che solitamente contengono ulteriore pubblicità e la possibilità di acquisto). BitDefender dispone di un database che contiene i link a questo tipo di siti.

Ogni link URL in un messaggio e-mail verrà esaminato sulla base del database URL. In caso di corrispondenza, il filtro aggiungerà un punteggio Spam alla e-mail.

Filtro Euristico

Il **Filtro Euristico** esegue una serie di test su tutte le componenti del messaggio (ovvero, non solo sull'intestazione ma anche sul corpo del messaggio sia in formato HTML che di testo), alla ricerca di parole, frasi, link o altri elementi caratteristici dello Spam.

Rileva inoltre i messaggi e-mail con SEXUALLY EXPLICIT nella riga del soggetto. Questi messaggi sono considerati SPAM.

Nota
A partire dal 19 Maggio 2004 lo Spam contenente materiale a sfondo sessuale deve includere l'avviso SEXUALLY EXPLICIT nell'oggetto, diversamente sarà passibile di multa per violazione della legge federale.

Filtro Bayesiano

Il modulo **Filtro Bayesiano** classifica i messaggi secondo informazioni statistiche relative alla frequenza di specifiche parole contenute nei messaggi classificati come Spam in confronto a quelli dichiarati come non-Spam (da voi o dal filtro euristico).

Ciò significa, ad esempio, che se una determinata parola di quattro lettere appare più spesso in uno Spam, è naturale desumere che esiste una notevole possibilità che il successivo messaggio in entrata contenente la stessa parola SIA Spam. Vengono prese in considerazione tutte le parole rilevanti all'interno di un messaggio. Sintetizzando le informazioni statistiche, viene valutata la probabilità globale che l'intero messaggio sia Spam.

Questo modulo presenta un'altra interessante caratteristica: lo si può "addestrare". Si adatta velocemente alla tipologia di messaggi ricevuti da un determinato utente e immagazzina informazioni su tutto. Per funzionare efficacemente, il filtro va addestrato, ovvero gli vanno presentati esempi di Spam e di messaggi leciti, proprio come si addestra un cane a rilevare determinati odori. A volte il filtro va anche corretto – stimolato a correggersi quando prende una decisione sbagliata.

Importante
Per correggere il modulo Bayesiano, utilizzare i pulsanti **E' Spam** e **Non è Spam** sulla «*Barra strumenti Antispam*» (p. 102).

Nota
Ogni volta che esegui un aggiornamento:

- nuove impronte d'immagini verranno aggiunte al **Filtro Immagine**;
- nuovi links verranno aggiunti al **Filtro URL**;
- nuove regole verranno aggiunte al **Filtro euristico**;

Questo aiuterà ad incrementare l'effettività del tuo motore Antispam.

Importante
Per proteggerti contro gli spammers, BitDefender può effettuareaggiornamenti automatici. Mantenere l'opzione di **Aggiornamento Automatico** attivata.

4.4. Modulo Firewall

Il Firewall protegge il vostro computer da tentativi di connessione non autorizzati in ingresso ed in uscita. E' come una guardia al vostro cancello – terrà sotto controllo la vostra connessione internet e terrà traccia di ciò a cui è consentito l'accesso a Internet e di ciò a cui è negato.

Un firewall è essenziale se si dispone di una banda larga o di una connessione DSL. E' efficace nel bloccare i cavalli di Troia (Trojan) e altri strumenti installati dagli hacker; strumenti che tentano di compromettere la vostra riservatezza e di inviare le vostre informazioni personali, come ad esempio i numeri della carta di credito, dal vostro computer agli hacker.

4.5. Modulo Update

Tutti giorni vengono trovati ed identificati nuovi virus. Per ciò è molto importante mantenere aggiornato il BitDefender con le ultime impronte dei virus. Di default, BitDefender controlla automaticamente ogni ora per possibili aggiornamenti.

Gli Aggiornamenti arrivano nei seguenti modi:

- **Aggiornamenti per motori Antivirus** - non appena compaiono nuove minacce, i file contenenti le impronte dei virus devono essere aggiornati per garantire una protezione aggiornata permanente contro queste nuove minacce. Questo tipo di aggiornamento è anche conosciuto come **Virus Definitions Update**.

- **Aggiornamenti per motori Antispam** - verranno aggiunte nuove regole ai filtri euristico ed URL, e nuove immagini al filtro immagini. Ciò contribuirà ad aumentare l'efficacia del vostro motore Antispam. Questo tipo di aggiornamento è anche conosciuto come **Antispam Update**.

- **Aggiornamento per I motori antispyware** - nuove firme antispyware saranno aggiunte al database. Questo tipo di aggiornamento è anche conosciuto come **Antispyware Update**.

- **Aggiornamenti del Prodotto** - quando viene rilasciata la nuova versione di un prodotto, vengono introdotte nuove funzionalità e tecniche di scansione al fine di migliorare l'efficienza del prodotto. Questo tipo di aggiornamento è anche conosciuto come **Product Update**.

Inoltre, dal punto di vista dell'intervento da parte dell'utente, possiamo prendere in considerazione:

- Aggiornamento automatico - l'antivirus contatta automaticamente il server BitDefender per verificare se è stato rilasciato un aggiornamento. Se è così, BitDefender sarà aggiornato

automaticamente. L'aggiornamento automatico può essere eseguito in qualsiasi momento, cliccando su **Aggiorna adesso** nel Modulo di Update.

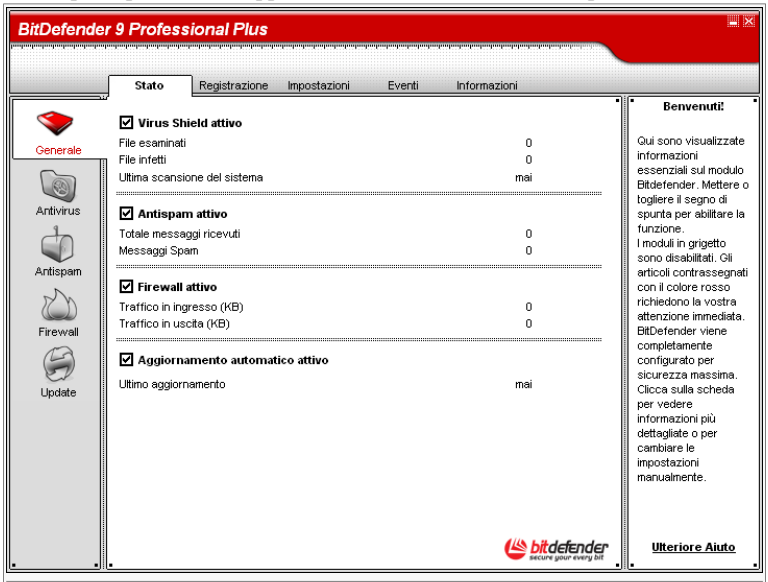
- Aggiornamento manuale - devi scaricare ed installare le ultime definizioni di virus manualmente.

Console di gestione

5. Vista principale

BitDefender 9 Professional Plus è stato progettato con una Console di Gestione centralizzata che consente la configurazione delle opzioni di protezione di tutti i moduli BitDefender. In altre parole, è sufficiente aprire la console di gestione per avere accesso a tutti i moduli: **Antivirus**, **Antispam**, **Firewall** ed **Update**.

Per accedere alla sezione comandi, usare il menu di inizio di Windows, seguendo questi passaggi: **Inizio del percorso** -> **Programmi** -> **BitDefender 9** -> **BitDefender 9 Professional Plus** o più rapidamente doppio click sull'**icona BitDefender** per il vassoio di sistema.



Console di Gestione

Sulla parte sinistra della console di gestione è possibile selezionare uno specifico modulo:

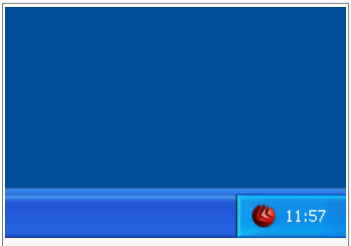
- General - in questa sezione è possibile vedere un sommario di tutte le principali impostazioni di BitDefender, dettagli di prodotto e le informazioni sui contatti. Qui è anche possibile registrare il prodotto.

- Antivirus - in questa sezione puoi configurare il modulo **Antivirus**.
- Antispam - in questa sezione puoi configurare il modulo **Antispam**.
- Firewall - in questa sezione puoi configurare il modulo **Firewall**.
- Update - in questa sezione puoi configurare il modulo **Update**.

Nella parte destra della sezione comandi potete vedere le informazioni per quanto riguarda la sezione in cui siete. L'opzione **Ulteriore Aiuto**, posizionata in basso a destra, apre il file **Aiuto**.

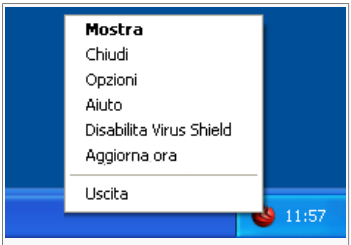
5.1. Barra di sistema

Quando la console è minimizzata, appare un'icona nella barra di sistema:



Barra di sistema

Se si esegue un doppio click su questa icona, si aprirà la console di gestione.



Menù contestuale

Inoltre, premendo sull'icona con il tasto destro, apparirà un menù a tendina contenente le seguenti opzioni.

- **Mostra** - apre la console di gestione.
- **Chiudi** - minimizza la console di gestione nella barra di sistema.
- **Opzioni** - aprire la sezione Impostazioni della Console di gestione.
- **Aiuto** - apre la documentazione elettronica.
- **Abilita / Disabilita Virus Shield** - abilita/disabilita la protezione on-access.
- **Aggiorna ora** - provvede ad un aggiornamento immediate.

- **Uscita -** chiude l'applicazione. Selezionando questa opzione, l'icona scomparirà dal carrello di sistema e per accedere alla console di gestione sarà necessario lanciarla nuovamente dal menu di Avvio.

Nota

- L'icona diventerà near, se disability uno o più dei moduli BitDefender. In questo modo saprai se qualche modulo è disabilitato senza aprire la console di gestione.
- L'icona lampeggierà quando ci sarà un aggiornamento disponibile.

5.2. Barra delle attività di scansione

La **Barra delle attività di scansione** è una visualizzazione grafica dell'attività di scansione sul vostro sistema.

Barra delle attività

Le barre verdi (**Zona File**) mostrano il numero di file esaminati al secondo, in una scala da 0 a 50.

Le barre rosse visualizzate nella **Zona Rete** mostrano il numero di Kbyte trasferiti (inviati e ricevuti da Internet) al secondo, in una scala da 0 a 100.

Nota

La **barra dell'attività di scansione** ti informerà quando il Virus Shield o il Firewall è inabilitato con una croce rossa nella zona corrispondente (**Zona file** o **Zona rete**). In questo modo saprete se siete protetti senza aprire la sezione comandi.

Quando non si vuole più vedere la visualizzazione grafica, si deve semplicemente premere sulla stessa con il tasto destro e selezionare **Nascondi**.

Nota

Per nascondere completamente questa finestra, deselezionare l'opzione **Abilita barra delle attività** (dal modulo **Generale**, sezione Impostazioni).

6. Modulo Generale

La sezione **Generale** di questa guida dell'utente consta dei seguenti punti:

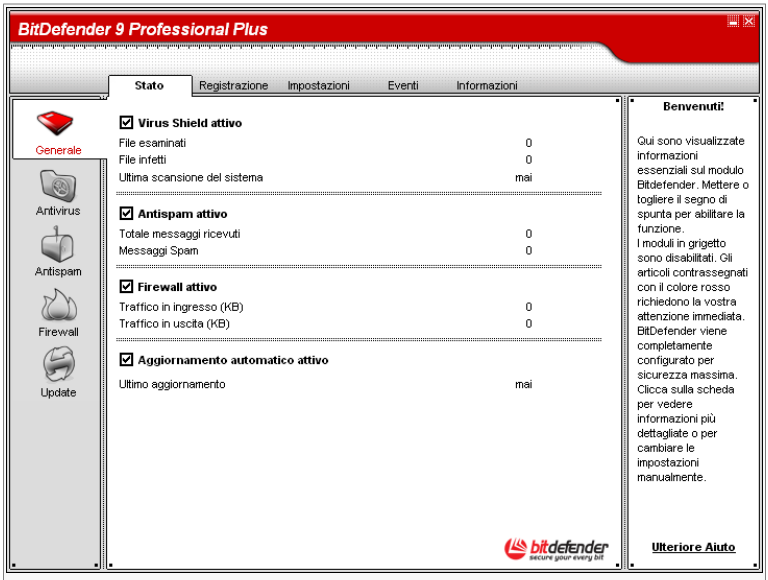
- Informazione generale
- Registrazione del prodotto
- Impostazioni della Console di Gestione
- Eventi
- Info

Nota

Per altri dettagli riguardo al modulo **Generale**, vedere la descrizione del «*Modulo Generale*» (p. 35).

6.1. Informazione generale

Per accedere a questa sezione clicca sulla linguetta **Stato** del modulo **Generale**.



Informazione generale

Da qui è possibile vedere le informazioni relative allo stato del prodotto.

Inserendo o togliendo la spunta nella casella di verifica, si possono abilitare o disabilitare le caratteristiche principali di BitDefender.

Avvertimento
Gli argomenti marcati in rosso richiedono la vostra immediata attenzione.

6.1.1. Virus Shield

Fornisce in tempo reale una protezione continua contro virus e altri minacce. È visualizzato il numero dei file scansionati, dei file infettati e la data dell'ultima scansione di sistema.

Nota
Per impedire ai virus di infettare il vostro computer, tenere abilitato il **Virus Shield**.

Avvertimento

Consigliamo vivamente di eseguire una scansione completa del sistema almeno una volta alla settimana. Per eseguire una scansione completa del sistema, accedere al **modulo Antivirus**, sezione Virus Scan, selezionare **Dischi Locali** e cliccare su **Esamina**.

6.1.2. Antispam

Lo Spam rappresenta un problema in continua crescita, sia per i privati che per le aziende. Si presenta sotto varie forme e dimensioni e ce n'è molto in giro. Il modula **Antispam** agisce con tutti i client di posta e può essere configurato dalla Console di Gestione (sezione **Antispam**).

Inoltre si integra direttamente con Microsoft Outlook e Microsoft Outlook Express consentendo una agevole interazione con i filtri Antispam attraverso un'interfaccia intuitiva di semplice utilizzo.

Nota

Per impedire allo Spam di entrare nella vostra Inbox, mantenere abilitato il **filtro Antispam**. Si veda come lavora BitDefender Antispam.

6.1.3. Firewall

Il Firewall personale vi protegge dagli attacchi Internet. Le regole del firewall impediscono agli hacker e ai software pericolosi di compromettere il vostro computer o i vostri dati personali. Le cifre visualizzate rappresentano il traffico Internet durante questa sessione.

Nota

Per essere protetti contro gli attacchi via Internet, mantenere il **Firewall** abilitato.

6.1.4. Aggiornamento Automatico

Ogni giorno vengono trovati ed identificati nuovi virus. Questo è il motivo per cui è molto importante mantenere BitDefender aggiornato con le nuove impronte dei virus. Visualizza la data dell'ultimo aggiornamento.

Nota

BitDefender può eseguire aggiornamenti automatici per proteggere i vostri dati critici. Mantenere abilitata l'opzione **Aggiornamento Automatico**.

6.2. Registrazione del prodotto

Per accedere a questa sezione clicca sulla linguetta **Registrazione** del modulo **Generale**.

Registrazione del prodotto

Questa sezione contiene le informazioni sullo stato della vostra licenza BitDefender. Qui si può registrare il prodotto e vederne la data di scadenza.

Il prodotto è spedito con una chiave di registrazione di prova della durata di 30 giorni. Al termine del periodo di prova, se si desidera acquistare il prodotto, ci si deve procurare una nuova chiave di licenza. Selezionare **Acquista ora!** per ottenere una nuova **Chiave di Licenza** dal negozio BitDefender online.

Clicca su **Registrazione online** per attivare il tuo prodotto BitDefender e poter così beneficiare del supporto tecnico ed altri servizi.

Per modificare la chiave di licenza preimpostata, selezionare **Inserire nuova chiave...**. Si aprirà la seguente finestra:

Registrazione

Digitare la chiave di licenza nel campo **Codice**. Selezionare **Registra** per concludere il processo di registrazione.

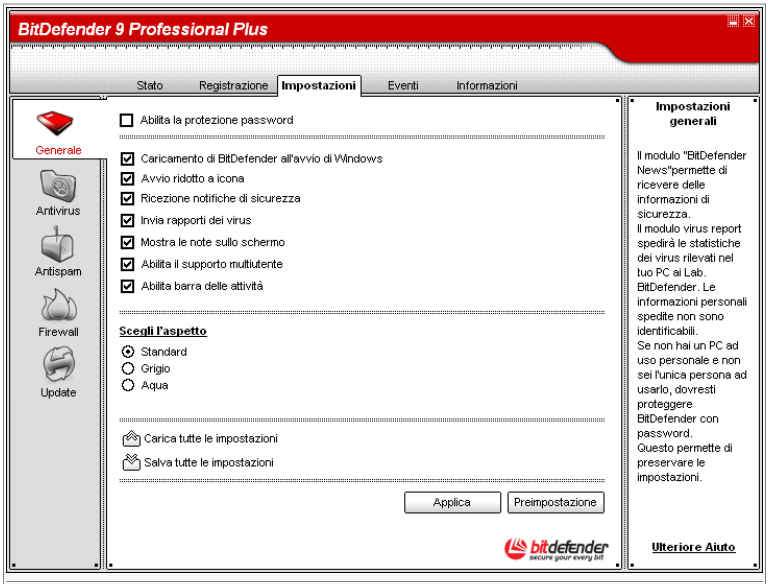
Se la chiave di licenza viene digitata in maniera errata, verrà chiesto di digitarla nuovamente.

Dopo aver digitato una chiave di licenza valida, apparirà un messaggio di conferma.

Nella sezione **Registrazione** si può ora vedere la data di scadenza della nuova chiave di licenza.

6.3. Impostazioni della Console di Gestione

Per accedere a questa sezione clicca sulla linguetta **Impostazioni** del modulo **Generale**.



Impostazioni della Console di Gestione

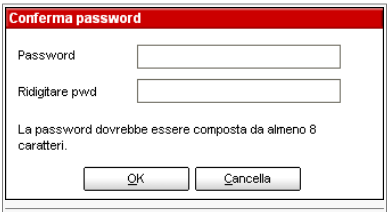
Da qui è possibile impostare il comportamento generale di BitDefender. BitDefender è caricato automaticamente all'avvio di Windows e successivamente minimizzato nella barra strumenti.

Sono disponibili le seguenti opzioni:

- **Abilita la protezione password** - consente l'impostazione di una password per proteggere la configurazione di BitDefender;

  Nota
  Se non siete l'unica persona ad utilizzare un determinato computer, consigliamo di proteggere le vostre Impostazioni BitDefender con una password.

  Se selezioni questa opzione, la Prossima finestra apparirà:



Conferma password

Inserire la password nel campo **Password**, inserirla nuovamente nel campo **Ridigitare pwd** e selezionare **OK**.

Da ora in poi se si desidera cambiare le opzioni di configurazione di BitDefender, vi verrà richiesto di inserire la password.

Importante
Se si dimentica la password, si deve riparare il prodotto per modificare la configurazione BitDefender.

- **Caricamento di BitDefender all'avvio di Windows** - esecuzione automatica di BitDefender all'avvio del sistema.

Nota
Si raccomanda di lasciare questa opzione selezionata.

- **Avvio ridotto a icona** - minimizza la Console di Gestione dopo il caricamento all'avvio del sistema. Nella barra di sistema apparirà soltanto l'icona BitDefender.
- **Ricezione notifiche di sicurezza** - riceve di volta in volta, dai server BitDefender, segnalazioni di sicurezza relative alla diffusione di nuovi virus.
- **Invia rapporti dei virus** - invia ai Laboratori BitDefender i rapporti relativi ai virus identificati sul vostro computer. Questo ci aiuta a tracciare la diffusione dei virus.

  I rapporti non contengono dati confidenziali, come il vostro nome, l'indirizzo IP o altri, e non verranno utilizzati per scopi commerciali. Le informazioni fornite conterranno solo il nome del virus e verranno utilizzate unicamente per creare rapporti statistici.
- **Mostra le note sullo schermo** - mostra finestre a tendina relative allo stato del prodotto.
- **Abilita il supporto multiutente** - permette ad altri utenti che possono usare questo computer di avere le loro impostazioni per il BitDefender.

Nota

Questa opzione può essere abilitata o disattivata dagli utenti con diritti di Amministratre sulla macchina in locale.

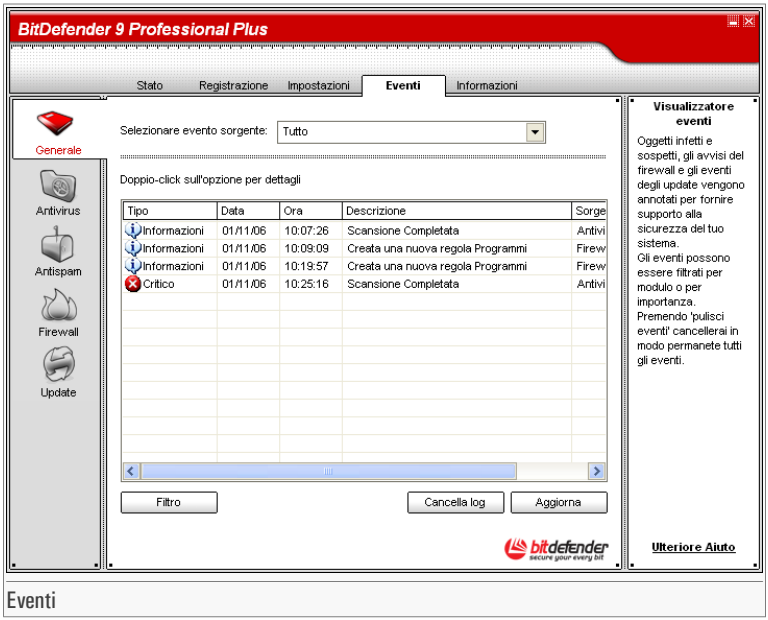
- **Abilitazione barra di attività -** abilita/disabilita la « *Barra delle attività di scansione* » (p. 47).
- **Scegli l'aspetto -** consente di selezionare il colore della Console di Gestione. Lo sfondo rappresenta l'immagine di secondo piano sull'interfaccia. Per selezionare uno sfondo diverso, fare click sul colore corrispondente.

Usare il pulsante **Salva tutte le impostazioni** / **Carica tutte le impostazioni** per salvare/ignorare le impostazioni che hai fatto per il BitDefender in un posto desiderato. In questo modo puoi utilizzare le stesse impostazioni dopo aver reinstallato o riparato il tuo prodotto BitDefender.

Selezionare **Applica** per salvare le modifiche oppure selezionare **Preimpostazione** per tornare alle impostazioni di default.

6.4. Eventi

Per accedere a questa sezione clicca sulla linguetta **Eventi** del modulo **Generale**.



Eventi

In questa sezione vengono presentati tutti gli eventi generati da BitDefender.

Ci sono tre tipi di eventi: **Informazioni**, **Attenzione** e **Critico**.

Esempi di eventi:

- **Informazioni** - quando è stata eseguita la scansione di una mail;
- **Attenzione** - quando è stato rilevato un file sospetto;
- **Critico** - quando è stato rilevato un file infetto.

Per ogni evento vengono fornite le seguenti informazioni: la data e l'ora in cui è avvenuto l'evento, una piccola descrizione, e la sua fonte (**Antivirus**, **Firewall** o **Aggiornamento**). Clicca due volte su un evento per visualizzare le proprietà.

Puoi filtrare questi eventi in 2 modi (per tipo o per fonte):

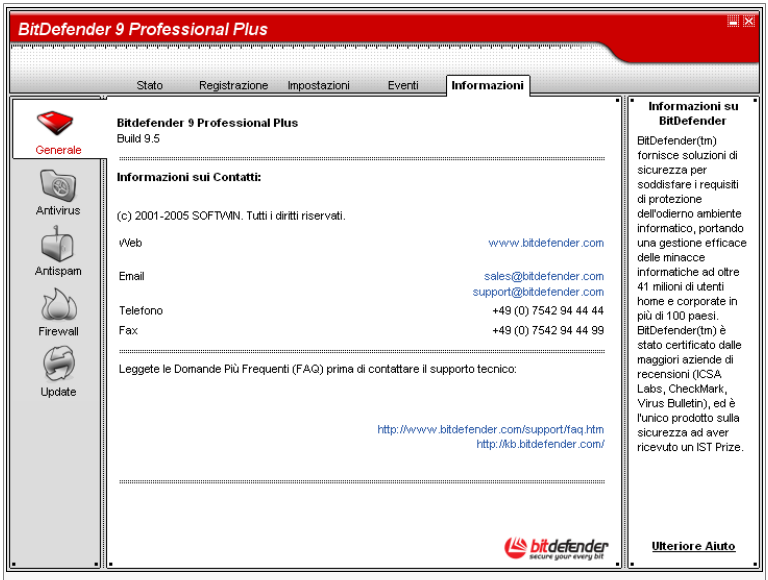
- Clicca su **Filtro** per selezionare quali tipi di evento visualizzare;
- Seleziona la fonte dell'evento dal menu a tendina;

Se la Console di Gestione è aperto nella sezione **Eventi** ed accade un evento nello stesso tempo, dovrai cliccare su **Aggiorna** per poter vedere quel evento.

Per cancellare tutti gli eventi dell'elenco, clicca su **Cancella log**.

6.5. Info

Per accedere a questa sezione clicca sulla linguetta **Info** del modulo **Generale**.



Informazione generale

In questa sezione troverete le informazioni di contatto e i dettagli del prodotto.

BitDefenderTM offre soluzioni di sicurezza tese a soddisfare le necessità di protezione negli odierni ambienti elaborativi, fornendo un'efficace gestione delle minacce per oltre 41 milioni di utenti privati e aziendali in più di 100 nazioni.

BitDefenderTM è certificato dai maggiori revisori indipendenti - **ICSA Labs**, **CheckMark** e **Virus Bulletin** ed è l'unico prodotto di sicurezza ad avere ottenuto un **Premio IST**.

7. Modulo Antivirus

La sezione **Antivirus** di questa guida dell'utente consta dei seguenti punti:

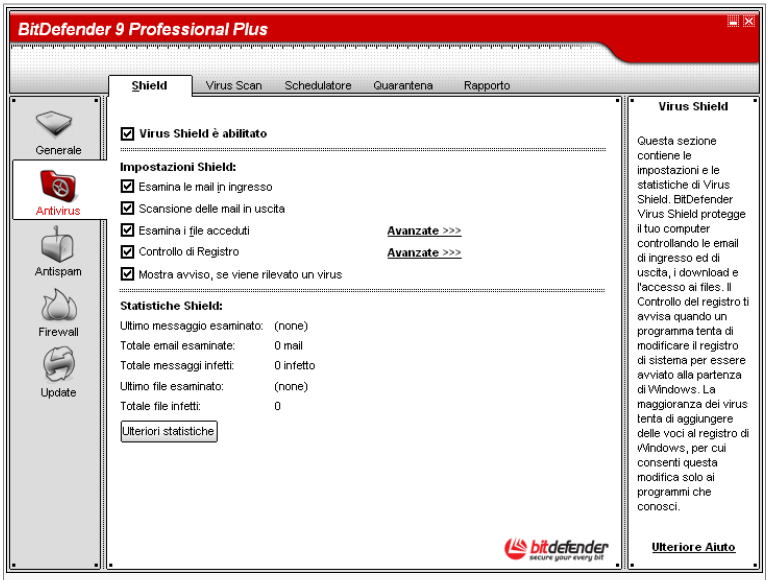
- Scansione all'accesso
- Scansione a richiesta
- Scansione programmata
- Quarantena
- Rapporto

Nota

Per altri dettagli riguardo al modulo **Antivirus**, vedere la descrizione del «*Modulo Antivirus*» (p. 35).

7.1. Scansione all'accesso

Per accedere a questa sezione clicca sulla linguetta **Shield** del modulo **Antivirus**.



Virus Shield

In questa sezione è possible configurare il **Virus Shield** e vedere le informazioni relative alla sua attività. **Virus Shield** protegge il vostro computer esaminando i messaggi e-mail, i download e tutti i file a cui si accede.

Nota
Per impedire ai virus di infettare il vostro computer, mantenere abilitato **Virus Shield**.

Nella parte inferiore della sezione è possibile osservare le statistiche **Virus Shield** relative ai file e ai messaggi e-mail. Selezionare **Ulteriori Statistiche** se si desidera visualizzare una finestra maggiormente esplicativa relativa a queste statistiche.

7.1.1. Controllo dei Registri

Una componente molto importante del sistema operativo di Windows si chiama **Registro**. E' dove Windows tiene le informazioni relative alle proprio configurazioni, ai programmi installati, all'utente e così via.

Il **Registro** è inoltre utilizzato per definire quali Programmi devono essere eseguiti automaticamente all'avvio di Windows. Spesso i virus lo utilizzano per essere eseguiti automaticamente quando l'utente riavvia il proprio computer.

Il **Controllo dei Registri** sorveglia il Registro di Windows – azione utile per rilevare i Trojan (Cavalli di Troia). Vi avviserà ogni volta che un programma tenterà di modificare una entrata del registro per poter essere eseguito all'avvio di Windows.

Allarme sul Registro

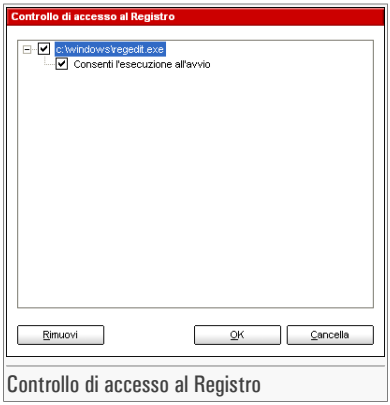
E' possibile vietare questa modifica selezionando **No** oppure consentirla selezionando **Sì**.

Se si desidera che BitDefender memorizzi questa risposta, si dovrà spuntare: **Memorizza questa risposta**.

Nota

Le vostre risposte costituiscono la base dell'elenco delle regole.

Se si desidera visualizzare l'elenco degli ingressi del registro, selezionare **Avanzato >>>** in corrispondenza a **Controllo di Registro**.



Controllo di accesso al Registro

Verrà creato un piccolo menu espandibile per ogni applicazione; il menu contiene tutte le modifiche al registro.

Per cancellare una entrata di registro, è sufficiente selezionarla e fare click su **Cancella**. Per disattivare temporaneamente una entrata di registro senza però cancellarlo, rimuovere la spunta dalla casella corrispondente.

Nota

BitDefender vi avviserà, di norma, quando installerete nuovi programmi che necessitano di esecuzione immediata dopo il successivo avvio del vostro computer. Nella maggior parte dei casi questi programmi sono leciti e ci si può fidare.

7.1.2. Impostazioni più importanti

Per selezionare un'opzione, cliccare con il mouse la casella corrispondente.

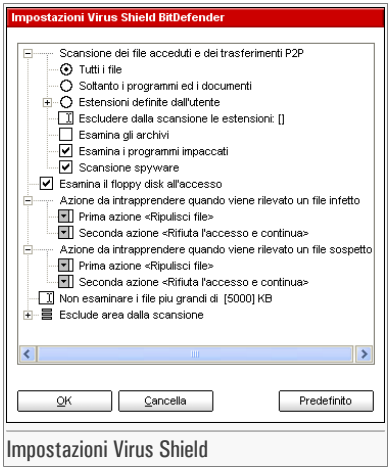
- **Esamina le mail in ingresso** - tutti i messaggi e-mail in entrata verranno esaminati.
- **Scansione delle mail in uscita** - esegue la scansione di tutti I messaggi in uscita.
- **Esamina i file acceduti** - tutti i file acceduti verranno esaminati.
- **Mostra avviso, se viene rilevato un virus** - verrà visualizzata una finestra di avviso quando verrà rilevato un virus in un file o in un messaggio e-mail.

  In presenza di un virus, si aprirà una finestra contenente il nome del virus, e che permetterà di selezionare un azione sul file infetto adottato dal BitDefender, e un link al sito BitDefender dove è possibile trovare ulteriori informazioni al riguardo. Per una e-mail infetta, la finestra di allerta contiene anche informazioni sul mittente e il destinatario.

  In caso che un file sospetto è scansionati, puoi lanciare un wizard dalla finestra di allerta che ti aiuterà a spedire il file ai Laboratori BitDefender per una ulteriore analisi. È possibile scrivere dalla tua e-mail per ricevere informazioni su questo report.

7.1.3. Altre opzioni

Gli utenti avanzati potrebbero approfittare dei vantaggi offerti dallo scan-setting che BitDefender offre. Il dispositivo di scansione può essere selezionato per le saltare le estensioni di file, directories o archiviche tu sai essere innocui. Clicca su **Avanzato** >>> corrispondente a **Scansione File Accessibili** per esplorarli.



Impostazioni Virus Shield

Selezionare la casella con "+" per aprire un'opzione oppure la casella con "-" per chiudere un'opzione.

Si può vedere come alcune opzioni di scansione, nonostante appaia il segno "+", non possano essere aperte. Il motivo è che queste opzioni non sono ancora state selezionate. Si può notare che sarà possibile aprirle una volta selezionate.

- **Scansione dei file acceduti e dei transferimenti P2P** - esamina i file acceduti e le comunicazioni tramite applicazioni Software di Messaggistica Istantanea (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Successivamente selezionare il tipo di file che si desidera esaminare.

  Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Tutti i file	Verranno esaminati tutti i file acceduti, indipendentemente dalla loro tipologia.

Opzione	Descrizione
Soltanto i programmi ed i documenti	Verranno esaminati solo i file di programma. Questo significa solo i file con le seguenti estensioni: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` e `.nws`.
Estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".
Escludere dalla scansione le stensioni	I file con le estensioni specificate dall'utente NON verranno esaminati. Le varie estensioni devono essere separate da ";".
Esamina gli archivi	Verranno esaminati anche gli archivi acceduti. Con questa opzione abilitata, il computer sarà più lento.
Esamina i programmi impaccati	Verranno esaminati tutti i file impaccati.
Scansione spyware	Esegue la scansione di applicazioni spyware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione fosse attiva.

- **Esamina il floppy disk all'accesso** - esamina il drive floppy, quando viene acceduto.
- **Azione in presenza di virus** - selezionare dall'elenco la prima azione da intraprendere sui file infetti. BitDefender consente la selezione di due azioni nel caso venga rilevato un file infetto.

  E' possibile selezionare una delle seguenti azioni:

Azione	Descrizione
Rifiuta l'accesso e continua	Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.
Ripulisci file	Per disinfettare il file infetto.

Azione	Descrizione
Cancella file	Cancella immediatamente i file infetti, senza alcun avviso.
Muovi file nella Quarantena	I file infetti vengono spostati nella quarantena.

- **Seconda azione da intraprendere nel caso la prima fallisse** - selezionare dall'elenco la seconda azione da intraprendere sui file infetti.

  Sono disponibili le seguenti opzioni:

Azione	Descrizione
Rifiuta l'accesso e continua	Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.
Cancella file	Cancella immediatamente i file infetti, senza alcun avviso.
Muovi file nella Quarantena	I file infetti vengono spostati nella quarantena.

  Le stesse azioni previste per file infetti sono disponibli per file sospetti.

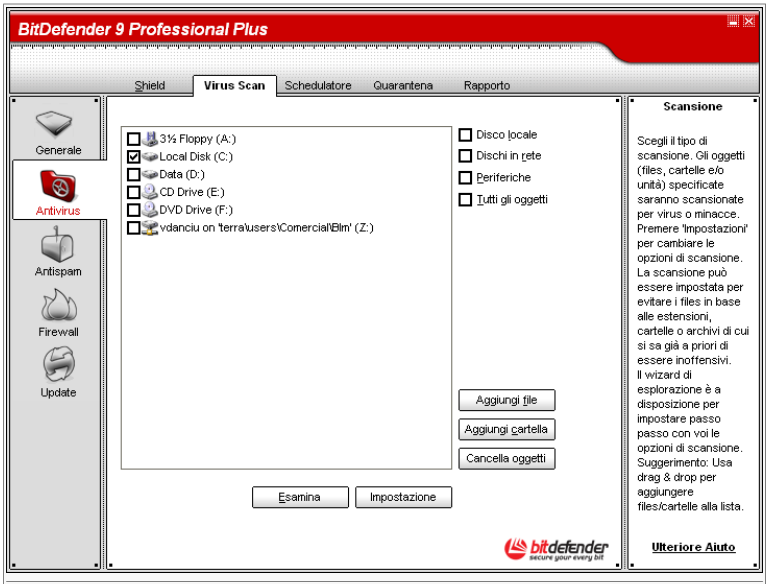
- **Non esaminare i file più grandi di** - digitare la dimensione massima dei file da esaminare. Se la dimensione è pari a 0 Kb, tutti i file verranno esaminati.

- **Esclude area dalla scansione** - selezionare "+" in corrispondenza a quest'opzione per specificare una cartella che verrà esclusa dalla scansione. La conseguenza sarà che l'opzione si espanderà e apparirà una nuova opzione, ovvero `Nuovo ogetto`. Selezionare la casella corrispondente al nuovo elemento e, dalla finestra di esplorazione, selezionare la cartella che si desidera escludere dalla scansione.

Selezionare **OK** per salvare le modifiche oppure selezionare **Preimpostazione** per tornare alle impostazioni di default.

7.2. Scansione a richiesta

Per accedere a questa sezione clicca sulla linguetta **Virus Scan** del modulo **Antivirus**.



Virus Scan

In questa sezione è possible configurare il BiDefender per scansionare il tuo computer.

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

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

BitDefender consente quattro tipi di scansione su richiesta:

- Scansione immediata - andranno seguiti alcuni passaggi per esaminare il vostro computer alla ricerca di virus;
- Scansione contestuale - selezionare un file o una cartella con il tasto destro e selezionare BitDefender Antivirus v9;
- Scansione Seleziona & Trascina - seleziona & trascina un file o una cartella sopra la Barra delle Attività di Scansione;

- Scansione programmata - è possibile programmare BitDefender per eseguire una scansione periodica del vostro sistema alla ricerca di virus.

7.2.1. Scansione immediata

Per eseguire una scansione del vostro computer alla ricerca di virus, vi invitiamo a seguire questi passaggi:

Passaggio 1/5 - Chiudere tutti i programmi aperti

Per consentire a BitDefender di eseguire una scansione completa, dovrete chiudere tutti i programmi aperti. E' soprattutto importante chiudere il vostro client di posta (come Outlook, Outlook Express oppure Eudora).

Passaggio 2/5 - Assicuratevi che BitDefender conosca i virus più recenti

Prima di far eseguire a BitDefender la scansione del vostro computer, dovreste assicurarvi che BitDefender sia aggiornato in quanto a impronte dei virus, poiché ogni giorno vengono scoperti ed identificati nuovi virus. E' possibile verificare la data dell'ultimo aggiornamento nella parte inferiore del modulo Update.

Passaggio 3/5 - Scegliere gli obiettivi da esaminare

Entrare nel modulo **Antivirus** all'interno della console di gestione e selezionare la tabella Esamina. La sezione contiene per default un'immagine della struttura di partizione del sistema. Potrete notare sul lato alcuni pulsanti e opzioni di scansione.

La sezione contiene i seguenti pulsanti:

- **Aggiungi file** - apre una finestra di visualizzazione da dove è possibile selezionare i file che si desidera esaminare.
- **Aggiungi cartella** - come sopra, ma seleziona quali cartelle si desidera far esaminare da BitDefender anziché specifici file.

Nota
Utilizzare seleziona & trascina per aggiungere file/cartelle all'elenco.

- **Cancella oggetti** - rimuove tutti i file / cartelle precedentemente selezionati dall'elenco degli oggetti da esaminare.

Nota
Possono essere cancellati solo i file / cartelle aggiunti successivamente e non quelli "visti" automaticamente da BitDefender.

- **Configura** - apre una finestra dove è possibile specificare quali file esaminare, l'azione da intraprendere sui file infetti, la creazione di messaggi di avviso, il salvataggio dei risultati di scansione nei file di rapporto.
- **Esamina** - lancia la scansione del sistema prendendo in considerazione le opzioni di scansione selezionate.

Oltre ai pulsanti sopra esposti, ci sono alter opzioni che permettono la selezione veloce dell'allocazione di scansione.

- **Dischi locali** - per esaminare i drive locali.
- **Dischi di rete** - per esaminare tutti i drive di rete.
- **Periferiche** - per esaminare i drive rimovibili (CD-ROM, unità floppy disk).
- **Tutti gli oggetti** - per esaminare tutti i drive, indipendentemente dal fatto che siano locali, sulla rete o rimovibili.

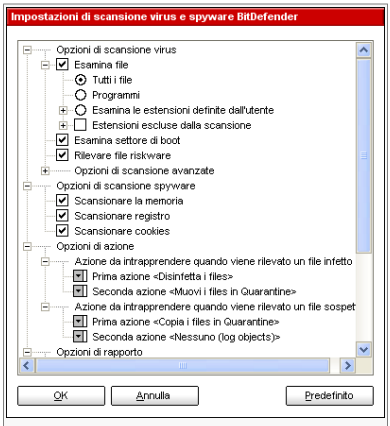
Nota
Se desiderate eseguire una scansione di tutto il vostro computer alla ricerca di virus, selezionare la casella corrispondente a **Tutti gli elementi**.

Importante
Se non avete familiarità con i computer, potrete semplicemente premere il pulsante **Esamina**. BitDefender darà inizio alla scansione del vostro computer utilizzando le impostazioni standard, comunque sufficienti.

Passaggio 4/5 - Selezione delle opzioni di scansione

Gli utenti esperti potrebbero voler approfittare delle varie possibilità di impostazione della scansione BitDefender. La scansione può essere evitata su particolari estensioni, cartelle o archivi che si conoscono come innocui. Questo potrebbe ridurre parecchio i tempi di scansione e incrementare la reattività del vostro computer durante una scansione.

Cliccare **Impostazioni** dalla sezione Scan per esplorare queste opzioni.



Impostazioni della Scansione

Le opzioni di scansione sono organizzate in menu espandibili, molto simili a quelli di esplorazione di Windows.

Le opzioni di scansione sono raggruppate in cinque categorie:

- **Opzioni di scansione virus**
- **Opzioni di scansione spyware**
- **Opzioni di azione**
- **Opzioni di rapporto**
- **Altre opzioni**

Nota

Selezionare la casella con "+" per aprire un'opzione oppure la casella con "-" per chiudere un'opzione.

- Specificare il tipo di oggetti da scansionare (archive, e-mail, messaggi ed altro) e altre opzioni. Ciò avviene attraverso la selezione di determinate opzioni dalla categoria **Opzioni di scansione virus**.

  Sono disponibili le seguenti opzioni di rilevazione:

Opzione		Descrizione
Esamina file	**Tutti i file**	Per esaminare tutti i file indipendentemente dal tipo.
	Programmi	Per esaminare soltanto i file di programma. Ciò significa solo i file con le seguenti estensioni: exe;

Opzione		Descrizione
		bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml e nws.
	Esamina le estensioni definite dall'utente	Per esaminare soltanto i file con le estensioni specificate dall'utente. Tali estensioni andranno separate da ";".
	Estensioni escluse dalla scansione	Per esaminare tutti i file tranne quelli con le estensioni indicate dall'utente. Tali estensioni andranno separate da ";".
Esamina settore di boot		Per esaminare i settori di avvio del sistema.
Rilevare file riskware		Esegue la scansione in cerca di pericoli diversi dai virus, come dialers ed adware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione fosse attiva.
Opzioni de scansione avanzate	**Apri i programmi impaccati**	Per esaminare i file impaccati.
	Apri gli archivi	Per eseguire la scansione all'interno degli archivi.
	Aprertura degli archivi email	Per eseguire la scansione all'interno degli archivi di posta.
	Usa la rilevazione euristica	Per usare la scansione euristica. L'obiettivo della scansione euristica è quello di identificare nuovi virus, basata su determinate caratteristiche ed algoritmi, prima della rilevazione di una definizione di virus. Possono apparire messaggi di falso allarme. Quando viene rilevato un file di questo tipo, il file viene classificato come sospetto. In questi casi raccomandiamo di inviare il file ai laboratori BitDefender per essere esaminato.
	Rileva corpi di virus incompleti	Per rilevare anche i corpi di virus incompleti.

- Specificare l'obiettivo della scansione spyware (processi, cookies e memoria). Ciò avviene attraverso la selezione di determinate opzioni dalla categoria **Opzioni di scansione spyware**.

  Sono disponibili le seguenti opzioni di rilevazione:

Opzione	Descrizione
Scansionare di memoria	Scansione di memoria.
Scansione registro	Scansione di voci di registro.
Scansionare cookies	Scansione di file cookie.

- Specificare l'azione da intraprendere sui file infetti o sospetti. Aprire **Opzioni di Azioni** per vedere tutte le azioni possibili su questo file.

  Selezionare le azioni quando si è rilevato un file infettato o ritenuto sospetto. Potete anche specificare altre azioni per infetti o sospetti file. Potete anche selezionare una seconda azione se la prima fallisce.

Azione	Descrizione
Nessuno(log oggetto)	Nessuna azione verrà eseguita sui file infetti. Questi file appariranno nel file di rapporto.
Chiedi all'utente prima di agire	Quando viene rilevato un virus apparirà una finestra che chiede all'utente di selezionare l'azione che si desidera eseguire su quel file. In virtù dell'importanza di quel file, è possibile scegliere se disinfettarlo, isolarlo nella zona di quarantena o cancellarlo.
Disinfetta i files	Per disinfettare i file infetti.
Cancella i files	Per cancellare i file infetti.
Rinomina i files	Per cambiare l'estensione dei file infetti. La nuova estensione dei file infetti sarà `.vir`. Rinominando i file infetti, viene rimossa la possibilità di eseguirli e pertanto di diffondere l'infezione. Contemporaneamente, potranno essere salvati per ulteriori esami ed analisi.
Copia i files nella Quarantena	Per copiare i file infetti nella zona di quarantena. Questo significa praticamente duplicare il file infetto e la copia di questo file sarà disponibile nella quarantena, ma il file infetto non verrà rimosso dalla iniziale locazione.

Azione	Descrizione
Muova i files in Quarantena	Per spostare i file infetti nella zona di quarantena.

- Specificare le opzioni per i file di rapporto. Aprire la categoria **Opzioni di rapporto** per vedere tutte le opzioni possibili.

Opzione		Descrizione
Mostra tutti i file nel raporto		Elenca tutti i file esaminati ed il loro stato (infetti o no) in un file di rapporto. Con questa opzione abilitata, il computer sarà più lento.
Crea file di rapporto	**Nome del file di rapporto** `vscan.log`	E' un campo modificabile che consente il cambiamento del nome del file di rapporto. Dovrete semplicemente selezionare questa opzione e digitare un nuovo nome.
	Limita la dimensione del file di rapporto a [0] KB	Limitare le dimensioni del file di rapporto. Digitare la dimensione massima del file.

Nota
E' possibile visualizzare il file di rapporto nella sezione Rapporto del modulo **Antivirus**.

- Specifica le altre opzioni. Apri la categoria **Altre opzioni**, da dove potrai selezionare le opzioni seguenti:

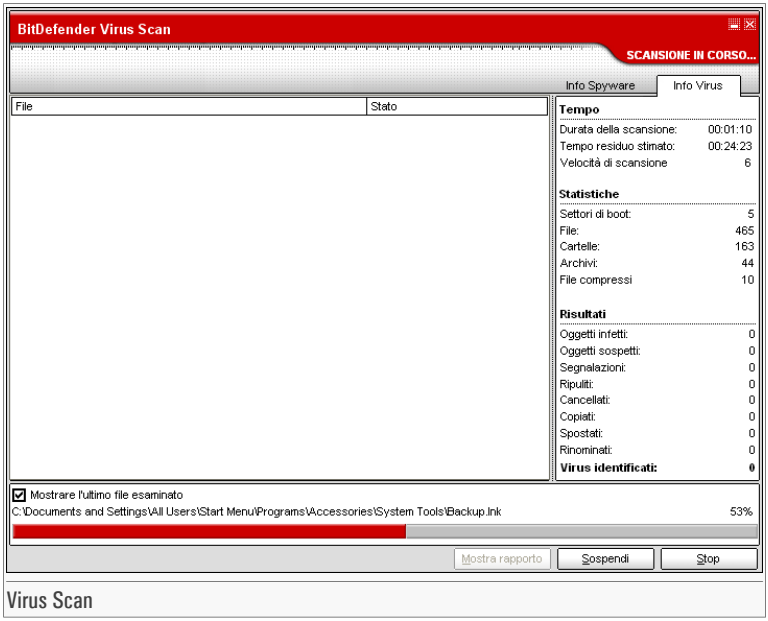
Opzione	Descrizione
Esegui il task di scansione con Bassa Priorità	Riduce la priorità del processo di scansione. Permetterai ad altri programmi di essere più veloci ed incrementerai il tempo necessario per finire il processo di scansione.
Spegne il PC quando la scansione è completata	Spegne il computer dopo che il processo di scansione è finito.
Sottoponi i files sospetti ai Laboratori BitDefender	Sarai invitato a inviare I files sospetti ai Laboratori BitDefender dopo che il processo di scansione è finito.
Minimizza la finestra di scansione nel systray	Iconizza la finestra di scansione sulla barra degli strumenti. Doppio clic sull'icona di BitDefender per aprirla.

Opzione	Descrizione
Abilita azione dopo il riavvio	Se le azioni richiedono reboot, prompt user per reboot immediato.

Selezionare **OK** per salvare le modifiche oppure selezionare **Predefinito** per tornare alle impostazioni di default.

Passaggio 5/5 - Scansione dei virus

Dopo aver selezionato le opzioni di scansione, dovrete soltanto avviare la scansione del sistema. Per fare ciò è sufficiente selezionare **Esamina**. Viene visualizzata la finestra di scansione:



Virus Scan

Durante la scansione in BitDefender è indicato l'avanzamento e compare un avviso nel caso in cui vengano trovati dei virus. Sulla destra è possibile visualizzare il progresso della scansione. In base all'obiettivo di scansione sono disponibili informazioni sugli spyware e/o i virus. Se entrambi sono disponibili, fare clic sulla scheda corrispondente per avere ulteriori informazioni sulla procedura di scansione di spyware o virus.

Selezionando la casella corrispondente a **Mostrare l'ultimo file esaminato**, saranno visibili solo le informazioni relative agli ultimi file esaminati.

Nota
La durata di scansione dipende dalla dimensione del drive del vostro disco fisso.

Tre pulsanti sono disponibili:

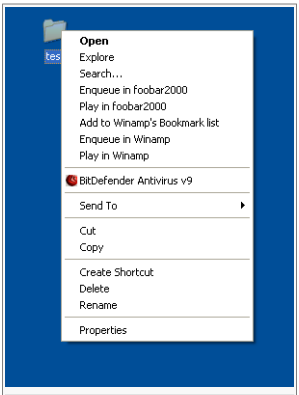
- **Stop** - apparirà una nuova finestra dove potrete terminare la verifica del sistema. Cliccare **Si&Chiudi** per uscitre dalla finestra di scansione.
- **Sospendi** - fermare temporaneamente il processo di scansione; si può continare cliccando su **Riprendi**.
- **Mostra rapporto** - aprire il rapporto di scansione.

Nota
Il file di rapporto viene automaticamente salvato nella sezione Rapporto del modulo **Antivirus**.

Un icona apparirà nel vassoio di sistema quando il processo di scansione è in funziona.

7.2.2. Scansione contestuale

Premere il tasto destro del mouse sul file o la cartella che si desidera esaminare e selezionare l'opzione **BitDefender Antivirus v9**.

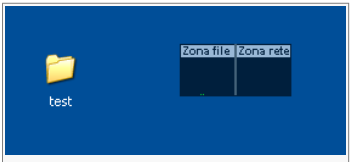


Scansione contestuale

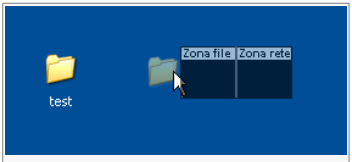
Verrà creato un file di rapporto chiamato `vscan.log` che può essere visualizzato nel modulo **Antivirus**, sezione Rapporto.

7.2.3. Scansione Seleziona e Trascina

Selezionare il file o la cartella che si desidera esaminare e trascinarla sulla **Barra delle Attività di Scansione**, come nella figura seguente.



Trascinare il file



Abbandonare il file

Verrà creato un file chiamato `activbar.log` che può essere visualizzato nel modulo **Antivirus**, sezione Rapporto.

In entrambi i casi apparirà la finestra di scansione. Qualora venga rilevato un virus apparirà una finestra di avviso.

Selezione azioni

Si può vedere il nome del file e il nome del virus.

Si può selezionare una delle opzioni specificate da intraprendere sul file infetto:

- **Ripulisci** - per disinfettare il file infetto;
- **Cancella** - per cancellare il file infetto;
- **Copia in quarantena** - per copiare il file infetto nella zona di quarantena;
- **Sposta in quarantena** - per spostare il file infetto nella zona di quarantena;
- **Rinomina** - per cambiare l'estensione dei file infetti. La nuova estensione dei file infetti sarà `.vir`.
- **Ignora** - per ignorare l'infezione. Non verrà intrapresa alcuna azione sul file infetto.

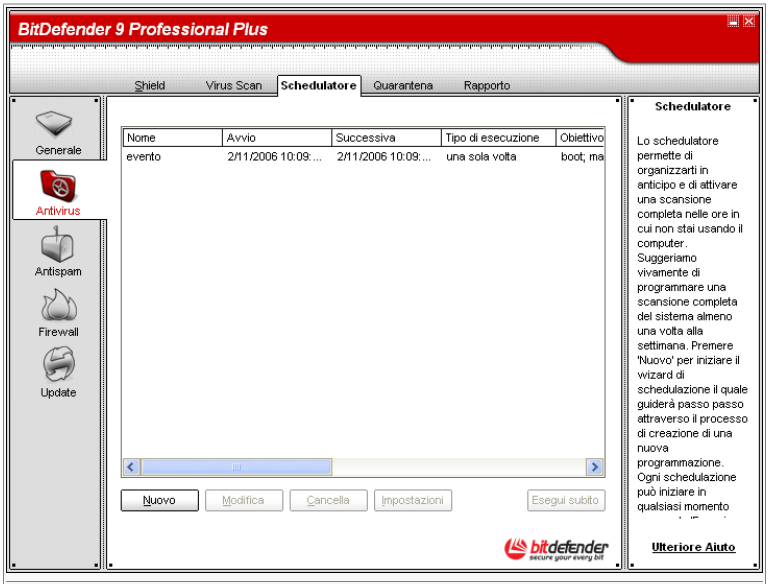
Se esaminate una cartella e desiderate che l'azione da intraprendere sia la stessa per tutti i file, selezionare l'opzione **Estendi a tutti**.

Nota
Se l'opzione **Ripulisci** non è attiva, significa che il file non può essere disinfettato. La scelta migliore è isolarlo nella zona di quarantena e mandarlo a noi per una analisi o cancellarlo.

Selezionare **OK**.

7.2.4. Scansione programmata

Per accedere a questa sezione clicca sulla linguetta **Schedulatore** del modulo **Antivirus**.



Schedulatore

Poiché la scansione può durare un certo tempo e poiché agisce meglio se vengono chiusi tutti gli altri programmi, la miglior cosa da fare è programmare la scansione nel momento in cui il vostro computer non viene usato. Ciò implica che l'utente deve precedentemente creare un così detto task, attività o evento di scansione.

Lo **Schedulatore** contiene il wizard per creare nuove funziona di scansione. Questo ti assisterà ogni volt ache ti serve per qualsiasi operazione con queste funziona di scansione, non impoorta se creando una nuopva funziona o modificandone una esistente.

La sezione **Schedulatore** contiene alcuni pulsanti per la gestione degli eventi di scansione.

- **Nuovo** - lancia la guida che condurrà attraverso la creazione di un nuovo evento di scansione.
- **Modifica** - modifica le proprietà degli eventi precedentemente creati. Inoltre lancia la guida.

Nota
Se si modifica il nome di un evento, un nuovo evento sarà introdotto con il nuovo nome digitato.

- **Cancella** - cancella gli eventi selezionati.

- **Esegui subito** - avvia immediatamente le funzioni selezionate.
- **Impostazioni** - visualizza le proprietà degli eventi selezionati.

La schermata dello Schedulatore contiene inoltre un elenco dove è possibile visualizzare tutti gli eventi della scansione, con i loro nomi, la data della prima esecuzione, la data dell'esecuzione successiva e il tipo di evento (periodico o solo una volta).

Se clicchi col tasto destro su un evento pianificato, apparirà un menu contestuale con delle opzioni simili a quelle descritte sopra.

Nota

Lo **Schedulatore** consente di programmare un numero illimitato di eventi di scansione programmati.

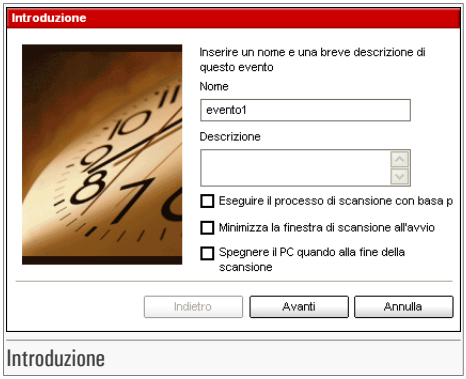
E' inoltre possibile navigare attraverso gli eventi di scansione utilizzando la tastiera: premere il pulsante **Delete** per cancellare gli eventi di scansione selezionati, premere il tasto **Enter** per visionare le proprietà degli eventi selezionati oppure premere il pulsante **Insert** per creare un nuovo evento (apparirà la guida allo Schedulatore).

Nota

Premere le frecce direzionali per muoversi nelle pagine in su, in giù, a destra o a sinistra.

Clicca su **Nuovo** per organizzare una nuova entrata nel Schedulatore. Questo lancerà la creazione guidata del Schedulatore, che ti permetterà di definire passo dopo passo la tua scansione.

Passaggio 1/9 - Introduzione



Introduzione

Digitare il nome del nuovo evento nel campo **Nome** e una breve descrizione nel campo **Descrizione**.

Sono disponibili le seguenti opzioni:

- **Eseguire il processo di scansione con Basa Priorità** - Riduce la priorità del processo di scansione. Permetterai ad altri programmi di essere più veloci ed incrementerai il tempo necessario per finire il processo di scansione.
- **Minimizza la finestra di scansione all' avvio** - Iconizza la finestra di scansione sulla barra degli strumenti. Doppio clic sull'icona di BitDefender per aprirla.
- **Spegnere il PC quando alla fine della scansione** - Spegne il computer dopo che il processo di scansione è finito.

Selezionare **Avanti** per continuare. Se si seleziona **Anulla**, apparirà una finestra che chiede di confermare l'opzione: abbandonare la guida o proseguire.

Passaggio 2/9 - Ora/data di avvio

Ora/data di avvio

Seleziona la frequenza di scansione:

- **Una volta** - lancia la scansione solo una volta, in un certo momento.
- **Periodicamente** - lancia la scansione periodicamente, a certi intervalli di tempo (ore, giorni, settimane, mesi, anni) comminciando da una data ed ora specificate.

Se si desidera che la scansione venga ripetuta a determinati intervalli, selezionare la casella corrispondente a **Periodicamente** e digitare nel campo modificabile **Ogni** il numero di minuti / ore / giorni / settimane / mesi / anni ai quali si desidera ripetere questo processo.

Nota

Si può selezionare la freccia verso l'alto / il basso di questa casella per aumentare / diminuire il numero di minuti / ore / giorni / settimane / mesi / anni.

Selezionare l'intervallo – minuti, ore, giorni, settimane, mesi, anni – al quale la scansione verrà ripetuta.

Importante

Se avete impostato l'opzione per una scansione ripetuta, l'evento verrà lanciato per un periodo di tempo illimitato. Per rinunciare all'evento, questo dovrà essere cancellato dall'elenco degli eventi della finestra Schedulatore.

Selezionare **Indietro** per andare al passaggio precedente oppure **Avanti** per continuare.

Passaggio 3/9 - Obiettivi della scansione

Obiettivi della scansione

Selezionare gli oggetti che si desidera scansionare: L'obiettivo della scansione è suddiviso in due categorie:

- **Scansione virus** - esegue la scansione di virus.

Nota
Selezionare la casella di controllo corrispondente per impostare l'obiettivo di scansione virus.

Sono disponibili le seguenti opzioni:

Opzione		Descrizione
Avvio		Scansiona il settore di avvio al fine di identificare virus di boot.
File		Scansiona i file.
	Posta	Scansiona gli archivi di posta al fine di rilevare virus di posta.
	Archivi	Scansiona l'interno degli archivi.
	File compattati	Scansiona i file impaccati.
	Scansione di oggetti a rischio	Esegue la scansione in cerca di pericoli diversi dai virus, come dialers ed adware. Questi file verranno trattati come file infetti.

- **Scansione spyware** - esegue la scansione di applicazioni spyware.

Nota
Selezionare la casella di controllo corrispondente per impostare l'obiettivo di scansione spyware.

Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Cookies	Scansione di file cookie.
Registro	Scansione di voci di registro.
Memoria	Scansione di memoria.

Per attivare/disattivare un obiettivo di scansione selezionare/deselezionare la casella di controllo corrispondente.

Selezionare **Indietro** per andare al passaggio precedente oppure **Avanti** per continuare.

Passaggio 4/9 - Percorso all'obiettivo

Percorso all'obiettivo

Specificare il percorso agli oggetti che verranno esaminati. Questo passo è necessario se hai scelto di eseguire la scansione dei file nella terza fase.

Questo schermata è a tutti gli effetti una finestra di esplorazione che consente di selezionare le partizioni e le cartelle da esaminare. Quando il cursore è posizionato su una cartella, apparirà il percorso completo a quella cartella nel campo situato sotto questa finestra di esplorazione.

Nota
Selezionare la casella con "+" per aprire un'opzione oppure quella con "-" per chiudere un'opzione.

Per selezionare le locazioni da sottoporre a scansione, è inoltre possibile utilizzare le opzioni di selezione rapida situate nella parte alta della finestra:

- **Dischi locali** - per esaminare tutti i drive locali;
- **Dischi di rete** - per esaminare tutti i drive di rete.

Selezionare **Indietro** per andare al passaggio precedente oppure **Avanti** per continuare.

Passaggio 5/9 - Maschera dei file

Maschera dei file

Specificare i tipi di file da esaminare. Questo passo è necessario se hai scelto di eseguire la scansione dei file nella terza fase.

Questo schermata è a tutti gli effetti una finestra di esplorazione che consente di selezionare le partizioni e le cartelle da esaminare. Quando il cursore è posizionato su una cartella, apparirà il percorso completo a quella cartella nel campo situato sotto questa finestra di esplorazione.

E' possibile selezionare:

- **Tutti** - per esaminare tutti i file, indipendentemente dal tipo;
- **Eseguibili e documenti** - per esaminare i file di programma e i documenti;

- **Estensioni definite dall'utente** - per esaminare solo i file le cui estensioni appaiono nell'elenco.

Nota
Tali estensioni devono essere separate da un punto e virgola ";".

Selezionare **Indietro** per andare al passaggio precedente oppure **Avanti** per continuare.

Passaggio 6/9 - Tipologia di analisi

Tipologia di analisi

Selezionare il tipo di scansione:

- **Non-Euristica** - significa la scansione dei file con la procedura basata sulle firme conosciute dei virus;
- **Euristica** - rappresenta un metodo basato su specifici algoritmi, avente l'obiettivo di identificare virus sconosciuti. Può occasionalmente segnalare codici sospetti in programmi normali, generando un così detto "falso positivo".

Sono disponibili le seguenti opzioni:

- **Spedisci i files sospetti ai Laboratori BitDefender** - Sarai invitato a inviare I files sospetti ai Laboratori BitDefender dopo che il processo di scansione è finito.

Selezionare **Indietro** per andare al passaggio precedente oppure **Avanti** per continuare.

Passaggio 7/9 - Tipologia di azione

Tipologia di azione

BitDefender consente la selezione di due azioni in caso di rilevazione di un file infetto. Selezionare le azioni per file infetti o sospetti.

Azione	Descrizione
Nessuno(log oggetto)	Nessuna azione verrà eseguita sui file infetti. Questi file appariranno nel file di rapporto.
Chiedi all'utente prima di agire	Quando viene rilevato un virus apparirà una finestra che chiede all'utente di selezionare l'azione che si desidera eseguire su quel file. In virtù dell'importanza di quel file, è possibile scegliere se disinfettarlo, isolarlo nella zona di quarantena o cancellarlo.
Disinfetta files	Per disinfettare i file infetti.
Cancella files	Per cancellare automaticamente, senza alcun avviso, tutti i file infetti.
Rinomina files	Per cambiare l'estensione dei file infetti. La nuova estensione dei file infetti sarà `.vir`. Rinominando i file infetti, viene rimossa la possibilità di eseguirli e pertanto di diffondere l'infezione. Allo stesso tempo, possono essere salvati per ulteriori verifiche ed analisi.
Copia files nella Quarantena	Per copiare i file infetti nella zona di quarantena. Questo significa praticamente duplicare il file infetto e la copia di

Azione	Descrizione
	questo file sarà disponibile nella quarantena, ma il file infetto non verrà rimosso dalla iniziale locazione.
Muovi files in Quarantena	Per spostare i file infetti nella zona di quarantena. Quando il virus è in quarantena, non può causare nessun danno.

Nota
Consigliamo di selezionare come prima azione **Disinfetta files** e come seconda azione **Muovi in Quarantena**.

Le stesse azioni previste per file infetti sono disponibli per file sospetti.

Selezionare **Indietro** per andare al passaggio precedente oppure **Avanti** per continuare.

Passaggio 8/9 - Rapporto informativo

Rapporto informativo

Per creare un rapporto di scansione selezionare **Crea file di rapporto**. In questo momento tutte le altre opzioni per la creazione di un file di rapporto verranno abilitate.

Digitare il nome del file di rapporto nella casella **Nome del file di rapporto**. Il nome di default è `schedule.log`. Esso conterrà tutte le informazioni relative al processo di scansione: il numero di virus identificati, il numero di file esaminati, il numero di file disinfettati o cancellati.

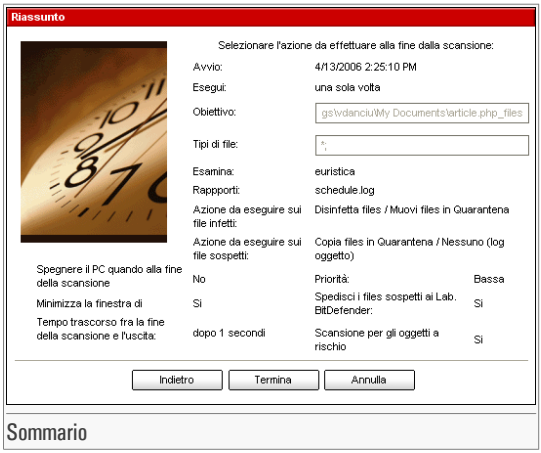
Puoi anche limitare la dimensione del file di rapporto. Inserisci la dimensione massima del file nel campo corrispondente.

Se desiderate visualizzare le informazioni relative ai file esaminati, infetti o non, selezionare l'opzione **Elenca tutti gli oggetti scansionati**. Con questa opzione abilitata, il computer sarà più lento.

Nota
Potrete visionare il file di rapporto nella sezione Rapporto del modulo **Antivirus**.

Selezionare **Indietro** per andare al passaggio precedente oppure **Avanti** per continuare.

Passaggio 9/9 - Sommario



Sommario

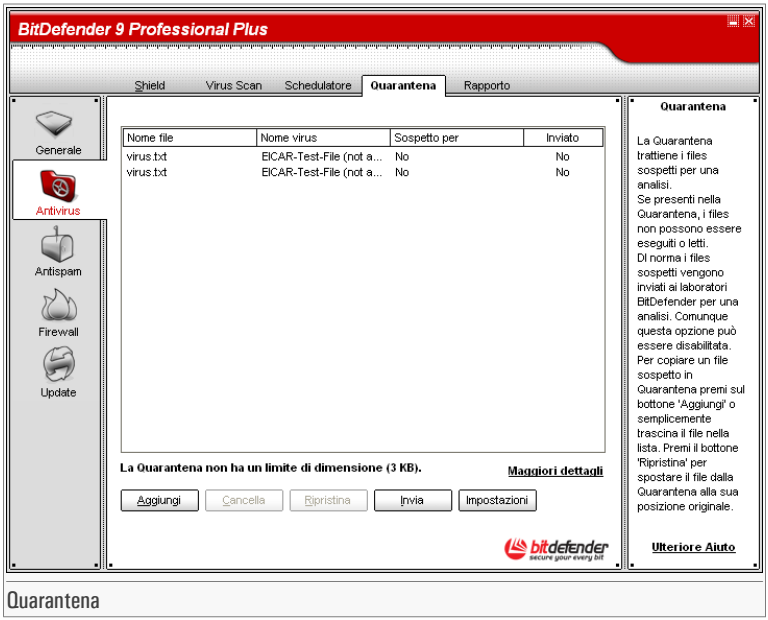
Questo è l'ultimo passaggio nella creazione di un evento di scansione. In questa finestra è possibile visionare tutte le impostazioni per l'evento di scansione ed apportare qualsiasi cambiamento ritornando ai passaggi precedenti (**Indietro**).

Se non si desidera apporre alcuna modifica, selezionare **Termina**.

Il nuovo evento apparirà nella sezione Schedulatore.

7.3. Quarantena

Per accedere a questa sezione clicca sulla linguetta **Quarantena** del modulo **Antivirus**.



Quarantena

BitDefender consente di isolare i file infetti o sospetti in un'area sicura, chiamata quarantena. Isolando questi file in quarantena, scompare il rischio di essere infettati e contemporaneamente si ha la possibilità di inviare questi file ai Laboratori BitDefender per ulteriori analisi.

La componente che garantisce la gestione dei file isolati è la **Quarantena**. Questo modulo è stato creato con una funzione di invio automatico dei file infetti ai Laboratori BitDefender.

Come potrete notare, la sezione **Quarantena** contiene un elenco di tutti i file che sono stati isolati fino a quel momento. Ogni file ha allegato il suo nome, la dimensione, la data di isolamento e la data di invio. Se desiderate visionare maggiori informazioni sui file in quarantena, selezionare **Maggiori dettagli**.

Nota

Quando un virus è in quarantena, non può più arrecare alcun danno in quanto non può essere eseguito o letto.

La sezione di **Quarantena** contiene alcuni pulsanti per la gestione di questi file.

- **Aggiungi** - aggiunge file alla quarantena. Utilizzare questo pulsante per mettere in quarantena un file sospettato di essere infetto. Si aprirà una finestra e si potrà selezionare il file dalla sua locazione sul disco. In questo modo il file viene copiato nella quarantena.

  Se desiderate spostare il file nella zona di quarantena dovrete selezionare la casella corrispondente a **Cancella dalla posizione originale**. Un metodo rapido per aggiungere un file sospetto nella Quarantena è quello di selezionarlo & trascinarlo nella lista di Quarantena.

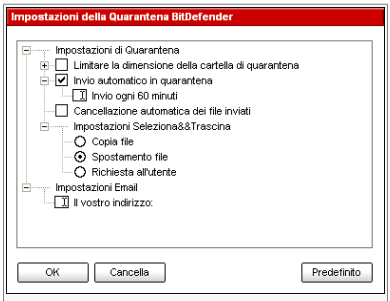
- **Cancella** - cancella i file selezionati dal vostro computer;

- **Ripristina** - rimanda il file selezionato nella sua posizione originale.

- **Invia** - invia i file selezionati ai Laboratori BitDefender per ulteriori analisi.

Importante
Si devono specificare alcune informazioni prima di inviare questi file. Per far ciò, selezionare **Impostazioni** e completare i campi della sezione **Impostazioni E-mail**, come descritto di seguito.

- **Impostazioni** - apre le opzioni avanzate per la zona di quarantena. Apparirà la seguente finestra:



Impostazioni di Quarantena

Le opzioni di Quarantena sono raggruppate in due categorie:
- **Impostazioni di Quarantena**
- **Impostazioni E-mail**

Nota
Selezionare la casella con "+" per aprire un'opzione oppure la casella con "-" per chiudere un'opzione.

Impostazioni di Quarantena

- **Limitare la dimensione della cartella di quarantena -** tiene sotto controllo la dimensione della quarantena. Questa opzione è abilitata per default e la sua dimensione è di 12000 KB. Se desideri cambiare questo valore , scrivi il nuovo intervallo nel campo corrispondente. Se si seleziona la casella di controllo che corrisponde a **Cancellazione automatica dei vecchi file**, quando la quarantena è piena e si aggiunge un nuovo file, i file più vecchi della quarantena vengono cancellati automaticamente in modo da creare spazio per il nuovo file aggiunto.

- **Invio automatico in quarantena -** invia automaticamente i file in Quarantena ai Laboratori Bitdefender per ulteriori analisi. E' possibile impostare il periodo di tempo tra due processi di invio consecutivi in termini di minuti nel campo **Invio automatico in quarantena**.

- **Cancellazione automatica dei file inviati -** cancella automaticamente i file in Quarantena dopo averli inviati ai Laboratori BitDefender per l'analisi.

- **Impostazioni Seleziona & Trascina -** se state utilizzando il metodo Seleziona &Trascina per aggiungere i file alla Quarantena, potrete specificare l'azione: copiare, spostare o chiedere all'utente.

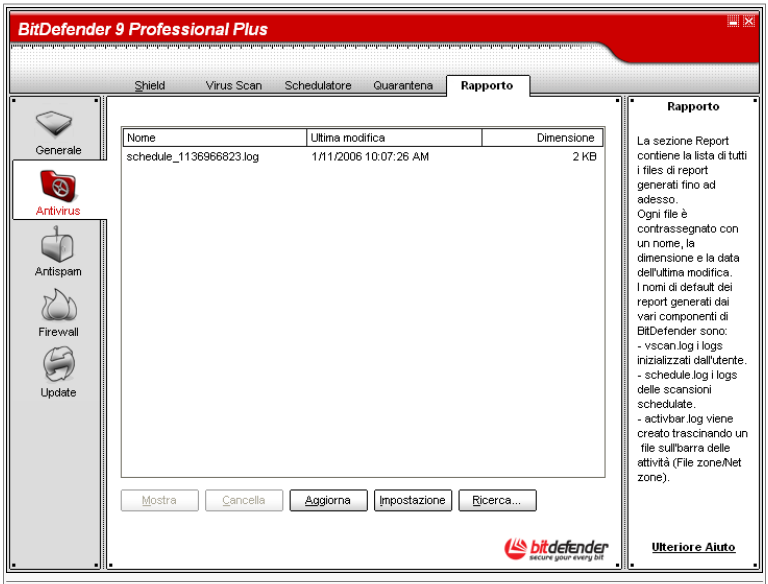
Impostazioni E-mail

- **Il vostro indirizzo -** inserire il vostro indirizzo e-mail in caso si voglia ricevere e-mail dai nostri esperti in relazione ai file sospetti inviati per l'analisi.

Selezionare **Ok** per salvare le modifiche oppure selezionare **Predefinito** per tornare alle impostazioni di default.

7.4. Rapporto

Per accedere a questa sezione clicca sulla linguetta **Rapporto** del modulo **Antivirus**.



Rapporto

La sezione **Rapporto** contiene un elenco di tutti i file di rapporto generati fino a quel momento. Ogni file ha allegato il proprio nome, la dimensione e la data dell'ultima modifica.

Quando si lancia un processo di scansione, l'utente ha la possibilità di optare per la creazione di un file di rapporto da dove potrà vedere le informazioni relative al processo di scansione. L'utente può visionare questi rapporti direttamente dalla console di gestione.

BitDefender terrà traccia della propria attività sul vostro computer. I file di rapporto di default sono i seguenti:

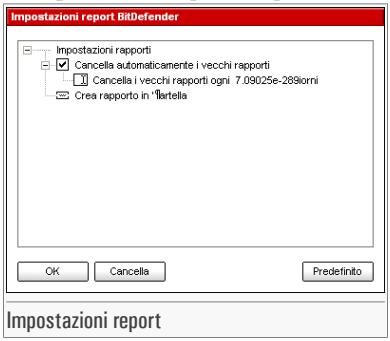
- Vscan.log viene creato quando esaminate a richiesta il vostro sistema;
- Schedule.log viene dalla scansione programmata che avete la possibilità di impostare;
- Activbar.log viene creato quando utilizzate la funzionalità Seleziona & Trascina.

La sezione **Rapporto** contiene alcuni pulsanti creati per la gestione di questi file di rapporto. La funzione di ogni pulsante è descritta qui di seguito:

Nota

I file di rapporto vengono salvati per default nella cartella dove BitDefender è installato. Se avete salvato i file di rapporto in un'altra cartella, dovrete utilizzare il pulsante **Ricerca...** per poterli localizzare.

- **Mostra** - apre il file di rapporto selezionatoe;
- **Cancella** - cancella il file di rapporto selezionato;
- **Aggiorna** - aggiorna la sezione dei **Rapporto**. Se la console di gestione è aperta alla sezione **Aggiorna** e nel frattempo eseguite una scansione del vostro computer, il nuovo file di rapporto con i risultati della scansione sarà visibile solo dopo aver selezionato **Aggiorna**.
- **Ricerca...** - apre una finestra nella quale è possibile selezionare i file di rapporto che si desiderano visionare.
- **Impostazione** - aprire le opzioni avanzate per I files dei report. Apparirà la seguente finestra:



Impostazioni report

Nota

Selezionare la casella con "+" per aprire un'opzione oppure quella con "-" per chiudere un'opzione.

- **Cancella automaticamente i vecchi rapporti** - mantenere sotto controllo il numero dei file di report, cancellando i più vecchi dopo uno specifico numero di giorni. L'intervallo di tempo di default è di 180 giorni. Se desideri cambiare questo valore , scrivi il nuovo intervallo nel campo corrispondente.
- **Crea rapporto in cartella** - specificare la cartella dove I file di Report andranno salvati.

Selezionare **Ok** per salvare le modifiche oppure selezionare **Predefinito** per tornare alle impostazioni di default.

8. Modulo Antispam

La sezione **Antispam** di questa guida dell'utente consta dei seguenti punti:

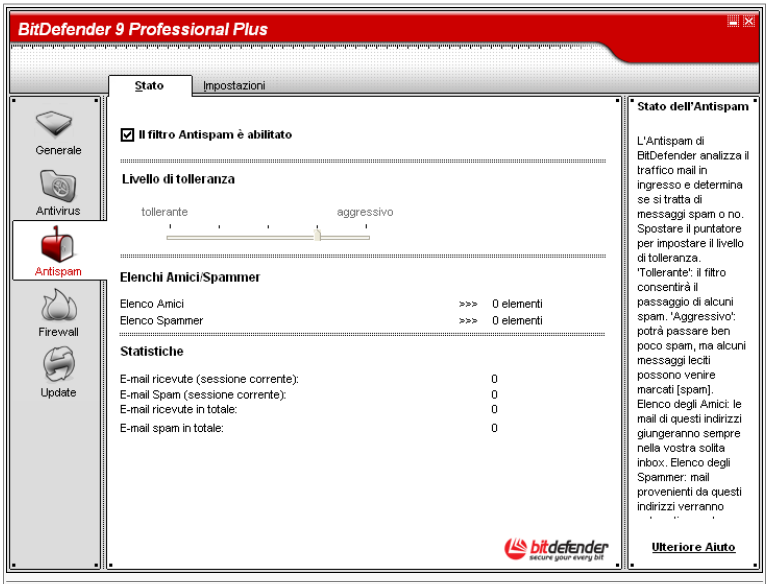
- Stato Antispam
- Impostazioni Antispam
- Configurazione da Microsoft Outlook / Outlook Express

Nota

Per altri dettagli riguardo al modulo **Antispam**, vedere la descrizione del «*Modulo Antispam*» (p. 35).

8.1. Stato Antispam

Per accedere a questa sezione clicca sulla linguetta **Stato** del modulo **Antispam**.



Stato Antispam

In questa sezione è possibile configurare il modulo **Antispam** e visionare le informazioni relative alla sua attività.

Nella sezione **Statistiche** è possibile visionare le statistiche relative al modulo Antispam. I risultati vengono presentati per sessione (da quando avete avviato il vostro computer) oppure è possibile visionare un riassunto dell'attività antispam da quando è stato installato il filtro Antispam.

Importante
Per impedire che lo Spam entri nella vostra **Inbox**, mantenere abilitato il **filtro Antispam**.

Per configurare il modulo **Antispam** è necessario procedere come segue:

8.1.1. Impostazione del livello di aggressività

Spostare l'indicatore per impostare il livello di tolleranza.

- **Tollerante** - significa che il filtro lascerà passare qualche Spam.

- **Aggressivo** - significa che ben poco Spam potrà passare, ma anche che alcuni messaggi leciti potranno essere contrassegnati (Spam).

8.1.2. Compilazione dell'elenco degli indirizzi

Gli elenchi degli indirizzi contengono informazioni relative agli indirizzi e-mail che vi inviano mail lecite o Spam.

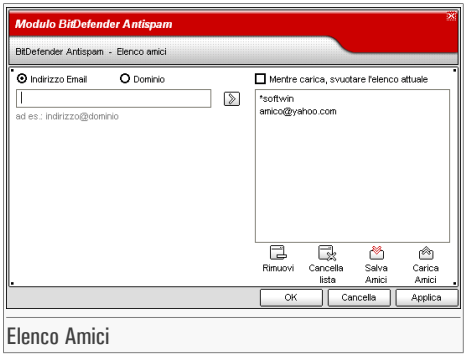
Elenco Amici

L'**Elenco Amici** è l'elenco di tutti gli indirizzi email dai quali volete sempre ricevere messaggi, indipendentemente dal loro contenuto. I messaggi provenienti dai vostri amici non verranno etichettati come spam, anche se il loro contenuto potrebbe assomigliare allo Spam.

Nota

Consigliamo di aggiungere i nomi e gli indirizzi dei vostri amici all'**Elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell'elenco, pertanto aggiungere gli amici contribuisce a garantire il passaggio dei messaggi leciti.

Per gestire l'**Elenco Amici**, selezionare >>> (in corrispondenza dell'**Elenco Amici**) oppure selezionare il pulsante **Amici** situato nella «*Barra strumenti Antispam*» (p. 102).



Elenco Amici

Qui potrete aggiungere o rimuovere elementi dall'**Elenco Amici**.

Se desiderate aggiungere un indirizzo email, selezionate il campo **Indirizzo Email**, digitate l'indirizzo e premete il pulsante . L'indirizzo apparirà nell'**Elenco Amici**.

Importante
Sintassi: <nome@dominio.com>.

Se desiderate aggiungere un dominio, selezionare il campo **Dominio**, introdurre il nome e premere il pulsante . Il dominio apparirà nell'**Elenco Amici**.

Importante
Sintassi:

- <@dominio.com>, <*dominio.com> e <dominio.com> - tutte le mail provenienti da <dominio.com> raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- <*dominio*> - tutte le mail provenienti da <dominio> (non importa il suffisso del dominio) raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- <*com> - tutte le mail con il suffisso di dominio <com> raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;

Per cancellare un elemento dall'elenco, selezionarlo e premere il pulsante **Rimuovi**.

Se premete il tasto **Cancella lista**, cancellerete tutti gli elementi dall'elenco, ma ,nota bene: è impossibile recuperarli.

Utilizzare i pulsanti **Salva Amici**/ **Carica Amici** per salvare/caricare l'**Elenco Amici** nella posizione desiderata. Il file avrà l'estensione .bwl.

Nota
Consigliamo di aggiungere i nomi e gli indirizzi dei vostri amici all'**Elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell'elenco, pertanto aggiungere gli amici contribuisce a garantire il passaggio dei messaggi leciti.

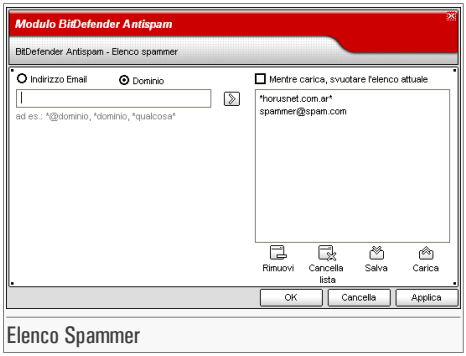
Selezionare **Applica** e **OK** per salvare & chiudere l'**Elenco Amici**.

Elenco Spammer

L'**Elenco Spammer** è l'elenco di tutti gli indirizzi e-mail dai quali non volete ricevere messaggi, indipendentemente dal loro contenuto.

Nota
Qualsiasi mail in arrivo da un indirizzo contenuto nell'**Elenco Spammer** verrà automaticamente marcato come Spam, senza alcun ulteriore processo.

Per gestire l'**Elenco Spammer**, selezionare >>> (in corrispondenza dell'**Elenco Spammer**) oppure premere il pulsante **Spammer** posizionato nella «*Barra strumenti Antispam*» (p. 102).



Elenco Spammer

Qui potrete aggiungere o rimuovere elementi dall'**Elenco Spammer**.

Se desiderate aggiungere un indirizzo email, selezionare il campo **Indirizzo Email**, inserire l'indirizzo e premere il pulsante . L'indirizzo apparirà nell'**Elenco Spammer**.

Importante
Sintassi: <nome@dominio.com>.

Se desiderate aggiungere un dominio, selezionare il campo **Dominio**, introdurre il nome e premere il pulsante . Il dominio apparirà nell'**Elenco Spammer**.

Importante
Sintassi:

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

Per cancellare un elemento dall'elenco, selezionarlo e premere il pulsante **Rimuovi**.

Se premete il tasto **Cancella lista**, cancellerete tutti gli elementi dall'elenco, ma ,nota bene: è impossibile recuperarli.

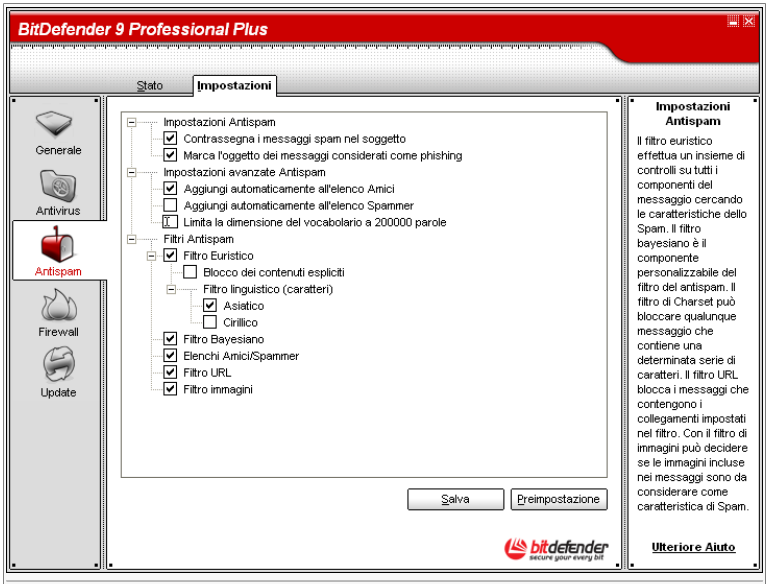
Utilizzare i pulsanti **Salva Spammer**/ **Carica Spammer** per salvare/caricare l'**Elenco Spammer** nella posizione desiderata. Il file avrà l'estensione `.bwl`.

Selezionare **Applica** e **OK** per salvare & chiudere l'**Elenco Spammer**.

Importante
Se si desidera installare nuovamente BitDefender, consigliamo prima di salvare gli elenchi **Amici** / **Spammer** e di ricaricarli al termine del processo di re-installazione.

8.2. Impostazioni Antispam

Per accedere a questa sezione clicca sulla linguetta **Impostazioni** del modulo **Antispam**.



Impostazioni Antispam

Qui potete abilitare/ o disabilitare ciascuno dei filtri Antispam e potete specificare alcune regolazioni per quanto riguarda il modulo di Antispam.

Sono disponibili tre categorie di opzioni (**Impostazioni Antispam**, **Impostazioni avanzate Antispam** e **Filtri Antispam**) organizzate con menu espandibili, simili a quelli di Windows.

Nota
Selezionare una casella con "+" per aprire una categoria oppure una casella con "-" per chiudere una categoria.

8.2.1. Impostazioni Antispam

- **Contrassegna i messagi spam nel soggetto** - tutti i messaggi email considerati come Spam verranno marcati con Spam nel soggetto.
- **Marca l'oggetto dei messagi considerati come phishing** - tutte le mail considerate messaggi di phishing saranno etichettate come SPAM sulla linea di Oggetto.

8.2.2. Impostazioni avanzate Antispam

- **Aggiungi automaticamente all'elenco Amici** - la prossima volta che si preme il pulsante **Non spam** dalla «*Barra strumenti Antispam*» (p. 102) il mittente verrà automaticamente aggiunto all'**elenco Amici**.
- **Aggiungi automaticamente all'elenco Spammer** - la prossima volta che si preme il pulsante **Spam** dalla «*Barra strumenti Antispam*» (p. 102) il mittente verrà automaticamente aggiunto all'**elenco Spammer**.

Nota
I pulsanti **Non spam** e **Spam** vengono utilizzate per addestrare il filtro Bayesiano.

- **Limita la dimensione del vocabolario a 200000 parole** - con questa opzione potete impostare la dimensione del dizionario Bayesiano – se minore è più veloce, se maggiore è più accurato.

Nota
La dimensione consigliata è: 200.000 parole.

8.2.3. Filtri Antispam

- **Filtro Euristico** - attivare/disattivare il Filtro Euristico;
- **Blocco dei contenuti espliciti** - attivare/ disattivare la scansione di messaggi "SESSUALMENTE ESPLICIT" nell'oggetto;
- **Filtro linguistico (caratteri)** - aprire il Filtro linguistico dal quale è possible selezionare e bloccare messaggi scritti in Cirillico e/o in caratteri asiatici;
- **Filtro Bayesiano** - attivare/disattivare il Filtro Bayesiano;
- **Elenchi Amici/Spammer** - attivare/disattivare i filtri basati sugli Elenchi Amici/Spammer;
- **Filtro URL** - attivare/disattivare il Filtro URL;
- **Filtro immagini** - attivare/disattivare il Filtro immagini.

Nota
Per attivare/disattivare un filtro, selezionare/pulire il checkbox corrispondente.

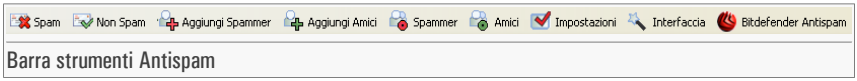
Selezionare **Applica** per salvare le modifiche oppure selezionare **Preimpostazione** per tornare alle impostazioni di default.

8.3. Configurazione da Microsoft Outlook / Outlook Express

BitDefender è integrato direttamente con Microsoft Outlook / Outlook Express con una barra degli strumenti intuitiva e di facile impiego.

8.3.1. Barra strumenti Antispam

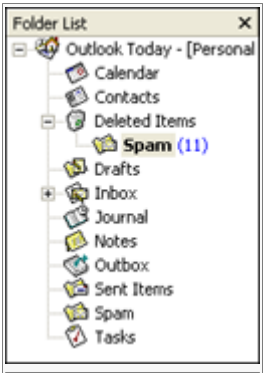
Nella parte superiore di Microsoft Outlook / Outlook Express si può osservare la barra strumenti BitDefender.



Barra strumenti Antispam

Importante
La differenza principale tra BitDefender Antispam per Microsoft Outlook e Outlook Express consiste nel fatto che i messaggi SPAM vengono spostati nella cartella **Spam** per Microsoft

Outlook mentre per Outlook Express vengono spostati nella cartella **Deleted Items**. In entrambi i casi i messaggi vengono marcati come SPAM nella riga dell'oggetto.



Cartella Spam

La cartella **Spam** creata da BitDefender Antispam per Microsoft Outlook viene inserita allo stesso livello delle entrate nell'**Elenco cartella**(Calendario, Contatti, ecc.).

Qui di seguito la spiegazione di ogni pulsante:

- **Spam** - spedire un messaggio al modulo Bayesiano indicando che la e-mail selezionata è spam. L'e-mail verrà marcata come SPAM e verrà spostata nella cartella **Spam**.

  I futuri messaggi con caratteristiche uguali verranno marcati come Spam.

  Nota
  E' possibile selezionare uno o più messaggi e-mail come si desidera.

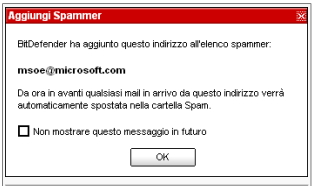
- **Non spam** - spedire un messaggio al modulo Bayesiano indicando che la e-mail selezionata non è spam. BitDefender non dovrebbe averla classificata. L'e-mail verrà spostata dalla cartella **Spam** alla cartella **Inbox**.

  I futuri messaggi con caratteristiche uguali non verranno più marcati come Spam.

  Nota
  E' possibile selezionare uno o più messaggi e-mail come si desidera.

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

- **Aggiungi spammer** - aggiungere il mittente della e-mail selezionata al vostro **Elenco Spammer**.



Aggiungi spammer

Selezionare **Non mostrare questo messaggio in futuro** se non si desidera la richiesta di conferma quando si aggiunge un indirizzo spammer all'elenco.

Selezionare **OK** per chiudere la finestra.

Le future e-mail provenienti da questo indirizzo verranno marcate come Spam.

Nota
E' possibile selezionare uno o più mittenti e-mail come si desidera.

- **Aggiungi Amici** - aggiungere il mittente della e-mail selezionata al vostro **Elenco Amici**.

Aggiungi Amici

Selezionare **Non mostrare questo messaggio in futuro** se non si desidera la richiesta di conferma quando si aggiunge un indirizzo di amici all'elenco.

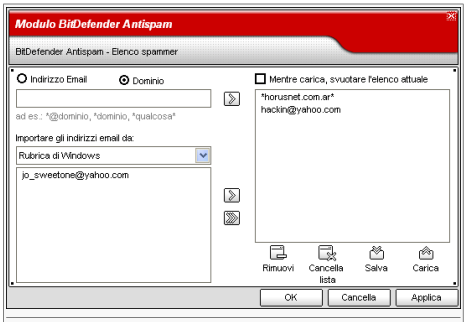
Selezionare **OK** per chiudere la finestra.

Si riceveranno sempre email provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

Nota
E' possibile selezionare uno o più mittenti e-mail come si desidera.

- **Spammer** - aprire l'**Elenco Spammer** che contiene tutte gli indirizzi e-mail dai quali non vuoi ricevere messaggi, in riferimento al loro contenuto.

Nota
Qualsiasi mail in arrivo da un indirizzo contenuto nell'**Elenco Spammer** verrà automaticamente marcato come Spam, senza alcun ulteriore processo.



Elenco Spammer

Da qui è possibile aggiungere o rimuovere elementi dall'**Elenco Spammer**.

Se si desidera aggiungere un indirizzo email, spuntare il campo **Indirizzo Email**, introdurre l'indirizzo e selezionare il pulsante . L'indirizzo apparirà nell'**Elenco Spammer**.

Importante
Sintassi: `<nome@dominio.com>`.

Se desiderate aggiungere un dominio, selezionare il campo **Dominio**, introdurre il nome e premere il pulsante . Il dominio apparirà nell'**Elenco Spammer**.

Importante
Sintassi:

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

Dal menu **Importa indirizzi mail da**, seleziona **Rubrica di Windows**/**Cartelle di Outlook Express**, per importare indirizzi mail da **Microsoft Outlook**/**Outlook Express**.

Per **Microsoft Outlook Express** apparirà una nuova finestra dove puoi selezionare la cartella che contiene gli indirizzi mail che vuoi aggiungere all'**Elenco Spammers**. Sceglili e clicca su **Seleziona**.

In entrambi i casi gli indirizzi e-mail appariranno nella lista di importazione. Selezionare quelli desiderati e fare click su per aggiungerli singolarmente all'**Elenco Spammer**. Facendo click su verranno aggiunti all'elenco tutti gli indirizzi.

Per cancellare un elemento dall'elenco, selezionarlo e premere il pulsante **Rimuovi**.

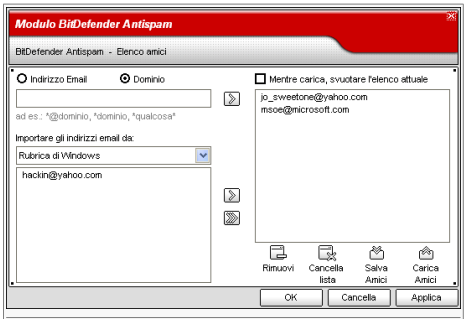
Se premete il tasto **Cancella lista**, cancellerete tutti gli elementi dall'elenco, ma ,nota bene: è impossibile recuperarli.

Utilizzare i pulsanti **Salva Spammer**/ **Carica Spammer** per salvare/caricare l'**Elenco Spammer.** nella posizione desiderata. Il file avrà l'estensione `.bwl`.

Selezionare **Applica** e **OK** per salvare & chiudere l'**Elenco Spammer**.

- **Amici** - aprire l'**Elenco Amici** che contiene tutti gli indirizzi e-mail dai quali tu vuoi sempre ricevere i loro messaggi, con riferimento al loro contenuto.

Nota
Qualsiasi mail in arrivo da un indirizzo contenuto nell'**Elenco Amici** verrà automaticamente inviato alla Inbox, senza alcun ulteriore processo.



Elenco Amici

Da qui è possibile aggiungere o rimuovere elementi dall'**Elenco Amici**.

Se si desidera aggiungere un indirizzo email, spuntare il campo **Indirizzo Email**, inserire l'indirizzo e selezionare il pulsante . L'indirizzo apparirà nell'**Elenco Amici**.

Importante
Sintassi: `<nome@dominio.com>`.

Se desiderate aggiungere un dominio, selezionare il campo **Dominio**, introdurre il nome e premere il pulsante . Il dominio apparirà nell'**Elenco Amici**.

Importante
Sintassi:

- <@dominio.com>, <*dominio.com> e <dominio.com> - tutte le mail provenienti da <dominio.com> raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- <*dominio*> - tutte le mail provenienti da <dominio> (non importa il suffisso del dominio) raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- <*com> - tutte le mail con il suffisso di dominio <com> raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;

Dal menu **Importa indirizzi mail da**, seleziona **Rubrica di Windows**/**Cartelle di Outlook Express**, per importare indirizzi mail da **Microsoft Outlook**/**Outlook Express**.

Per **Microsoft Outlook Express** apparirà una nuova finestra dove puoi selezionare la cartella che contiene gli indirizzi mail che vuoi aggiungere all'**Elenco Amici**. Sceglili e clicca su **Seleziona**.

In entrambi i casi gli indirizzi e-mail appariranno nella lista di importazione. Selezionare quelli desiderati e fare click su per aggiungerli singolarmente all'**Elenco Amici**. Facendo click su verranno aggiunti all'elenco tutti gli indirizzi.

Per cancellare un elemento dall'elenco, selezionarlo e premere il pulsante **Rimuovi**.

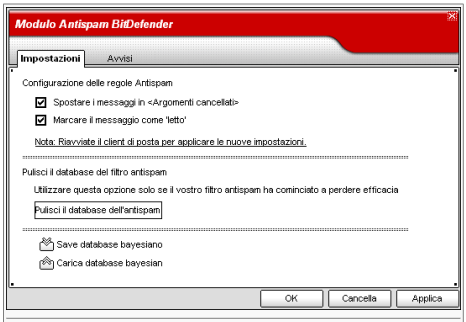
Se premete il tasto **Cancella lista**, cancellerete tutti gli elementi dall'**Elenco Amici**, ma ,nota bene: è impossibile recuperarli.

Utilizzare i pulsanti **Salva Amici**/ **Carica Amici** per salvare/caricare l'**Elenco Amici** nella posizione desiderata. Il file avrà l'estensione .bwl.

Nota
Consigliamo di aggiungere i nomi e gli indirizzi dei vostri amici all'**Elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell'elenco, pertanto aggiungere gli amici contribuisce a garantire il passaggio dei messaggi leciti.

Selezionare **Applica** e **OK** per salvare & chiudere l'**Elenco Amici**.

- **Impostazioni** - apre la finestra **Impostazioni**, dove puoi specificare diverse opzioni per il modulo **Antispam**.



Impostazioni

Sono disponibili le seguenti opzioni:

- **Spostare i messaggi in Argomenti cancellati** - per spostare i messaggi Spam nella cartella **Deleted Items** (solo per Microsoft Outlook Express);
- **Marcare il messaggio come letto** - per marcare tutti i messaggi Spam come letti così da non essere disturbati quando arrivano nuovi messaggi Spam.

Se il vostro filtro antispam è molto impreciso, può rendersi necessario pulire il database del filtro e addestrare nuovamente il Filtro Bayesiano. Selezionare **Pulisci il database dell'antispam** se si desidera impostare nuovamente il database Bayesiano.

Utilizza I tasti **Salva database bayesiano**/ **Carica database bayesiano** per salvare / scaricare il database bayesiano nell'ubicazione desiderata. Il file avrà l'estensione `.dat`.

Selezionare la tabella **Avvisi** se si desidera accedere alla sezione dove è possibile disattivare la comparsa della finestra di conferma per i pulsanti **Aggiungi spammer** e **Aggiungi amici**.

- **Interfaccia** - apre la guida che vi condurrà attraverso il processo di addestramento del filtro Bayesiano in modo da aumentare ulteriormente l'efficacia di BitDefender Antispam. E' inoltre possibile aggiungere indirizzi dalla vostra **Rubrica** agli **Elenchi Amici / Spammer**.
- **BitDefender Antispam** - apre la Console di Gestione.

8.3.2. Finestra di configurazione

La prima volta che si lancerà Microsoft Outlook apparirà una guida che vi aiuterà a configurare l'Elenco Amici e l' Elenco Spammer e ad addestrare il Bayesiano in modo da aumentare ulteriormente l'efficacia di filtri Antispam.

Nota

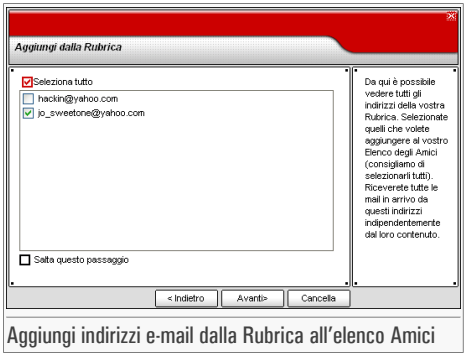
La creazione guidata può essere lanciata quando vuoi, cliccando sul tasto **Interfaccia** nella «*Barra strumenti Antispam*» (p. 102).

Passaggio 1/6 - Finestra di benvenuto

Finestra di benvenuto

Selezionare **Avanti**.

Passaggio 2/6 - Aggiungi indirizzi e-mail dalla Rubrica all'elenco Amici

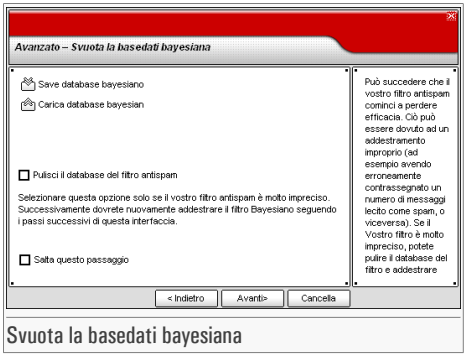


Aggiungi indirizzi e-mail dalla Rubrica all'elenco Amici

Da qui è possibile vedere tutti gli indirizzi della vostra **Rubrica**. Selezionare quelli che si desidera aggiungere al vostro **elenco Amici** (suggeriamo di selezionarli tutti). Si riceveranno tutti i messaggi e-mail provenienti da questi indirizzi, indipendentemente dal loro contenuto.

Selezionare **Salta questo passaggio**, se si desidera andare oltre. Selezionare **Indietro** per andare al passaggio precedente oppure **Avanti** per continuare.

Passaggio 3/6 - Svuota la basedati bayesiana



Svuota la basedati bayesiana

Nel tempo, si potrà notare che il vostro Filtro Antispam comincia ad essere meno efficace. Il motivo potrebbe essere quello di un addestramento improprio (ovvero nel caso in cui si sia erroneamente marcato un certo numero di messaggi legittimi come Spam e viceversa). Se il

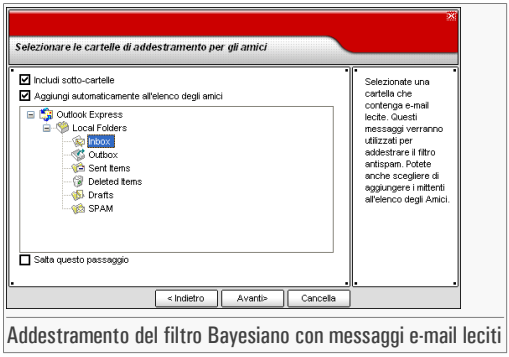
vostro filtro risulta essere molto in accurato, potrebbe essere necessario pulire il database del filtro e addestrare nuovamente il filtro seguendo le fasi successive di questa guida.

Selezionare **Pulisci il database del filtro antispam** se si desidera impostare nuovamente il database Bayesiano.

Utilizza I tasti **Salva database bayesiano**/ **Carica database bayesiano** per salvare / scaricare il database bayesiano nell'ubicazione desiderata. Il file avrà l' estensione `.dat`.

Selezionare **Salta questo passaggio**, se si desidera andare oltre. Selezionare **Indietro** per andare al passaggio precedente oppure **Avanti** per continuare.

Passaggio 4/6 - Addestramento del filtro Bayesiano con messaggi e-mail leciti



Addestramento del filtro Bayesiano con messaggi e-mail leciti

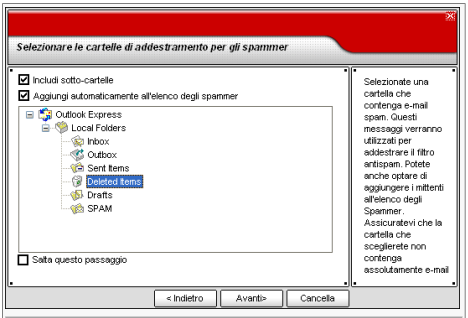
Selezionare una cartella che contenga messaggi e-mail leciti. Questi messaggi verranno utilizzati per addestrare il filtro Antispam.

Nella parte superiore della finestra sono disponibili 2 opzioni:

- **Includi sotto-cartelle** - per includere le sottocartelle nella vostra selezione;
- **Aggiungi automaticamente all'elenco degli amici** - per aggiungere i mittenti all'**elenco Amici**.

Selezionare **Salta questo passaggio**, se si desidera andare oltre. Selezionare **Indietro** per andare al passaggio precedente oppure **Avanti** per continuare.

Passaggio 5/6 - Addestramento del filtro Bayesiano con messaggi SPAM



Addestramento del filtro Bayesiano con messaggi SPAM

Selezionare una cartella che contenga messaggi e-mail Spam. Questi messaggi verranno utilizzati per addestrare il filtro Antispam.

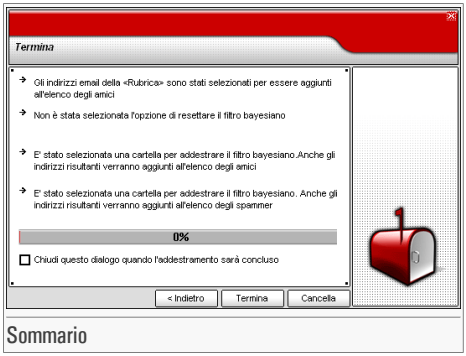
Importante
Assicurarsi che la cartella scelta non contenga assolutamente e-mail lecite, altrimenti la prestazione antispam verrà notevolmente ridotta.

Nella parte superiore della finestra sono disponibili 2 opzioni:

- **Includi sotto-cartelle** - per includere le sottocartelle nella vostra selezione;
- **Aggiungi automaticamente all'elenco degli spammer** - per aggiungere i mittenti all'**elenco Spammer**.

Selezionare **Salta questo passaggio**, se si desidera andare oltre. Selezionare **Indietro** per andare al passaggio precedente oppure **Avanti** per continuare.

Passaggio 6/6 - Sommario



In questa finestra si potranno osservare tutte le impostazioni della guida alla configurazione. Si potrà eseguire qualsiasi modifica ritornando la passo precedente (selezionare **Indietro**).

Se non si desidera apporre nessuna modifica, selezionare **Termina**.

9. Modulo Firewall

La sezione **Firewall** di questa guida dell'utente consta dei seguenti punti:

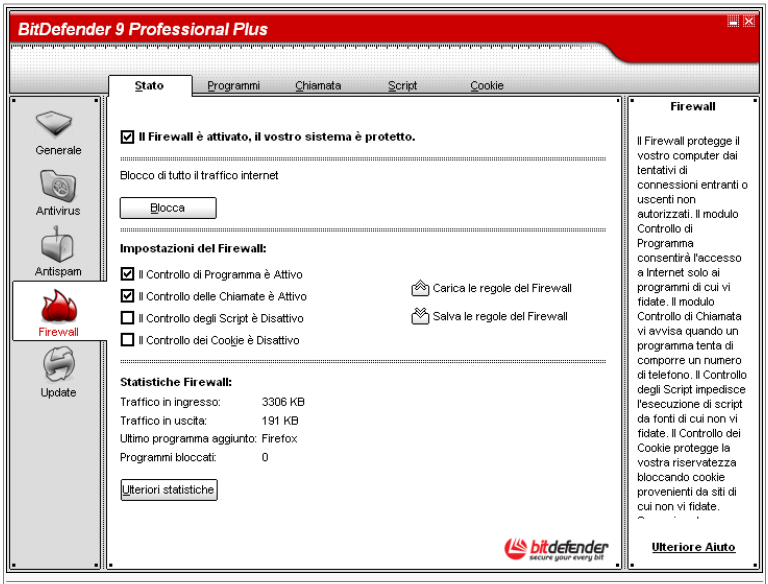
- Stato Firewall
- Controllo dei Programmi
- Controllo delle Chiamate
- Controllo degli Script
- Controllo dei Cookie

Nota

Per altri dettagli riguardo al modulo **Firewall**, vedere la descrizione del «*Modulo Firewall*» (p. 40).

9.1. Stato Firewall

Per accedere a questa sezione clicca sulla linguetta **Stato** del modulo **Firewall**.



Stato Firewall

Il **Firewall** protegge il vostro computer da tentativi di connessione non autorizzati in ingresso ed in uscita.

Nota
Per essere protetti contro gli attacchi via Internet, mantenere il **Firewall** abilitato.

In questa sezione puoi attivare / disattivare qualunque protezione offerta dal modulo **Firewall** (Controllo programmi, Controllo dial, Controllo script e Controllo cookies). La protezione si attiva quando la casella corrispondente viene selezionata.

Selezionare **Blocca** per bloccare tutto il traffico Internet.

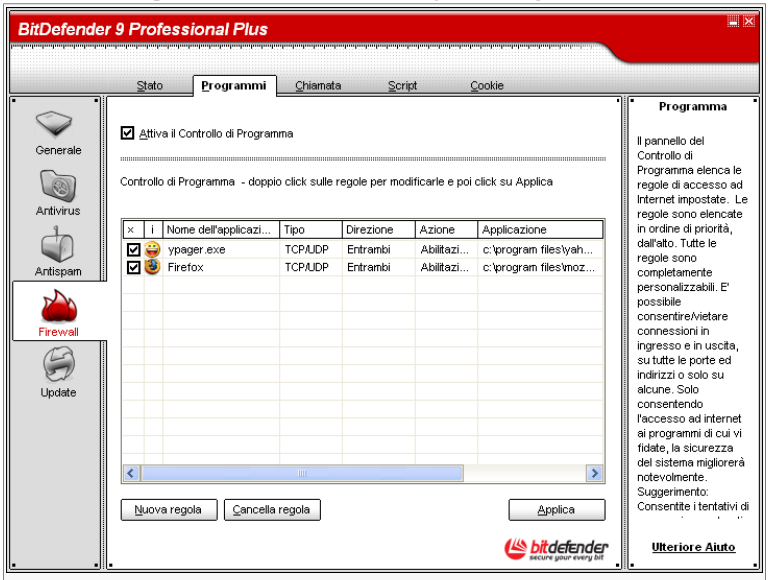
Nota
Se non siete l'unica persona che utilizza questo computer, consigliamo di proteggere le impostazioni del vostro BitDefender con una password. Per impostare una password, accedere al modulo **Generale**, sezione Impostazioni, ed utilizzare l'opzione **Abilita protezione password**.

Utilizzare i pulsanti **Salva le regole del Firewall** / **Carica le regole del Firewall** per salvare / caricare le regole nella posizione desiderata. In questo modo uoi utilizzare le stesse regole dopo aver installato o riparato il tuo prodotto BitDefender.

In Nella parte inferiore della sezione è possibile vedere le statistiche BitDefender relative al traffico ed ai programmi. Selezionare **Ulteriori statistiche** se si desidera vedere la finestra con maggiori informazioni relative a queste statistiche.

9.2. Controllo dei Programmi

Per accedere a questa sezione clicca sulla linguetta **Programmi** del modulo **Firewall**.



Controllo dei Programmi

Il **Controllo dei Programmi** è la parte più importante del vostro firewall. Monitorizza quali programmi possono utilizzare la vostra connessione Internet. Ciò è essenziale per fermare i cavalli di Troia (Trojan).

Con il **Controllo dei Programmi** abilitato, BitDefender chiederà il vostro permesso ogni volta che un nuovo programma tenterà di inviare o ricevere informazioni da o verso Internet:

Allarme del Firewall

E' possibile visionare quanto segue: l'applicazione che sta tentando di accedere ad Internet, l'indirizzo IP e la porta alla quale l'applicazione sta tentando di connettersi.

Selezionare la casella **Memorizza questa risposta** e fare click su **Sì** oppure **No** e verrà creata una regola, applicata ed elencata nella tabella delle regole. Non si riceveranno più notifiche quando l'evento si ripeterà.

Importante
Consentire tentativi di connessione verso l'interno solo da indirizzi IP o da domini di cui vi fidate.

Le regole vengono aggiunte all'elenco quando si risponde alle domande poste da BitDefender in relazione ad un nuovo programma che sta tentando di accedere a Internet.

E' possibile accedere ad ogni regola memorizzata dalla sezione **Programmi** per ulteriori perfezionamenti della configurazione.

Importante
La priorità delle regole è dal basso in alto, cioè l'ultima regola ha la più alta priorità. Seleziona & Trascina le regole per cambiare la loro priorità.

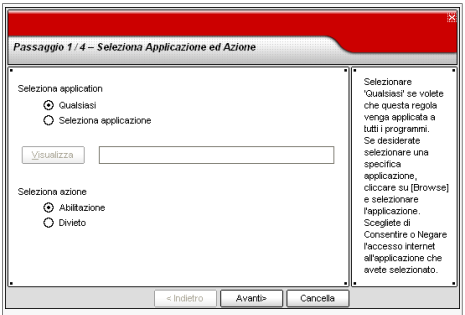
Per cancellare una regola è sufficiente selezionarla e premere **Cancella regola**. Per modificare gli attributi di una regola, fare doppio click sul suo campo. Per disattivare temporaneamente una regola senza però cancellarla, rimuovere la spunta dalla casella corrispondenta.

Le regole possono essere inserite automaticamente (attraverso la finestra di avviso) oppure manualmente (selezionare **Nuova regola** e scegliere i parametri per la regola). Apparirà il primo passaggio della guida alla configurazione.

9.2.1. Installazione guidata della configurazione

L' installazione guidata si divide in 4 passaggi.

Passaggio 1/4 - Selezione applicazione ed azione



Selezione applicazione ed azione

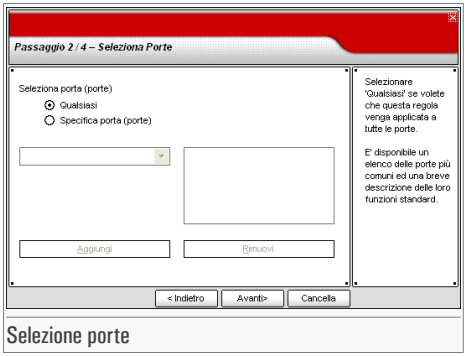
E' possibile impostare i parametri:

- **Applicazione** - selezionare l'applicazione per la regola. E' possibile scegliere solo una applicazione (selezionare **Seleziona applicazione**, successivamente **Visualizza** e selezionare l'applicazione) oppure tutte le applicazioni (basta selezionare **Qualsiasi**).
- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Abilitazione	L'azione verrà consentita.
Divieto	L'azione non verrà consentita.

Selezionare **Avanti**.

Passaggio 2/4 - Selezione porte



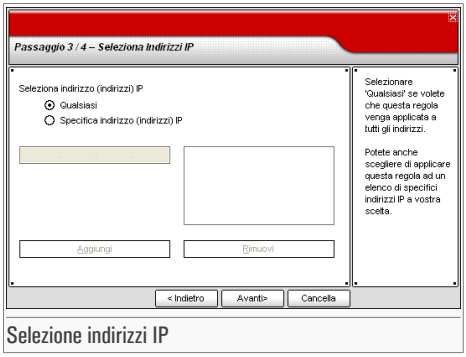
Selezione porte

E' disponibile un elenco con le porte più comuni ed una breve descrizione per aiutarvi a selezionare solo specifiche porte. Selezionare **Specifica porta**, scegliere le porte sulle quali applicare la regola e selezionare **Aggiungi**.

Se si seleziona **Qualsiasi** verranno selezionate tutte le porte. Se si desidera cancellare una porta, è sufficiente selezionarla e premere **Rimuovi**.

Selezionare **Avanti**.

Passaggio 3/4 - Selezione indirizzi IP



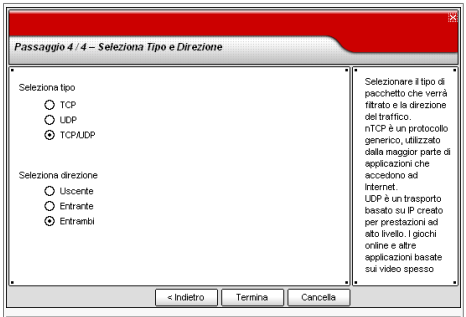
Selezione indirizzi IP

Selezionare **Specifica indirizzo**, digitare gli indirizzi IP sui quali verrà applicata la regola e selezionare **Aggiungi**.

Se si seleziona **Qualsiasi**, verranno selezionati tutti gli indirizzi IP. Se si desidera cancellare un indirizzo IP, è sufficiente selezionarlo e premere **Rimuovi**.

Selezionare **Avanti**.

Passaggio 4/4 - Selezione tipo e direzione



Selezione tipo e direzione

Imposta i parametri:

- **Tipo di Protocollo** - selezionare i protocolli TCP, UDP o entrambi.

Tipo	Descrizione
TCP	Transmission Control Protocol - TCP consente a due sistemi di stabilire una connessione e di scambiare flussi di dati. TCP garantisce la consegna dei dati e garantisce inoltre che i pacchetti verranno consegnati nello stesso ordine in cui sono stati inviati.
UDP	User Datagram Protocol - UDP è un trasporto basato su IP creato per alte prestazioni. I giochi e altre applicazioni basate su video spesso utilizzano UDP.
TCP/UDP	Transmission Control Protocol e User Datagram Protocol.

- **Direzione** - selezionare la direzione del traffico.

Direzione	Descrizione
Uscente	La regola verrà applicata solo al traffico in uscita.

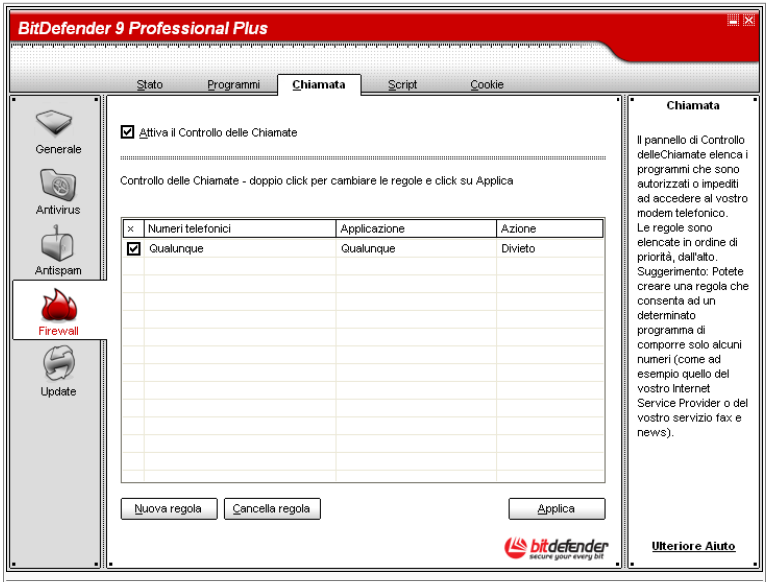
Direzione	Descrizione
Entrante	La regola verrà applicata solo al traffico in entrata.
Entrambi	La regola verrà applicata in entrambi i casi.

Selezionare **Termina**.

Selezionare **Applica** per salvare le modifiche.

9.3. Controllo delle Chiamate

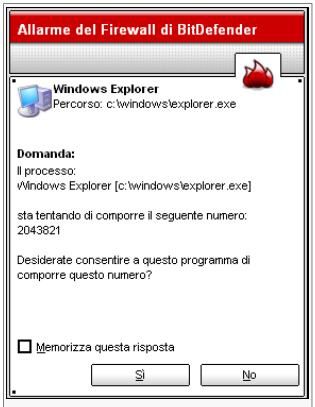
Per accedere a questa sezione clicca sulla linguetta **Chiamata** del modulo **Firewall**.



Controllo delle Chiamate

I dialer sono applicazioni che usano i modem dei computer per comporre diversi numeri telefonici. Solitamente i dialer vengono utilizzati per accedere a varie locazioni componendo numeri telefonici molto costosi.

Con il **Controllo delle Chiamate** si dovrà decidere quali connessioni a diversi numeri telefonici consentire o bloccare. Questa funzione monitorizza tutti i dialer che tentano di accedere al modem del computer, avvisando immediatamente l'utente e chiedendogli di scegliere se bloccare o consentire tali operazioni:



Allarme del Firewall

Si potranno vedere il nome dell'applicazione e il numero di telefono.

Selezionare la casella **Memorizza questa risposta** e fare click su **Sì** oppure **No** e verrà creata una regola, applicata ed elencata nella tabella delle regole. Non si verrà più avvisati quando l'applicazione tenterà di comporre lo stesso numero telefonico.

E' possibile accedere a qualsiasi regola memorizzata dalla sezione **Chiamata** per ulteriori perfezionamenti della configurazione.

Importante
La priorità delle regole è dal basso in alto, cioè l'ultima regola ha la più alta priorità. Seleziona & Trascina le regole per cambiare la loro priorità.

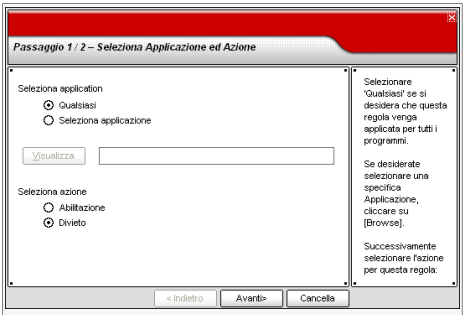
Per cancellare una regola è sufficiente selezionarla e premere **Cancella regola**. Per modificare gli attributi di una regola, fare doppio click sul suo campo. Per disattivare temporaneamente una regola senza però cancellarla, rimuovere la spunta dalla casella corrispondenta.

Le regole possono essere inserite automaticamente (attraverso la finestra di avviso) oppure manualmente (selezionare **Nuova regola** e scegliere i parametri per la regola). Apparirà il primo passaggio della guida alla configurazione.

9.3.1. Installazione guidata della configurazione

L' installazione guidata si divide in 2 passaggi.

Passaggio 1/2 - Selezione applicazione ed azione



Selezione applicazione ed azione

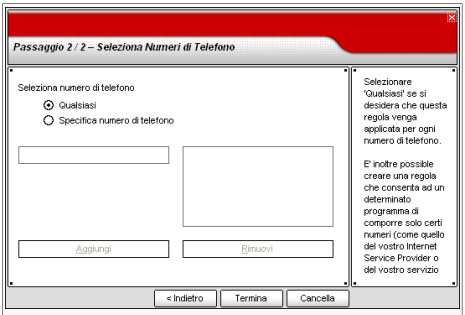
E' possibile impostare i parametri:

- **Applicazione** - selezionare l'applicazione per la regola. E' possibile scegliere solo una applicazione (selezionare **Seleziona applicazione**, successivamente **Visualizza** e selezionare l'applicazione) oppure tutte le applicazioni (basta selezionare **Qualsiasi**).
- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Abilitazione	L'azione verrà consentita.
Divieto	L'azione non verrà consentita.

Selezionare **Avanti**.

Passaggio 2/2 - Selezione dei numeri di telefono



Selezione dei numeri di telefono

Selezionare **Specifica numero di telefono**, digitare i numeri di telefono per i quali verrà creata una regola e selezionare **Aggiungi**.

Nota

E' possibile utilizzare caratteri jolly nell'elenco dei numeri telefonici banditi; ad es.: 1900* significa che tutti i numeri che iniziano con 1900 verranno bloccati.

Selezionare **Qualsiasi** se volete che questa regola venga applicata a tutti i numeri di telefono. Se desiderate cancellare un numero, è sufficiente selezionarlo e premere **Rimuovi**.

Nota

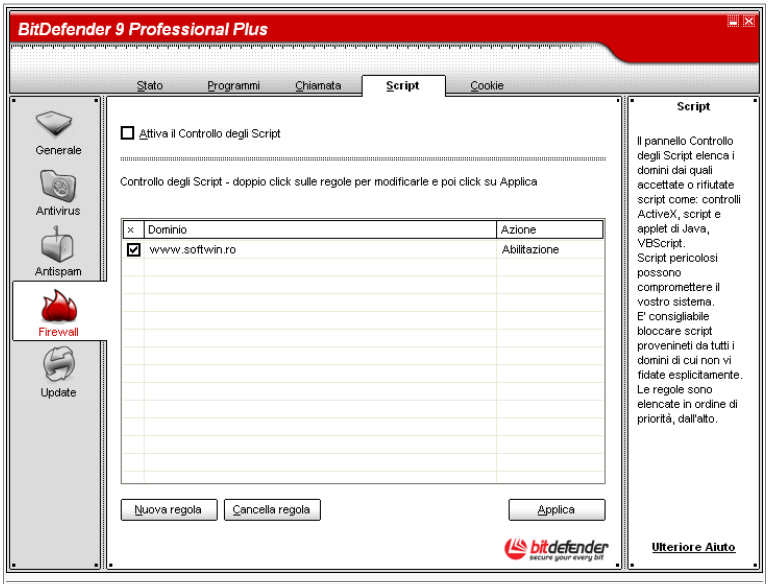
E' inoltre possibile creare una regola che consenta ad un determinato programma di comporre solo determinati numeri (come ad esempio quello del vostro Service Provider oppure quello del vostro servizio fax).

Selezionare **Termina**.

Selezionare **Applica** per salvare le modifiche.

9.4. Controllo degli Script

Per accedere a questa sezione clicca sulla linguetta **Script** del modulo **Firewall**.

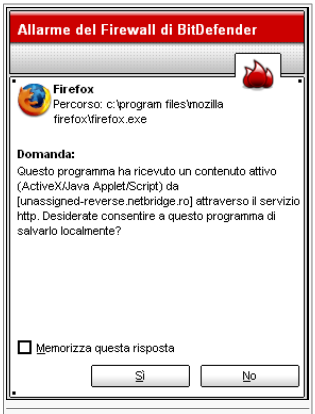


Controllo degli Script

Gli Script e altri codici come i ActiveX control e i Java applet, utilizzati per create pagine web interattive, possono essere programmati per avere effetti dannosi. Gli elementi ActiveX, ad esempio, possono ottenere un accesso totale ai vostri dati e possono leggere dati dal vostro computer, cancellare informazioni, catturare password e intercettare messaggi mentre siete online. Bisognerebbe accettare contenuti attivi solo dai siti che si conoscono e di cui ci si fida.

BitDefender vi consente di scegliere se eseguire questi elementi o bloccare la loro esecuzione.

Con il **Controllo degli Script** sarete coinvolti nel decidere di quali siti web vi fidate e di quali non vi fidate. BitDefender chiederà il vostro permesso ogni volta che un sito web tenta di attivare uno script o altri contenuti attivi:



Allarme del Firewall

E' possibile visualizzare il nome della risorsa.

Selezionare la casella **Memorizza questa risposta** e fare click su **Sì** oppure **No** e verrà creata una regola, applicata ed elencata nella tabella delle regole. Non si verrà più avvisati quando lo stesso sito tenterà di inviarvi contenuti attivi.

E' possibile accedere a qualsiasi regola memorizzata dalla sezione **Script** per ulteriori perfezionamenti della configurazione.

Importante
La priorità delle regole è dal basso in alto, cioè l'ultima regola ha la più alta priorità. Seleziona & Trascina le regole per cambiare la loro priorità.

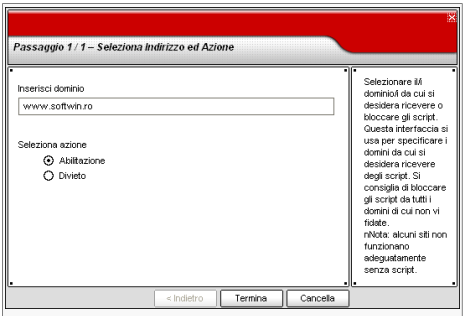
Per cancellare una regola è sufficiente selezionarla e premere **Cancella regola**. Per modificare gli attributi di una regola, fare doppio click sul suo campo. Per disattivare temporaneamente una regola senza però cancellarla, rimuovere la spunta dalla casella corrispondenta.

Le regole possono essere inserite automaticamente (attraverso la finestra di avviso) oppure manualmente (selezionare **Nuova regola** e scegliere i parametri per la regola). Apparirà il primo passaggio della guida alla configurazione.

9.4.1. Installazione guidata della configurazione

L'installazione della configurazione corrisponde alla procedura dello passo 1.

Passaggio 1/1 - Selezione indirizzo ed azione



Selezione indirizzo ed azione

E' possibile impostare i parametri:

- **Dominio** - digitare il dominio sul quale applicare la regola.
- **Azione** - selezionare l'azione della regola.

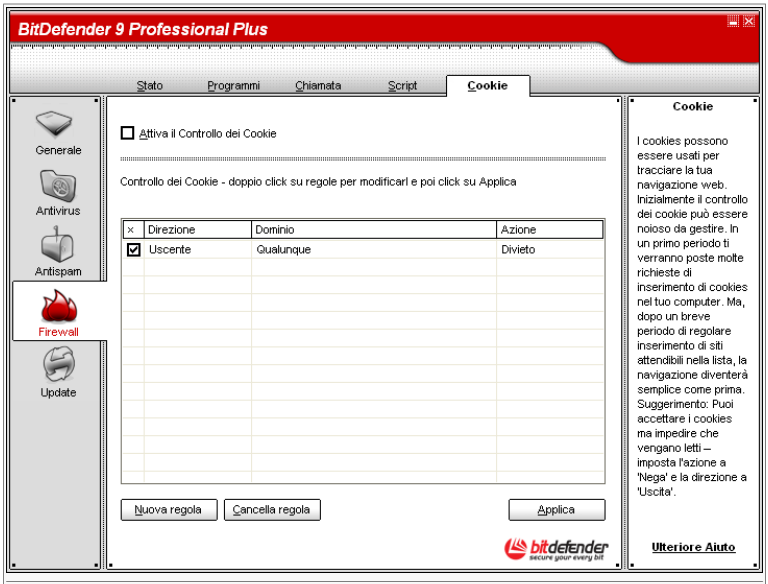
Azione	Descrizione
Abilitazione	Gli script da quel dominio verranno eseguiti.
Divieto	Gli script da quel dominio non verranno eseguiti.

Selezionare **Termina**.

Selezionare **Applica** per salvare le modifiche.

9.5. Controllo dei Cookie

Per accedere a questa sezione clicca sulla linguetta **Cookie** del modulo **Firewall**.



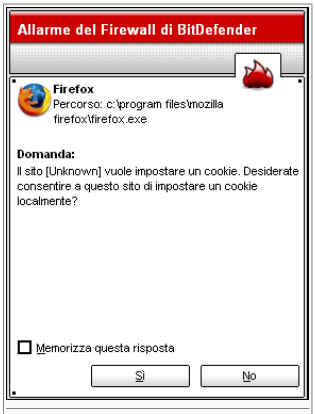
Controllo dei Cookie

I cookie sono molti frequenti su Internet. Si tratta di piccoli file immagazzinati sul vostro computer. I siti web creano questi cookie per tenere traccia di specifiche informazioni che vi riguardano.

Generalmente i Cookie vengono creati per rendere facilitare le cose. Ad esempio possono aiutare i siti web a ricordare il vostro nome e le vostre preferenze, così da non doverli inserire ad ogni visita.

I cookie però possono anche essere utilizzati per compromettere la vostra riservatezza, tenendo traccia delle vostre abitudini di navigazione.

E' qui che il **Controllo dei Cookie** vi sarà di aiuto. Quando è attivato, il **Controllo dei Cookie** chiederà il vostro permesso ogni volta che un sito web tenta di impostare un cookie:



Allarme del Firewall

E' possibile visualizzare il nome dell'applicazione che sta tentando di inviare il file cookie.

Selezionare la casella **Memorizza questa risposta** e fare click su **Sì** oppure **No** e verrà creata una regola, applicata ed elencata nella tabella delle regole. Non si verrà più avvisati quando ci si collegherà successivamente allo stesso sito.

Ciò aiuterà a scegliere i siti web di cui ci si fida e quelli di cui non ci si fida.

Nota

A causa del notevole numero di cookie utilizzati oggi giorno su Internet, il **Controllo dei Cookie** può risultare inizialmente abbastanza noioso. All'inizio porrà molte domande riguardo ai siti che tentano di piazzare i cookie sul vostro computer. Non appena si aggiungeranno i vostri siti abituali all'elenco delle regole, la navigazione diventerà semplice come prima.

E' possibile accedere a qualsiasi regola memorizzata dalla sezione **Cookie** per ulteriori perfezionamenti della configurazioneg.

Importante

La priorità delle regole è dal basso in alto, cioè l'ultima regola ha la più alta priorità. Seleziona & Trascina le regole per cambiare la loro priorità.

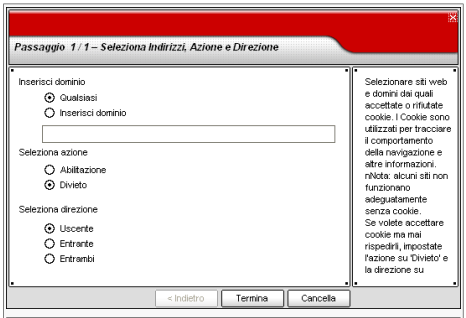
Per cancellare una regola è sufficiente selezionarla e premere **Cancella regola**. Per modificare gli attributi di una regola, fare doppio click sul suo campo. Per disattivare temporaneamente una regola senza però cancellarla, rimuovere la spunta dalla casella corrispondenta.

Le regole possono essere inserite automaticamente (attraverso la finestra di avviso) oppure manualmente (selezionare **Nuova regola** e scegliere i parametri per la regola). Apparirà il primo passaggio della guida alla configurazione.

9.5.1. Installazione guidata della configurazione

L'installazione della configurazione corrisponde alla procedura dello passo 1.

Passaggio 1/1 - Selezione indirizzo, azione e direzione



Selezione indirizzo, azione e direzione

E' possibile impostare i parametri:

- **Dominio** - digitare il dominio sul quale applicare la regola.
- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Abilitazione	I cookie da quel dominio verranno eseguiti.
Divieto	I cookie da quel dominio non verranno eseguiti.

- **Direzione** - seleziona la direzione del traffico.

Direzione	Descrizione
Uscente	La regola verrà applicata solo per i cookie che vengono rispediti al sito connesso.
Entrante	La regola verrà applicata solo per i cookie che vengono ricevuti dal sito connesso.
Entrambi	La regola verrà applicata in entrambi i casi.

Selezionare **Termina**.

Nota

Si possono accettare i cookie, ma non conviene mai rispedirli, cioè impostando l'azione **Divieto** e la direzione **Uscente**.

Selezionare **Applica** per salvare le modifiche.

10. Modulo Update

La sezione **Update** di questa guida dell'utente consta dei seguenti punti:

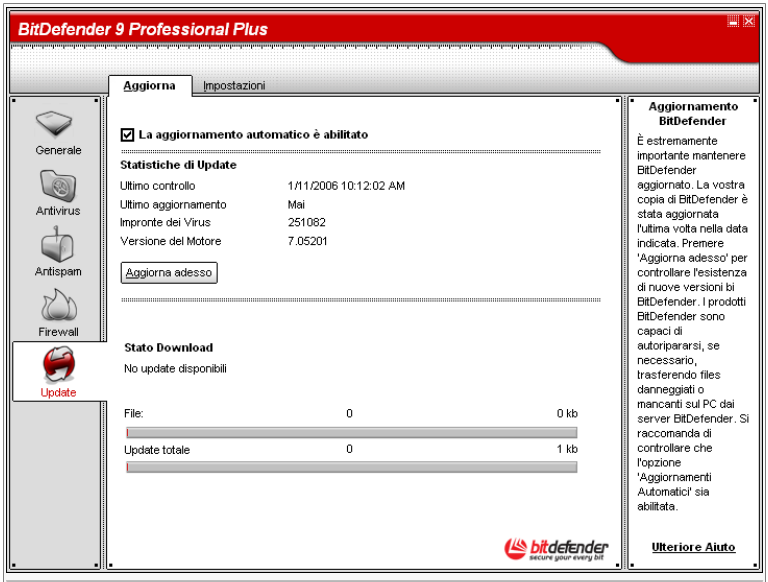
- Aggiornamento automatico
- Aggiornamento manuale
- Impostazioni dell'aggiornamento

Nota

Per altri dettagli riguardo al modulo **Update**, vedere la descrizione del «*Modulo Update*» (p. 40).

10.1. Aggiornamento automatico

Per accedere a questa sezione clicca sulla linguetta **Aggiorna** del modulo **Update**.



Aggiornamento automatico

Se sei connesso ad Internet con banda larga o DSL, BitDefender si preoccupa di farlo da solo. Controllo se ci sono nuove impronte di virus ogni volta che accendi il tuo computer ed ogni **ora** dopo il primo controllo.

Se un aggiornamento viene rilevato, dipendendo dalle opzioni impostate nella sezione di Aggiornamento automatico, ti verrà chiesto di confermare l'aggiornamento o questo verrà eseguito automaticamente.

L'aggiornamento automatico può essere eseguito in qualsiasi momento, cliccando su **Aggiorna adesso**. Questo aggiornamento è conosciuto anche come **Aggiornamento su richiesta dell'utente**.

Il modulo **Update** si collegherà al server di aggiornamento di BitDefender e verificherà se c'è qualche aggiornamento disponibile. Se rileva un aggiornamento, dipendendo delle opzioni impostate nella sezione Impostazioni update manuale, verrà chiesto di confermare l'aggiornamento o questo verrà eseguito automaticamente.

Importante
Può essere necessario riavviare il computer una volta completato l'aggiornamento. Noi consigliamo di farlo al più presto possibile.

Nota
Se sei collegato ad Internet mediante una connessione telefonica, allora è una buona idea avere come abitudine regolare l'aggiornamento di BitDefender su richiesta dell'utente.

10.2. Aggiornamento manuale

Questo metodo permette di installare le ultime definizioni di virus. Per installare un upgrade del prodotto nella sua ultima versione, utilizzare l'Aggiornamento automatico.

Importante
Utilizza l'aggiornamento manuale quando l'automatico non possa essere eseguito o quando il computer non sia collegato ad Internet.

Ci sono 2 modi di eseguire l'aggiornamento manuale:

- Con il file `weekly.exe`;
- Con degli `archivi zip`.

10.2.1. Aggiornamento manuale con il file `weekly.exe`

Il pacchetto di aggiornamento `weekly.exe` viene rilasciato ogni Venerdì, ed include tutte le definizioni di virus e motori di scansione disponibili fino alla data di rilascio.

Per aggiornare BitDefender usando `weekly.exe`, segue questi passi:

1. Scarica weekly.exe e salvalo localmente sul tuo disco duro.
2. Localizza il file scaricato e clicca due volte per lanciare la guida all'aggiornamento.
3. Clicca su **Avanti**.
4. Controlla **Accetto i termini dell'accordo di licenza** e clicca su **Avanti**.
5. Clicca su **Installa**.
6. Clicca su **Fine**.

10.2.2. Aggiornamento manuale con `archivi zip`

Ci sono due archivi zip sul server di aggiornamento, che contengono gli aggiornamenti dei motori di scansione e le impronte dei virus: `cumulative.zip` e `daily.zip`.

- `cumulative.zip` viene rilasciato ogni settimana di Lunedì ed include tutti gli aggiornamenti sulle definizioni di virus e motori di scansione fino alla data di rilascio.
- `daily.zip` viene rilasciato ogni giorno ed include tutti gli aggiornamenti sulle definizioni di virus e motori di scansione dall'ultimo cumulative fino alla data corrente.

BitDefender utilizza architettura basata nel servizio. Per ciò, la procedura per sostituire le definizioni di virus e diversa a seconda del sistema operativo:

- Windows NT-SP6, Windows 2000, Windows XP.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP

Passi da seguire:

1. **Scarica l'aggiornamento appropriato .** Se è Lunedì, per favore scarica il cumulative.zip e salvalo sul tuo disco quando ti venga proposto. Altrimenti, per favore scarica il daily.zip

e salvalo sul disco. Se è la prima volta che esegui l'aggiornamento usando il processo manuale, per favore scarica tutti due gli archivi.

2. Ferma la protezione antivirus BitDefender

   - **Esci dal Pannello di Controllo di BitDefender .** Clicca con il tasto destro sull'icona di BitDefender nella barra degli strumenti e seleziona **Esci**.

   - **Apri i Servizi .** Clicca su **Avvio**, poi **Pannello di Controllo**, doppio clic su **Strumenti di Amministrazione** e clicca su **Servizi**.

   - **Ferma il servizio Scudo Virus di BitDefender .** Seleziona servizio **Scudo Virus di BitDefender** della lista e clicca su **Fermare**.

   - **Ferma il servizio Server di Scansione di BitDefender .** Seleziona servizio **Server di Scansione di BitDefender** della lista e clicca su **Fermare**.

3. **Estrai il contenuto dell'archivio .** Se tutti i due archivi sono disponibili, inizia dal `cumulative.zip`. Estrai il contenuto nella cartella `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` e accetta di sovrascrivere sui file esistenti.

4. Riavvia la protezione antivirus BitDefender.

   - **Inizia il servizio Server di Scansione di BitDefender .** Seleziona servizio **Server di Scansione di BitDefender** della lista e clicca su **Inizia**.

   - **Inizia il servizio Scudo Virus di BitDefender .** Seleziona servizio **Scudo Virus di BitDefender** della lista e clicca su **Inizia**.

   - Apri il Panello di controllo di BitDefender.

Windows 98, Windows Millennium

Passi da seguire:

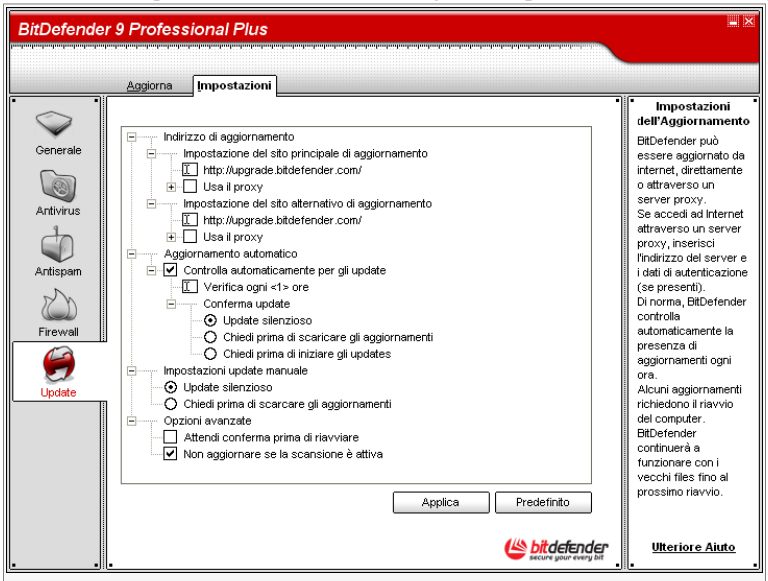
1. **Scarica l'aggiornamento appropriato .** Se è Lunedì, per favore scarica il cumulative.zip e salvalo sul tuo disco quando ti venga proposto. Altrimenti, per favore scarica il daily.zip e salvalo sul disco. Se è la prima volta che esegui l'aggiornamento usando il processo manuale, per favore scarica tutti due gli archivi.

2. **Estrai il contenuto dell'archivio .** Se tutti i due archivi sono disponibili, inizia dal `cumulative.zip`. Estrai il contenuto nella cartella `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` e accetta di sovrascrivere sui file esistenti.

3. Riavvia il computer.

10.3. Impostazioni dell'aggiornamento

Per accedere a questa sezione clicca sulla linguetta **Impostazioni** del modulo **Update**.



Impostazioni dell'aggiornamento

Gli aggiornamenti possono essere eseguiti dalla rete locale, su Internet, direttamente o attraverso un server proxy.

La finestra con le impostazioni dell'aggiornamento contiene 4 categorie di opzioni (**Indirizzo di aggiornamento**, **Aggiornamento automatico**, **Impostazioni update manuale** ed **Opzioni avanzate**) organizzate in un menu espandibile, simile a quelle di Windowss.

Nota
Clicca sui quadretti "+" per aprire una categoria e sui quadretti "-" per chiuderla.

10.3.1. Indirizzo di aggiornamento

Per aggiornamenti più affidabili e veloci, puoi configurare 2 ubicazioni per l'aggiornamento: una **Ubicazione principale dell'aggiornamento** ed un'**Ubicazione alternativa dell'aggiornamento**. Per tutte e due devi configurare le seguenti opzioni:

- **Ubicazione aggiornamento** - Se sei connesso ad una rete locale, la quale ha le impronte dei virus di BitDefender localmente, puoi cambiare a qua l'ubicazione degli aggiornamenti. Di default è: http://upgrade.bitdefender.com.
- **Usa il proxy** - Nel caso in cui l'azienda usi un server proxy, seleziona questa opzione. Devono essere specificate le seguenti impostazioni:
  - **Proxy** - inserisce l'indirizzo IP o il nome del server proxy e la porta che usa BitDefender per accedere al server proxy.

    Importante
    Sintassi: `nome:porta` o `ip:porta`.

  - **Utente** - inserisci un nome utente riconosciuto dal proxy.

    Importante
    Sintassi: `dominio\utente`.

  - **Password del proxy** - inserisci la password valida per l'utenza specificata previamente.

10.3.2. Aggiornamento automatico

- **Controla automaticamente per gli update** - BitDefender controlla automaticamente i nostri server per aggiornamenti disponibili.
- **Verifica ogni x ore** - Imposta con quale frequenza BitDefender controlla per aggiornamenti. L'intervallo di tempo predefinito è di un'ora.

- **Update silenzioso** - BitDefender scarica ed implementa l'aggiornamento automaticamente.
- **Chiedi prima di scaricare gli aggiornamenti** - ogni volta che c'è un aggiornamento disponibile, ti verrà chiesto prima di scaricarlo.
- **Chiedi prima di iniziare gli updates** - ogni volta che si scarica un aggiornamento, ti verrà chiesto prima di installarlo.

Importante
Se scegli **Chiedi prima di scaricare gli aggiornamenti** o **Chiedi prima di iniziare gli updates** , e poi chiudi&esci del pannello di controllo, l'aggiornamento automatico non verrà eseguito.

10.3.3. Impostazioni update manuale

- **Update silenzioso** - l'aggiornamento manuale sarà eseguito in sottofondo.
- **Chiedi prima di scaricare gli aggiornamenti** - ogni volta che esegui un aggiornamento manuale, ti verrà chiesto prima di scaricare ed installare gli aggiornamenti.

Importante
Se scegli **Chiedi prima di scaricare gli aggiornamenti**, e poi chiudi&esci del pannello di controllo, l'aggiornamento manuale non verrà eseguito.

10.3.4. Opzioni avanzate

- **Attendi conferma prima di riavviare** - Se un aggiornamento richiede un riavvio, il prodotto continuerà a lavorare con i vecchi file finche il sistema venga riavviato. Non verrà chiesto all'utente di riavviare, a fin che il processo di aggiornamento non interferisca con il lavoro dell'utente.
- **Non aggiornare se la scansione è attiva** - BitDefender non verrà aggiornato se è in corso un processo di scansione. In tal modo la procedura di aggiornamento BitDefender non interferisce con le operazioni di scansione.

Nota
Se BitDefender è aggiornato durante una scansione, la procedura di scansione viene interrotta.

Clicca su **Applica** per salvare le modifiche o clicca su **Preimpostazione** per ripristinare le impostazioni predefinite.

Pratiche consigliate

11. Pratiche consigliate

La sezione **Pratiche consigliate** di questa guida dell'utente consta dei seguenti punti:

- Antivirus
- Antispam

11.1. Antivirus

Passi da seguire per assicurare un computer libero di virus e spyware:

1. Una volta finito il processo d'installazione, per favore registra il tuo prodotto, come descritto nella sezione «*Registrazione del prodotto*» (p. 52).

2. Esegue un aggiornamento su richiesta dell'utente delle impronte dei virus, come descritto nella sezione «*Aggiornamento automatico*» (p. 133).

3. Esegue una scansione completa del tuo sistema , come descritto nella sezione « *Scansione immediata* » (p. 67).

4. Nella sezione Stato del modulo **Generale**, mantenere attivate le più importante prestazioni di BitDefender: **Virus Shield**, **Firewall** ed **Aggiornamento automatico**.

5. Programma il tuo BitDefender per eseguire la scansione del tuo sistema almeno una volta alla settimana, come descritto nella sezione «*Scansione programmata*» (p. 76).

11.2. Antispam

Passi da seguire per mantenere lo Spam lontano dal tuo computer:

1. Se stai usando Microsoft Outlook o Microsoft Outlook Express, segui il processo di configurazione guidata che si apre la prima volta che accedi al tuo client di posta. Puoi anche aprirlo da «*Barra strumenti Antispam*» (p. 102).

2. Aggiungi all'elenco amici, gli indirizzi della gente dalla quale hai assolutamente bisogno di ricevere posta.

Nota
BitDefender non blocca i messaggi da quelli inclusi nell'elenco; per ciò, aggiungere degli amici assicura che i messaggi legittimi arrivino.

3. Educa il « *Filtro Bayesiano* » (p. 39). Ogni volta che ricevi un messaggio che tu consideri spam, ma che BitDefender non etichettò come tale, per favore selezionalo e clicca sul tasto **Spam** nella barra degli strumenti di BitDefender. I prossimi messaggi con le stesse caratteristiche verrà catalogato come SPAM.

Nota
Il **filtro Bayesiano** si attiva solo dopo che l'hai insegnato con più di 60 messaggi legittimi. Per questo devi seguire la configurazione guidata.

4. Mantieni il tuo BitDefender aggiornato.

Nota
Ogni volta che esegui un aggiornamento:
- nuove impronte d'immagini verranno aggiunte al **Filtro immagini**;
- nuovi links verranno aggiunti al **Filtro URL**;
- nuove regole verranno aggiunte al **Filtro euristico**.

Questo aiuterà ad incrementare l'effettività del tuo motore Antispam.

5. Configura il filtro Carattere. La maggioranza dei messaggi spam sono scritti con caratteri degli alfabeti cirillico e/o asiatici. Configura questo filtro se vuoi rifiutare tutte le mail scritte con questi caratteri.

Nota
Puoi attivare/disattivare ogni uno di questi filtri nella sezione Impostazioni del modulo **Antispam**.

CD di soccorso BitDefender

BitDefender 9 Professional Plus arriva con un CD avviabile (CD di soccorso BitDefender basato su LinuxDefender), capace di eseguire la scansione e disinfettare tutti i hard disk esistenti prima che si inizi il tuo sistema operativo.

Dovresti usare il CD di soccorso BitDefender ogni volta che il tuo sistema operativo non lavora correttamente per via di infezioni di virus. Quello succede normalmente quando non usi un prodotto antivirus.

L'aggiornamento delle impronte dei virus è fatta automaticamente, senza l'intervento dell'utente, ogni volta che inizi il CD di soccorso BitDefender.

12. Descrizione generale

LinuxDefender è una distribuzione di Knoppix ri-masterizzato di BitDefender, il quale integra l'ultima soluzione di sicurezza di BitDefender per Linux nel CD GNU/Linux Knoppix Live, offrendo protezione istantanea SMTP antivirus/antispam ed un antivirus di desktop capace di eseguire la scansione e disinfettare hard disk esistenti (includendo partizioni NTFS di Windows), condivisioni remote di Samba /Windows o NFS mount points. E anche inclusa una configurazione basata su web dell'interfaccia con le soluzioni BitDefender.

Prestazioni importanti

- Protezione istantanea della posta (Antivirus & Antispam)
- Soluzioni Antivirus per il tuo hard disk
- Supporto scrittura NTFS (usando Captive project)
- Disinfezione di file infetti nelle partizioni di Windows XP

12.1. Cos'è KNOPPIX?

Citazione da http://knopper.net/knoppix:

« KNOPPIX è un CD avviabile con una raccolta di software GNU/Linux (http://www.linux.com/), rilevamento automatico di hardware, e supporto per più schede grafiche, schede audio, dispositivi SCSI e USB ed altre periferiche. KNOPPIX può essere usato come demo di Linux, CD educativo, sistema di soccorso, o adattato ed usato come piattaforma per prodotti demo di software commerciale. Non è necessario installare niente su un hard disk. »

12.2. Requisiti di sistema

Prima di avviare LinuxDefender , devi verificare prima se il tuo sistema compie i seguenti requisiti.

Tipo di processore Compatibile x86, minimo 166 MHz, ma non sperare un alto rendimento in questo caso. Un processore di generazione i686, a 800 MHz sarebbe una scelta migliore.

Memoria	Il valore minimo accettato è 64MB, per una migliore prestazione è consigliato 128MB.
CD-ROM	LinuxDefender si esegue da un CD-ROM, per cui sono richiesti un CD-ROM ed un BIOS da dove avviarlo.
Connessione Internet	Anche se LinuxDefender funzionerà senza connessione alla rete, le procedure di aggiornamento richiederanno un link HTTP attivo, persino attraverso alcuni server proxy. Per ciò, per una protezione aggiornata, la connessione ad Intrnet è obbligatoria.
Risoluzione grafica	Una risoluzione grafica di almeno 800x600 e consigliata per la amministrazione basata su web.

12.3. Software incluso

Il CD di soccorso BitDefender include i seguenti pacchetti software.

- BitDefender SMTP Proxy (Antispam & Antivirus)
- Amministratore Remoto BitDefender (configurazione basata su web)
- BitDefender edizione Linux (scanner antivirus) + interfaccia GTK
- Documentazione BitDefender (formatto PDF & HTML)
- Extras BitDefender (Artwork, Leaflets)
- Linux-Kernel 2.6
- Captive NTFS write project
- LUFS - Linux Userland File System
- Strumenti per recupero dati e riparazione del sistema, anche per altri sistemi operative
- Strumenti di analisi della rete e della sicurezza per amministratori di rete
- Soluzione Amanda backup
- thttpd
- Analizzatore del traffico di rete Ethereal, IPTraf IP LAN Monitor
- Revisore sicurezza di rete Nessus
- Soluzione per ridimensionamento, salvataggio e recupero di partizioni
- Adobe Acrobat Reader
- Web Browser Mozilla Firefox

12.4. Soluzioni di sicurezza Linux BitDefender

Il CD LinuxDefender include BitDefender SMTP proxy Antispam / Antivirus per Linux, Amministrazione remota BitDefender (interfaccia basato su web per configurare il Proxy SMTP BitDefender) e lo scanner antivirus Bitdefender, edizione Linux su misura.

12.4.1. Proxy SMTP BitDefender

BitDefender per Server di posta Linux – SMTP Proxy e una soluzione d'ispezione di contenuto sicuro, la quale fornisce protezione antivirus e antispam a livello gateway, mediante la scansione di tutto il traffico di posta per malware conosciuto o sconosciuto. Come risultato di una proprietà unica della tecnologia, BiDefender per Server di posta è compatibile con la maggioranza delle piattaforme di posta esistenti e certificate "RedHat Ready".

La soluzione Antivirus e Antispam esegue la scansione, disinfetta e filtra il traffico di posta per ogni server di posta esistente, indipendentemente della piattaforma e sistema operativo. Il Proxy SMTP BitDefender è iniziato al avvio ed esegue la scansione di tutto il traffico mail in entrata. Per configurare il Proxy SMTP BitDefender, utilizza l'Amministratore Remoto BitDefender , seguendo le seguenti istruzioni.

12.4.2. Amministratore Remoto BitDefender

Puoi configurare e gestire i servizi BitDefender in remoto (dopo aver configurato la tua rete) o localmente, seguendo questi passi:

1. Inizia il browser Firefox e vai sul URL dell'Amministratore Remoto BitDefender: https://localhost:8139 (o clicca due volte sull'icona dell'Amministratore Remoto BitDefender sul tuo desktop)
2. Accedi con nome utente "bd" e password "bd
3. Scegli "SMTP Proxy" dal menu a sinistra
4. Imposta il server Real SMTP e la porta di ascolto
5. Aggiungi i domini di posta da trasmettere
6. Aggiungi i domini di rete da trasmettere
7. Seleziona "Antispam" dal menu di sinistra per configurare le capacità dell'antispam
8. Seleziona "Antivirus" per configurare le azioni dell'Antivirus BitDefender (cosa fare quando si trova un virus, ubicazione di quarantina)
9. In più, puoi configurare "Mail di notificha" e capacità di fare logging ("Logger")

12.4.3. BitDefender Edizione Linux

Lo scanner antivirus incluso nel LinuxDefender viene integrato direttamente sul desktop. Questa versione utilizza un interfaccia grafico GTK +.

Semplicemente sfoglia il tuo hard disk (o condivisioni remote montate), clicca con il tasto destro su qualche file o cartella e seleziona “Esegue la scansione con BitDefender”. BitDefender Edizione Linux eseguirà la scansione gli elementi selezionati e mostra un rapporto sullo stato. Per opzioni più dettagliate vedere la documentazione di BitDefender Edizione Linux (nella cartella Documentazione BitDefender o pagina manuale) ed il programma **/opt/BitDefender/lib/bdc**.

13. Guida LinuxDefender

13.1. Avvio e chiusura

13.1.1. Avvio di LinuxDefender

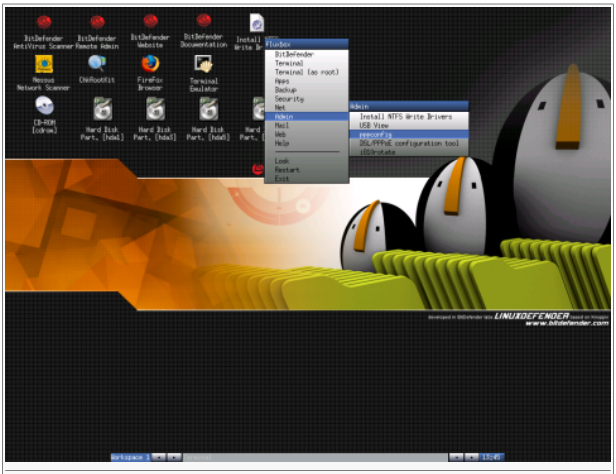
Per avviare il CD, configura il BIOS del tuo computer per avviarsi dal CD, inserisci il CD nell'unità e riavvia il computer. Assicurati che il tuo computer possa avviarsi dal CD.

Attendi finche viene mostrata la finestra seguente e segue le istruzioni sulla schermata per avviare LinuxDefender.

Finestra di avvio

Premi F2 per opzioni dettagliate. Premi F3 per opzioni dettagliate in tedesco. Premi F4 per opzioni dettagliate in francese. Premi F5 per opzioni dettagliate in spagnolo. Per un avvio veloce con le opzioni predefinite, premi solo INVIO.

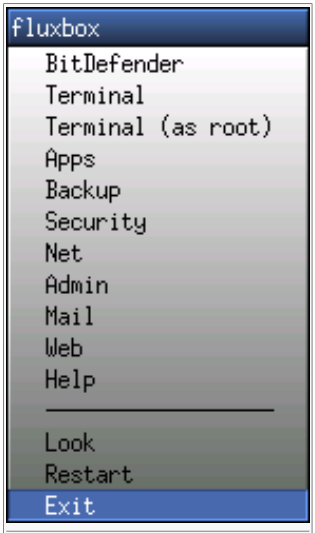
Quando il processo di avvio è finito vedrai il seguente desktop. Adesso puoi cominciare ad usare LinuxDefender.



Il Desktop

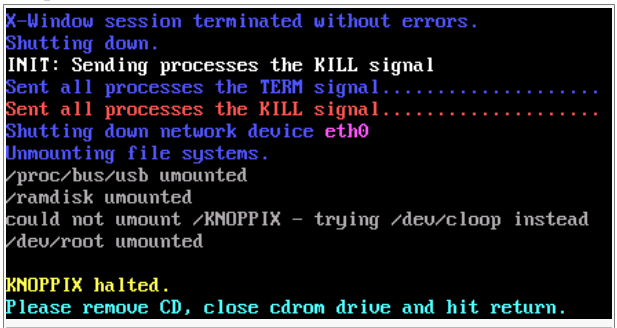
13.1.2. Chiusura di LinuxDefender

Per uscire correttamente da LinuxDefender è consigliato smontare tutte le partizioni montate usando il commando **umount**, o cliccando con il tasto destro sulle icone delle partizioni sul desktop e selezionando **Unmount**. Quindi puoi chiudere il tuo computer in modo sicuro selezionando **Exit** dal menu di LinuxDefender (tasto destro per aprirlo) o usando il commando **halt** su un terminale.



Scegli "Uscire"

Quando LinuxDefender abbia chiuso con successo, mostrerà una schermata come l'immagine seguente. Puoi rimuovere il CD per riavviare dal disco duro. Adesso va bene spegnere il tuo computer o riavviarlo.



Attendi questo messaggio alla chiusura

13.2. Configura la connessione ad Internet

Se sei in una rete DHCP ed hai una scheda di rete ethernet, la connessione Internet dovrebbe già essere rilevata e configurata. Per una configurazione manuale, segue questi passi.

1. Apri il menu di LinuxDefender (tasto destro) e seleziona **Terminal** per aprire una sessione.
2. Scrivi **netcardconfig** nella sessione aperta per lanciare lo strumento di configurazione della rete.
3. Se la tua rete usa DHCP, seleziona **yes** (se non sei sicuro, chiede all'amministratore della tua rete). Se non, vedi sotto.
4. La connessione di rete dovrebbe essere configurata automaticamente adesso. Puoi vedere la tua IP e le configurazioni della scheda di rete con il commando **ifconfig**.
5. Se hai una IP statica (non usi DHCP), rispondi **No** alla domanda DHCP.
6. Esegue le istruzioni sullo schermo. Se non sei sicuro di cosa scrivere, contatta il tuo amministratore di sistema o della rete per più dettagli.

Se tutto va bene, puoi controllare la tua connessione Internet "pingando" `bitdefender.com`.

```
$ ping -c 3 bitdefender.com
```

Se stai usando una connessione telefonica, scegli **pppconfig** dal menu Amministrazione di LinuxDefender. Quindi segui le istruzioni sullo schermo per configurare una connessione ad Internet PPP.

13.3. Aggiornamento di BitDefender

I pacchetti di BitDefender per LinuxDefender stanno usando i dischi di memoria del sistema per i file aggiornabili. In questo modo, puoi aggiornare tutte le impronte dei virus, motori di scansione o database antispam, anche quando stai eseguendo il sistema da un supporto di solo lettura, come il cd LinuxDefender.

Assicurati di avere una connessione ad Internet funzionante. Apri l'Amministratore Remoto di BitDefender e seleziona **Live! Update** del menu a sinistra. Premi **Update Now** per controllare se c isono nuovi aggiornamenti.

Altrimenti, puoi emettere il seguente commando su una sessione.

```
# /opt/BitDefender/bin/bd  update
```

Tutti i processi di aggiornamento vengono registrati nel Registro predefinito di BitDefender. Puoi vederlo nel seguente commando.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

Se stai usando un proxy per le connessioni in uscita, configura le impostazioni del Proxy nel menu **Live! Update**, tasto **Configuration**.

13.4. Scansione virus

13.4.1. Come accedo ai miei dati di Windows?

Supporto scrittura NTFS

Il supporto scrittura NTFS è disponibile usando il Captive NTFS write project. Hai bisogno di due file driver della installazione di Windows: `ntoskrnl.exe` e `ntfs.sys`. Attualmente, solo i driver di Windows XP sono supportati. Nota che puoi usarli per accedere anche partizioni Windows 2000/NT/2003.

Installare i driver NTFS

Per accedere alle tue partizioni NTFS di Windows e poter scrivere su dei dati, devi prima installare i driver NTFS. Se non stai usando NTFS per le tue partizioni Windows, ma FAT, o necessiti acesso ai tuoi dati, puoi montare direttamente i dischi ed accedere a Windows come a qualsiasi disco Linux.

Per aggiungere supporto per le partizioni NTFS, devi installare prima i driver NTFS, dai tuoi hard disk, condivisioni remote, penne USB o dal Aggiornamento Windows. È consigliato usare i driver da un'ubicazione sicura perché i driver locali dal host di Windows possono essere infetti o corrotti.

Clicca due volte sull'icona **Install NTFS Write Drivers** sul desktop per eseguire **BitDefender Captive NTFS Installer**. Seleziona la prima opzione se vuoi installare i driver dal hard disk locale.

Se i driver sono in un'ubicazione comune, usa **Quick search** per trovare i driver.

Altrimenti, puoi specificare dove si trovano i tuoi driver. O puoi scaricare i drivers dall'aggiornamento di Windows SP1.

I driver non vengono installati nel hard disk, ma vengono usati temporaneamente da LinuxDefender per accedere alle partizioni di Windows NTFS. Se il programma installa i driver NTFS, puoi cliccare due volte sulle icona Partizioni NTFS del desktop e sfogliare il contenuto. Per un potente file manager, usa il Midnight Commander dal menu di LinuxDefender (o scrivi **mc** in una sessione).

13.4.2. Come eseguo una scansione antivirus?

Sfoglia le tue cartelle, clicca con il tasto destro su un file o directory e seleziona **Send to**. Dopo scegli **BitDefender Scanner**.

O puoi emettere questo commando come ruta, da un terminale. Lo **BitDefender Antivirus Scanner** commincierà con il file o cartella selezionato come ubicazione predefinita da eseguire la scansione.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Quindi clicca su **Start Scan**.

Se vuoi configurare l'opzione antivirus, seleziona il tasto **Configure Antivirus** dal pannello sinistro del programma.

13.5. Costruisce una soluzione istantanea per il filtraggio delle mail (TOASTER)

Puoi usare LinuxDefender per creare ad hoc una soluzione per filtraggio delle mail, senza installare alcun software ne modificare il server di posta. L'idea e mettere un sistema LinuxDefender di fronte al tuo server di posta, permettendo a BitDefender di eseguire la scansione per virus e spam su tutto il traffico SMTP e trasmetterlo al server di posta reale.

13.5.1. Prerequisiti

Avrai bisogno di un PC con CPU Pentium 3 o posteriore, almeno 256 MB di RAM e unità CD/DVD da dove farlo partire. Sarà il sistema LinuxDefender a dover ricevere tutto il traffico SMTP al posto del server di posta reale. Ci sono molti modi di fare questa configurazione.

1. Cambia l'IP del tuo server di posta reale ed assegna la vecchia IP al sistema LinuxDefender
2. Cambia i utpi DNS in modo tale che l'entrata MX per i tuoi domini punti al sistema LinuxDefender
3. Configura i tuoi Clients di posta per usare il nuovo sistema LinuxDefender come server SMTP
4. Cambia le impostazioni del tuo firewall in modo che inoltri / reindirizzi tutte le connessioni SMTP verso il sistema LinuxDefender invece del server di posta reale

La guida LinuxDefender non spiegha nessuno dei temi sovraindicati. Per altre informazioni devi consultare le guide di rete Linux e la documentazione su Netfilter.

13.5.2. L'email Toaster

Lancia il tuo CD di LinuxDefender e attende finche il sistema Windows X sia caricato e funzionante.

Per configurare il Proxy SMTP BitDefender, doppio click sull'icona **BitDefender Remote Admin** dal desktop. Apparirà la seguente finestra. Utilizza nome utente bd e password bd per accedere l'Amministratore Remoto BitDefender.

Dopo l'acesso, sarai in condizioni di configurare il Proxy SMTP BitDefender.

Scegli **SMTP Proxy** per configurare il server di posta reale che vuoi proteggere contro spam e virus.

Scegli **Email domains** per inserire tutti i domini di posta dai quali vuoi accettare mail.

Premi su **Add Email Domain** o **Add Bulk Domains** e segue le istruzioni per impostare il collegamento ai domini di posta.

Seleziona il tasto **Net domains** per inserire tutte le reti verso dove vuoi trasmettere posta.

Premi su **Add Net Domain** o **Add Bulk Net Domains** e segue le istruzioni per impostare il collegamento ai domini di rete.

Seleziona **Antivirus** dal menu a sinistra per scegliere cosa fare quando un virus viene trovato, e per configurare altre opzioni antivirus.

Adesso, tutto il traffico SMTP è sotto scansione e filtraggio da BitDefender. Di default, tutti i messaggi infetti saranno puliti o cestinati, e tutti i messaggi spam rilevati da BitDefender saranno segnati nel Oggetto con la parola `[SPAM]`. L'intestazione (`X-BitDefender-Spam: Yes/No`) viene aggiunta su tutte le mail per facilitare il filtraggio dal lato Client.

13.6. Esegui una verifica della sicurezza di rete

Assieme ale capacità anti-malwre, recupero dati e filtraggio mail, LinuxDefender arriva con un set di strumenti che eseguono una revisione approfondita della sicurezza di rete & host. Anche l'analisi forense dei sistemi compromessi è possibile usando gli strumenti di sicurezza inclusi nel LinuxDefender. Leggi questa piccola guida per imparare come puoi avviare una revisione veloce della sicurezza dei tuoi host e reti.

13.6.1. Controlla per Rootkits

Prima di cominciare a cercare questioni di sicurezza su dei computer in rete, assicurati che il tuo host LinuxDefender non sia compromesso. Puoi eseguire la scansione dei hard disk installati, come descritto nella **Scan for viruses**, o puoi eseguire la scansione per Rootkits in Unix.

Prima, monta tutte le partizioni del tuo hard disk, con doppio click sulle loro icone del desktop o usando il commando **mount** nella sessione. Quindi doppio click sull'icona **ChkRootKit** per controllare il contenuto del CD o lanciare il commando **chkrootkit** nella sessione, usando il parametro `-r NEWROOT` per specificare la nuova / (root) directory dello host.

```
# chkrootkit -r /dev/hda3
```

Se viene trovato un rootkit, chkrootkit mostrerà la scoperta in **GRASSETTO**, usando lettere maiuscole.

13.6.2. Nessus – Lo Scanner in rete

Cos'è Nessus. « Nessus è lo scanner (open-source) di vulnerabilità più popolare, usato in più di 75.000 organizzazioni in tutto il mondo. Tante delle organizzazioni più grosse al mondo si stanno rendendo conto del significativo risparmio sui costi, mediante l'uso di Nessus per la revisione di dispositivi ed applicazioni commercialmente critici per l'azienda. »

Nessus può essere utilizzato per eseguire la scansione remota di tuoi computer in rete contro diverse vulnerabilità. Consiglia anche alcune misure da prendere, in modo di mitigare rischi di sicurezza e prevenire incidenti nella sicurezza.

Clicca due volte sull'icona **Nessus Security Scanner** sul desktop, o esegui **startnessus** da un terminale. Attende finche viene mostrata la seguente finestra. Dipendendo delle tue risorse Hardware, lo scaricamento di Nessus può durare fino a 10 minuti, con tutti i suoi più di 5.000 plugins che contengono database di vulnerabilità. Utilizza il nome utente `knoppix` e la password `knoppix` per accedere.

Clicca sulla linguetta **Target selection** ed inserisce l'indirizzo IP del computer o i nomi dei host sui quali devi eseguire la scansione per vulnerabilità. Assicurati di personalizzare tutte le opzioni di scansione d'accordo con la tua rete o la configurazione del tuo sistema, prima di iniziare la scansione, per risparmiarti tonnellate di banda e risorse ed avere un risultato della scansione più accurato. Quindi clicca su **Start the scan**.

Quando il processo di scansione è stato completato, Nessus mostra le scoperte ed i consigli. Puoi salvare il rapporto in tanti formatti, anche HTML con grafici e torte. Il rapporto salvato può essere visualizzato nel tuo browser preferito.

13.7. Controlla la salute della RAM del tuo sistema

Solitamente, quando il tuo sistema ha un comportamento inaspettato(si blocca o si riavvia da solo ogni tanto), può essere un problema di memoria. Puo controllare i moduli della tua RAM con il programma **memtest**, come descritto sotto.

Avvia il tuo computer dal CD LinuxDefender. Scrivi **memtest** nel momento del avvio e premi Invio.

Il programma Memtest comincerà immediatamente ed eseguirà numerosi test per controllare lo stato della memoria. Puoi configurare quali test eseguire ed altre opzioni del Memtest, premendo `c`.

Un'esecuzione completa del Memtest può durare fino a 8 ore, dipendendo della capacità e velocità dei tuoi sistemi RAM. È consigliato lasciare eseguire Memtest tutti i suoi test per controllare completamente per errori di RAM. Puoi uscire in qualsiasi momento, premendo ESC.

Se hai intenzioni di comprare un nuovo Hardware (un sistema completo o soltanto alcuni componenti), è consigliato usare LinuxDefender ed il memtest per controllarlo da errori o questioni di compatibilità.

Ottenere aiuto

14. Supporto

14.1. Dipartimento di supporto

Come stimato fornitore, SOFTWIN si sforza in offrire ai suoi clienti un alto livello di supporto veloce ed accurato. Il Centro Supporto elencato sotto è in continuo aggiornamento con le più nuove descrizioni dei virus e risposte a domande comuni, in modo che tu possa ottenere l'informazione necessaria puntualmente.

In SOFTWIN, la dedicazione al risparmio dei soldi e del tempo degli utenti, mediante la fornitura dei prodotti più avanzati ai migliori prezzi, è stata sempre una delle principali priorità. Inoltre, noi pensiamo che un business con successo è basato in una buona comunicazione ed un impegno per l'eccellenza nel supporto all'utente.

Sei benvenuto a chiedere support a <support@bitdefender.com> in qualsiasi momento. Per una risposta veloce, per favore includi nella tua mail il maggior numero di dettagli possibile sul tuo BitDefender, sul tuo sistema, e descrivi i problema con la maggior accuratezza possibile.

14.2. Aiuto On-line

14.2.1. BitDefender Knowledge Base(Archivio D'informazione BitDefender)

L' Archivio D'informazione BitDefender è un deposito d'informazione sui prodotti BitDefender. Conserva, in un formatto facilmente accessibile, rapporti sui risultati del supporto tecnico in corso ed attività di disinfezione dei team di supporto e sviluppo di BitDefender , assieme a più articoli su prevenzione virus, la gestione delle soluzioni BitDefender e spiegazioni dettagliate, e tanti altri articoli.

L'Archivio D'informazione BitDefender è aperto al pubblico e gratuitamente esplorabile. Questa ricchezza d'informazione è un altro modo ancora di fornire ai clienti di BitDefender dalle conoscenze tecniche e comprensione necessarie. Tutte le richieste valide d'informazione o rapporti su difetti, provenienti di clienti di BitDefender trovano prima o poi la loro strada fino al'Archivio D'informazione BitDefender, come rapporti di disinfezione, dei modi di aggirare le truffe, o articoli informativi, in modo di supplementare i file di aiuto dei prodotti.

L' Archivio D'informazione BitDefender è disponibile in qualsiasi momento su http://kb.bitdefender.com.

14.3. Contatti

La comunicazione efficiente è la chiave di un business con successo. Negli ultimi 10 anni SOFTWIN ha stabilito una reputazione inestimabile nel eccedere le aspettative di clienti e partners, con lo sforzo costante nelle migliori comunicazioni. Per favore non esitare a contattarci riguardo qualsiasi questione o domanda.

14.3.1. Indirizzi Web

Dipartimento vendite: <sales@bitdefender.com>
Supporto tecnico: <support@bitdefender.com>
Documentazione: <documentation@bitdefender.com>
Programma partner: <partners@bitdefender.com>
Marketing: <marketing@bitdefender.com>
Rapporti con i Media: <pr@bitdefender.com>
Opportunità di lavoro: <jobs@bitdefender.com>
Invio virus: <virus_submission@bitdefender.com>
Invio spam: <spam_submission@bitdefender.com>
Report Abuse: <abuse@bitdefender.com>
Pagina web del prodotto: http://www.bitdefender.com
Archivi ftp del prodotto: ftp://ftp.bitdefender.com/pub
Distributori locali: http://www.bitdefender.com/partner_list
Archivio D'informazione BitDefender: http://kb.bitdefender.com

14.3.2. Indirizzi

Gli uffici (succursali) di BitDefender sono pronti a rispondere a qualunque richiesta riguardo le loro aree di operazioni, in materie commerciale e generale. I loro rispettivi indirizzi e contatti sono elencati sotto.

Germany

Softwin GmbH
Karlsdorfer Straße 56 88069
Tettnang
Technischer Support: <support@bitdefender.de>
Vertrieb: <vertrieb@bitdefender.de>

Phone: 07542/94 44 44
Fax: 07542/94 44 99
Product web site: http://www.bitdefender.de

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Technical support: <support@bitdefender.us>
Sales: <sales@bitdefender.us>
Phone: 954 776 62 62, 800 388 80 62
Fax: 954 776 64 62, 800 388 80 64
Product web site: http://www.bitdefender.us

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>
Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

15. Domande frequenti

1. Generale

D: Come faccio a sapere se BitDefender sta effettivamente lavorando?

R: Nel modulo **Generale**, accedere alla sezione Stato e consultare le statistiche.

D: Quali sono i requisiti di sistema?

R: Puoi trovarli nella sezione «*Requisiti del sistema*» (p. 19).

D: Come si disinstalla BitDefender?

R: La procedura di rimozione è descritta nella sezione «*Rimozione, riparazione e modifica delle caratteristiche di BitDefender*» (p. 22).

D: Come posso registrarmi al BitDefender?

R: La procedura di registrazione è descritta nella sezione «*Registrazione del prodotto*» (p. 52).

2. Antivirus

D: Come si esegue una scansione completa?

R: Nel modulo **Antivirus**, accedere alla sezione Virus Scan, selezionare **Dischi locali** e selezionare **Esamina**.

D: Quante volte andrebbe effettuata la scansione sul mio computer?

R: Consigliamo di effettuare una scansione del vostro computer almeno una volta alla settimana.

D: Come si effettua automaticamente la scansione di ogni file che trasferisco sul mio computer?

R: BitDefender esamina tutti i file all'accesso. Bisogna semplicemente lasciare attivo il Virus Shield.

D: Come si programma BitDefender per effettuare una scansione del mio computer periodicamente?

R: Nel modulo **Antivirus**, accedere alla sezione Schedulatore, selezionare **Nuovo** e seguire la guida.

D: Cosa succede ai file nell'area di quarantena?

R: E' possibile inviare questi file ai Laboratori BitDefender per analizzarli, ma prima andranno specificate le impostazioni e-mail (accedere alla sezione Quarantena e selezionare **Impostazioni**).

3. Antispam

D: Cosa vuol dire spam?

R: Per Spam si intendono e-mail commerciali non richieste.

D: Come funziona BitDefender Antispam?

R: Si prega di vedere la sezione «*Modulo Antispam*» (p. 35).

D: Dove finisce lo spam?

R: Se utilizzate **Microsoft Outlook** / **Microsoft Outlook Express**, i messaggi spam vengono spostati nella **Cartella Spam** / **Cartella argomenti cancellati**.

Nota
Se utilizzate un client di e-mail diverso da Microsoft Outlook o Microsoft Outlook Express, dovrete create una regola per spostare i messaggi e-mail contrassegnati come Spam da BitDefender in una cartella personalizzata di quarantina. BitDefender allega il prefisso [SPAM] al soggetto dei messaggi considerati come Spam.

D: Ho bloccato un indirizzo e-mail, ma continuo a ricevere messaggi e-mail da quell'indirizzo. Perché?

R: Se ricevete spam da un indirizzo che avete bloccato, vi preghiamo di assicurarvi che l'indirizzo non sia contenuto anche nella White list. La **White list** ha precedenza sulla Black list.

D: Cos'è la White list?

R: E' un elenco di tutti gli indirizzi e-mail dai quali desiderate sempre ricevere messaggi, indipendentemente dal loro contenuto.

D: Cos'è la Black list?

R: E' un elenco di tutti gli indirizzi e-mail dai quali non desiderate ricevere messaggi, indipendentemente dal loro contenuto.

D: Cos'è il Filtro Carattere?

R: E' un filtro che blocca tutti i messaggi e-mail scritti con caratteri cirillici e/o asiatici.

D: Cos'è il Filtro Immagine?

R: È un filtro che consente di cercare le immagini all'interno dei messaggi e di confrontare quelle trovate con le immagini presenti nel database BitDefender. In caso di riconoscimento, la e-mail verrà etichettata come Spam.

D: Cos'è il Filtro URL?

R: E' un filtro che ricerca nei messaggi i link e che confronta quelli trovati con i link contenuti nel Filtro URL del database BitDefender. In caso di corrispondenza, il filtro aggiungerà un punteggio Spam alla e-mail.

D: Cos'è il Filtro euristico?

R: E' un filtro che esegue una serie di test su tutti i componenti del messaggio (ovvero non solo sull'intestazione, ma anche sul corpo del messaggio sia in formato HTML che di testo), alla ricerca di parole, frasi, link o altre caratteristiche dello spam. Il risultato è l'assegnazione di un punteggio spam alla e-mail.

D: Cos'è il Filtro Bayesiano?

R: E' un filtro che classifica i messaggi secondo informazioni statistiche relative alla percentuale con la quale appaiono specifiche parole nei messaggi classificati come Spam rispetto a quelli dichiarati non-Spam (da voi o dal filtro euristico).

4. Firewall

D: Come posso bloccare l'intero traffico Internet?

R: Nel modulo **Firewall**, sezione Stato selezionare **Blocca**.

D: A cosa serve il Controllo delle Applicazioni?

R: Il **Controllo delle Applicazioni** tiene traccia di tutti i programmi che si connettono a Internet ed è essenziale per bloccare i Trojan (Cavalli di Troia).

D: A cosa serve il Controllo delle Chiamate?

R: Il **Controllo delle Chiamate** monitorizza tutte le chiamate che tentano di accedere al modem di un computer, avvisando immediatamente l'utente e chiedendogli di scegliere se bloccare o consentire tali operazioni.

D: A cosa serve il Controllo degli Script?

R: Il **Controllo degli Script** monitorizza tutti i siti web che tentano di attivare uno script o altri contenuti attivi. Dovrete decidere di quali siti web vi fidate e di quali non vi fidate.

D: A cosa serve il Controllo dei Cookie?

R: Il **Controllo dei Cookie** garantisce la vostra privacy quanto usate Internet.

5. Aggiornamento

D: Perchè è necessario aggiornare BitDefender?

R: Ogni volta che si esegue un aggiornamento, verranno aggiunte nuove impronte di virus ai motori di scansione, nuove imagini delle firme verranno aggiunte al **Filtro Immagine**, nuovi links saranno aggiunti al **filtro URL**, nove regole saranno aggiunte al **Euristico** e nuove firme antispyware saranno aggiunte al database.

D: Come si fa ad aggiornare BitDefender?

R: Per default, BitDefender si aggiornerà automaticamente ogni ora. E' inoltre possibile effettuare gli aggiornamenti manualmente o modificare il tempo di intervallo dell'aggiornamento automatico all'interno del modulo Aggiornamento.

Glossario

Active X	ActiveX è una modalità di scrittura dei Programmi affinché possano essere invocati da altri Programmi e sistemi operativi. La tecnologia ActiveX viene utilizzata con Microsoft Internet Explorer per generare pagine Web interattive che sembrino e si comportino come applicazioni e non come semplici pagine statiche. Con gli elementi ActiveX, gli utenti possono chiedere o rispondere a domande, adoperare dei pulsanti ed interagire in altri modi con la pagina Web. I controlli ActiveX vengono spesso scritti utilizzando il linguaggio Visual Basic. Gli ActiveX sono noti per una totale mancanza di controlli di sicurezza; gli esperti di sicurezza dei computer scoraggiano il loro utilizzo attraverso Internet.
Adware	L' adware è spesso combinato con un' applicazione Host offerta senza spese quando l'utente accetta l'adware. Le applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove si spiega il proposito della applicazione. Non viene commesa quindi alcuna offesa o scortesia. Comunque, i pop-up di avvertimento possono rappresentare un fastidio, ed in alcuni casi degrada il funzionamento del sistema. Inoltre, l'informazione che viene raccolta da queste applicazioni può causare inconvenienti riguardo alla privacy degli utenti non completamente ben informati sui termini del'accordo di licenza.
Aggiornamento	La nuova versione di un prodotto software o hardware creato per sostituire una versione precedente dello stesso prodotto. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul vostro computer; diversamente non sarà possibile installare l'aggiornamento.

	BitDefender dispone del proprio modulo di aggiornamento che consente la verifica manuale degli aggiornamenti oppure l'aggiornamento automatico del prodotto.
Applet Java	Programma Java concepito per funzionare solo su pagine web. Per utilizzare un applet su una pagina web, bisognerà specificare il nome dell'applet e la dimensione (lunghezza e larghezza -in pixel) che l'applet può utilizzare. Quando si accede alla pagina web, il browser scarica l'applet dal server e lo esegue sulla macchina dell'utente (il client). Gli Applet differiscono dalle applicazioni in quanto sono governati da un rigido protocollo di sicurezza. Ad esempio, nonostante gli applet vengano lanciati sul client, essi non possono leggere o scrivere dati nella macchina dell'utente. Inoltre, gli applet sono ulteriormente limitati in modo che possano leggere e scrivere dati solo dallo stesso dominio dai quali provengono.
Archivio	Disco, nastro o cartella che contiene file memorizzati. Un file che contiene uno o più file in forma compressa.
Backdoor	Breccia nella sicurezza di un programma deliberatamente implementata dal costruttore o dal manutentore. La presenza di tali "brecce" non sempre è dolosa: su alcuni sistemi operativi, ad esempio, vengono utilizzate per l'accesso con utenze privilegiate per servizi tecnici o per i programmatori del venditore a scopo di manutenzione.
Barra di sistema	Introdotta con Windows 95, carrellala barra di sistema è situato nella barra strumenti di Windows (solitamente in basso vicino all'orologio) e contiene icone miniaturizzate per un semplice accesso alle funzioni di sistema, come ad esempio il fax, la stampante, il modem, il volume ed altro. Fare doppio click o fare click con il tasto destro su un'icona per vedere ed accedere ai dettagli ed ai controlli.
Browser	Abbreviazione di Web browser, un'applicazione software utilizzata per localizzare e visualizzare pagine Web. I due browser più noti sono Netscape Navigator e Microsoft Internet Explorer. Entrambi sono Browser grafici, ovvero in grado di visualizzare sia grafici che testo. Inoltre, i browser più moderni possono presentare informazioni multimediali, incluso suoni

	e animazione, nonostante richiedano i plug-in per alcuni formati.
Client mail	Un client e-mail è un'applicazione che vi consente di inviare e ricevere e-mail.
Cookie	Nell'industria di Internet, i cookie vengono descritti come piccoli file contenenti informazioni relative ai computer individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia dei vostri interessi e gusti online. In questo regno, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire direttamente ciò che si dichiara essere il proprio interesse. Per molte persone è una lama a doppio taglio, poiché da una parte è efficace e consente di far vedere solo ciò che viene dichiarato interessante. Dall'altra parte, implica in effetti un "tracciamento" di dove si va e di cosa si seleziona. Comprensibilmente in questo modo nascerà un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come un " SKU number" (il codice a barre sul retro delle confezioni che vengono passati alla scansione della cassa). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.
Definizione di virus	Caratteristica binaria di un virus, utilizzata dal programma antivirus alfine di rilevare ed eliminare il virus stesso.
Disk drive	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. I drive di disco possono essere interni (incorporati all'interno di un computer) oppure esterni (collocati in un meccanismo separato e connesso al computer).
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 on-line sul computer di un utente. Si può inoltre riferire al processo di copiatura di un file da un file server di rete su un computer della rete.

E-mail	Posta elettronica. Servizio che invia messaggi ai computer attraverso reti locali o globali.
Elementi di startup	Qualsiasi file posizionato in questa cartella si aprirà quando il computer viene avviato. Ad esempio, una schermata di avvio, un file sonoro da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure programmi applicativi che possono essere elementi di startup. Normalmente in questa cartella viene posizionato un alias di un file, anziché il file stesso.
Estensione del nome di un file	Porzione del nome di un file che segue il punto finale e che indica il tipo di dati inclusi nel file. Molti sistemi operativi utilizzano estensioni del nome del file, come Unix, VMS e MS-DOS. Sono normalmente composti da uno a tre lettere (alcuni vecchi supporti OS non più di tre). Esempi: “c” per codici sorgente C, “ps” per PostScipt, “txt” per testi arbitrari.
Euristico	Un metodo basato su regole per l’identificazione di nuovi virus. Questo metodo di scansione non si basa su specifiche impronte dei virus. Il vantaggio della scansione euristica è di non venire ingannata dalle nuove varianti dei virus esistenti. Può comunque occasionalmente segnalare codici sospetti in programmi normali, generando "falsi positivi".
Eventi	Azione oppure accadimento segnalato da un programma. Gli eventi possono rappresentare azioni dell’utente, come fare un click con il mouse o premere un tasto sulla tastiera oppure accadimenti 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	File che elenca le azioni avvenute. BitDefender mantiene un file di rapporto che elenca i percorsi esaminati, le cartelle, il numero di archivi e file esaminati, quanti file infetti e sospetti sono stati trovati.
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.

Linea di commando	In un'interfaccia a linea di comando, l'utente digita i comandi nello spazio previsto direttamente sullo schermo, utilizzando il linguaggio di commando.
Macro virus	Tipo di virus del computer codificato come macro all'interno di un documento. Molte applicazioni, come ad esempio Microsoft Word ed Excel, supportano potenti linguaggi macro. Queste applicazioni consentono di codificare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.
Memoria	Aree di immagazzinaggio interne nel computer. Il termine memoria identifica l'immagazzinaggio dati sotto forma di chip; la parola storage viene utilizzata per la memoria su nastri o su dischi. Ogni computer dispone di un certo quantitativo di memoria fisica, solitamente chiamata memoria principale oppure RAM.
Non euristico	Questo metodo di scansione si basa su specifiche impronte di virus. Il vantaggio della scansione non-euristica è di non essere ingannato da ciò che potrebbe sembrare un virus e non genera falsi allarmi.
Percorso	Le esatte direzioni per raggiungere un file su un computer. Queste direzioni vengono solitamente descritte attraverso il sistema di casellario gerarchico dall'alto al basso. La strada tra due punti qualsiasi, come ad esempio il canale di comunicazioni tra due computer.
Phishing	L'atto d'inviare una mail ad un utente fingendo di essere una ditta legittima ed affermata, nel tentativo di truffare l'utente, facendole cedere informazione privata che verrà usata per furti d'identità. La e-mail indirizza gli utenti a visitare una pagina Web, dove gli viene chiesto di aggiornare informazioni personali, come password e carte di credito, numero della previdenza sociale e del conto in banca, che questa legittima organizzazione ha già. In ogni caso, la pagina Web è finta, e organizzata soltanto per rubare l'informazione del utente.
Porta	Interfaccia su un computer alla quale è possibile connettere un supporto. I Personal Computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, schermi e tastiere. Esternamente i Personal Computer

	hanno porte per la connessione dei modem, delle stampanti, dei mouse e altri supporti periferici. Nelle reti TCP/IP e UDP, un punto di arrivo ad una connessione logica. Il numero della porta identifica di che tipo di porta si tratta. Ad esempio, la porta 80 viene usata per il traffico HTTP.
Programmi impaccati	File in formato compresso. Molti sistemi operativi e molte applicazioni contengono comandi che vi consentono di impaccare un file in modo da occupare meno memoria. Ad esempio, supponiamo che abbiate un file di testo che contenga dieci caratteri spazio consecutivi. Normalmente occuperebbe dieci byte di memoria. Un programma che impacca i file sostituirebbe gli spazi con un carattere speciale serie_di_spazi seguito dal numero di spazi sostituiti. In questo caso i dieci spazi occuperebbero solo due byte. Questa è solo una tecnica di impaccaggio – ce ne sono molte altre.
Script	Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.
Settore di boot	Settore all'inizio di ogni disco che identifica l'architettura del disco (dimensione del settore, dimensione del cluster, ecc.). Nei dischi di avvio, il settore di boot contiene anche un programma che carica il sistema operativo.
Spam	Posta elettronica pubblicitaria. Generalmente conosciuto come qualsiai e-mail non richiesta.
Spyware	Accede alla connessione internet dell'utente senza che l'utente se ne accorga, normalmente a scopo pubblicitario. Le applicazioni Spyware vengono tipicamente come un componente nascosto di programmi freeware o shareware che possono essere scaricati da Internet. Tuttavia, deve essere segnalato che la maggioranza delle applicazioni shareware o freeware non arrivano con spyware. Una volta installato, lo spyware esegue il monitoraggio dell'attività dell' utente su Internet e trasmette questa informazione di nascosto a qualcun altro. Lo spyware può anche raccogliere informazione su indirizzi mail e addirittura passwords e numeri di carta di credito.

Lo spyware è simile a un Cavallo di Troia che gli utenti installano senza volere quando installano qualcos'altro. Un modo comune di diventare una vittima dello spyware è scaricare certi file peer-to-peer scambiando prodotti che sono disponibili oggi.

A parte delle questioni dell'etica e la privacy, lo spyware approfitta dell' utente usando risorse di memoria del computer "mangiandosi" larghezza di banda dal momento in cui invia informazione alla sua "casa" usando l' internet dell' utente. Dato che lo spyware sta usando memoria e risorse del sistema, le applicazioni eseguite in sottofondo (background) possono portare alla caduta del sistema o alla instabilità.

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

Trojan — Programma distruttivo che si maschera da applicazione benevola. Diversamente dai virus, i cavalli di Troia non si replicano ma possono comunque essere altrettanto distruttivi. Un tipo di cavallo di Troia particolarmente insidioso è un programma che dichiara di pulire i virus del vostro computer ma che al contrario introduce i virus nel vostro computer.

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

Virus — Programma o parte di codice caricato sul vostro computer senza che voi lo sappiate e che viene eseguito contro la vostra volontà. La maggior parte dei virus è anche in grado di auto replicarsi. Tutti i virus del computer sono creati dall'uomo. E' relativamente facile produrre un semplice virus in grado di copiare sé stesso innumerevoli volte. Persino un virus così

	semplice è pericoloso in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di virus ancora più pericoloso è quello in grado di trasmettere sé stesso attraverso le reti superando i sistemi di sicurezza.
Virus di boot	Virus che infetta il settore di boot di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infettato con un virus di boot, farà sì che il virus venga attivato nella memoria. Da quel momento in poi, ogni volta che si esegue il boot del sistema, il virus sarà attivo nella memoria.
Virus polimorfico	Virus che modifica la propria forma con ogni file che infetta. In quanto non dispongono di caratteristiche binarie costanti, tali virus sono difficili da identificare.
Worm(baco)	Programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.