

Premessa

Questo documento fornisce le indicazioni iniziali per aiutare l'utente a comprendere i concetti e le operazioni di base di Outpost Firewall Pro 2009. Questa guida contiene anche le modalità principali che l'utente può utilizzare per personalizzare Outpost Firewall Pro secondo le sue esigenze.

Indice

1	Installare e Registrare Outpost Firewall	4
1.1	Requisiti di Sistema	4
1.2	Installare Outpost Firewall Pro	4
1.3	Registrare Outpost Firewall Pro	10
2	Intercaccia Utente e Controlli di Base	12
2.1	La Barra degli Strumenti	13
2.2	Il Pannello di Sinistra e il Pannello delle Informazioni	13
2.3	System Tray Icon	15
	L'Icona nella System Tray	15
2.4	Linguaggio Interfaccia	16
3	Configurazione di Base	17
3.1	Avviare e terminare la Protezione	17
3.2	Gestire lo Stato della Protezione	19
3.2	Selezionare il Livello di Protezione del Firewall	20
3.2.1	Avviare in Modalità Regole Assistite	22
3.2.2	Smart Advisor	24
3.3	Avviare in Modalità Auto-Apprendimento	24
3.4	Avviare in modalità Intrattenimento	25
3.5	Proteggere la Configurazione con una Password	25
4	Aggiornare Outpost Firewall Pro	27
4.1	Configurare gli Aggiornamenti	27
4.2	Agnitum ImproveNet	29
5	Effettuare un Controllo del Sistema	31
5.1	Selezionare il Tipo di Controllo	31
5.2	Controllare Percorsi Specifici	32
5.3	Rimuovere il Malware Rilevato	32
5.4	Visualizzare i Risultati del Controllo	34
6	Disinstallare Outpost Firewall Pro	35
7	Risoluzioni Problemi	36
	Informazioni su Agnitum	37

1 Installare e Registrare Outpost Firewall

1.1 Requisiti di Sistema

Outpost Firewall Pro può essere installato sui sistemi operativi Windows 2000 SP4, Windows XP, Windows Server 2003, o Windows Vista. I requisiti minimi di sistema sono:

- CPU: 450 MHz Intel Pentium o compatibile;
- Memoria RAM: 256 MB;
- Spazio libero su hard disk: 50 MB.

Note:

- Outpost Firewall Pro sia nella versione dei sistemi operativi a 32-bit e sia in quella a 64-bit. Vi preghiamo di scaricare la versione corrispondente dal sito www.agnitum.it.
- Non sono richieste schede di rete o modem speciali e nessuna impostazione di rete particolare per il normale utilizzo del software.
- Outpost Firewall Pro non dovrebbe essere eseguito insieme ad altri programmi di sicurezza. Il funzionamento con altri prodotto di sicurezza può causare l'instabilità del sistema (es. blocchi) e può far funzionare il tuo sistema in una modalità non sicura.

1.2 Installare Outpost Firewall Pro

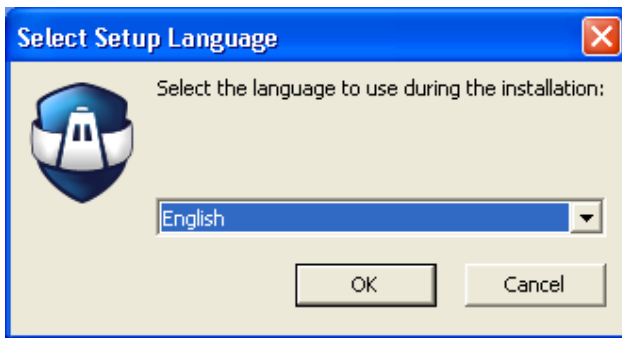
La procedura di installazione di Outpost Firewall Pro è simile a quella della maggior parte dei programmi per Windows.

Per avviare il programma di installazione del sistema:

1. **Molto Importante!** Prima di installare Outpost Firewall Pro, disinstallare qualsiasi altro software firewall presente sul tuo computer e riavviare.
2. Chiudere tutte le applicazioni aperte.
 - a) se installi il prodotto scaricato dal sito, clicca su OutpostFirewallProInstall.exe;
 - b) se installi il prodotto da un disco, il wizard di installazione si dovrebbe avviare automaticamente. Se non si avvia automaticamente, clicca su **Start** di Windows e seleziona **Esegui**. Nel campo **Apri** della finestra **Esegui**, inserisci il percorso completo al file del programma di installazione (OutpostFirewallProInstall.exe). Per esempio, se il programma di installazione è sul disco D: nella cartella Downloads e nella sottocartella Outpost, digita questa stringa nel campo
D:\downloads\outpost\OutpostFirewallProInstall.exe
3. Clicca **OK**.

Il programma di installazione si compone di diversi passaggi. Ogni passaggio ha un pulsante **Avanti** che ti permette di passare al punto successivo della procedura, un pulsante **Indietro** per ritornare al punto precedente e un pulsante **Annulla** per uscire dall'installazione e annullare l'intera procedura di installazione.

L'installazione inizia con la finestra **Seleziona Lingua**.

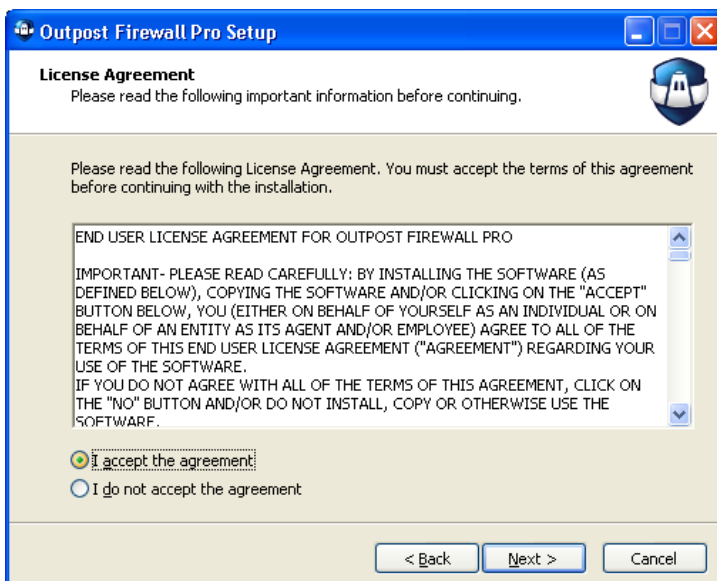


Scegli il linguaggio per l'interfaccia di Outpost Firewall Pro e clicca **OK**. L'installazione mostrerà la finestra **Benvenuto** presenta le caratteristiche di base del prodotto:

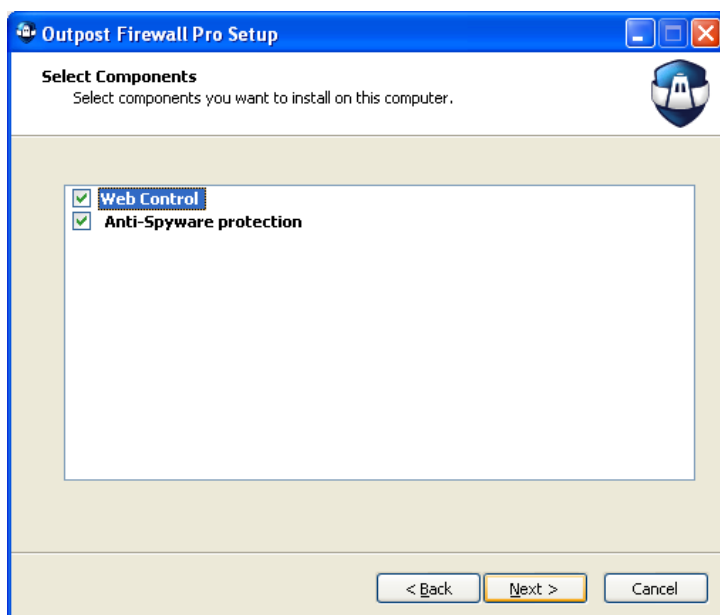


Dopo aver cliccato su **Avanti** ti verrà chiesto di accettare l'Accordo di Licenza per usare **Outpost Firewall Pro**.

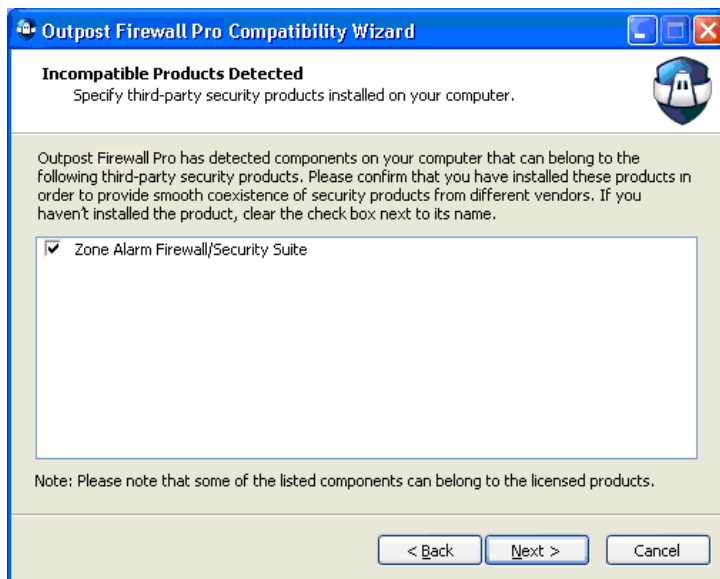
Leggilo attentamente. Il pulsante **Avanti** di questa finestra si abilita solamente se selezioni l'opzione **Accetto l'accordo** che indica la presa visione dell'accordo:



Il passaggio successivo ti permette di scegliere i componenti del prodotto che desideri installare sul computer. Seleziona la casella corrispondente e clicca **Avanti**.



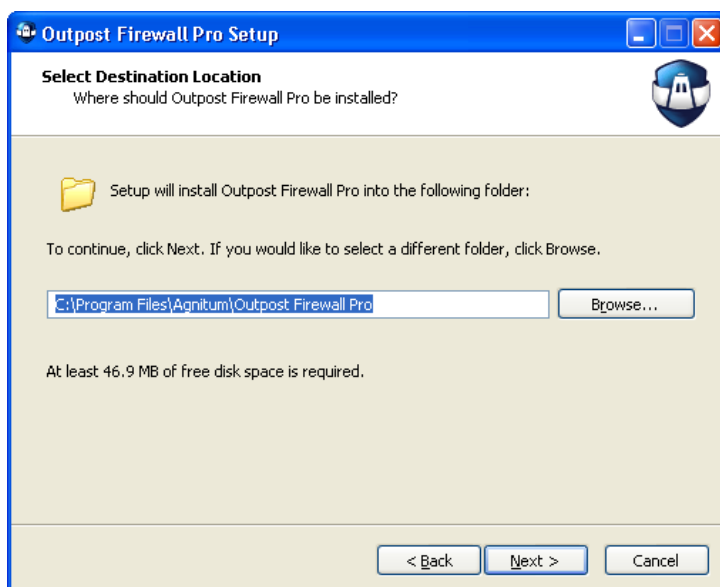
Nel caso in cui tu non abbia rimosso tutti i software di sicurezza di terze parti, il programma di installazione mostrerà una finestra contenente i software incompatibili:



Rilevando *un prodotto incompatibile* sul tuo sistema il programma di installazione non potrà continuare senza che tu rimuova il prodotto.

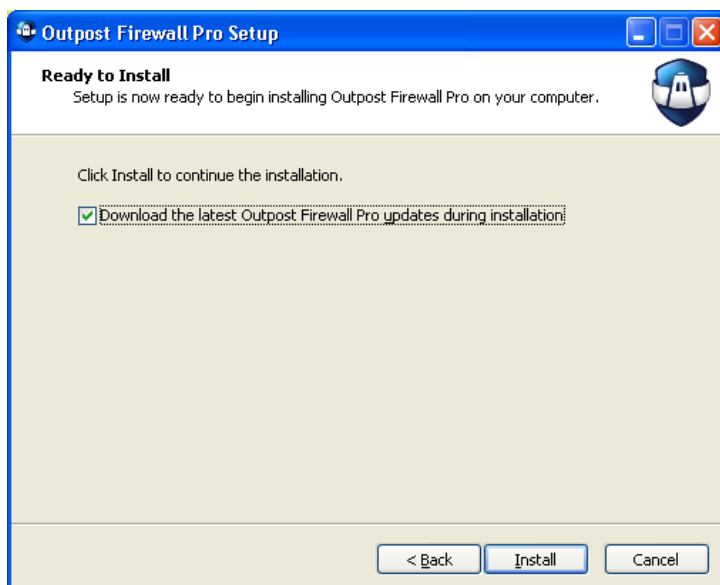
Rilevando *un prodotto parzialmente compatibile* il programma di installazione ti proporrà una delle possibili opzioni da applicare al prodotto.

Dopo aver accettato l'Accordo di Licenza, il pulsante **Avanti** ti porta alla schermata **Seleziona il Percorso di Destinazione**:



Seleziona una cartella dove vuoi installare i file di Outpost Firewall Pro. Puoi usare la cartella predefinita o selezionarla manualmente.

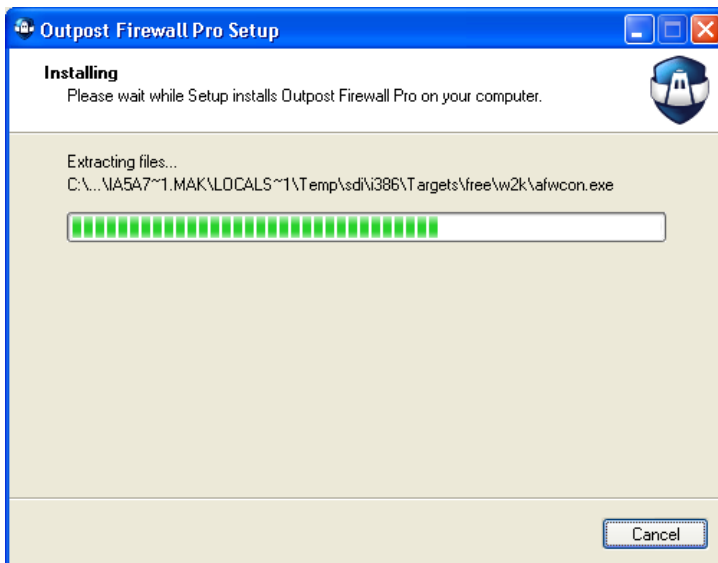
Se vuoi cambiare il percorso predefinito dei file, clicca **Sfoggia**. Seleziona la cartella o crearne una e clicca **OK**. Clicca **Avanti** per passare all'ultimo punto prima dell'installazione vera e propria:



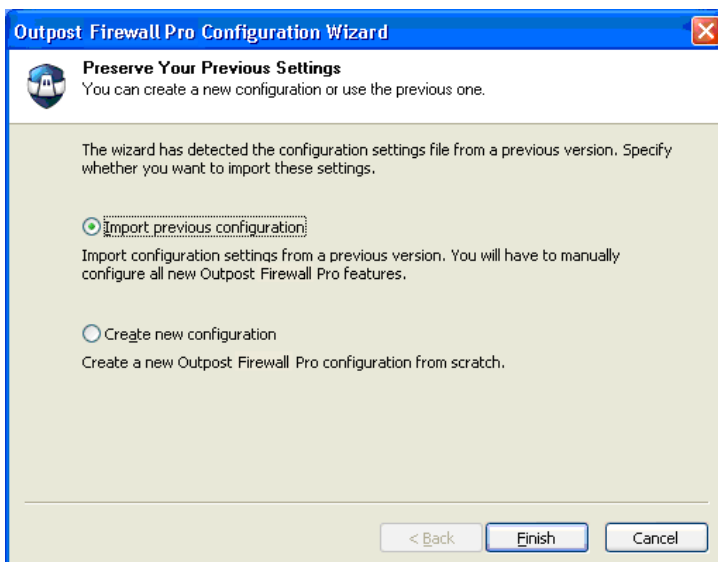
Seleziona l'opzione **Scarica gli ultimi aggiornamenti di Outpost Firewall Pro durante l'installazione** per scaricare le regole predefinite per il prodotto.

Questo è il passaggio finale prima di avviare il processo di installazione. Se hai bisogno di annullare qualche opzione scelta, clicca **Indietro**. Quando sei pronto a procedere con l'installazione, clicca **Installa**.

Il programma mostra la finestra di stato dell'installazione:

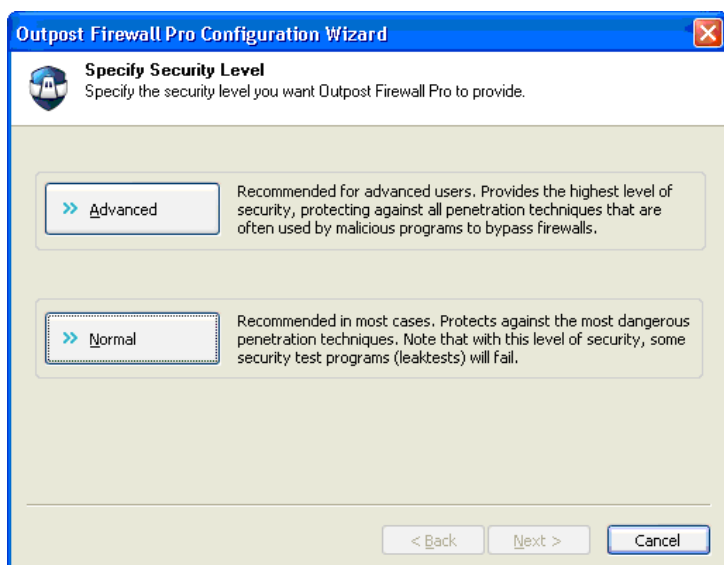


Dopo aver terminato l'installazione, la **Configurazione Assistita** ti aiuterà a creare una nuova configurazione o a importarne una precedente se hai installato il prodotto sopra a una vecchia versione:



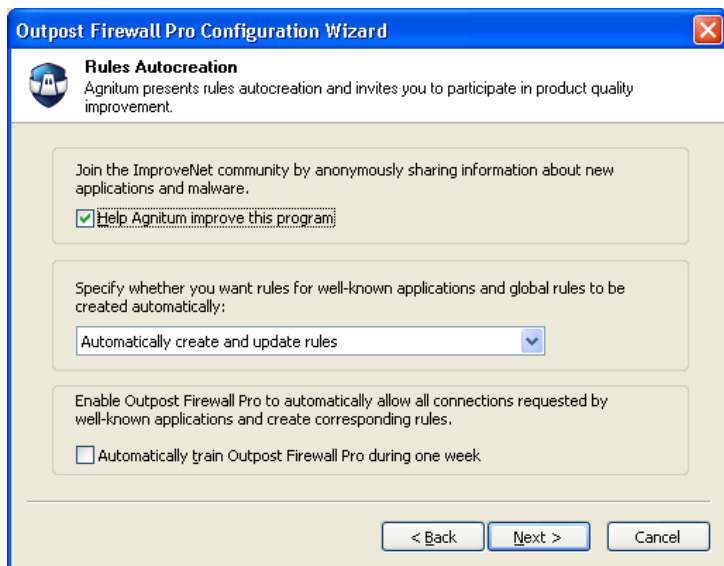
Durante l'importazione di una precedente configurazione il sistema copierà automaticamente le impostazioni salvate dalla versione più vecchia, fatto ciò dovrai riavviare il computer per completare l'installazione di Outpost Firewall Pro.

Durante la creazione di una nuova configurazione il programma di configurazione ti permetterà di selezionare un livello di sicurezza necessaria:



La sicurezza **Avanzata** fornisce il livello più alto di sicurezza e protegge contro tutte le tecniche di penetrazione che vengono usate spesso dai programmi pericolosi per oltrepassare i firewall. Sicurezza **Normale** protegge contro le tecniche di penetrazione più pericolose. Questa riduce le richieste del prodotto a cui gli utenti devono rispondere e si raccomanda nella maggior parte dei casi.

Seleziona il livello desiderato per proseguire sino al passaggio **Creazione Automatica delle Regole e partecipare al programma ImproveNet:**



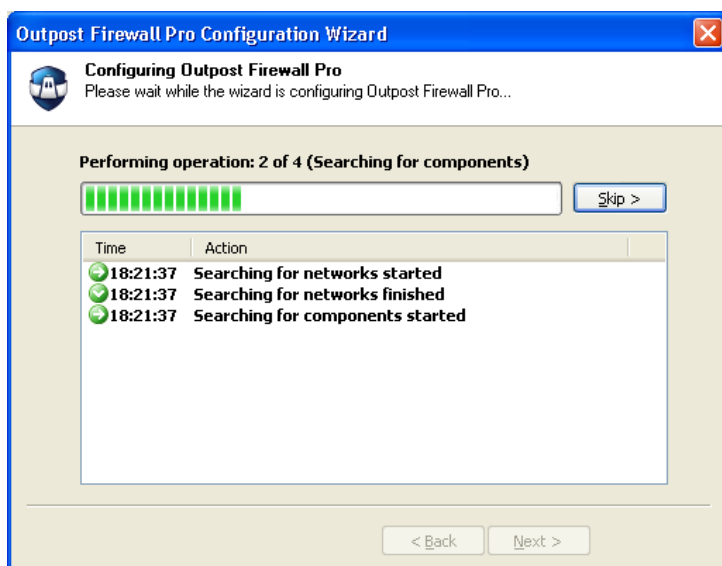
A questo punto, puoi anche aderire al programma ImproveNet di Agnitum per aiutare a migliorare la qualità, la sicurezza e le caratteristiche di controllo dei prodotti Agnitum selezionando **Aiuta Agnitum a migliorare questo programma.**

Il passaggio della **Creazione Automatica delle Regole**, che ti permette di creare automaticamente le regole, così le regole per le applicazioni più conosciute verranno create automaticamente alla loro prima richiesta di azione (per esempio, l'accesso alla rete o la modifica della memoria di un processo).

L'opzione **Istruisci automaticamente Outpost Firewall per una settimana** permette al prodotto di creare automaticamente le regole necessarie.

Dopo aver cliccato su **Avanti**, Outpost Firewall Pro controlla automaticamente il tuo sistema e regola tutte le sue impostazioni senza la tua supervisione. Configura le impostazioni di rete, costruisce il database del Controllo Componenti, e, in caso tu abbia scelto di usare le regole predefinite, cerca le

applicazioni conosciute installate sul tuo computer che potrebbero richiedere l'accesso a Internet e configura un livello di accesso alla rete appropriato per ognuna di loro:



Clicca **Fine** per applicare le modifiche e salvare la configurazione. Ti verrà chiesto di riavviare il tuo sistema:



Importante:

- Non lanciare manualmente Outpost Firewall Pro usando il tasto **Start** o l'Explorer di Windows dopo averlo installato. Devi riavviare il tuo computer prima che Outpost Firewall Pro possa iniziare a proteggere il tuo sistema.

1.3 Registrare Outpost Firewall Pro

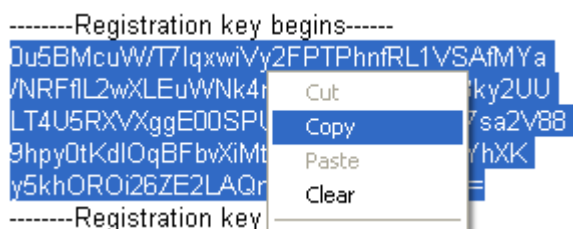
Si può provare Outpost Firewall Pro prima di procedere all'acquisto, gratuitamente per un periodo limitato senza dover pagare nulla. Dopo il periodo di prova, se decidi di mantenere il software e di ricevere gli aggiornamenti per un anno, devi registrare la tua copia pagando un piccolo costo.

Se hai acquistato una scatola di Outpost Firewall Pro in un negozio, segui le istruzioni riportate nella carta di registrazione.

Se hai scaricato la tua copia dal sito di Agnitum, per registrare la tua versione, devi acquistare una chiave di registrazione. Segui le istruzioni sulla pagina <http://www.agnitum.it/> per ricevere la chiave di registrazione via e-mail.

Come inserire la tua chiave di registrazione

1. Quando ricevi la tua chiave di registrazione, apri il messaggio email che la contiene e seleziona tutto il testo compreso tra **Registration key begins** e **Registration key ends** usando il mouse (clicca on il pulsante sinistro appena prima del primo carattere della prima riga della chiave, rilascia il pulsante dopo aver selezionato l'intera chiave come mostrato nell'immagine successiva).
2. Clicca con il pulsante destro del mouse in un punto qualsiasi del testo evidenziato (dal punto 1) e seleziona **Copia** dal menu contestuale per copiare la tua chiave di registrazione negli appunti (un'area generalmente non visibile di Windows usata per le azioni di Copia e Incolla).



3. Seleziona **Start > Programmi > Agnitum > Outpost Firewall Pro** e clicca **Inserisci Chiave di Registrazione**. Nella finestra **Inserisci Chiave**, clicca su **Incolla** e la tua chiave di registrazione (copiata negli appunti al punto 2) verrà inserita nel campo bianco dagli Appunti:



4. Clicca **OK** per salvare la tua chiave e chiudere la finestra.

Quando acquisti una licenza di Outpost Firewall Pro, di fatto ottieni due licenze:

- Una licenza per l'uso di Outpost Firewall Pro (a vita);
- Una licenza per gli aggiornamenti e il supporto della durata di un anno (incluse le ultime versioni di Outpost Firewall Pro).

Terminato un anno puoi comprare un rinnovo di licenza per un altro anno di aggiornamenti e supporto (contratto annuale di Aggiornamento e Supporto) o semplicemente continuare a usare la tua ultima versione aggiornata di Outpost Firewall Pro. Per acquistare un rinnovo, visita questa pagina: <http://www.agnitum.it>.

Nota:

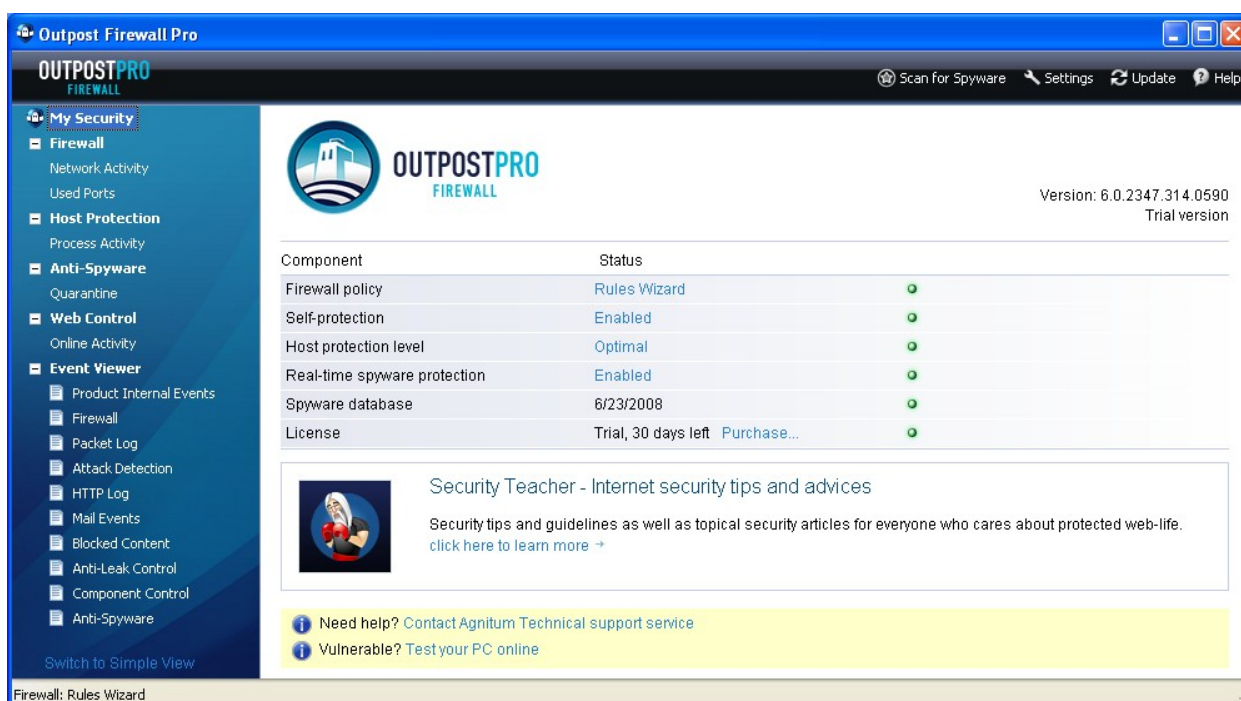
- Outpost Firewall Pro e Outpost Security Suite Pro sono prodotti indipendenti e le loro chiavi di registrazione non sono intercambiabili. Ciò significa che la chiave di registrazione di Outpost Firewall Pro non è valida per Outpost Security Suite Pro e vice versa. Assicurati di inserire la chiave di registrazione corretta.

2 Intercaccia Utente e Controlli di Base

Quando esegui Outpost Firewall Pro per la prima volta, viene mostrata la sua finestra principale. La finestra principale è il tuo pannello di controllo centrale per il prodotto. Il suo scopo è di lasciarti controllare le operazioni di rete del tuo computer e modificare le impostazioni del prodotto.

La finestra principale è molto simile a Windows Explorer, così dovrebbe essere familiare alla maggior parte degli utenti e renderla semplice da usare.

La finestra principale si presenta così:



Per mostrare la finestra principale quando questa è minimizzata nella system tray:

1. Clicca con il pulsante destro l'icona nella system tray dell'Antivirus.
2. Seleziona **Mostra/Nascondi**.

Per chiudere la finestra principale di Outpost Firewall Pro, clicca la **X** nell'angolo in alto a destra. Ricorda che ciò non chiude il prodotto, la finestra principale viene semplicemente minimizzata e l'icona del prodotto rimane nella system tray indicando che è in funzione e che sta proteggendo il tuo sistema.

La finestra principale contiene:

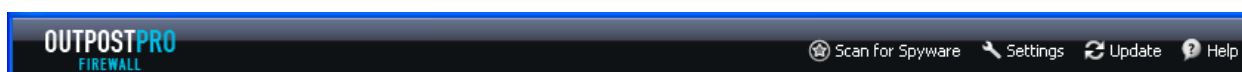
- **La barra degli strumenti**
- **Il Pannello Sinistro**
- **Il Pannello delle Informazioni**
- **La Barra di Stato**

La barra di stato è in basso alla finestra principale. Viene usata per mostrare lo stato attuale di Outpost Firewall Pro.

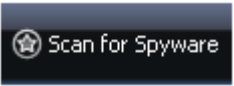
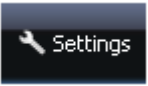

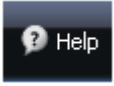
2.1 La Barra degli Strumenti

La barra degli strumenti è in alto nella finestra principale. Per vedere a cosa serve ogni pulsante, passaci sopra il cursore per un secondo. Ogni pulsante nella barra degli strumenti (escluso il pulsante **Impostazioni**) si riferisce a una delle funzioni del prodotto. Questi pulsanti sono semplicemente un modo facile e diretto per raggiungere le loro funzioni saltando diverse finestre e avere accesso alle stesse funzioni.

La barra degli strumenti si presenta in questo modo:



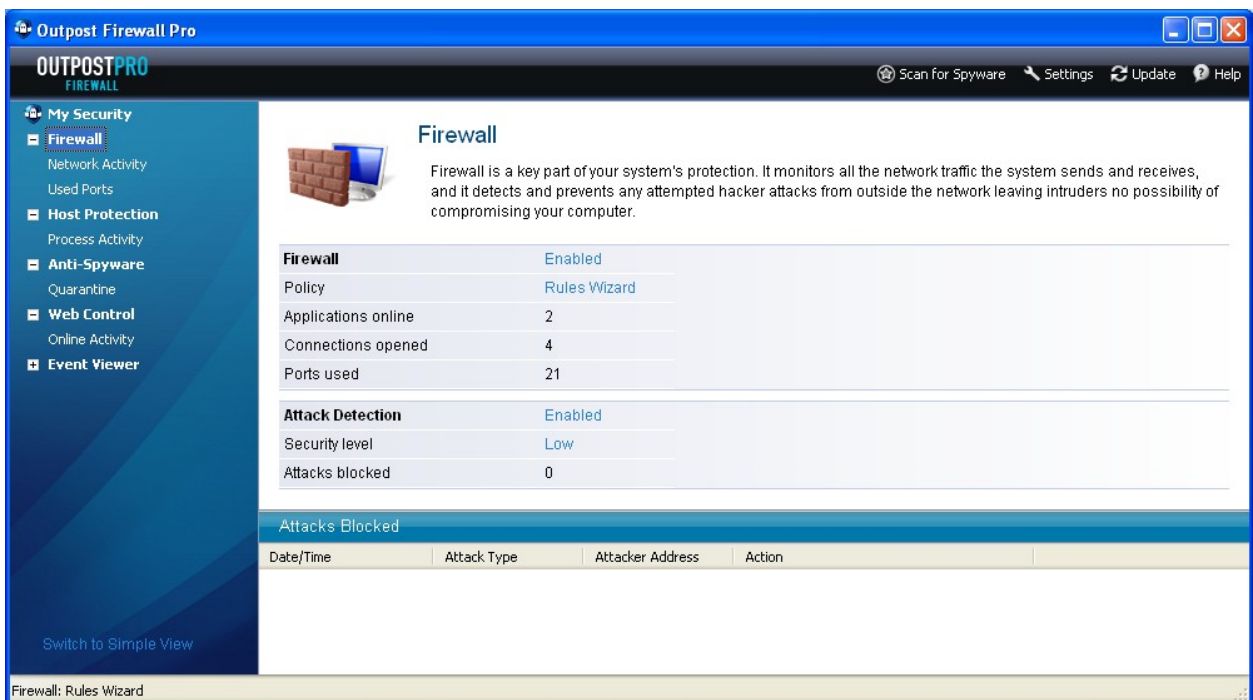
Questi sono i pulsanti presenti nella barra degli strumenti:

Pulsante	Funzione
	Avvia il controllo dei malware nel sistema.
	Apri la finestra delle Impostazioni di Outpost Firewall Pro.
	Scarica gli ultimi aggiornamenti del prodotto inclusi i database anti-malware.
	Apri il file della guida.

2.2 Il Pannello di Sinistra e il Pannello delle Informazioni

Per rappresentare in modo semplice le informazioni raccolte, Outpost Firewall Pro utilizza due pannelli. Quello di sinistra è molto simile al pannello che, sempre sulla sinistra, trovate nel Windows Explorer. Questo mostra tutta una serie di categorie: connessioni, porte e plug-in. Il pannello informativo fornisce invece dati specifici riguardanti qualsiasi categoria selezionata precedentemente sulla sinistra.

I pannelli si presentano nel seguente modo:



Per aiutarti, Outpost Firewall Pro ti permette di passare tra visualizzazione semplice e esperta in base alla tua esperienza nell'utilizzare programmi di sicurezza. Per impostazione predefinita, il prodotto mostrerà la **Visualizzazione Semplice**. Se non sei un utente esperto, consigliamo la **Visualizzazione Semplice**, che non contiene pagine difficili da comprendere. Se sei un utente esperto, raccomandiamo la **Visualizzazione Esperta**, che fornisce più informazione sulle capacità del prodotto e sulle prestazioni del sistema. Potrebbe essere utile per seguire le attività del sistema e per avere il controllo della situazione qualora accadesse qualcosa.

Per passare da una visualizzazione all'altra, clicca **Passa alla Visualizzazione Esperta** o **Passa alla Visualizzazione Semplice** in basso nel pannello sinistro.

Nota:

- Passare da una visualizzazione all'altra non influenza le funzionalità fornite dal prodotto.

Come accade con Windows Explorer, ogni riga che comincia con il simbolo più di un plug-in (+) può essere esplosa per mostrare tutte le relative sottocategorie. Ogni riga che comincia invece con un segno meno (-) mostra che quella riga è stata già espansa. Cliccando sul segno meno, ognuna di esse può essere nuovamente nascosta per risparmiare spazio sullo schermo.

Il pannello sinistro e il pannello delle informazioni mostrano le informazioni riguardanti i contenuti delle seguenti categorie:

- **Firewall**

Selezionando questa categoria nel pannello sinistro verranno mostrate le informazioni generali sul firewall, come il suo stato attuale, il livello di protezione, gli attacchi rilevati e le statistiche generali sulle connessioni aperte. Quando si espande, questa categoria mostra le seguenti voci:

- *Attività di Rete*

Elenca tutte le applicazioni e i processi che hanno connessioni attive e i dettagli su queste connessioni.

- *Porte Usate*

Elenca tutte le applicazioni e i processi che usano delle porte per una connessione di rete.

- **Protezione Host**

Mostra informazioni generali sulla Protezione Host, come il livello di sicurezza locale, lo stato del Controllo Anti-Leak, del Controllo Componenti e dell'autoprotezione a alcune statistiche generali.

- *Attività processi*

Elenca tutti gli eventi locali nel sistema controllati dalla Protezione Host.

- **Anti-Spyware**

Mostra le informazioni generali sulle funzionalità del componente Anti-Spyware e sullo stato del database delle firme digitali malware, come anche alcune statistiche generali sugli oggetti rilevati.

- *Quarantena*

Elenca tutti gli oggetti posti in quarantena.

- **Controllo Web**

Mostra informazioni generali sul componente Controllo Web, come anche il suo stato attuale, il suo livello di sicurezza e le statistiche generali sul contenuto filtrato.

- *Attività Online*


Elenca tutti gli elementi di contenuto processati dal filtro.

- **Visualizzatore Eventi**

Mostra le statistiche dettagliate per tutti i sistemi e le attività del prodotto per categoria.

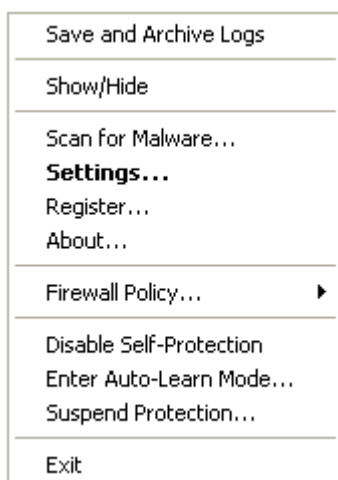
2.3 System Tray Icon

L'Icona nella System Tray

Un altro elemento per controllare il prodotto è l'icona posta nella system tray. La system tray è la parte più a destra della Barra degli strumenti di Windows. Qui viene caricata l'icona con un punto interrogativo sullo scudo blu  ((icona predefinita di Outpost Firewall Pro). Quando vedi questa icona, significa che Outpost Firewall Pro sta funzionando e ti sta proteggendo.

Questa icona è uno dei mezzi principali per accedere ai molti controlli, impostazioni e rapporti del prodotto. Cliccando con il tasto destro del mouse su questa icona ottieni il seguente menu contestuale.

L'icona nella system tray si presenta come segue:



In questo menu sono disponibili i seguenti comandi:

- **Salva e Archivia i Rapporti**

Questo comando è disponibile solamente se il parametro **Registra le informazioni di debug** presente nel menu **Rapporti** delle impostazioni di Outpost Firewall Pro è abilitato. Aggiorna i file di rapporto di Outpost Firewall Pro nella sotto cartella **Rapporto** della cartella di installazione di Outpost Firewall Pro (per default *C:\Programmi\Agnitum\Outpost Firewall Pro*) e crea l'archivio *feedback.zip* che contiene tutti i file di rapporto.

- **Mostra/Nascondi**

Mostra o nasconde la finestra principale di Outpost Firewall Pro.

- **Controllo Malware**

Avvia un controllo di sistema malware.

- **Impostazioni**

Mostra la finestra delle **Impostazioni**.

- **Registra**

(Disponibile solo nella modalità di prova.) Ti permette di inserire la tua chiave di registrazione per ottenere un anno di aggiornamenti e supporto gratuito di Outpost Firewall Pro.

- **Informazioni**

Mostra la versione attuale di Outpost Firewall Pro e il suo database, elenca ogni modulo del pacchetto e il loro numero di versione, e fornisce le informazioni sulla licenza.

- **Livello di protezione del Firewall (o Abilita Firewall)**

Apri un sottomenu dove puoi cambiare il livello di protezione del firewall di Outpost Firewall Pro in una delle modalità disponibili: **Blocca tutto**, **Blocca la maggior parte**, **Regole Assistite**, **Permetti la maggior parte**, e **Disabilita**. Se il firewall viene disabilitato, puoi abilitarlo.

- **Disabilita Autoprotezione (o Abilita Autoprotezione)**

Disabilita (abilita) l'autoprotezione di Outpost Firewall Pro.

- **Entra in Modalità Autoapprendimento (o Esci dalla Modalità Autoapprendimento)**

In Modalità Autoapprendimento Outpost Firewall Pro permette tutte le attività delle applicazioni durante un tempo specificato per creare delle regole corrispondenti.

- **Sospendi Protezione (o Ripristina Protezione)**

Disabilita (abilita) la protezione di Outpost Firewall Pro.

- **Esci**

Apri una finestra che ti permette sia di chiudere la GUI e sia di fermare il prodotto così da non proteggere il sistema o passare alla modalità background.

Nota:

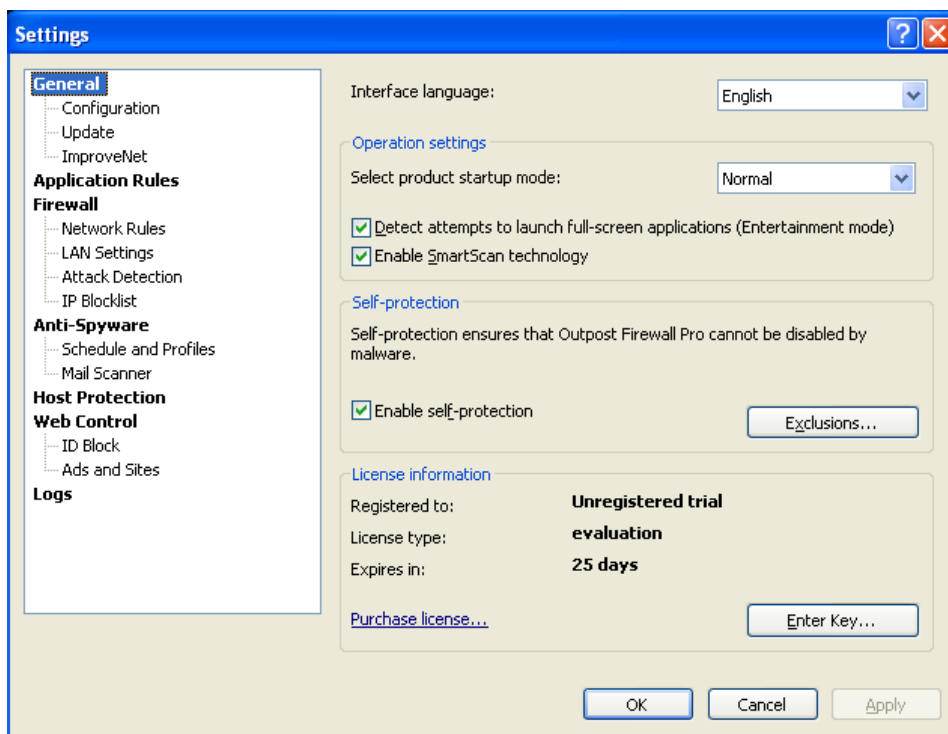
- L'icona sulla system tray non è visibile in modalità background.

2.4 Linguaggio Interfaccia

La lingua dell'interfaccia viene selezionata durante l'installazione di Outpost Firewall Pro, ma puoi scegliere di cambiarla anche durante l'uso di Outpost Firewall Pro se lo desideri. Per far ciò:

1. Apri la finestra principale del programma cliccando due volte sull'icona posta nella system tray.
2. Clicca **Impostazioni** sulla barra degli strumenti.
3. Seleziona la lingua richiesta dall'elenco **Lingua dell'Interfaccia**.

4. Clicca **OK** per salvare i cambiamenti.




Per rendere effettivo il cambio di lingua in Outpost Firewall Pro. La finestra di avviso ti ricorda che verrà mostrato dopo aver cliccato **OK** al punto 4.

3 Configurazione di Base

Outpost Firewall Pro inizia a funzionare non appena viene installato. Le sue impostazioni iniziali sono ottimizzate per la maggior parte delle situazioni e si raccomanda di mantenerle così fin quando non si abbia piena padronanza del prodotto, a questo punto puoi personalizzarle a seconda delle tue particolari esigenze.

Questa sezione fornisce una breve panoramica dei controlli di base di Outpost Firewall Pro che un utente neofita dovrebbe conoscere quando inizia a usare il prodotto, partendo con: come avviare e terminare la protezione, come creare una nuova configurazione, come proteggere le tue impostazioni da modifiche non autorizzate e su come la speciale Modalità Intrattenimento ti permette di rimanere protetto mentre stai giocando online.

3.1 Avviare e terminare la Protezione

Per default, viene caricato automaticamente sul tuo computer all'avvio fornendo protezione immediata. Ogni volta che viene caricato, nella system tray viene caricata l'icona di default con un punto interrogativo bianco sullo scudo blu  in basso a destra della barra degli strumenti di Windows. Quando vedi questa icona, significa che Outpost Firewall Pro sta funzionando e proteggendo il tuo sistema..

Cliccando due volte sull'icona si apre la finestra principale di Outpost Firewall Pro. Quando clicchi sul pulsante di chiusura in alto a destra della finestra, non stai chiudendo il firewall. La finestra principale viene minimizzata e l'icona del firewall rimane nella system tray indicando che il firewall sta funzionando e protegge il tuo sistema.

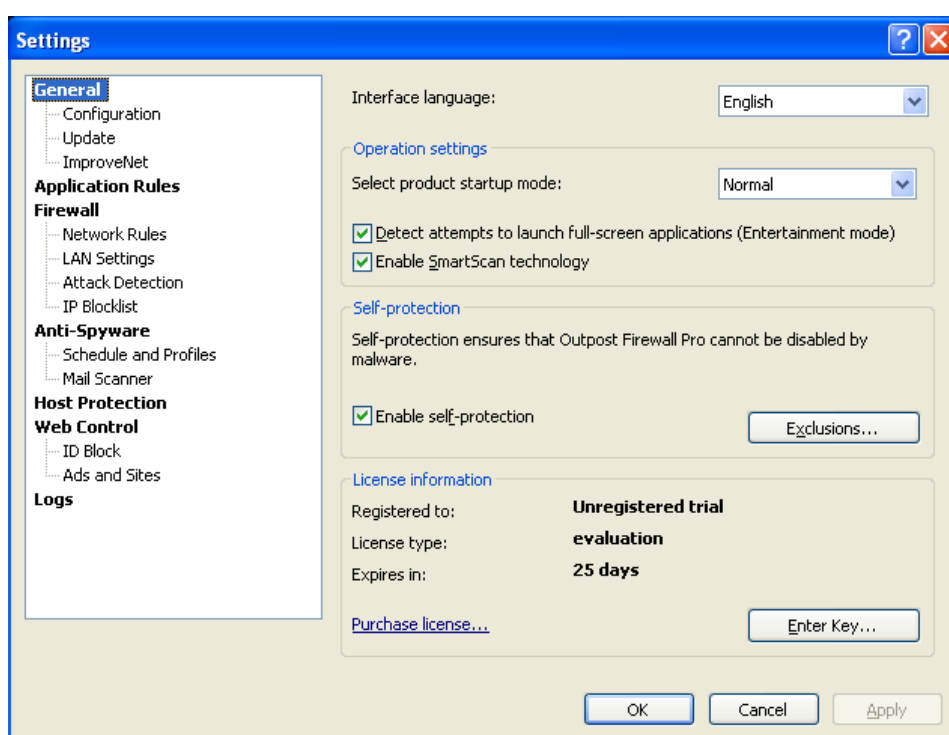
Per fermare Outpost Firewall Pro completamente e non proteggere più il tuo sistema, clicca con il pulsante destro del mouse sull'icona di Outpost Firewall Pro nella system tray, clicca **Esci**, seleziona **Esci da Outpost Firewall Pro e chiudi il servizio** dall'elenco e clicca su **OK**

Modalità di Avvio

Outpost Firewall Pro ti permette di controllare il suo comportamento all'avvio del sistema. Per selezionare una delle tre modalità di avvio, clicca su **Impostazioni** nella barra degli strumenti. Nella pagina **Generale** sotto **Parametri operazione** sono presenti le seguenti modalità:

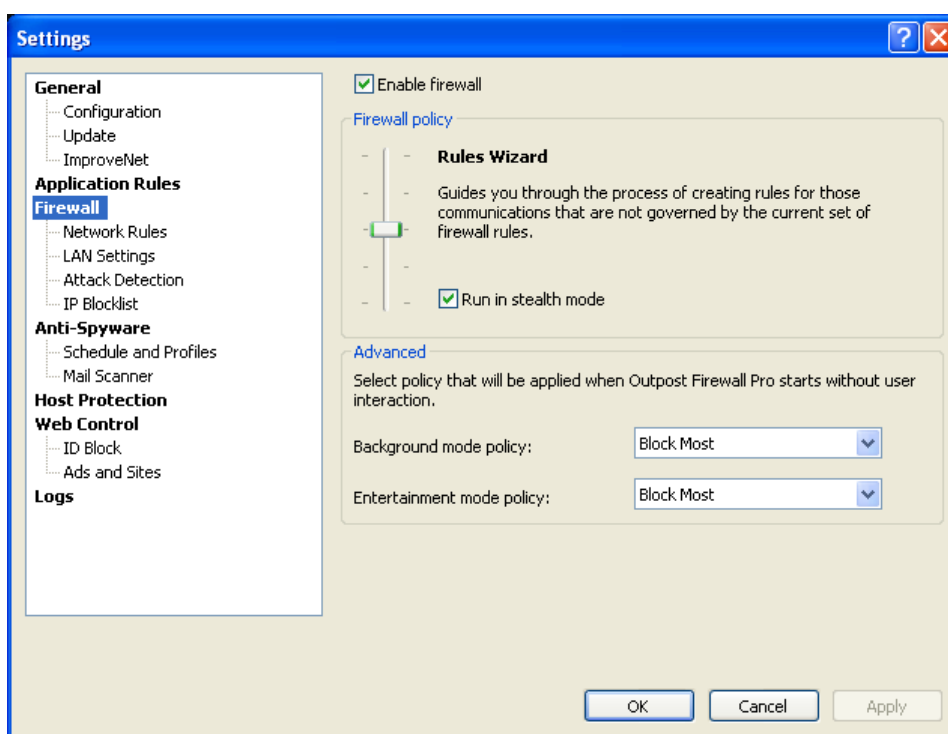
- **Normale.** La modalità di default. Carica Outpost Firewall Pro automaticamente all'avvio e mostra la sua icona nella system tray.
- **Background.** Se viene selezionato, Outpost Firewall Pro viene avviato in modalità invisibile, senza la sua icona nella system tray o senza la presenza di alcuna finestra. La modalità nascosta serve per due scopi: per salvaguardare le risorse di sistema e per permettere a un genitore o a un amministratore di sistema di bloccare del traffico o del contenuto non desiderato in modo completamente invisibile per l'utente.

Un'altra ragione per usare la modalità background è per risparmiare risorse di sistema.



Note:

La modalità Regole Assistite non viene supportata quando Outpost Firewall Pro lavora in modalità nascosta visto che in questa modalità non viene richiesta alcuna interazione dell'utente, devi specificare quale livello di protezione del firewall usare quando Outpost Firewall Pro si avvia in modalità nascosta. Per specificare il livello di protezione da applicare, clicca **Impostazioni**, seleziona **Firewall**, e seleziona il livello di protezione desiderato dall'elenco **Livello di protezione in modalità Background**









Puoi richiamare Outpost Firewall Pro quando vuoi selezionando **Start > Tutti i Programmi > Agnitum > Outpost Firewall Pro** e cliccando **Outpost Firewall Pro**. Per chiudere la GUI di Outpost Firewall Pro e tornare alla modalità background, clicca con il tasto destro sull'icona in basso a destra del prodotto, clicca **Esci**, seleziona **Passa alla modalità** e clicca **OK**.

- **Disabilita** - Se viene selezionato, Outpost Firewall Pro non verrà eseguito all'avvio. Il tuo sistema non verrà protetto.

3.2 Gestire lo Stato della Protezione

Per ragioni di sicurezza, spesso è cruciale conoscere lo stato della tua protezione e definire velocemente la modalità di sicurezza di ogni modulo. La pagina **Mia Sicurezza** (la prima pagina mostrata quando clicchi sull'icona nella system tray) ti fornisce un elenco di componenti critici del prodotto e della loro attuale modalità, così puoi velocemente valutare una situazione accedendo con un click alle impostazioni di ogni componente per regolare il comportamento di Outpost Firewall Pro.

Component	Status
Firewall policy	Rules Wizard 
Self-protection	Enabled 
Host protection level	Advanced 
Real-time spyware protection	Enabled 
Spyware database	10.Jun.08 
License	Single, 83 days left. 

Vengono mostrate le seguenti informazioni dei componenti:

- **Livello di protezione del Firewall.** Cliccando il link nella colonna **Stato** si apriranno le impostazioni del **Firewall**, che ti permettono di cambiare la sua policy.



- **Modalità autoprotezione.** Cliccando il link nella colonna **Stato** cambierà lo stato di autoprotezione.
- **Livello di Protezione Host.** Cliccando il link nella colonna **Stato** si apriranno le impostazioni della **Protezione Host**, permettendoti di cambiare questo libero.
- **Stato della protezione malware in tempo reale.** Cliccando il link nella colonna **Stato** si apriranno le impostazioni dell'**Anti-Malware**, permettendoti di cambiarle.
- **Data del database Malware.** Cliccando sul link **Aggiornamento** disponibile nel caso di database scaduto partirà il processo di aggiornamento.
- **Informazioni licenza.** Mostra il tipo di licenza in tuo possesso e se non sei ancora registrato, ti permette di registrare facilmente il prodotto cliccando sul link **Registra**.


Se un componente opera in una modalità, che è diversa da quella ottimale (raccomandata), verrà evidenziata la linea corrispondente che ti permette di sapere che quel componente non fornisce il livello di protezione richiesto. Se il componente viene disabilitato, la linea corrispondente verrà evidenziata in rosso così puoi sapere che quel componente non ti sta proteggendo.

3.2 Selezionare il Livello di Protezione del Firewall

Una delle caratteristiche più utili e importanti del firewall è rappresentata dalle policy. Una policy è il comportamento di base che si desidera venga adottato da Outpost Firewall Pro nel momento in cui il computer entra in un ambiente Internet o in qualsiasi altro tipo di rete. La policy **Blocca la maggior parte**, per esempio, rende Outpost Firewall Pro particolarmente diffidente mentre **Permetti la maggior parte** rende Outpost Firewall Pro molto permissivo.

Outpost Firewall Pro può funzionare in accordo con le seguenti policy:

Icon	Policy	Description
	Blocca tutto	Blocca tutte le comunicazioni in entrata e in uscita.
	Blocca la maggior parte	Blocca tutte le comunicazioni che non hai specificatamente permesso nelle regole globali o nelle regole delle applicazioni.
	Regole Assistite	Ti guida attraverso la creazione di una regola per ogni tipo di comunicazione che non è stata già controllata dalle regole attualmente in uso.
	Permetti la maggior parte	Sono consentite tutte le connessioni di rete escluse quelle esplicitamente bloccate dalle regole globali o dalle regole delle applicazioni.

In base alla modalità scelta verrà mostrata la relativa icona di Outpost Firewall Pro sulla system tray del proprio sistema operativo. Così sarà possibile controllare il tipo di policy scelta semplicemente dando un'occhiata all'icona sulla system tray. Se Outpost Firewall Pro è disabilitato, l'icona diventa rossa  e sono consentite tutte le connessioni.

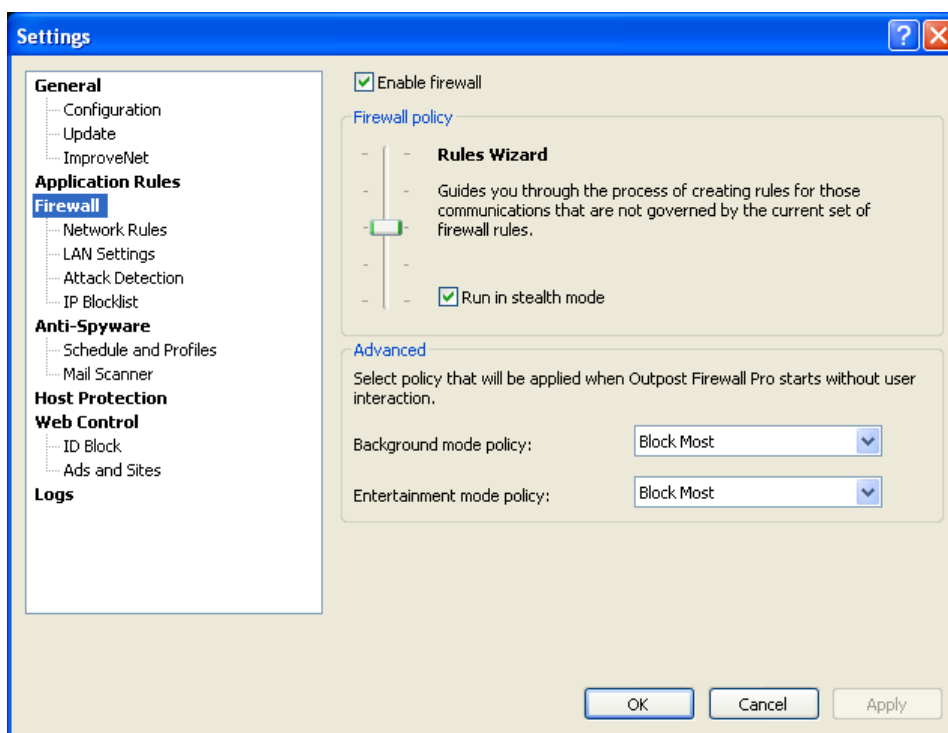
Note:

- Se Outpost Firewall Pro funziona in modalità background, non viene mostrata alcuna icona.

Cambiare il livello di protezione del firewall

Per modificare l'attuale livello di protezione del firewall:

1. Clicca **Impostazioni** sulla barra degli strumenti.
2. Seleziona la pagina **Firewall**.
3. Seleziona il livello di protezione muovendo il regolatore in alto o in basso e clicca su **OK**.



Per disabilitare completamente il firewall, svuota la casella **Abilita firewall**.

Suggerimento:

- Puoi cambiare il livello di protezione del firewall direttamente dall'icona sulla system tray. Cliccare con il tasto destro del mouse sull'icona, selezionare **Livello di Protezione**, e selezionare il livello desiderato dal menu.

Importante:

- Se il firewall viene disabilitato, anche la Rilevazione Attacchi viene disabilitata.

Avviare in modalità invisibile

La modalità invisibile ti permette di definire se il tuo computer risponderà alle scansioni sulle porte o se le bloccherà in modo silente, rendendosi così invisibile agli hacker. Normalmente, quando il tuo computer riceve una richiesta di connessione alla porta non usata da alcuna connessione in entrata o in uscita, lascia che gli altri computer sappiano che questa porta non viene usata inviando un messaggio di notifica "port unreachable". In modalità invisibile, il tuo computer non risponderà, in questo modo sembrerà spento o non connesso a Internet. In questo caso, i pacchetti inviati alle porte non usate saranno semplicemente ignorati dal firewall senza alcun messaggio di notifica al server sorgente sia attraverso ICMP e TCP.

Per passare alla modalità invisibile, clicca **Impostazioni** sulla barra degli strumenti, seleziona il menu **Firewall** e seleziona/svuota la casella **Esegui in modalità invisibile**.

Nota:

- Si raccomanda di mantenere Outpost Firewall Pro la modalità invisibile a meno che si si abbia una buona ragione per fare altrimenti.

Nota:

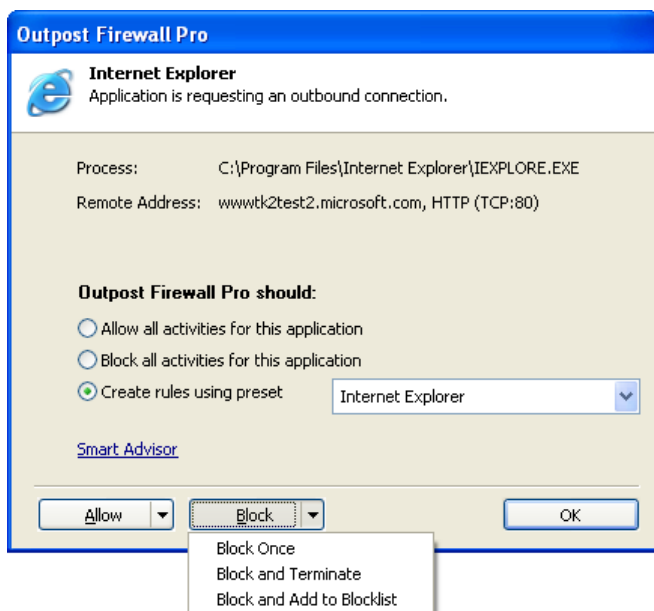
- Dato che la policy Regole Assistite non viene supportata da Outpost Firewall Pro quando si è in modalità background o in Modalità Intrattenimento (queste modalità non prevedono l'intervento dell'utente), hai la necessità di specificare in modo esplicito quale livello di protezione del firewall deve essere applicata quando Outpost Firewall Pro passa a una di queste modalità. Per maggiori informazioni vedi i link corrispondenti.

3.2.1 Avviare in Modalità Regole Assistite

Al momento dell'installazione, di default Outpost Firewall Pro viene installato in modalità **Regole Assistite**. Questa modalità ti aiuta a decidere se permettere ad un'applicazione di connettersi alla rete. La modalità Regole Assistite ti sarà di aiuto nello specificare le impostazioni da utilizzare per ogni singola applicazione.

La Modalità Regole Assistite renderà la tua vita (digitale) un po' più semplice. Invece di dover generare una nuova regola, spesso complessa, ogni volta che una nuova applicazione tenta di accedere al computer, la modalità Regole Assistite farà il lavoro per te basandosi su regole già presenti, relative a tutte le applicazioni più note. Di norma, la modalità Regole Assistite suggerisce persino la selezione migliore per il singolo caso. A meno che si conosca una scelta migliore, le raccomandazioni dell'assistente saranno sempre aderenti all'esigenza del caso.

Le Regole Assistite propongo una richiesta simile alla seguente:



In Modalità **Regole Assistite** ha le seguenti scelte per un'applicazione:

- **Permetti tutte le attività per questa applicazione**

Solamente per le applicazioni completamente affidabili. Verranno consentite tutte le richieste di quest'applicazione.

- **Blocca tutte le attività per questa applicazione**

Solamente per le applicazioni che non dovrebbero connettersi alla rete. Vengono disabilitate tutte le attività di rete di questa applicazione.

- **Creare delle regole usando quelle predefinite**

Per le applicazioni che possono ottenere l'accesso di rete tramite protocolli specifici, attraverso porte, ecc. Crea una regola che limita gli accessi di rete a particolari porte e protocolli utilizzando impostazioni predefinite dai nostri tecnici durante test di laboratorio atti a simulare situazioni simili.

Selezionare l'applicazione richiesta dall'elenco e cliccare su **OK** per permettere di controllare questa applicazione in accordo con le regole specificate. Puoi creare delle regole personalizzate per questa applicazione selezionando **Personalizza** dall'elenco e specificando le impostazioni della regola richiesta.

Nota:

- Nel caso in cui alcune applicazioni richiedano la connessione ad un server che abbia diversi indirizzi IP, Outpost Firewall Pro automaticamente rileva tutti gli indirizzi e configura le regole corrispondenti per tutti gli indirizzi IP del server in accordo con l'azione che tu specificherai.

- **Permetti**

Permette di selezionare una delle seguenti azioni (clicca accanto al pulsante **Permetti** per aprire il menu):

- **Permetti una volta**

L'azione predefinita. Questa è per le applicazioni su cui hai un dubbio ma vuoi verificare il loro comportamento in rete. La connessione viene consentita per questa volta. Non vengono create regole per l'applicazione e la prossima volta che questa applicazione tenta di stabilire una connessione di rete, apparirà la stessa finestra.

- **Modalità Autoapprendimento**

Permette la connessione e passa Outpost Firewall alla Modalità Autoapprendimento, creando le regole che permettono tutte le connessioni richieste.

- **Blocca**

Permette di selezionare una delle seguenti azioni (clicca sulla freccia accanto al pulsante **Blocca** per aprire il menu):

- **Blocca una volta**

Per le applicazioni delle quali non ti fidi ma non vuoi bloccare per sempre. Il collegamento di rete sarà bloccato per questa volta soltanto. Un successivo tentativo atto a stabilire un collegamento di rete provoca la visualizzazione della finestra di attenzione. Nessuna regola è generata per l'applicazione.

- **Blocca e Termina**

Blocca la connessione richiesta e termina il processo che la richiede. Non viene creata alcuna regola e al successivo tentativo dell'applicazione di stabilire una connessione di rete verrà proposta all'utente la stessa finestra di richiesta.

- **Blocca e aggiungi all'Elenco Bloccati**

Blocca la connessione richiesta e pone l'indirizzo IP remoto nell'elenco degli IP bloccati.

Note:

- Le Regole Assistite non sono supportate quando Outpost Firewall Pro viene avviato in modalità background, così come non viene richiesta alcuna interazione dell'utente in modalità nascosto.

- Per maggiori informazioni sulla creazione delle regole, vedi Gestire l'Accesso alla Rete delle Applicazioni.
- Se ti serve aiuto per rispondere a una richiesta del prodotto, clicca **Smart Advisor** per ricevere un consiglio sull'evento in corso.

3.2.2 Smart Advisor

Durante il suo funzionamento, Outpost Firewall Pro interagisce costantemente con l'utente per mezzo delle 'finestre di dialogo, o richieste. Queste potrebbero apparire, per esempio, quando il programma si comporta in maniera differente rispetto alle sue regole che lo gestiscono con un elemento o un componente o una connessione richiesta per cui non c'è una regola e l'utente dovrà intervenire.

Per assistere l'utente nel prendere una decisione, Outpost Firewall Pro fornisce informazioni aggiuntive sull'oggetto e suggerisce quali sono quelle disponibili attraverso il link **Smart Advisor** incluso nella finestra di richiesta. Dopo aver cliccato su **Smart Advisor**, viene fornita una nuova finestra con i dettagli per l'attività di Outpost Firewall Pro da selezionare, come le proprietà di un eseguibile che richiede una connessione e una descrizione dei programmi per i quali l'attività potrebbe essere tipica con un suggerimento.

3.3 Avviare in Modalità Auto-Apprendimento

Per ridurre il numero di richieste da parte delle Regole Assistite durante la prima fase dell'operazione, puoi impostare Outpost Firewall Pro per memorizzare (auto-apprendimento) le attività tipiche compiute da un sistema abilitando la modalità Auto-Apprendimento.

In questo modo, Outpost Firewall Pro assume tutte le attività del programma che sono legittime e di conseguenza permette l'accesso alla rete e l'interazione con i processi a tutte i programmi richiesti. Quando programmi differenti accedono a Internet e interagiscono con altri software per la prima volta, Outpost Firewall Pro memorizza le loro identità e crea le regole di permesso per tutte le connessioni richieste. Le regole create rimarranno effettive dopo la fine del periodo di auto-apprendimento e quando il computer torna alla normale modalità di controllo. Se esiste la regola per la connessione richiesta, la connessione viene gestita in accordo con queste regole, così i tuoi programmi potranno continuare ad accedere a internet senza innescare una richiesta di "nuova connessione".

Per abilitare la modalità Auto-Apprendimento, clicca con il destro sull'icona di Outpost Firewall Pro nella system tray e seleziona **Entra in Modalità Auto-Apprendimento**. Specifica il periodo per il quale Outpost Firewall Pro debba essere istruito e clicca **OK**.

Dopo il periodo di tempo specificato, il software abilita automaticamente la creazione automatica delle regole e gli aggiornamenti così il traffico di rete viene processato secondo le regole create durante il periodo di auto-apprendimento e secondo le regole che si basano su quelle predefinite.

Per tornare alla modalità normale prima di terminare il periodo specificato, clicca due volte sull'icona di Outpost Firewall Pro nella system tray e seleziona **Lascia la Modalità Auto-Apprendimento**.

Nota:

- La Modalità Auto-Apprendimento può essere un rischio per la sicurezza perché le regole di permesso vengono create per tutte le connessioni richieste. Perciò mentre sei in modalità Auto-Apprendimento, assicurati di non eseguire applicazioni sconosciute o non affidabili e di non visitare siti pericolosi.

3.4 Avviare in modalità Intrattenimento

Mentre stai giocando o vedendo un film potresti voler evitare le richieste e gli allarmi del prodotto che possono distrarre la tua attenzione e comunque rimanere protetto, specialmente se stai giocando online.

Outpost Firewall Pro fornisce una speciale **Modalità Intrattenimento** dove la protezione è attiva senza che all'utente vengano proposte numerose richieste di intervento o allarmi. Ogni volta che viene avviata un'applicazione a schermo intero - un gioco o un filmato in media player, per esempio, - rileva questo evento e suggerisce di passare alla modalità Intrattenimento.

Per permettere a Outpost Firewall Pro di rilevare le applicazioni a schermo pieno e per farti suggerire di passare alla modalità Intrattenimento, clicca **Impostazioni** sulla barra degli strumenti e seleziona **Rileva i tentativi di eseguire le applicazioni a schermo intero (modalità Intrattenimento)**. Per impostare la policy della modalità Intrattenimento, clicca il menu **Firewall** e seleziona la policy dal menu corrispondente. Questo livello di protezione firewall verrà applicato ogni volta che Outpost Security Suite Pro entra in modalità Intrattenimento e se non vi è più necessità tornerà come era prima di passare alla modalità Intrattenimento.

La modalità Intrattenimento propone una richiesta simile alla seguente:



Puoi abilitare o disabilitare la modalità Intrattenimento per specifiche applicazioni cliccando su **Impostazioni** nella barra degli strumenti, selezionando il menu **Regole Applicazione** e cliccando due volte sull'applicazione richiesta. Sul menu **Opzioni**, seleziona l'azione necessaria dall'elenco **Quando un'applicazione sta entrando in modalità a schermo intero**:

Note:

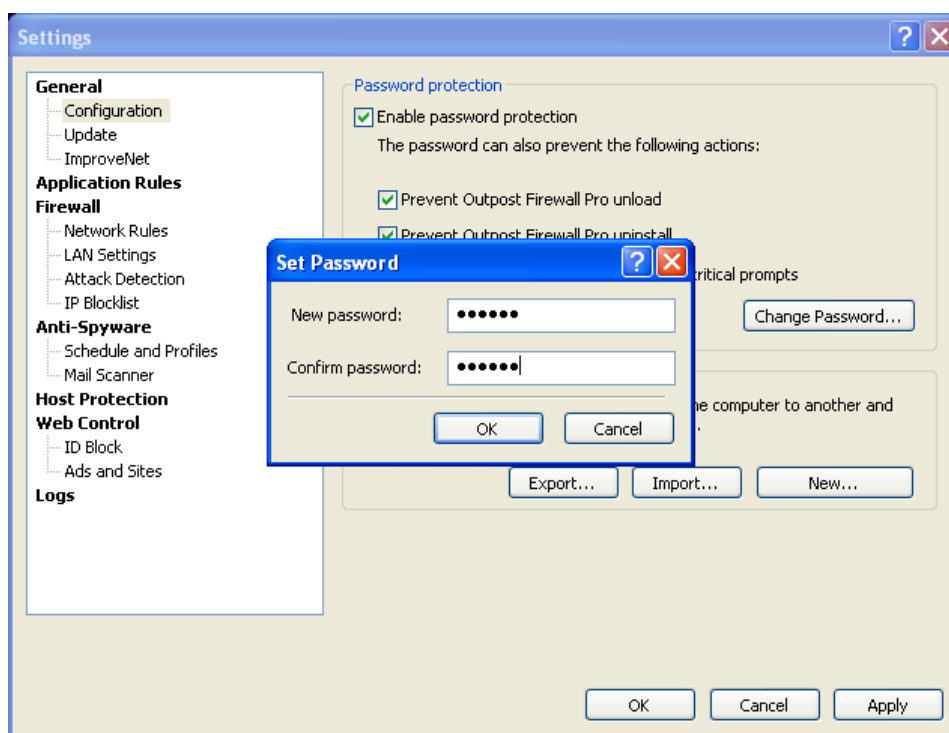
- Quando stai operando in modalità background, Outpost Firewall Pro non ha bisogno di entrare in modalità Intrattenimento.

3.5 Proteggere la Configurazione con una Password

Outpost Firewall Pro ti dà la possibilità di proteggere le impostazioni che hai specificato dall'eventualità che vengano alterate senza il tuo permesso. Proteggendole con password, le impostazioni del prodotto non possono essere cambiate da altre persone. Puoi, per esempio, bloccare l'accesso ai siti non adeguati ai tuoi figli e sai che le tue impostazioni non possono essere alterate.

Impostare la password

Per impostare la password, clicca **Impostazioni** nella barra degli strumenti, seleziona la pagina **Configurazione** e seleziona **Abilita protezione password**:



Specifica la password nell'apposito campo, confermalala e clicca **OK** per salvarla. Clicca **OK** e inizierai a proteggere le impostazioni con la password. Dopo di ciò, ogni volta che qualcuno tenta di ottenere l'accesso alle impostazioni del prodotto o di creare una nuova configurazione gli verrà richiesta questa password.

Cambiare la password

Per cambiare la password, clicca **Impostazioni** nella barra degli strumenti, seleziona la pagina **Configurazione** e clicca **Cambia password** sotto **Protezione password**. Specifica e conferma la nuova password, poi clicca **OK**.

Disabilitare la password

Per disabilitare la password, clicca **Impostazioni** nella barra degli strumenti, seleziona la pagina **Configurazione** e deseleziona **Abilita la protezione password**. Dopo aver cliccato su **OK**, tutte le impostazioni del firewall saranno accessibili a ogni persona che usa il computer.

Puoi proteggere inoltre Outpost Firewall Pro dalla chiusura e dalla disinstallazione selezionando le caselle corrispondenti. Ciò impedisce alle persone non autorizzate di disabilitare la tua protezione e le restrizioni che hai impostato ed è molto utile per i genitori che vogliono avere il controllo sulla navigazione in Internet dei loro figli e per i datori di lavoro che vogliono limitare l'attività dei loro dipendenti.

Seleziona **Chiedi password sulla risposta alle richieste non critiche** se vuoi che Outpost Firewall Pro richieda la password quando un utente risponde alle finestre delle Regole Assistite e della protezione Host.

Nota:

- Ricorda la tua password. se dimentichi la password, dovrai reinstallare Outpost Firewall Pro o persino il sistema operativo.

4 Aggiornare Outpost Firewall Pro

L'aggiornamento è una delle procedure chiave per la sicurezza che dovresti effettuare regolarmente. Siccome spesso appare un nuovo malware, i benefici di avere una soluzione per la sicurezza aggiornata e ben configurata giustificano ampiamente il tempo speso per l'aggiornamento. Non aggiornando solamente il database antivirus e spyware, ma anche migliorando le precedenti versioni del software superando le problematiche incontrate dagli sviluppatori e dagli utenti. Considerando che la maggior parte degli aggiornamenti avvengono in background, non ci sono valide ragioni per non tenere adeguatamente aggiornato il software.

L'aggiornamento di Outpost Firewall Pro è automatico al 100%, incluso il download dei componenti aggiornati, l'installazione di questi file e le modifiche al Registro. Poiché è di vitale importanza per la tua sicurezza usare ultime tecnologie, l'aggiornamento è stato ideato nel modo più semplice e automatico possibile.

Di default, gli aggiornamenti vengono cercati ogni ora. Se hai bisogno di scaricare gli aggiornamenti immediatamente, clicca **Aggiornamento** sulla barra degli strumenti. Il wizard dell'aggiornamento di Outpost Firewall Pro eseguirà tutte le operazioni necessarie, scaricando gli ultimi componenti del prodotto disponibili, il database malware e le regole predefinite. Quando il processo è completo, clicca **Fine**. Puoi effettuare gli aggiornamenti manualmente quando preferisci cliccando su **Start > Tutti i Programmi > Agnitum > Outpost Firewall Pro > Aggiorna**.

Agnitum ti permette di cambiare la pianificazione degli aggiornamenti regolari e ti suggerisce di partecipare al programma Agnitum ImproveNet per aiutare gli altri a impostare nuove regole per l'aggiornamento.

Nota:

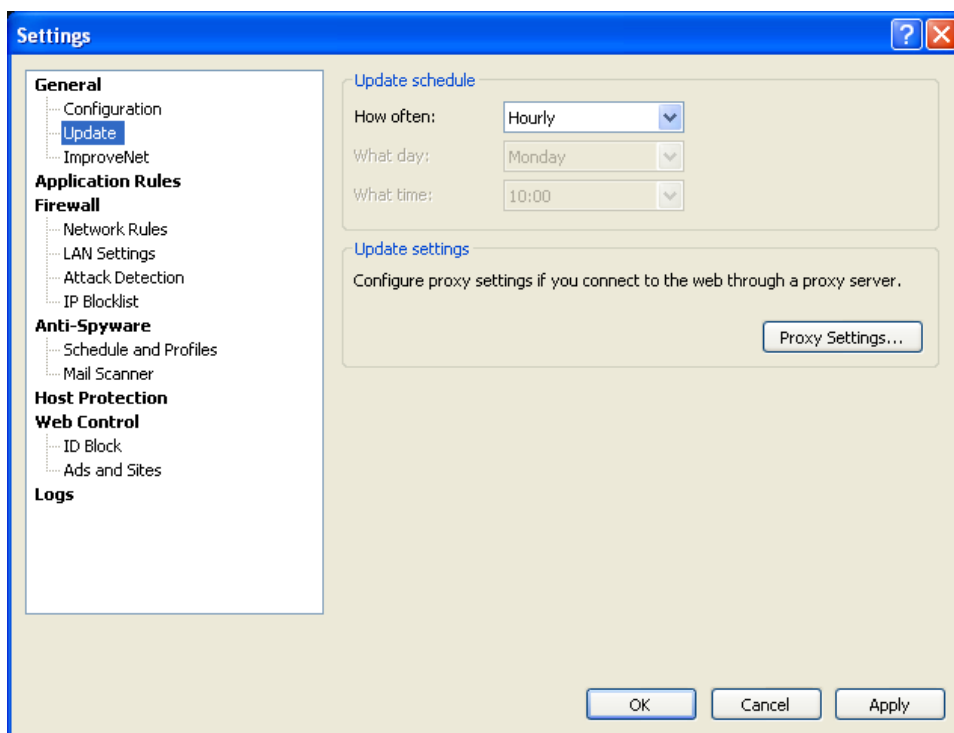
- L'attuale versione di Outpost Firewall Pro e l'elenco dei moduli sono disponibili nella pagina **Aggiornamento** delle impostazioni del prodotto.

4.1 Configurare gli Aggiornamenti

Per configurare gli aggiornamenti di Outpost Firewall Pro, clicca **Impostazioni** sulla barra degli strumenti e seleziona la pagina **Aggiornamento**.

Pianificazione

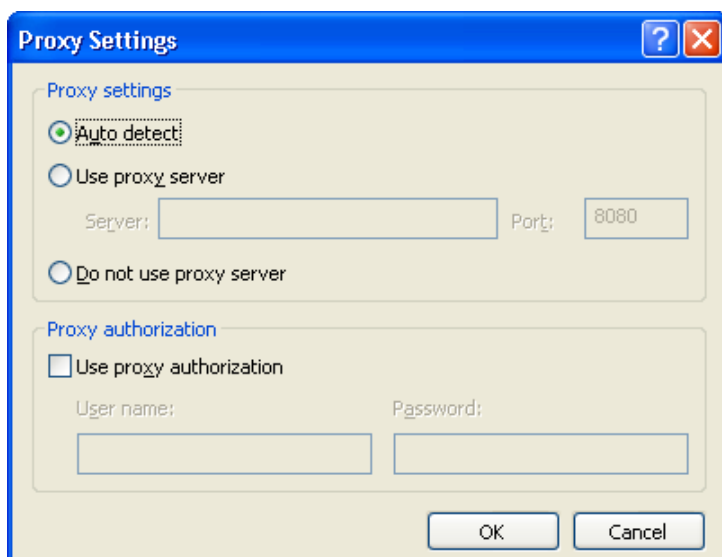
Di default, gli aggiornamenti sono schedulati a ogni ora, comunque, puoi scegliere tu quando desideri scaricare gli aggiornamenti di Outpost Firewall Pro. Per farlo, clicca su **Impostazioni** nella barra degli strumenti e seleziona la pagina **Aggiornamento**.



Sotto **Pianificazione Aggiornamenti** puoi specificare la frequenza del download degli aggiornamenti selezionando il parametro desiderato nell'elenco **Quanto spesso**. Se selezioni gli aggiornamenti settimanali, puoi specificare anche un giorno per gli aggiornamenti e l'ora esatta in cui il prodotto scaricherà gli aggiornamenti. Se selezioni gli aggiornamenti quotidiani, puoi specificare l'ora del giorno in cui scaricarli. Se selezioni **Manualmente**, gli aggiornamenti non verranno controllati senza che tu clicchi su **Aggiornamento** nella barra degli strumenti.

Impostazioni Proxy

Se ti connetti attraverso un server proxy, puoi configurare le impostazioni di connessione cliccando su **Impostazioni Proxy** nella pagina **Aggiornamento** delle impostazioni del prodotto. La rilevazione automatica di un proxy è l'opzione di default, ma puoi specificare il server e il numero di porta manualmente. Per far ciò, seleziona **Usa server proxy** sotto **Impostazioni Proxy** e digita il nome del server e il numero di porta nei campi forniti:



Oltre a specificare il server proxy, puoi definire se questo richiede l'autorizzazione selezionando **Usa autorizzazione proxy** sotto **Autorizzazione Proxy** e specifica le credenziali di accesso (nome utente e password).

Se (quando ti connetti a Internet) il tuo computer usa un server proxy, ma vuoi che il processo di aggiornamento venga compiuto direttamente dal server degli sviluppatori, seleziona **Non uso un server proxy**.

Se non usi un server proxy, puoi selezionare l'opzione **Non uso un server proxy** o **Rileva automaticamente**.

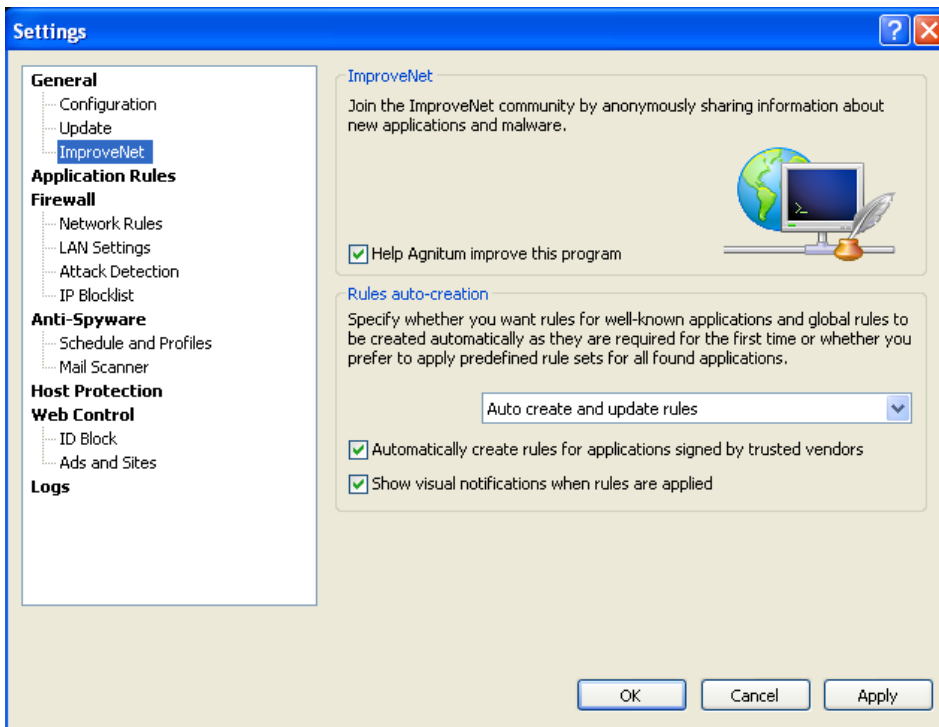
4.2 Agnitum ImproveNet

Ti invitiamo a contribuire a rendere Internet più sicuro attraverso il libero e cooperativo programma Agnitum Improvenet per migliorare la qualità, la sicurezza e le caratteristiche di controllo dei prodotti. Non devi far nulla. Semplicemente accettare di inviare dati non personali ed anonimi ogni settimana per espandere il database di Outpost Firewall Pro delle applicazioni conosciute, così da rendere disponibili un maggior numero di regole per l'accesso automatico. Ciò ridurrà il numero di finestre che richiederanno la tua attenzione.

Con il tuo consenso, Outpost Firewall Pro raccoglierà informazioni solo sulle applicazioni abilitate ad accedere alla rete del tuo computer. I dati vengono raccolti in forma anonima, ciò significa che non verrà raccolto alcun nome, indirizzo, identificativo di rete e nessun'altra informazione personale o identificativa. Semplicemente Outpost Firewall Pro raccoglierà dati sulle applicazioni abilitate ad accedere alla rete per le quali non esistono regole predefinite, e su ogni sistema di regole creato, e sulle statistiche generali delle applicazioni usate. L'informazione viene compressa e inviata una volta alla settimana in modo invisibile così da non disturbare le tue attività.

Dopo che una nuova regola di accesso viene ricevuta e convalidata, viene automaticamente condivisa con tutti gli utenti Outpost Firewall Pro attraverso gli Aggiornamenti insieme agli altri aggiornamenti del prodotto.

Per aiutarci a servire la comunità di Internet, ti preghiamo di aderire al programma Agnitum Improvenet. Semplicemente cliccando il menu **Impostazioni > ImproveNet** e selezionando **Aiuta a migliorare questo programma**. Puoi disabilitare questa caratteristica quando vuoi togliendo il segno di spunta da questa casella:



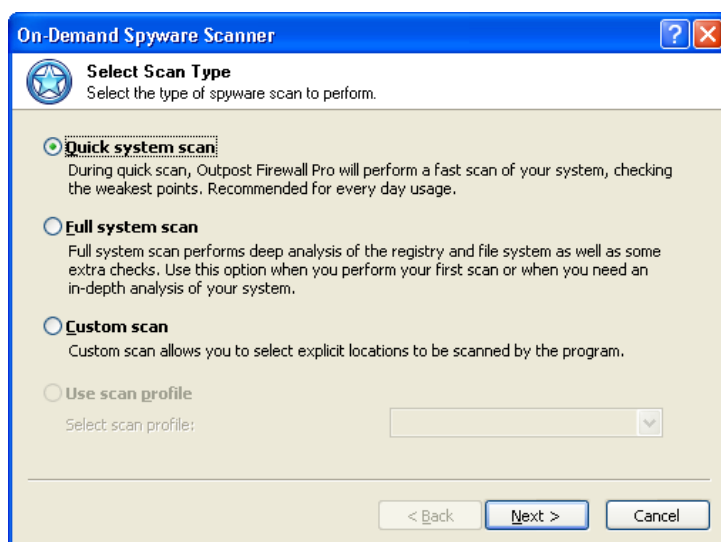
5 Effettuare un Controllo del Sistema

Il controllo globale del sistema On-demand ti lascia controllare e rimuovere le minacce sugli hard disk, nelle cartelle di rete, nei DVD, e nelle memorie esterne a seconda delle tue esigenze. Escludendo i percorsi e i tipi di file dal controllo (posizioni e/o tipi di file che tu non reputi possano essere vulnerabili a un'infezione), puoi specificare in modo molto flessibile le aree da controllare secondo le tue esigenze.

Si raccomanda di effettuare un controllo completo subito dopo l'installazione di Outpost Firewall Pro per verificare che sul tuo sistema non sia già presente del malware. Per far ciò, avvia lo **Scanner Malware On-Demand** cliccando sul **Controlla** nella barra degli strumenti. Puoi anche avviare lo scanner con la finestra principale chiusa cliccando con il destro sull'icona nella system tray e selezionando l'opzione **Controlla Malware**. Il wizard ti aiuta a specificare le impostazioni del controllo e ti guida per l'intero processo del controllo del sistema.

5.1 Selezionare il Tipo di Controllo

T Il primo passo ti permette di selezionare il tipo di controllo del sistema. Sono disponibili le seguenti opzioni:



- **Controllo rapido del sistema.** Questa opzione compie un rapido controllo del sistema verificando i punti più vulnerabili come i processi in memoria, le chiavi di registro più delicate, e determinati file e cartelle. Quest'opzione è consigliata nell'uso quotidiano.
- **Controllo completo del sistema.** Un controllo completo del sistema è un'analisi profonda del registro e dei file di sistema come anche ulteriori verifiche (verifica dei processi in memoria, controllo cookie, controllo dei valori di avvio). Questa verifica dovrebbe essere effettuata quando controlli il tuo sistema per la prima volta. L'operazione può richiedere diverso tempo in base alla velocità del tuo processore, il numero di applicazioni presenti nel computer e la quantità di dati che possiedi nei tuoi dischi.
- **Controllo Personalizzato.** Questa opzione ti permette di selezionare esplicitamente i percorsi da controllare. Puoi selezionare le opzioni sopra o puoi scegliere direttamente cosa controllare del tuo file system.
- **Usa profilo di scansione.** Questa opzione ti permette di selezionare un profilo di controllo personalizzato. Questa opzione è disponibile solo quando esiste almeno un profilo di scansione.

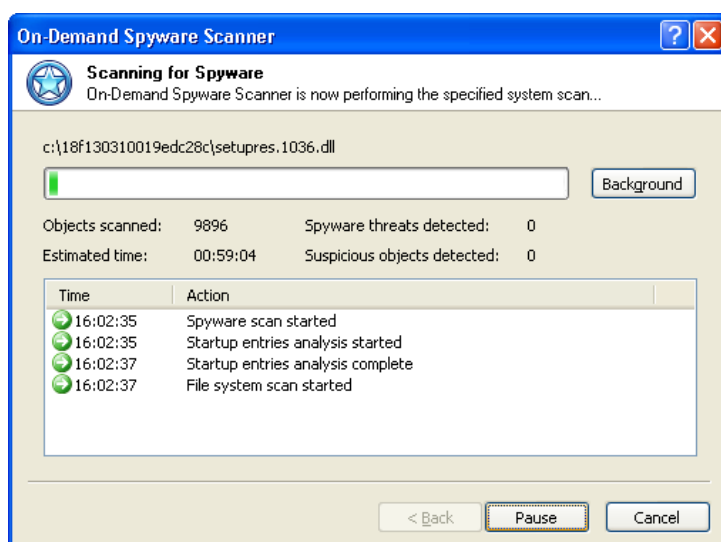
Suggerimento:

- Per aumentare le prestazioni del controllo, puoi far sì che Outpost Firewall Pro crei dei file cache d' stato in ogni cartella controllata selezionando **Abilita Tecnologia SmartScan** nel menu **Generale** delle proprietà del prodotto. Da notare, che i file di cache sono invisibili e che comunque possono causare dei falsi positivi negli strumenti anti-rootkit.

Dopo aver selezionato il tipo di controllo e, se necessario, il nome del profilo di scansione, clicca **Avanti** per continuare.

5.2 Controllare Percorsi Specifici

Dopo aver cliccato su **Avanti**, Outpost Firewall Pro inizia a controllare gli oggetti e i percorsi selezionati. La finestra successiva mostra le seguenti statistiche riferite al processo di controllo: il numero di oggetti controllati, il tempo stimato per la scansione e il numero degli oggetti rilevati come potenzialmente pericolosi:



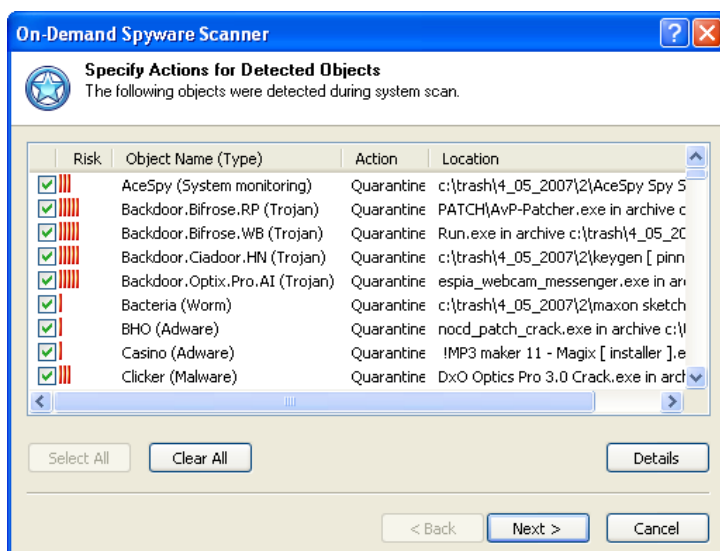
Il processo di controllo può essere eseguito in modalità background. Se vuoi lavorare con Outpost Firewall Pro mentre è in funzione il controllo, clicca **Background** e il wizard verrà minimizzato. Per vedere di nuovo la finestra completa, seleziona **Anti-Malware** nel pannello sinistro della finestra principale e clicca **Mostra Dettagli** nel pannello informativo.

Per uscire da un controllo e vedere in qualsiasi momento i suoi risultati, clicca **Annulla**.

Quando il controllo è terminato, viene mostrato automaticamente (se trovati) un elenco degli oggetti rilevati. Se il tuo sistema è pulito (es. non sono stati trovati oggetti sospetti), vengono mostrate solo le statistiche del controllo.

5.3 Rimuovere il Malware Rilevato

La finestra **Specifica le Azioni per gli Oggetti Rilevati** ti permette di visualizzare il malware rilevato così puoi rimuoverlo dal tuo sistema. Accanto a ogni malware viene mostrato il grado di rischio, la categoria a cui appartiene, e l'azione da eseguire su questo:



Doppio click per vedere un elenco di tutti i punti del computer in cui si trova l'oggetto.

Per cambiare l'azione, clicca con il destro l'oggetto e seleziona l'azione dal menu.

Seleziona le caselle accanto agli oggetti che vuoi processare e clicca **Avanti**. Outpost Firewall Pro poi effettua le azioni specificate—disinfetta l'oggetto, lo rimuove dal percorso dove è registrato e dalla memoria o lo mette in quarantena così da poterlo ripristinare nel caso in cui alcuni software non dovessero funzionare senza o se preferisci eliminarli completamente. Mentre si trova in quarantena, il malware non ha effetti sul tuo sistema. Per maggiori informazioni sulla quarantena malware, vedi Quarantena Malware.

Ogni software che non selezioni rimarrà intatto e continuerà a essere attivo sul tuo sistema.

Suggerimento:

- Se sai che un programma trovato non è un malware ma, in effetti, un software legittimo e non vuoi trattarlo come spyware o virus (per esempio per usare un'applicazione freeware, che deve mostrare pubblicità di un particolare programma adware), puoi aggiungere questi programmi all'elenco delle esclusioni. Outpost Firewall Pro ignorerà i programmi nell'elenco delle esclusioni e non mostrerà allarmi quando viene rilevata la loro attività. Inoltre, questi programmi non verranno mostrati nell'elenco degli spyware trovati.

Puoi specificare anche i file e le cartelle, che non dovranno essere controllate da Outpost Security Suite Pro per il malware.

Puoi aggiungere un oggetto rilevato all'elenco delle esclusioni, clicca con il destro sul suo nome e seleziona **Aggiungi Malware all'Elenco Ignora** o **Aggiungi File all'Elenco Ignora**.

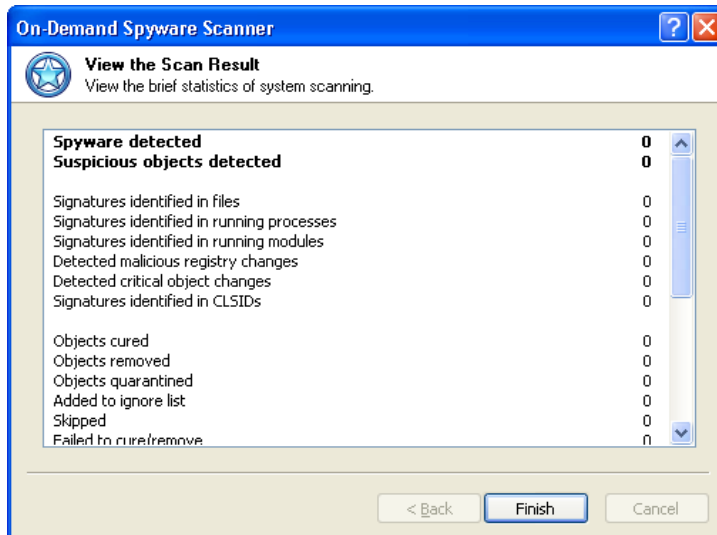
Puoi rimuovere successivamente gli oggetti dagli elenchi usando **Esclusioni** nella pagina **Anti-Malware** della finestra **Impostazioni** del prodotto.

Importante:

- Un cookie non è uno spyware, ma può essere usato come file ospite per trasferire informazioni private dal tuo computer a uno specifico sito web. I programmi spyware installati sul tuo computer possono scrivere le tue informazioni private nei file cookie, che possono essere letti in seguito dal sito che richiede questi cookie nel momento in cui visiti successivamente quel sito.

5.4 Visualizzare i Risultati del Controllo

L'ultima finestra del wizard mostra un rapporto del controllo dove puoi vedere il numero di malware rilevati, disinfettati, rimossi e messi in quarantena e altri dettagli. Dopo aver visto i risultati, clicca **Fine** per chiudere il wizard:



Nota:

- Per vedere gli oggetti che il componente Anti-Spyware ha rilevato e rimosso, apri la sezione **Visualizzatore Eventi** nel pannello sinistro della finestra principale di Outpost Firewall Pro e seleziona il rapporto **Anti-Spyware**.

6 Disinstallare Outpost Firewall Pro

Per disinstallare Outpost Security Suite Pro:

1. Clicca con il tasto destro del mouse sull'icona di Outpost Security Suite Pro posta nella system tray e seleziona **Esci**.
2. Clicca su **Start** nella barra degli strumenti di Windows e seleziona **Pannello di Controllo > Installazione Applicazioni**.
3. Seleziona Agnitum **Outpost Firewall Pro** e clicca **Rimuovi**.
4. Clicca su **Si** per confermare la rimozione.

Il programma ti chiederà in modo facoltativo di inviare un rapporto di feedback, per poter specificare le ragioni della rimozione. Ciò aiuterà gli sviluppatori a migliorare le prossime versioni del prodotto.

Tutte le azioni necessarie verranno eseguite automaticamente. Alla fine ti verrà richiesto di riavviare il sistema.

Nota:

- Per evitare conflitti con il programma riavvia il sistema dopo aver completato il processo di rimozione.

7 Risoluzioni Problemi

Se hai bisogno di assistenza per il funzionamento di Outpost Firewall Pro, visita la nostra pagina di supporto su <http://www.agnitum.it>. Tra le opzioni di supporto disponibili ci sono la knowledge base, la documentazione, il forum di supporto, le risorse web relative al prodotto, e il contatto diretto con i nostri ingegneri.

Informazioni su Agnitum

Agnitum Ltd. è una società di sviluppo software impegnata nella distribuzione e nel supporto di prodotti di sicurezza software di alta qualità. Agnitum offre due linee di prodotti - Outpost Security Suite Pro PRO, per la sicurezza dei computer personali o di famiglia, e Outpost Network Security, che assicura la protezione delle postazioni e le prestazioni delle reti aziendali. Agnitum fornisce soluzioni di sicurezza per grandi imprese, piccole e medie società, così come per i PC dei singoli utenti.

Distributore esclusivo per l'Italia:

Future Time S.r.l.
Viale Luca Gaurico 257 - 00143 Roma
www.futuretime.eu

Indirizzo della Sede Principale:

Acropoleos Avenue
8 Mabella Court
Nicosia, Cyprus