F-Secure Anti-Virus 2013

Sommario

Capitolo 1: Installazione.....5

Prima di eseguire la prima installazione.....6
Installazione del prodotto per la prima volta.....6
Installazione e aggiornamento delle applicazioni.....6
Guida in linea e assistenza tecnica.....7

Capitolo 2: Operazioni preliminari.....9

Come utilizzare gli aggiornamenti automatici.....10
Verifica dello stato di aggiornamento.....10
Modifica della impostazioni di connessione a Internet.....10
Verificare lo stato della rete della protezione in tempo reale.....11
Come visualizzare le operazioni effettuate dal prodotto.....11
Visualizza cronologia notifiche.....11
Modificare le impostazioni di notifica.....11
Rete di protezione in tempo reale.....12
Cos'è la rete di protezione in tempo reale.....12
Vantaggi della rete di protezione in tempo reale.....12
Dati forniti.....13
Protezione della privacy.....14
Come partecipare alla Rete di protezione in tempo reale.....14
Domande relative alla rete di protezione in tempo reale.....15
Come verificare la validità dell'abbonamento.....15
Centro azioni.....15
Attiva un abbonamento.....16

Capitolo 3: Introduzione.....17

Visualizzazione dello stato generale di protezione.....18
Visualizzazione delle statistiche prodotto.....18
Gestione degli aggiornamenti del prodotto.....19
Visualizza versioni database.....19
Modifica le impostazioni di rete mobile.....19
Informazioni su virus e malware.....20
Virus.....20
Spyware.....21
Rootkit.....21
Riskware.....21

Capitolo 4: Protezione del computer dal malware.....23
Come analizzare il computer.....24
Scansione automatica di file.....24
Scansione manuale di file.....26
Scansione della posta elettronica.....29
Visualizzazione dei risultati di scansione.....30
Modalità di esclusione di file dalla scansione.....30
Esclusione di tipi di file.....30
Esclusione di file in base alla posizione.....31
Visualizzazione delle applicazioni escluse.....32
Come utilizzare la quarantena.....32
Visualizzazione degli elementi in quarantena.....33
Ripristino degli elementi in quarantena.....33
Informazioni su DeepGuard.....33
Attivazione o disattivazione di DeepGuard.....34
Consentire le applicazioni bloccate da DeepGuard.....34
Utilizzo di DeepGuard in modalità compatibilità.....34
Cosa fare con gli avvisi di comportamento sospetto 35

Capitolo

1

Installazione

Argomenti:

- *Prima di eseguire la prima installazione*
- *Installazione del prodotto per la prima volta*
- *Installazione e aggiornamento delle applicazioni*
- *Guida in linea e assistenza tecnica*

Prima di eseguire la prima installazione

Grazie per aver scelto F-Secure.

Per installare il prodotto è necessario quanto indicato:

- Il CD di installazione o un pacchetto di installazione. Se si sta utilizzando un netbook senza unità CD, è possibile scaricare il pacchetto di installazione da *www.f-secure.com/netbook*.
- Il codice di abbonamento.
- Una connessione a Internet.

Se si dispone di un prodotto di sicurezza di un altro fornitore, il programma di installazione tenterà di rimuoverlo automaticamente. Se ciò non si verifica, rimuoverlo manualmente.

Nota: Se sul computer sono presenti più account, quando si effettua l'installazione, accedere con i privilegi di amministratore.

Installazione del prodotto per la prima volta

Istruzioni per installare il prodotto.

Seguire le istruzioni indicate per installare il prodotto.

1. Inserire il CD o fare doppio clic sul programma di installazione scaricato.

   Se il CD non si avvia automaticamente, andare a Esplora risorse di Windows, fare doppio clic sull'icona del CD-ROM e poi fare doppio clic sul file di installazione per avviare l'installazione.

2. Seguire le istruzioni sullo schermo.

   - Se il prodotto è stato acquistato su Cd presso un rivenditore, la chiave di abbonamento è situata sulla copertina della guida rapida per l'installazione.
   - Se il prodotto è stato scaricato da F-Secure eStore, la chiave di abbonamento è inclusa nell'email di conferma dell'ordine di acquisto.

   Potrebbe essere necessario riavviare il computer per convalidare l'abbonamento e scaricare gli ultimi aggiornamenti da Internet. Se si sta eseguendo l'installazione da CD, ricordarsi di rimuovere il CD di installazione prima di riavviare il computer.

Installazione e aggiornamento delle applicazioni

Istruzioni per attivare un nuovo abbonamento.

Seguire le istruzioni per attivare il nuovo abbonamento o per installare una nuova applicazione utilizzando il pannello di avvio:

Nota: È possibile trovare l'icona del pannello di avvio sulla barra di sistema di Windows.

1. Sulla barra di avvio, fare clic con il pulsante destro del mouse sull'icona all'estrema destra.
   Si apre un menu a comparsa.
2. Selezionare **Visualizza abbonamenti**
3. In **Abbonamenti**, andare alla pagina **Stato abbonamento** e fare clic su **Attiva abbonamento**.
   Si apre la finestra**Attiva abbonamento**.

4. Immettere il codice di abbonamento per l'applicazione e fare clic su **OK**.
5. Dopo aver convalidato e attivato l'abbonamento, fare clic su **Chiudi**.
6. In **Abbonamenti**, andare alla pagina **Stato di installazione**. Se l'installazione non si avvia automaticamente, seguire queste istruzioni:
   a) Fare clic su **Installa**.
   Si apre la finestra di installazione.
   b) Fare clic su **Avanti**.
   L'applicazione viene scaricata e l'installazione si avvia.
   c) Quando l'installazione è completa, fare clic su **Chiudi**.

Il nuovo abbonament è stato attivato.

Guida in linea e assistenza tecnica

È possibile accedere alla guida in linea del prodotto facendo clic sulla relativa icona oppure premendo F1 in qualsiasi schermata del prodotto.

Dopo aver registrato la licenza, si ha diritto a servizi aggiuntivi come gli aggiornamenti gratuiti del prodotto e l'assistenza per il prodotto. È possibile eseguire la registrazione all'indirizzo *www.f-secure.com/register*.

Capitolo

2

Operazioni preliminari

Argomenti:

- *Come utilizzare gli aggiornamenti automatici*
- *Come visualizzare le operazioni effettuate dal prodotto.*
- *Rete di protezione in tempo reale*
- *Come verificare la validità dell'abbonamento*

Informazioni introduttive sul prodotto.

In questa sezione viene descritto come modificare le impostazioni comuni e come gestire gli abbonamenti attraverso la barra di esecuzione.

Le impostazioni comuni della barra di esecuzione possono essere applicate a tutti i programmi installati sulla barra di esecuzione. Invece di modificare le impostazioni separatamente in ciascun programma, è possibile semplicemente modificare le impostazioni comuni, che verranno quindi utilizzate da tutti i programmi installati.

Le impostazioni comuni della barra di esecuzione comprendono:

- Download consente di visualizzare le informazioni sugli aggiornamenti scaricati e di verificare manualmente se sono disponibili nuovi aggiornamenti.
- Impostazioni di connessione consentono di modificare la modalità di connessione del computer a Internet.
- Notifiche consentono di visualizzare notifiche precedenti e impostare il tipo di notifica che si desidera visualizzare.
- Impostazioni sulla privacy consentono di selezionare se connettere o meno il computer alla rete di protezione in tempo reale.

È anche possibile gestire gli abbonamenti per i programmi installati attraverso la barra di esecuzione.

Come utilizzare gli aggiornamenti automatici

Gli aggiornamenti automatici consentono di tenere il computer aggiornato.

Quando il computer è connesso a Internet, il prodotto scarica automaticamente gli ultimi aggiornamenti. Il traffico di rete viene rilevato non disturbando il normale utilizzo di Internet anche in caso di connessione lenta.

Verifica dello stato di aggiornamento

Visualizzare la data e l'ora dell'ultimo aggiornamento.

Quando gli aggiornamenti automatici sono attivi, il prodotto riceve aggiornamenti automaticamente quando risulta attiva una connessione a Internet.

Per verificare se sono installati gli ultimi aggiornamenti:

1. Sulla barra di avvio, fare clic con il pulsante destro del mouse sull'icona all'estrema destra.
   Viene visualizzato un menu a comparsa.
2. Selezionare **Apri impostazioni comuni**.
3. Selezionare **Aggiornamenti automatici** > **Download**.
4. Fare clic su **Verifica ora**.
   Il prodotto si collega a Internet e verifica la presenza degli ultimi aggiornamenti. Se il prodotto non risulta aggiornato, vengono recuperati gli ultimi aggiornamenti.

   Nota: se per connettersi a Internet si utilizza un modem o una linea ISDN, per cercare gli aggiornamenti è necessario che la connessione sia attiva

Modifica della impostazioni di connessione a Internet

Di norma non è necessario modificare le impostazioni predefinita, ma è possibile configurare la modalità di connessione a Internet del server, in modo da ricevere gli aggiornamenti automaticamente.

Per modificare le impostazioni di connessione a Internet, procedere come segue.

1. Sulla barra di avvio, fare clic con il pulsante destro del mouse sull'icona all'estrema destra.
   Viene visualizzato un menu a comparsa.
2. Selezionare **Apri impostazioni comuni**.
3. Selezionare **Aggiornamenti automatici** > **Connessione**.
4. Nell'elenco **Connessione a Internet**, selezionare la modalità secondo la quale il computer è connesso a Internet.
   - Selezionare **Considera connessione sempre attiva** se si dispone di una connessione di rete permanente.

     Nota: se il computer non dispone di una connessione permanente alla rete ed è impostato per la connessione remota a richiesta, selezionare **Considera connessione sempre attiva** può determinare la creazione di connessioni remote multiple.
   - Selezionare **Rileva connessione** per recuperare gli aggiornamenti solo quando è presente una connessione di rete attiva.
   - Selezionare **Rileva traffico** per scaricare gli aggiornamenti solo quando il prodotto rileva altro traffico di rete.

     Suggerimento: in caso di un'insolita configurazione dell'hardware, selezionando l'impostazione **Rileva connessione** viene rilevata una connessione di rete attiva anche quando tale connessione non è presente. In tal caso selezionare **Rileva traffico**.

5. Nell'elenco **Proxy HTTP**, selezionare se il computer utilizza o meno un *server proxy* per connettersi a Internet.
   - Selezionare **Nessun proxy HTTP** se il computer è connesso direttamente a Internet.
   - Selezionare **Configura manualmente proxy HTTP** per configurare le impostazioni del *Proxy HTTP*.
   - Nell'elenco **Proxy HTTP**, selezionare se il computer utilizza o meno un *server proxy* per la connessione a Internet.

Verificare lo stato della rete della protezione in tempo reale

Il funzionamento ottimale della maggioranza delle funzionalità dipende dalla connettività della rete della protezione in tempo reale.

In caso di problemi di rete o se il firewall blocca il traffico di rete della protezione in tempo reale, viene visualizzato lo stato 'disconnesso'. Se no nsono installate funzionalità che richiedono l'accesso alla rete della protezione in tempo reale, viene visualizzato lo stato 'non in uso'.

Per verificare lo stato, procedere come segue.

1. Sulla barra di avvio, fare clic con il pulsante destro del mouse sull'icona all'estrema destra.
   Viene visualizzato un menu a comparsa.
2. Selezionare **Apri impostazioni comuni**.
3. Selezionare **Aggiornamenti automatici** > **Connessione**.

Nella **rete di protezione in tempo reale**, è possibile visualizzare lo stato corrente della rete di protezione in tempo reale.

Come visualizzare le operazioni effettuate dal prodotto.

È possibile visualizzare le azioni intraprese dal prodotto per proteggere il computer nella pagina **Notifiche**.

Quando si inizia a utilizzare il prodotto, viene visualizzata una notifica. Ad esempio, quando viene rilevato e bloccato un virus. Alcune notifiche possono anche essere inviate dal fornitore di servizi, ad esempio per notificare la disponibilità di nuovi servizi.

Visualizza cronologia notifiche

È possibile visualizzare quali notifiche sono riportate nella cronologia notifiche

Per visualizzare la cronologia delle notifiche:

1. Sulla barra di avvio, fare clic con il pulsante destro del mouse sull'icona all'estrema destra.
   Viene visualizzato un menu a comparsa.
2. Selezionare **Apri impostazioni comuni**.
3. Selezionare **Altro** > **Notifiche**.
4. Fare clic su **Mostra cronologia notifiche**.
   Viene aperto l'elenco della cronologia delle notifiche.

Modificare le impostazioni di notifica

È possibile selezionare il tipo di notifica che deve visualizzare il prodotto.

Per modificare le impostazioni di notifica:

1. Sulla barra di avvio, fare clic con il pulsante destro del mouse sull'icona all'estrema destra.

Viene visualizzato un menu a comparsa.

2. Selezionare **Apri impostazioni comuni**.
3. Selezionare **Altro** > **Notifiche**.
4. Selezionare o annullare la selezione di **Consenti messaggi del programma** per attivare o disattivare i messaggi del programma.

   Quando questa impostazione è attivata, il prodotto visualizzerà notifiche dai programmi installati.
5. Selezionare o annullare la selezione di **Consenti messaggi promozionali** per attivare o disattivare ii messaggi promozionali.
6. Fare clic su **OK**.

Rete di protezione in tempo reale

Il presente documento illustra la rete di protezione in tempo reale, un servizio online di F-Secure Corporation che identifica le applicazioni e i siti Web attendibili garantendo la protezione da malware e dalle minacce dei siti Web.

Cos'è la rete di protezione in tempo reale

La rete di protezione in tempo reale è un servizio online che offre risposte rapide alle ultime minacce basate su Internet.

In qualità di partecipante alla Rete di protezione in tempo reale, è possibile aiutare F-Secure a rafforzare la protezione dalle minacce nuove ed emergenti. La Rete di protezione in tempo reale raccoglie statistiche di applicazioni sconosciute, dannose o sospette e della relativa attività sul dispositivo. Queste informazioni sono anonime e vengono inviate a F-Secure Corporation per l'analisi dei dati combinata. F-Secure utilizza le informazioni analizzate per migliorare la protezione del dispositivo dalle nuove minacce e dai file dannosi.

Funzionamento della rete di protezione in tempo reale

In qualità di partecipante alla Rete di protezione in tempo reale, è possibile fornire informazioni sulle applicazioni e i siti Web sconosciuti e sulle applicazioni dannose nonché sull'utilizzo dei siti Web. La Rete di protezione in tempo reale non tiene traccia dell'attività su Web né raccoglie informazioni sui siti Web già analizzati; inoltre, non raccoglie informazioni sulle applicazioni non dannose installate sul computer.

Se non si desidera fornire i dati, la Rete di protezione in tempo reale non raccoglie informazioni sulle applicazioni intallate o sui siti Web visitati. Tuttavia, è necessario che il prodotto esegua query sui server F-Secure per la reputazione delle applicazioni, dei siti Web dei messaggi e di altri oggetti. La query viene eseguita utilizzando un checksum crittografico in cui lo stesso oggetto di query non viene inviato a F-Secure. F-Secure non tiene traccia dei dati per utente; viene incrementato solo il contatore del file o del sito Web.

Non è possibile bloccare tutto il traffico di rete diretto alla rete di protezione in tempo reale poiché è parte integrante della protezione offerta dal prodotto.

Vantaggi della rete di protezione in tempo reale

La rete di protezione in tempo reale offre una protezione accurata e più rapida dalle nuove minacce senza inviare avvisi non necessari per applicazioni sospette che non sono pericolose.

In qualità di partecipanete alla Rete di protezione in tempo reale, l'utente può contribuire a rilevare i nuovi malware e a eliminare i possibili falsi positivi dal database di definizione dei virus di F-Secure.

Chi contribuisce al servizio della rete di protezione in tempo reale offre aiuto ad altri utenti e viene ricambiato. Quando la rete di protezione individua un'applicazione sospetta sul dispositivo di un utente, quest'ultimo beneficia dei risultati delle analisi condotto al rilevamento della medesima applicazione su altri dispositivi. La rete di protezione in tempo reale migliora le prestazioni generali dei dispositivi, poiché il prodotto per la

sicurezza installato non analizza nuovamente le applicazioni già analizzate e classificate come attendibili dalla rete di protezione in tempo reale. Inoltre, le informazioni sui siti Web pericolosi e sui messaggi di posta indesiderata vengono condivise mediante la rete di protezione in tempo reale e il servizio è così in grado di fornire una protezione più accurata contro le minacce dei siti Web e i messaggi spam.

Quanti più utenti partecipano alla Rete di protezione in tempo reale, tanto meglio vengono protetti i singoli partecipanti.

Dati forniti

In qualità di partecipante alla Rete di distribuzione in tempo reale, l'utente fornisce le informazioni sulle applicazioni memorizzate sul proprio dispositivo e sui siti Web visitati. In questo modo, la Rete di protezione in tempo reale è in grado di proteggere dalle nuove applicazioni dannose e dai siti Web sospetti.

Analisi della reputazione del file

La rete fi protezione in tempo reale raccoglie informazioni solo sulle applicazioni che non dispongono di una reputazione sicura e conosciuta e sui file sospetti o che presumibilmente contengono malware.

La Rete di protezione in tempo reale raccoglie informazioni anonime sulle applicazioni non infette e sospette sul dispositivo. La Rete di protezione in tempo reale raccoglie informazioni solo sui file eseguibili (ad esempio i file Portable Executable sulla piattaforma Windows, con estensioni file .cpl, .exe, .dll, .ocx, .sys, .scr e .drv).

Le informazioni raccolte includono:

- percorso dell'applicazione sul dispositivo
- dimensioni del file con data di creazione o di modifica
- attributi file e provilegi,
- informazioni sulla firma
- versione corrente del file e l'azienda che lo ha creato
- fonte del file o URL di download
- F-Secure DeepGuard i risultati dell'analisi anti-virus sui file sottoposti a scansione e
- altre informazioni simili

La Rete di protezione in tempo reale non raccoglie mai informazioni sui documenti personali, a meno che in essi non siano state trovate infezioni. Per qualsiasi tipi di file dannoso, raccoglie il nome dell'infezione e lo stato di disinfezione del file.

Attraverso la rete di protezione in tempo reale è anche possibile inviare applicazioni sospette (solo file PE) a scopo di analisi. La rete di protezione in tempo reale non raccoglie alcuna informazioni contenuta nei documenti personali che non vengono mai caricati a scopo di analisi.

Invio di file per l'analisi

Con la rete di protezione in tempo reale, è possibile inviare in analisi le applicazioni sospette.

È possibile inviare singole applicazioni sospette manualmente quando il prodotto lo richiede. È possibile inviare solo i file eseguibili portabili. La rete di protezione in tempo reale non carica mai i documenti personali.

Analisi della reputazione del sito Web

La rete di protezione in tempo reale non tiene traccia dell'attività Web degli utenti né raccoglie informazioni sui siti già analizzati. Garantisce che i siti Web visitati siano sicuri durante la navigazione. Quando l'utente visita un sito Web, la rete ne verifica l'attendibilità e notifica l'utente in caso il sito sia stato classificato come sospetto o dannoso.

Se il sito visitato contiene elementi sospetti o pericolosi o una minaccia riconosciuta, la reti di protezione in tempo reale raccoglie l'URL del sito in modo che sia possibile analizzare i contenuti della pagina Web.

Se l'utente visita un sito Web già classificato, la rete di protezione in tempo reale raccoglie il nome di domini e sottodomini e in alcuni casi il percorso della pagina in modo che sia possibile analizzare e classificare tale sito. Tutti i parametri di URL che contengono informazioni riconducibili agli utenti in formato personale vengono rimossi per la privacy.

Nota: La rete di protezione in tempo reale non classifica né analizza le pagine Web delle reti private e pertanto non raccoglie alcuna informazioni relativa agli indirizzi IP delle reti private (ad esempio quelli delle intranet aziendali).

Analisi delle informazioni di sistema

La rete di protezione in tempo reale raccoglie il nome e la versione del sistema operativo, le informazioni sulla connessione Internet e le statistiche di utilizzo della rete di protezione in tempo reale (ad esempio, il numero di volte che è stata richiesta la reputazione del sito Web e la media del tempo impiegato per restituire tali risultati) in modo che sia possibile controllare e migliorare il servizio offerto.

Protezione della privacy

F-Secure trasferisce i dati in modo sicuro rimuovendo automaticamente le informazioni personali in essi contenute.

La Rete di protezione in tempo reale rimuove i dati di identificazione prima di inviarli a F-Secure ed esegue la crittografia di tutte le informazioni raccolte durante il trasferimento, per proteggerle dall'accesso non autorizzato. Le informazioni raccolte non vengono elaborate individualmente, ma raggruppate con le informazioni provenienti da altri partecipanti alla Rete di protezione in tempo reale. Tutti i dati vengono analizzati ai fini della statistica e in maniera anonima, vale a dire che i dati non vengono in alcun modo collegati all'utente.

Qualsiasi informazione in grado di identificare gli utenti viene esclusa dai dati raccolti. La rete di protezione in tempo reale non raccoglie gli indirizzi IP privati o le informazioni personali degli utenti, quali indirizzi e-mail, nomi utente e password. Eventuali dati raccolti non intenzionalmente in grado di identificare gli utenti non verranno utilizzati per raggiungere gli utenti

F-Secure applica rigide misure di protezione e precauzioni fisiche, amministrative e tecniche per proteggere le informazioni raccolte durante il trasferimento, l'archiviazione e l'eleborazione. I dati vengono archiviati in posizioni sicure su server controllati da F-Secure, collocati presso i nostri uffici e quelli degli appaltatori. Solo al personale autorizzato è consentito accedere alle informazioni raccolte.

F-Secure potrebbe condividere le informazioni raccolte, in forma anonima, con società affiliate, distributori e partner.

Come partecipare alla Rete di protezione in tempo reale

Ogni utente può contribuire a migliorare l'affidabilità della rete di protezione in tempo reale fornendo informazioni su programmi e siti Web dannosi.

È possibile scegliere di partecipare alla Rete di protezione in tempo reale durante l'installazione. Con le impostazioni di installazione predefinite, è possibile fornire i dati alla Rete di protezione in tempo reale. È possibile modificare queste impostazioni successivamente nel prodotto.

Per modificare le impostazioni della Rete di protezione in tempo reale, seguire le istruzioni riportate di seguito:

1. Sulla barra di avvio, fare clic con il pulsante destro del mouse sull'icona all'estrema destra.
   Viene visualizzato un menu a comparsa.
2. Selezionare **Apri impostazioni comuni**.
3. Selezionare **Altro** > **Privacy**.
4. Selezionare la casella di controllo relativa alla partecipazione per diventare un partecipante alla Rete di protezione in tempo reale.

Domande relative alla rete di protezione in tempo reale

Recapiti per eventuali domande sulla rete di protezione in tempo reale

Per ulteriori domande sulla rete di protezione in tempo reale, contattare:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finlandia

http://www.f-secure.com/en/web/home_global/support/contact

L'ultima versione del criterio è sempre disponibile sul sito Web di F-Secure

Come verificare la validità dell'abbonamento

Il tipo e lo stato dell'abbonamento vengono mostrati sulla pagina **Stato abbonamento**.

Quando l'abbonamento sta per scadere o se è scaduto, lo stato di protezione globale del programma sull'icona della barra di esecuzione corrispondente cambia.

Per controllare la validità dell'abbonamento:

1. Sulla barra di avvio, fare clic con il pulsante destro del mouse sull'icona all'estrema destra. Viene visualizzato un menu a comparsa.
2. Selezionare **Visualizza abbonamenti**.
3. Selezionare **Stato abbonamento** per visualizzare informazioni sugli abbonamenti per i programmi installati.
4. Selezionare **Stato di installazione** per visualizzare i programmi disponibili da installare.

Sulla pagina **Statistiche** vengono inoltre visualizzati lo stato dell'abbonamento e la data di scadenza. Se l'abbonamento è scaduto, è necessario rinnovarlo per continuare a ricevere gli aggiornamenti e utilizzare il prodotto.

Nota: quando l'abbonamento è scaduto, l'icona di stato del prodotto lampeggia nella barra delle applicazioni.

Centro azioni

Il centro azioni mostra le notifiche importanti che richiedono attenzione.

Se l'abbonamento è scaduto o sta per scadere, il centro azioni invia una notifica. Il colore di sfondo e il contenuto del messaggio del centro azioni dipendono dal tipo di abbonamento e dallo stato:

- Se l'abbonamento sta per scadere e sono disponibili abbonamenti gratuiti, il messaggio presenta uno sfondo bianco e il pulsante **Attiva**.
- Se l'abbonamento sta per scadere e non sono disponibili abbonamenti gratuiti, il messaggio presenta uno sfondo giallo e i pulsanti **Acquista** e **Inserisci codice**. Se è stato già acquistato un nuovo abbonamento, è possibile fare clic sul pulsante **Inserisci codice** per indicare un codice di abbonamento e attivare il nuovo abbonamento.
- Se l'abbonamento è scaduto e sono disponibili abbonamenti gratuiti, il messaggio presenta uno sfondo rosso e il pulsante **Attiva**.

- Se l'abbonamento è scaduto e non sono disponibili abbonamenti gratuiti, il messaggio presenta uno sfondo rosso e i pulsanti **Acquista** e **Inserisci codice**. Se è stato già acquistato un nuovo abbonamento, è possibile fare clic su **Inserisci codice** per fornire il codice di abbonamento e attivare il nuovo abbonamento.

Nota: Il collegamento **Mostra cronologia notifiche** nel centro azioni mostra un elenco di messaggi di notifica dei prodotti e non i messaggi precedenti del centro azioni.

Attiva un abbonamento

Quando si dispone di un nuovo codice di abbonamento o codice campagna per un prodotto, è necessario attivarlo.

Per attivare un abbonamento:

1. Sulla barra di avvio, fare clic con il pulsante destro del mouse sull'icona all'estrema destra.
   Viene visualizzato un menu a comparsa.
2. Selezionare **Visualizza abbonamenti**.
3. Scegliere una delle opzioni indicate:
   - Fare clic su **Attiva abbonamento**.
   - Fare clic su **Attiva codice campagna**.
4. Nella finestra di dialogo che viene aperta, immettere il nuovo codice di abbonamento o il codice campagna e fare clic su **OK**.

   Suggerimento: Se il codice di abbonamento è stato ricevuto via e-mail, è possibile copiarlo dal messaggio e-mail e incollarlo nell'apposito campo.

Dopo aver immesso il nuovo codice di abbonamento, la nuova data di validità dell'abbonamento viene visualizzata nella pagina **Stato abbonamento**.

Capitolo

3

Introduzione

Argomenti:

- *Visualizzazione dello stato generale di protezione*
- *Visualizzazione delle statistiche prodotto*
- *Gestione degli aggiornamenti del prodotto*
- *Informazioni su virus e malware*

Questo prodotto protegge il computer in uso da virus e altre applicazioni dannose.

Il prodotto esegue la scansione di file e analizza applicazioni aggiornandosi automaticamente. Non richiede alcun intervento da parte dell'utente.

Visualizzazione dello stato generale di protezione

La pagina **Stato** mostra la panoramica delle funzionalità del prodotto installate e il loro stato corrente.

Per aprire la pagina **Stato** procedere come segue.

Nella schermata principale, fare clic su **Stato**.

Viene visualizzata la pagina **Stato**.

Le icone mostrano lo stato del programma e delle funzionalità di sicurezza.

Icona di stato	Nome stato	Descrizione
	OK	Il computer è protetto. La funzionalità è attiva e funziona correttamente.
	Informazioni	Il prodotto informa l'utente dello stato speciale di una funzionalità. Ad esempio, la funzionalità è in fase di aggiornamento.
	Avviso	Il computer non risulta completamente protetto. Ad esempio, il prodotto non riceve aggornamenti da molto tempo oppure lo stato di una funzionalità richiede attenzione.
	Errore	Il computer non è protetto Ad esempio, l'abbonamento è scaduto o una funzionalità critica non è attiva.
	Disattivata	Una funzionalità non critica è stata disattivata.

Visualizzazione delle statistiche prodotto

È possibile visualizzare le operazioni effettuate dal programma dal momento dell'installazione nella schermata **Statistiche**.

Per aprire la schermata **Statistiche**:

Nella pagina principale fare clic su **Statistiche**.

Viene visualizzata la pagina **Statistiche**.

- **Ultima verifica aggiornamenti completata** mostra la data e l'ora dell'ultimo aggiornamento

- **Scansione antivirus e antispyware** mostra il numero di file analizzati e disinfettati dal momento dell'installazione.
- In **Applicazioni** viene visualizzato il numero di programmi che DeepGuard ha consentito o bloccato dal momento dell'installazione.
- **Connessioni firewall** mostra il numero di connessioni consentite e bloccate dal momento dell'installazione.
- **Filtro antispam e antiphishing** mostra quanti messaggi e-mail validi sono stati rilevati e quanti invece sono stati classificati come messaggi di spam dal prodotto.

Gestione degli aggiornamenti del prodotto

Il prodotto esegue l'aggiornamento automatico della protezione.

Visualizza versioni database

Nella pagina **Aggiornamenti database** è possibile visualizzare l'ora e i numeri di versione dell'ultimo aggiornamento.

Per aprire la pagina**Aggiornamenti database**:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Selezionare **Altre impostazioni** > **Versioni database**.

La pagina **Versioni database** mostra la data dell'ultimo aggiornamento delle definizioni virus e spyware, di DeepGuard e dei filtri antispam e antiphishing, oltre ai rispettivi numeri di versione.

Modifica le impostazioni di rete mobile

Permette di scegliere se scaricare o meno gli aggiornamenti di protezione quando si utilizza la rete mobile.

Nota: Questa funzionalità è disponibile solo in Microsoft Windows 7.

Per impostazione predefinita, gli aggiornamenti di protezione vengono sempre scaricati quando ci si trova sotto copertura della rete dell'operatore in uso del proprio paese. Tuttavia, gli aggiornamenti vengono sospesi quando ci si trova in un altro paese e si utilizza la rete di un operatore diverso. Ciò avviene in quanto le tariffe di connettività potrebbero variare in base all'operatore e al paese in cui ci si trova. Si consiglia di non modificare questa impostazione in quanto permette di utilizzare meno banda e risparmiare sui costi, quando ci si trova all'estero.

Nota: Questa impostazione riguarda solo le connessioni di rete mobile. Se il computer è collegato a una rete fissa o wireless, gli aggiornamenti vengono scaricati automaticamente.

Per modificare questa impostazione:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Selezionare **Altre impostazioni** > **Banda larga mobile** > **Scarica aggiornamenti della protezione**.
3. Selezionare l'opzione di aggiornamento desiderata per le connnessioni alla rete mobile:

   - **Solo nella rete dell'operatore domestico**

     Quando si utilizza la rete dell'operatore del proprio paese, gli aggiornamenti vengono sempre scaricati. Se si utilizza la rete di un altro operatore all'estero, gli aggiornamenti vengono sospesi. Si consiglia di

selezionare questa opzione per tenere gli aggiornamenti di protezione costantemente aggiornati evitando costi imprevisti.

- **Mai**

  Gli aggiornamenti non vengono scaricati quando si utilizza la banda larga mobile.

- **Sempre**

  Gli aggiornamenti vengono sempre scaricati, indipendentemente dalla rete in uso. Selezionare questa opzione se si desidera tenere costantemente aggiornata la protezione del proprio computer indipendentemente dai costi.

4. Se si desidera operare una scelta ogni volta che si esce dalla rete dell'operatore domestico, selezionare **Richiedi a ogni uscita dalla rete dell'operatore domestico**.

Aggiornamenti di protezione sospesi

Se si utilizza la rete mobile in un paese diverso da quello del proprio operatore, gli aggiornamenti di protezione potrebbero essere sospesi.

In questo caso, viene visualizzata la notifica di **sospensione** nell'angolo inferiore destro dello schermo. Gli aggiornamenti vengono sospesi in quanto i prezzi delle connessioni potrebbero variare tra un operatore e l'altro, ad esempio, a seconda dei paesi. Potrebbe essere utile non modificare questa impostazione se si desidera risparmiare larghezza di banda ed eventualmente anche i costi, durante la visita. Tuttavia, se si desidera modificare questa impostazione, fare clic sul collegamento **Modifica**.

Nota:

Questa funzionalità è disponibile solo in Microsoft Windows 7.

Informazioni su virus e malware

I malware sono programmi progettati appositamente per danneggiare il computer, utilizzandolo per scopi illegali senza che l'utente ne sia consapevole o per sottrarre informazioni dal computer.

I malware possono:

- assumere il controllo del browser Web,
- reindirizzare i tentativi di ricerca,
- mostrare pubblicità indesiderate,
- tenere traccia dei siti Web visitati,
- sottrarre informazioni personali, ad esempio, coordinate bancarie,
- utilizzare il computer per inviare spam,
- utilizzare il computer per attaccare altri computer.

Inoltre, i malware possono rallentare il computer e renderlo instabile. Si può sospettare la presenza di *malware* nel computer se questo improvvisamente diventa molto lento e si blocca spesso.

Virus

I virus normalmente sono programmi in grado di allegarsi ai file e replicarsi ripetutamente; sono in grado di alterare e sostituire i contenuti di altri file in modo da poter danneggiare il computer.

Un *virus* è un programma normalmente installato all'insaputa dell'utente sul computer. Una volta installato, il virus tenta di replicarsi. Il virus:

- utilizza parte delle risorse di sistema del computer,
- può alterare o danneggiare i file nel computer,

- probabilmente tenta di utilizzare il computer per infettarne altri,
- può consentire l'uso del computer per scopi illegali.

Spyware

Gli spyware sono programmi che raccolgono le informazioni personali degli utenti.

I programmi spyware possono raccogliere dati personali, tra cui:

- siti Internet visitati,
- indirizzi di posta elettronica presenti nel computer,
- password,
- numeri di carta di credito.

Quasi sempre, i programmi spyware si installano senza il permesso esplicito dell'utente. Gli spyware potrebbero essere installati insieme a un programma utile o attraverso l'inganno: l'utente potrebbe essere portato a fare clic su un'opzione in una finestra di popup non legittima.

Rootkit

I rootkit sono programmi che rendono difficile il rilevamento di altri *malware*.

I rootkit nascondono file e processi. In genere, lo fanno per nascondere attività dannose per il computer. Quando un rootkit nasconde *malware* non è facile individuarne la presenza sul computer.

Questo prodotto contiene uno scanner per rootkit che analizza specificamente la presenza di rootkit, per impedire ai *malware* di nascondersi.

Riskware

I riskware non sonoprogettati specificamente per danneggiare il computer, ma potrebbe farlo se utilizzato in modo scorretto.

Un riskware non è propriamente un malware. I programmi riskware eseguono operazioni utili ma potenzialmente pericolose.

Esempi di riskware:

- programmi di messaggistica istantanea come IRC (Internet relay chat),
- programmi per il trasferimento di file su Internet da un computer a un altro,
- programmi di telefonia Internet (VoIP, *Voice over Internet Protocol*).
- Software di accesso remoto, come VNC,
- scareware, che potrebbero indurre l'utente ad acquistare software di protezione fasulli o
- software progettati per ignorare le verifiche CD o le protezioni alle copie di CD.

Se il programma è stato installato esplicitamente e impostato correttamente, è improbabile che risulti dannoso.

Se il riskware è stato installato all'insaputa dell'utente, è molto probabile che abbia scopi dannosi e andrebbe eliminato.

Capitolo

4

Protezione del computer dal malware

Argomenti:

- *Come analizzare il computer*
- *Modalità di esclusione di file dalla scansione*
- *Come utilizzare la quarantena*
- *Informazioni su DeepGuard*

La scansione antivirus e antispyware protegge il computer dai programmi che possono trafugare informazioni personali, danneggiare il server o utilizzarlo a scopi illegali.

Per impostazione predefinita, tutti i tipi di malware vengono gestiti non appena rilevati, in modo che non possano causare danni.

Per impostazione predefinita, la scansione antivirus e antispyaware analizza automaticamente le unità disco locali, i supporti multimediali rimovibili (come CD e unità portatili) e il contenuto scaricato. È possibile impostare la scansione automatica della posta elettronica.

La scansione antivirus e antispyware verifica anche eventuali modifiche apportate al sistema che potrebbero indicare al presenza di *malware*. Se si verificano eventuali modifiche al sistema pericolose, ad esempio alle impostazioni di sistema, o modifiche ai processi di sistema, DeepGuard impedisce l'esecuzione del programma, poiché molto probabilmente si tratta di *malware*.

Come analizzare il computer

Quando la Scansione antivirus e antispyware è attiva, analizza il computer in automatico alla ricerca di file dannosi. È anche possibile eseguire la scansione manuale dei file e impostare scansioni pianificate.

Si consiglia di lasciare sempre attiva la Scansione antivirus e antispyware. L'utente può eseguire la scansione manuale dei file quando lo desidera per assicurarsi che non vi siano file dannosi nel computer in uso o per analizzare file che sono stati esclusi dalla scansione in tempo reale.

Impostando una scansione pianificata, la Scansione antivirus e antispyware rimuove file dannosi dal computer in uso a orari prestabiliti.

Scansione automatica di file

La scansione in tempo reale protegge il computer eseguendo la scansione di tutti i file all'accesso e bloccando l'accesso ai file contenenti *malware*.

Quando il computer in uso cerca di accedere a un file, la Scansione in tempo reale lo analizza per rilevare la presenza di malware prima di consentire al computer di accedervi. Se la Scansione in tempo reale rileva contenuti dannosi, mette il file in quarantena prima che possa causare danni.

La scansione in tempo reale influisce sulle prestazioni del computer?

Normalmente, il processo di scansione non viene rilevato dall'utente perché richiede una quantità ridotta di tempo e di risorse di sistema. La quantità di tempo e di risorse di sistema necessaria per la scansione in tempo reale dipende, ad esempio, da contenuti, posizione e tipo di file.

File la cui scansione richiede più tempo:

- File su unità rimovibili, quali CD, DVD e unità USB portatili.
- File compressi, ad esempio i file *.zip*.

  Nota: Per impostazione predefinita, i file compressi non vengono sottoposti a scansione.

La scansione in tempo reale può rallentare il computer se:

- si possiede un computer che non soddisfa i requisiti di sistema oppure
- si accede contemporaneamente a numerosi file. Ad esempio, quando si apre una directory contenente molti file che devono essere analizzati.

Attivazione o disattivazione della scansione in tempo reale

Lasciare attiva la scansione in tempo reale per arrestare il *malware* prima che possa danneggiare il computer in uso.

Per attivare o disattivare la scansione in tempo reale:

1. Nella schermata principale, fare clic su **Stato**.
2. Fare clic su **Modifica impostazioni su questa pagina**.

   Nota: È necessario disporre di diritti amministrativi per disattivare le funzionalità di protezione.

3. Attivare o disattivare la **Scansione antivirus e antispyware**.
4. Fare clic sul link **Chiudi**.

Gestione automatica dei file dannosi

La scansione in tempo reale è in grado di gestire automaticamente i file dannosi senza richiedere l'intervento dell'utente.

Per lasciare che la scansione in tempo reale gestisca automaticamente i file dannosi:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Selezionare **Protezione del computer** > **Scansione antivirus e antispyware**.
3. Selezionare **Gestisci automaticamente file dannosi**.

Se si sceglie di non gestire automaticamente i file dannosi, la scansione in tempo reale chiede se si desidera analizzare un file dannoso al momento del rilevamento.

Gestione dello spyware

La Scansione antivirus e antispyware blocca lo spyware immediatamente durante il tentativo di avvio.

Prima che un'applicazione spyware venga avviata, il prodotto la blocca consentendo all'utente di decidere quale azione intraprendere.

Quando viene rilevato uno spyware, scegliere una delle seguenti azioni:

Azione da eseguire.	Operazioni eseguite sullo spyware
Gestisci automaticamente	Lasciare decidere al prodotto l'azione migliore da intraprendere, in base al tipo di spyware rilevato.
Mettere lo spyware in quarantena	Spostare lo spyware nella quarantena, dove non può danneggiare il computer in uso.
Eliminare lo spyware	Rimuovere tutti i file con contenuti spyware dal computer in uso.
Bloccare solo lo spyware	Bloccare l'accesso allo spyware senza rimuoverlo dal computer in uso.
Escludere lo spyware dalla scansione	Consentire l'esecuzione dello spyware escludendolo dalla scansione in futuro.

Gestione del riskware

La Scansione antivirus e antispyware blocca il riskware immediatamente durante il tentativo di avvio.

Prima che un'applicazione riskware venga avviata, il prodotto la blocca consentendo all'utente di decidere quale azione intraprendere.

Quando viene rilevato un riskware, scegliere una delle seguenti azioni:

Azione da eseguire.	Operazioni eseguite sul riskware
Bloccare solo il riskware	Bloccare l'accesso al riskware senza rimuoverlo dal computer in uso.
Mettere il riskware in quarantena	Spostare il riskware nella quarantena, dove non può danneggiare il computer in uso.
Eliminare il riskware	Rimuovere tutti i file con contenuti riskware dal computer in uso.
Escludere il riskware dalla scansione	Consentire l'esecuzione del riskware escludendolo dalla scansione in futuro.

Rimozione automatica dei cookie di tracciamento

Rimuovendo i cookie di tracciamento, i siti Web non sono più in grado di tenere traccia dei siti Internet visitati.

I cookie di tracciamento sono file di piccole dimensioni che consentono ai siti Web di registrare i siti visitati. Per mantenere i cookie di tracciamento disattivati nel computer in uso, seguire le seguenti istruzioni:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Selezionare **Protezione del computer** > **Scansione antivirus e antispyware**.
3. Selezionare **Rimuovi cookie di tracciamento**.
4. Fare clic su **OK**.

Scansione manuale di file

È possibile eseguire la scansione manuale di file, ad esempio quando si connette al proprio computer un dispositivo esterno, per assicurarsi che questo non contenga malware.

Avvio della scansione manuale

È possibile analizzare l'intero computer per la ricerca di un *malware* specifico o eseguire la scansione di un determinato percorso.

Se si sospetta la presenza di uno specifico tipo di *malware* è possibile limitarsi ad analizzare questo. Se si sospetta dell'integrità di una data posizione nel computer, è possibile analizzare solo questa. Le scansioni richiederanno molto meno tempo rispetto a una scansione dell'intero computer.

Per avviare una scansione manuale del computer:

1. Nella pagina principale, fare clic sulla freccia sotto **Analizza**.

   Vengono visualizzate le opzioni di scansione.

2. Selezionare il tipo di scansione.

   Selezionare **Modifica impostazioni di scansione** per ottimizzare la modalità di scansione manuale di virus e altre applicazioni dannose nel computer in uso.

3. Se è selezionato **Scegliere gli elementi da analizzare**, viene visualizzata una finestra in cui è possibile selezionare il percorso da analizzare.
   Viene visualizzata la **Scansione guidata**.

Tipi di scansione

È possibile analizzare l'intero computer o cercare un particolare tipo di malware o analizzare un determinato percorso.

Segue l'elenco dei diversi tipi di scansione:

Tipo di scansione	File analizzati	Utilizzo consigliato
Scansione antivirus e antispyware	Parti del computer alla ricerca di virus, spyware e riskware	Questo tipo di scansione risulta più rapido di una scansione completa. Esegue la ricerca di malware solo in determinate parti del computer che contengono file installati. Questo tipo di scansione è consigliato se si desidera verificare rapidamente che il computer sia al riparo da malware e, qualora presenti, eliminarli.
Scansione completa del computer	Tutto il computer (dischi interni ed esterni) alla ricerca di virus, spyware e riskware	Quando si vuole avere certezza assoluta dell'assenza di malware o riskware nel computer. Questo tipo di scansione richiede tempi più lunghi rispetto agli altri. Prevede una scansione antimalware rapida e l'analisi del disco fisso. Controlla anche la presenza di elementi che potrebbero celare da un rootkit.

Tipo di scansione	File analizzati	Utilizzo consigliato
Scegliere gli elementi da analizzare	Un file o un'unità specifica alla ricerca di virus, spyware e riskware	Quando si sospetta che un determinato percorso sul computer contenga malware, ad esempio nel caso in cui quel percorso sia stato la destinazione di file scaricati da fonti potenzialmente pericolose, quali reti di condivisione per file peer-to-peer. I tempi della scansione dipendono dalle dimensioni della cartella analizzata. La scansione si conclude velocemente se, ad esempio, la cartella da analizzare contiene un numero ridotto di file di piccole dimensioni.
Scansione antirootkit	Le parti fondamentali del sistema, dove un elemento sospetto può rappresentare un problema di sicurezza Esegue la scansione di file , cartelle, unità o processi nascosti	Quando si sospetta che sul computer sia stato installato un rootkit. Ad esempio, se è stata rilevata da poco la presenza di un malware e si desidera avere la sicurezza che non abbia installato un rootkit.

Scansione in Esplora risorse

È possibile analizzare dischi, cartelle e file per individuare eventuali *virus*, *spyware* e *riskware* in Esplora risorse.

Per analizzare un disco, una cartella o un file:

1. Selezionare con il pulsante destro del mouse il disco, la cartella o il file da analizzare.
2. Dal menu visualizzato con il pulsante destro del mouse, selezionare **Analizza cartelle per ricerca virus** (il nome dell'opzione dipende dall'oggetto dell'analisi).
   Si apre la finestra **Scansione guidata** e l'analisi comincia.

Se viene individuato un *virus* o *spyware*, la **Scansione guidata** indica le operazioni da eseguire per effettuare le pulizia.

Selezione di file da analizzare

Selezionare i tipi di file in cui analizzare la presenza di *virus* e *spyware* nelle scansioni manuali o pianificate.

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Selezionare **Altre impostazioni** > **Scansione manuale**.
3. In **Opzioni di scansione**, selezionare le seguenti impostazioni:

Analizza solo i tipi di file conosciuti Per eseguire la scansione solo dei tipi di file che più probabilmente sono infetti, ad esempio, i file eseguibili. Questa opzione consente anche di rendere più veloce la scansione. Saranno sottoposti a scansione i file con le seguenti estensioni: `.ani`, `.asp`, `.ax`, `.bat`, `.bin`, `.boo`, `.chm`, `.cmd`, `.com`, `.cpl`, `.dll`, `.doc`, `.dot`, `.drv`, `.eml`, `.exe`, `.hlp`, `.hta`, `.htm`, `.html`, `.htt`, `.inf`, `.ini`, `.job`, `.js`, `.jse`, `.lnk`, `.lsp`, `.mdb`, `.mht`, `.mpp`, `.mpt`, `.msg`, `.ocx`, `.pdf`, `.php`, `.pif`, `.pot`, `.ppt`, `.rtf`, `.scr`, `.shs`, `.swf`, `.sys`, `.td0`, `.vbe`, `.vbs`, `.vxd`, `.wbk`, `.wma`, `.wmv`, `.wmf`, `.wsc`, `.wsf`, `.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2` e `.hqx`.

Analizza i file compressi	Per analizzare file e cartelle di archivio procedere come segue.
Utilizza euristica avanzata	Per utilizzare l'euristica disponibile durante la scansione per individuare al meglio malware nuovi o sconosciuti. **Nota:** Se si seleziona questa opzione, la scansione dura più a lungo e restituisce una maggiore quantità di falsi positivi (file innocui indicati come pericolosi).

4. Fare clic su **OK**.

Nota: I file nell'elenco degli elementi esclusi non vengono analizzati anche se qui sono stati selezionati per la scansione.

Cosa fare in caso di rilevamento di file dannosi

Selezionare la modalità di gestione dei file dannosi in caso di rilevamento.

Per selezionare l'azione da intraprendere in caso di rilevamento di contenuti dannosi durante la scansione manuale:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Selezionare **Altre impostazioni** > **Scansione manuale**.
3. Alla voce **Quando virus o spyware vengono rilevati**, scegliere una delle seguenti opzioni:

Opzione	Descrizione
Chiedi (opzione predefinita)	È possibile selezionare l'azione da intraprendere per ogni elemento rilevato durante la scansione manuale.
Pulisci i file	Il prodotto cerca di disinfettare automaticamente i file infetti rilevati durante la scansione manuale. **Nota:** Se il prodotto non riesce a pulire il file infetto, questo viene messo in quarantena (tranne in caso di rilevamento in rete o su unità rimovibile), per evitare che danneggi il computer in uso.
Metti file in quarantena	Il prodotto sposta eventuali file dannosi rilevati durante la scansione manuale nella quarantena, dove non possono danneggiare il computer.
Elimina file	Il prodotto elimina eventuali file dannosi rilevati durante la scansione manuale.
Crea solo rapporto.	Il prodotto lascia intatti eventuali file dannosi rilevati durante la scansione manuale, registrandone il rilevamento nel rapporto di scansione. **Nota:** Se la scansione in tempo reale è disattivata, eventuali malware sono sempre in grado di danneggiare il computer se si seleziona questa opzione.

Nota: In caso di rilevamento di file dannosi durante la scansione pianificata, la pulizia viene eseguita in automatico.

Pianificazione di una scansione

Impostare il computer in modo che analizzi e rimuova automaticamente virus e altre applicazioni dannose quando non viene utilizzato. In alternativa, impostare l'esecuzione periodica della scansione per rassicurarsi che il computer sia pulito.

Per pianificare una scansione:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Selezionare **Altre impostazioni** > **Scansione programmata**.
3. Attivare la **Scansione pianificata**.
4. Selezionare quando si desidera avviare la scansione.

Opzione	Descrizione
Ogni giorno	Eseguire quotidianamente la scansione del computer in uso.
Ogni settimana	Eseguire la scansione del computer in uso in determinati giorni della settimana selezionandoli dall'elenco.
Ogni mese	Eseguire la scansione del computer in uso in determinati giorni del mese. Per selezionarli: 1. Selezionare una delle opzioni **Giorno**. 2. Selezionare il giorno del mese dall'elenco accanto al giorno selezionato.

5. Selezionare quando si desidera avviare la scansione nei giorni selezionati.

Opzione	Descrizione
Ora di inizio	Avviare la scansione all'ora prestabilita.
Con computer sia inattivo da	Avviare la scansione dopo che il computer è rimasto inutilizzato per il periodo di tempo specificato.

La scansione pianificata utilizza le impostazioni di quella manuale durante l'analisi. Tuttavia, differisce da questa poiché analizza sempre gli archivi e pulisce automaticamente i file dannosi.

Scansione della posta elettronica

La scansione della posta elettronica protegge l'utente dalla ricezione di file dannosi presenti nelle e-mail.

Per rilevare virus all'interno delle e-mail, la scansione antivirus e antispyware deve essere attiva.

Per attivare la scansione e-mail:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Selezionare **Protezione del computer** > **Scansione antivirus e antispyware**.
3. Selezionare **Rimuovi allegati e-mail dannosi**.
4. Fare clic su **OK**.

Quando vengono analizzati messaggi e-mail e allegati

La scansione antivirus e antispyware è in grado di rimuovere contenuti dannosi dalle e-mail ricevute.

La scansione antivirus e antispyware rimuove messaggi e-mail dannosi ricevuti da programmi di posta elettronica quali Microsoft Outlook e Outlook Express, Microsoft Mail o Mozilla Thunderbird. Analizza i messaggi e gli allegati e-mail non crittografati ogni volta che il programma li riceve dal server di posta elettronica utilizzando il procollo POP3.

La scansione antivirus e antispyware non è in grado di analizzare messaggi e-mail nella posta sul Web, come Hotmail, Yahoo! mail o Gmail. Si è comunque protetti dai *virus* anche se non si rimuovono gli allegati dannosi o se si utilizza la posta sul Web. Quando si aprono allegati e-mail, la scansione in tempo reale rimuove eventuali allegati dannosi prima che possano causare danni.

Nota: La scansione in tempo reale protegge solo il computer in uso ma non gli altri utenti. Tale scansione non analizza i file allegati prima che questi vengano aperti. Ciò significha che se si utilizza la posta sul Web e si inoltra un messaggio prima di aprirne l'allegato, si potrebbe inoltrare una e-mail infetta ad altri utenti.

Visualizzazione dei risultati di scansione

La cronologia virus e spyware mostra tutti i file dannosi rilevati dal prodotto.

A volte, quando viene rilevato un contenuto dannoso, il prodotto non riesce a eseguire l'azione selezionata. Ad esempio, se si seleziona la pulizia dei file e uno di questi non può essere pulito, il prodotto lo sposta nella quarantena. Questi dati possono essere visualizzati nella cronologia virus e spyware.

Per visualizzare la cronologia:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Selezionare **Protezione del computer** > **Scansione antivirus e antispyware**.
3. Fare clic su **Visualizza cronologia di rimozione**.

La cronologia virus e spyware mostra i seguenti dati:

- data e ora di rilevamento del file dannoso,
- nome del malware e relativo percorso all'interno del computer in uso e
- azione eseguita.

Modalità di esclusione di file dalla scansione

A volte l'utente potrebbe voler escludere alcuni file o applicazioni dalla scansione. Gli elementi esclusi non vengono analizzati se prima non vengono rimossi dall'elenco degli elementi esclusi.

Nota: Gli elenchi di esclusione sono separati per la scansione manuale e in tempo reale. Ad esempio, se un file viene escluso dalla scansione in tempo reale, viene comunque analizzato durante la scansione manuale a meno che non venga escluso dal relativo elenco.

Esclusione di tipi di file

Quando vengono esclusi in base al tipo, i file con determinate estensioni non vengono analizzati alla ricerca di contenuti dannosi.

Per aggiungere o rimuovere tipi di file che si desidera escludere:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Scegliere se si desidera escludere il tipo di file dalla scansione in tempo reale o da quella manuale:
   - Selezionare **Protezione del computer** > **Scansione antivirus e antispyware** per escludere il tipo di file dalla scansione in tempo reale.
   - Selezionare **Altre impostazioni** > **Scansione manuale** per escludere il tipo di file dalla scansione manuale.
3. Fare clic su **Escludi file dalla scansione**.
4. Per escludere un tipo di file:
   a) selezionare la scheda **Tipi di file**.
   b) Selezionare **Escludi file con queste estensioni**.
   c) Immettere un'estensione che identifichi il tipo di file da escludere nel campo accanto al pulsante **Aggiungi**.

      Per specificare i file privi di estensione, immettere ".". È possibile utilizzare il carattere jolly "?" per rappresentare un singolo carattere qualsiasi, oppure "*" per rappresentare qualsiasi numero di caratteri.

      Ad esempio, per escludere i file eseguibili, immettere exe nel campo.
   d) Fare clic su **Aggiungi**.
5. Ripetere il passo precedente per tutte le altre estensioni da escludere dalla scansione antivirus.
6. Fare clic su **OK** per chiudere la finestra di dialogo **Escludi dalla scansione**.
7. Fare clic su **OK** per applicare le nuove impostazioni.

I tipi di file selezionati vengono esclusi dalle scansioni future.

Esclusione di file in base alla posizione

Quando vengono esclusi in base al percorso, i file in determinate unità o cartelle non vengono analizzati alla ricerca di contenuti dannosi.

Per aggiungere o rimuovere i percorsi di file che si desidera escludere:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.
2. Scegliere se si desidera escludere il percorso dalla scansione in tempo reale o da quella manuale:
   - Selezionare **Computer** > **Scansione antivirus e antispyware** per escludere il percorso dalla scansione in tempo reale.
   - Selezionare **Computer** > **Scansione manuale** per escludere il percorso dalla scansione manuale.
3. Fare clic su **Escludi file dalla scansione**.
4. Per escludere un file, un'unità o una cartella:
   a) selezionare la scheda **Oggetti**.
   b) Selezionare **Escludi oggetti (file, cartelle, ...)**.
   c) Fare clic su **Aggiungi**.
   d) Selezionare il file, l'unità o la cartella da escludere dalla scansione antivirus.

      Nota: alcune unità possono essere rimovibili, ad esempio CD, DVD o unità di rete. Le unità di rete e le unità rimovibili vuote non possono essere escluse.

   e) Fare clic su **OK**.
5. Ripetere il passaggio precedente per escludere altri file, unità, o cartelle dalla scansione.
6. Fare clic su **OK** per chiudere la finestra di dialogo **Escludi dalla scansione**.
7. Fare clic su **OK** per applicare le nuove impostazioni.

Le cartelle, le unità e i file selezionati vengono esclusi dalle scansioni future.

Visualizzazione delle applicazioni escluse

È possibile visualizzare le applicazioni che sono state escluse dalla scansione e rimuoverle dall'elenco degli elementi esclusi se si desidera analizzarle in futuro.

Se la scansione in tempo reale o quella manuale rilevano un'applicazione che opera come un spyware o un riskware ma che l'utente ritiene sicura, egli può escluderla dall'analisi, in modo tale che il prodotto non visualizzi più avvisi a tale riguardo.

Nota: Un'applicazione non può essere esclusa se opera come un virus o un software dannoso.

È possibile escludere direttamente le applicazioni. Le applicazioni nuove vengono visualizzate nell'elenco di esclusione se escluse dall'utente durante la scansione.

Per visualizzare le applicazioni escluse dalle scansioni:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Scegliere se si desidera visualizzare le applicazioni che sono state escluse dalla scansione in tempo reale o da quella manuale:
   - Selezionare **Computer** > **Scansione antivirus e antispyware** per visualizzare le applicazioni che sono state escluse dalla scansione in tempo reale.
   - Selezionare **Computer** > **Scansione manuale** per visualizzare le applicazioni che sono state escluse dalla scansione manuale.
3. Fare clic su **Escludi file dalla scansione**.
4. Selezionare la scheda **Applicazioni**.

   Nota: è possibile escludere soltanto le applicazioni spyware e riskware, non i virus.

5. Se si desidera analizzare nuovamente un'applicazione esclusa:
   a) Selezionare l'applicazione che si desidera includere nella scansione.
   b) Fare clic su **Rimuovi**.
6. Fare clic su **OK** per chiudere la finestra di dialogo **Escludi dalla scansione**.
7. Fare clic su **OK** per uscire.

Come utilizzare la quarantena

La quarantena è un archivio sicuro per i file potenzialmente pericolosi.

I file in quarantena non possono diffondersi o provocare alcun danno al computer.

Il prodotto può spostare in quarantena *malware*, *spyware* e *riskware* in modo da renderli innocui. È possibile ripristinare le applicazioni o i file dalla quarantena in un secondo momento, se necessario.

Se un elemento in quarantena non è necessario, è possibile eliminarlo. L'eliminazione di un elemento in quarantena causa la rimozione definitiva dell'elemento dal computer.

- In generale, è possibile eliminare i *malware* in quarantena.
- Nella maggior parte dei casi, è possibile eliminare lo *spyware* in quarantena. C'è la possibilità che lo *spyware* in quarantena faccia parte di un programma software legale e che la sua rimozione impedisca il

corretto funzionamento del programma. Per tenere il programma sul computer, è possibile ripristinare lo *spyware* dalla quarantena.

- Il *riskware* in quarantena può essere un programma software legale. Se il programma è stato installato e impostato dall'utente, è possibile ripristinarlo dalla quarantena. Se il *riskware* è stato installato all'insaputa dell'utente, è molto probabile che sia stato inserito con intenti dannosi e andrebbe eliminato.

Visualizzazione degli elementi in quarantena

È possibile visualizzare ulteriori informazioni sugli elementi in quarantena.

Per visualizzare informazioni dettagliate sugli elementi in quarantena:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Selezionare **Protezione del computer** > **Scansione antivirus e antispyware**.
3. Fare clic su **Visualizza quarantena**.
   La pagina **Quarantena** mostra il numero totale degli elementi memorizzati in quarantena.
4. Per visualizzare informazioni dettagliate sulle voci nella quarantena, fare clic su **Dettagli**.

   È possibile ordinare il contenuto in base al nome del malware o al percorso file.

   Verrà visualizzato un elenco dei primi 100 elementi con il tipo di quarantena, il nome e il percorso di installazione originale.
5. Per ulteriori informazioni sugli elementi in quarantena, fare clic sull'icona accanto all'elemento della colonna **Stato**.

Ripristino degli elementi in quarantena

È possibile ripristinare elementi dalla quarantena quando si rendono necessari.

È possibile ripristinare applicazioni o file dalla quarantena quando si rendono necessari. Non ripristinare alcun elemento dalla quarantena se non si è certi che non rappresenti una minaccia. Gli elementi ripristinati vengono riportati alla posizione originale nel computer.

Ripristino degli elementi in quarantena

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Selezionare **Protezione del computer** > **Scansione antivirus e antispyware**.
3. Fare clic su **Visualizza quarantena**.
4. Selezionare gli elementi in quarantena da ripristinare.
5. Fare clic su **Ripristina**.

Informazioni su DeepGuard

DeepGuard analizza il contenuto dei file e il comportamento delle applicazioni, monitorando quelle non attendibili.

DeepGuard blocca *virus* e *worm* nuovi e non ancora scoperti. Blocca inoltre applicazioni pericolose che cercano di apportare modifiche al computer in uso ed evita a quelle sospette di accedere a Internet.

Quando DeepGuard rileva una nuova applicazione che cerca di apportare modifiche potenzialmente dannose al sistema, ne consente l'esecuzione in un'area sicura, in cui questa non può danneggiare il computer.

DeepGuard analizza poi le modifiche che ha cercato di apportare e, in base a ciò, valuta la possibilità che si tratti di *malware*. Se vi è la possibilità che l'applicazione sia un *malware*, DeepGuard la blocca.

Le modifiche potenzialmente dannose al sistema rilevate da DeepGuard includono:

- modifiche alle impostazioni di sistema (registro di configurazione di Windows),
- tentativi di disattivare programmi di sistema importanti, ad esempio programmi di sicurezza come questo prodotto,
- tentativi di modifica di file di sistema importanti.

Attivazione o disattivazione di DeepGuard

Lasciare attivo DeepGuard per evitare che applicazioni sospette possano apportare modifiche potenzialmente dannose al sistema del computer in uso.

Se si utilizza Windows XP, assicurarsi che Service Pack 2 sia installato prima di attivare DeepGuard.

Per attivare o disattivare Deepguard:

1. Nella schermata principale, fare clic su **Stato**.
2. Fare clic su **Modifica impostazioni su questa pagina**.

   Nota: È necessario disporre di diritti amministrativi per disattivare le funzionalità di protezione.

3. Attivare o disattivare **DeepGuard**.
4. Fare clic sul link **Chiudi**.

Consentire le applicazioni bloccate da DeepGuard

È possibile controllare le applicazioni consentite e bloccate da DeepGuard.

A volte DeepGuard potrebbe bloccare l'esecuzione di un'applicazione sicura, anche se l'utente la ritiene tale e desidera utilizzarla. Ciò si verifica perché l'applicazione cerca di apportare modifiche potenzialmente dannose al sistema. L'utente potrebbe inoltre averla bloccata involontariamente quando è stato visualizzato un popup di DeepGuard.

Per consentire un'applicazione bloccata da DeepGuard:

1. Nella pagina principale, fare clic su **Strumenti**.
2. Fare clic su **Applicazioni**.
   Viene visualizzato l'elenco **Applicazioni monitorate**.
3. Individuare l'applicazione che si desidera consentire.

   Nota: È possibile fare clic sull'intestazione delle colonne per ordinare l'elenco. Ad esempio, fare clis sulla colonna **Autorizzazione** per ordinare l'elenco in gruppi di programmi consentiti e negati.

4. Selezionare **Consenti** nella colonna **Autorizzazione**.
5. Fare clic sul link **Chiudi**.

DeepGuard consente nuovamente all'applicazione di apportare modifiche al sistema.

Utilizzo di DeepGuard in modalità compatibilità

Per la massima protezione, DeepGuard modifica temporaneamente i programmi in esecuzione. Alcuni programmi verificano di non essere danneggiati o di non aver subito modifiche e potrebbero non essere compatibili con questa funzionalità. Ad esempio, i giochi online con strumenti anti-cheat verificano di non essere stati modificati in alcun modo quando vengono eseguiti. In questi casi, è possibile attivare la modalità compatibilità.

Per attivare la modalità compatibilità:

1. Nella pagina principale fare clic su **Impostazioni**.

   Nota: È necessario disporre di diritti amministrativi per modificare le impostazioni.

2. Selezionare **Protezione del computer** > **DeepGuard**.
3. Selezionare **Utilizza modalità compatibilità**.
4. Fare clic su **OK**.

Cosa fare con gli avvisi di comportamento sospetto

DeepGuard monitora le applicazioni non attendibili. Se un'applicazione monitorata cerca di accedere a Internet, di apportare modifiche al sistema o si comporta in modo sospetto, DeepGuard la blocca.

Una volta selezionata l'opzione **Avvisa in caso di comportamento sospetto** nelle impostazioni di DeepGuard, quest'ultimo invia una notifica in caso di rilevamento di applicazioni potenzialmente dannose o quando l'utente avvia un'applicazione dalla reputazione sconosciuta.

Per decidere l'azione da intraprendere con l'applicazione bloccata da DeepGuard:

1. Fare clic su **Dettagli** per visualizzare ulteriori informazioni sul programma.
   La sezione Dettagli mostra:
   - il percorso dell'applicazione,
   - la reputazione dell'applicazione nella Rete di protezione in tempo reale e
   - il grado di frequenza dell'applicazione.
2. Decidere se ritenere attendibile l'applicazione bloccata da DeepGuard:
   - Scegliere **Applicazione attendibile. Consenti di continuare.** se non si desidera bloccare l'applicazione.

     È più probabile che un'applicazione sia sicura se:
     - DeepGuard ha bloccato l'applicazione in risposta a un'azione intrapresa dall'utente,
     - l'utente riconosce l'applicazione oppure
     - l'applicazione proviene da una fonte attendibile.
   - Scegliere **Applicazione non attendibile. Mantieni bloccata.** se si desidera continuare a bloccare l'applicazione.

     È meno probabile che l'applicazione sia sicura se:
     - il grado di frequenza dell'applicazione è basso,
     - l'applicazione ha una reputazione sconosciuta oppure
     - l'utente non riconosce l'applicazione.
3. Se si desidera inviare un'applicazione sospetta per farla esaminare:
   a) Fare clic su **Segnala applicazione a F-Secure**.
   Il prodotto mostra le condizioni di invio.
   b) Fare clic su **Accetta** se si accettano le condizioni e si desidera inviare il campione.

   Si consiglia di inviare un campione quando:
   - DeepGuard blocca un'applicazione che l'utente riconosce come sicura oppure
   - l'utente sospetta che l'applicazione potrebbe essere un *malware*.