Aggiunte alla documentazione

Software di sicurezza Zone Alarm versione 7.1

Nel presente documento vengono trattate le nuove funzionalità non incluse nelle versioni localizzate del manuale utente. Fare clic sull'argomento desiderato nell'elenco seguente per visualizzare ulteriori informazioni.

- **Centro protezione identità ZoneAlarm—**Aiuta gli utenti a impedire, rilevare e, se necessario, porre rimedio a un eventuale furto di identità.
- **Modalità Gioco—**Interrompe temporaneamente la maggior parte delle scansioni, degli aggiornamenti e degli avvisi di software di sicurezza Zone Alarm per consentire all'utente di eseguire giochi sul computer limitando le interruzioni.
- **Protezioni di sistema speciali OSFirewall—**Determina se i programmi installati sul computer possono eseguire determinate azioni, come modificare la pagina iniziale di Internet Explorer oppure installare controlli ActiveX.
- **Opzioni della scansione antivirus—**Offre la possibilità di ignorare i file di dimensioni superiori a quelle specificate e include un database esteso di malware.
- **Scansione della memoria di sistema—**Esegue la scansione della RAM del computer.
- **Elenco delle eccezioni—**Offre la possibilità di gestire un elenco di elementi che devono essere ignorati dalle scansioni antivirus del software di sicurezza Zone Alarm.
- **Controllo dei programmi—**Offre la modalità Apprendimento automatico che riduce al minimo gli avvisi dei programmi durante la fase di "apprendimento" del computer da parte del software di sicurezza Zone Alarm.
- **Impostazione delle opzioni di sicurezza della rete—**Offre la possibilità di permettere o bloccare il traffico internet che utilizza il Protocollo Internet versione 6 (IPv6).
- **Correzioni alla documentazione e aggiornamenti**

Centro protezione identità ZoneAlarm

Con la diffusione dell'e-commerce, della memorizzazione elettronica dei dati e dell'invio di informazioni a mailing list, l'incidenza del furto di identità è aumentata negli ultimi anni. Gli hacker utilizzano malware per intercettare informazioni personali online, mentre i ladri rubano CD e portatili contenenti informazioni sui clienti oppure intercettano la corrispondenza con informazioni riservate (per esempio offerte di carte di credito pre-pagate).

Il Centro protezione identità ZoneAlarm è un sito Web che aiuta gli utenti a impedire, rilevare e, se necessario, porre rimedio a un eventuale furto di identità. Questo sito offre suggerimenti sulla protezione dell'identità, nonché risorse per il monitoraggio dell'utilizzo delle informazioni personali e su come porre rimedio al furto di identità.

L'accesso al Centro protezione identità può essere effettuato da ZoneAlarm Pro e ZoneAlarm Security Suite.

Per visitare il Centro protezione identità ZoneAlarm:

1. Selezionare **Protezione identità|Principale**.
2. Nell'area Centro protezione identità, fare clic su **Vai al Centro protezione identità ZoneAlarm**.

Modalità Gioco

La modalità Gioco interrompe temporaneamente la maggior parte delle scansioni, degli aggiornamenti e degli avvisi di software di sicurezza Zone Alarm per consentire all'utente di eseguire giochi sul computer limitando le interruzioni. Grazie a questa modalità l'utente può accettare o rifiutare temporaneamente tutte le richieste di autorizzazione dei programmi, per consentire a software di sicurezza Zone Alarm di rispondere automaticamente a tali richieste senza visualizzare gli avvisi. Le scansioni e gli aggiornamenti di prodotti automatici sono posticipati fino a quando non viene disattivata la modalità Gioco. La modalità Gioco rimane attiva fino a quando l'utente non la disattiva oppure fino a quando non viene disattivato software di sicurezza Zone Alarm o si spegne il computer.

La modalità Gioco interrompe tutti gli avvisi informativi e gli avvisi in cui si chiede all'utente di prendere una decisione, inclusi gli avvisi generati dall'impostazione Chiedi nell'elenco dei programmi, come gli avvisi di autorizzazione generati dai programmi che tentano di inviare posta elettronica o di agire come server, e gli avvisi di OSFirewall, che chiedono all'utente di consentire o negare un comportamento considerato insolito o sospetto. Le impostazioni della modalità Gioco non incidono sulle impostazioni Blocca o Consenti nell'elenco dei programmi. Se software di sicurezza Zone Alarm è stato configurato per bloccare sempre un determinato programma, continuerà a bloccarlo anche se si attiva la modalità Gioco con l'impostazione Consenti.

L'utilizzo della modalità Gioco potrebbe ridurre la sicurezza del sistema. Se si sceglie di consentire tutte le richieste di autorizzazione, si potrebbero aumentare le

probabilità che un programma dannoso attacchi il computer o riesca ad accedere ai dati. Se, dall'altra parte, si sceglie di negare tutte le richieste, si potrebbero interrompere le funzioni di un programma legittimo. Per questo è opportuno attivare la modalità Gioco solo per la durata del gioco.

Per attivare la modalità Gioco:

1. Fare clic col pulsante destro del mouse sull'icona nell'area di notifica del sistema e scegliere **Modalità Gioco...**
2. Nella finestra di dialogo Attivazione modalità Gioco che viene visualizzata, fare clic su una delle opzioni seguenti:

   Rispondi a tutti gli avvisi con "consenti"—Le richieste di autorizzazione saranno accettate.

   Rispondi a tutti gli avvisi con"nega"—Le richieste di autorizzazione saranno rifiutate.
3. Lasciare la finestra di dialogo aperta oppure ridurla a icona, ma non chiuderla (se si chiude la finestra, la modalità Gioco verrà disattivata).

   Quando la modalità Gioco è attiva, software di sicurezza Zone Alarm visualizza un'icona speciale () nell'area di notifica del sistema.

Per disattivare la modalità Gioco:

Eseguire una delle operazioni seguenti:

- Nella finestra di dialogo Attivazione modalità Gioco, fare clic su **Annulla** oppure sul pulsante Chiudi (X) nell'angolo superiore destro per chiudere la finestra.
- Nella finestra Attivazione modalità Gioco, fare clic su **Interrompi modalità Gioco**.
- Fare clic col pulsante destro del mouse sull'icona nell'area di notifica del sistema e scegliere **Interrompi modalità Gioco**.

La modalità Gioco viene disattivata automaticamente se si spegne il computer oppure si disattiva software di sicurezza Zone Alarm.

Protezioni di sistema speciali OSFirewall

La protezione di OSFirewall, che è attivata per impostazione predefinita, rileva i programmi che cercano di utilizzare il sistema operativo per attività sospette sul computer. È anche possibile configurare diverse protezioni di sistema speciali OSFirewall, per determinare se i programmi installati sul computer possono

eseguire determinate azioni, come modificare la pagina iniziale di Internet Explorer oppure installare controlli ActiveX.

Le protezioni di sistema speciali OSFirewall consentono di impedire alcuni dei comportamenti sospetti classificati come livello Medio nell'appendice "Comportamento dei programmi".

Per configurare le impostazioni di OSFirewall:

1. Selezionare **Controllo dei programmi**|**Principale**.
2. Nell'area Controllo dei programmi, fare clic su **Personalizza**.
3. Nella finestra di dialogo Impostazioni personalizzate Controllo dei programmi che viene visualizzata, selezionare la scheda **OSFirewall**.
4. Selezionare o deselezionare **Attiva OSFirewall**, come desiderato (per configurare le protezioni di sistema speciali OSFirewall nel prossimo passaggio, questa casella di controllo deve essere selezionata).
5. In alternativa, è possibile configurare varie protezioni di sistema speciali OSFirewall. Fare clic sul campo Stato di un'azione inclusa nell'elenco e selezionare **Consenti**, **Nega**, **Chiedi** o **Utilizza Impostazione programma**. Se si sceglie Utilizza Impostazione programma, software di sicurezza Zone Labs utilizza le impostazioni di SmartDefense Advisor o le impostazioni manuali.
6. Fare clic su **Applica** per salvare le impostazioni e lasciare la finestra di dialogo aperta, oppure fare clic su **OK** per salvare le impostazioni e chiudere la finestra di dialogo.

Opzioni della scansione antivirus

È possibile configurare la scansione antivirus in modo che ignori i file di dimensione superiore a quella specificata (l'impostazione predefinita è 8 MB). Questa opzione riduce i tempi di scansione senza aumentare i rischi, perché in genere i file virus hanno dimensioni minori di 8 MB. Anche se i file di grandi dimensioni esclusi dalla scansione potrebbero contenere virus, il computer rimarrà comunque protetto se è attiva la scansione all'accesso.

Inoltre, è possibile attivare il database esteso, che include un elenco completo di malware oltre all'elenco standard di virus. Tuttavia, alcuni malware elencati nel database esteso potrebbero essere già elencati nel database standard antispyware, quindi potrebbero essere esaminati due volte dalla scansione. Inoltre, l'elenco di malware del database esteso potrebbe includere programmi considerati validi.

Specificare le opzioni della scansione antivirus

1. Selezionare **Antivirus/Antispyware**|**Principale**, quindi fare clic su **Opzioni avanzate**.

   Viene visualizzata la finestra di dialogo Opzioni avanzate.

2. Sotto **Gestione virus**, selezionare **Opzioni di scansione**.

3. Selezionare o deselezionare la casella di controllo **Salta se l'oggetto supera**.

   Se si seleziona questa casella di controllo, specificare una dimensione massima nella casella **MB**.

4. Selezionare o deselezionare la casella di controllo **Attiva database esteso**, quindi fare clic su **OK**.

Scansione della memoria di sistema

Per eseguire la scansione della memoria di sistema, eseguire i passaggi seguenti.

Eseguire la scansione della memoria di sistema

1. Selezionare **Antivirus/Antispyware|Principale.**
2. Fare clic su **Opzioni avanzate**.

   Viene visualizzata la finestra di dialogo Opzioni avanzate.

3. Sotto Gestione virus, selezionare **Destinazioni della scansione**.
4. Selezionare le unità, le cartelle e i file da sottoporre a scansione.
5. Selezionare o deselezionare la casella di controllo **Scansione settori di avvio di tutte le unità locali**.
6. Selezionare o deselezionare la casella di controllo **Attiva scansione posta elettronica**, quindi fare clic su **OK**.

Elenco delle eccezioni

Sebbene alcuni programmi considerati sospetti dal database esteso possano potenzialmente danneggiare il computer o rendere i dati vulnerabili agli hacker, sono presenti molte applicazioni valide che vengono comunque rilevate come virus durante una scansione. Se si utilizza una di queste applicazioni, è possibile escluderla dalle scansioni antivirus aggiungendola all'elenco delle eccezioni. Per aggiungere programmi all'elenco delle eccezioni fare clic con il pulsante destro del mouse sull'elemento nell'elenco Risultati scansione e scegliere Ignora sempre nel menu.

Una volta inseriti nell'elenco delle eccezioni, questi programmi non verranno più rilevati durante le scansioni antivirus. Se all'elenco delle eccezioni è stato aggiunto accidentalmente un virus, è possibile rimuoverlo manualmente.

Rimuovere virus dall'elenco delle eccezioni

1. Selezionare **Antivirus/Antispyware|Principale**, quindi fare clic su **Opzioni avanzate**.
2. Sotto Gestione virus, selezionare **Eccezioni**.
3. Nella sezione Eccezioni cura virus, selezionare il virus che si desidera rimuovere, quindi fare clic su **Rimuovi dall'elenco**.
4. Fare clic su **OK**.

Controllo dei programmi

Il software di sicurezza Zone Alarm offre diversi metodi di controllo dei programmi. Il Controllo dei programmi di base consente di determinare i diritti di accesso e server dei singoli programmi. Il Controllo dei programmi avanzato impedisce al malware di danneggiare programmi attendibili. Il controllo di interazione delle applicazioni avvisa l'utente se un processo cerca di usare un altro processo oppure un programma cerca di avviare un altro programma. La protezione di OSFirewall rileva i programmi che cercano di utilizzare il sistema operativo per attività sospette sul computer.

Per limitare il numero di avvisi, utilizzare una delle funzioni seguenti:

- Se si utilizza il software di sicurezza Zone Alarm con antivirus, utilizzare il livello di Controllo dei programmi Apprendimento automatico. Questa funzione offre un livello moderato di protezione durante i primi 7-21 giorni di utilizzo del software di sicurezza Zone Alarm. Dopo la fase di "apprendimento" del computer da parte del software di sicurezza Zone Alarm, il livello di Controllo dei programmi viene reimpostato a Massimo.
- Per trarre vantaggio dalle impostazioni dei programmi consigliate da Zone Alarm, utilizzare SmartDefense Advisor insieme al Controllo dei programmi.

Impostare il livello di Controllo dei programmi

1. Selezionare **Controllo dei programmi**|**Principale**.
2. Nella sezione Controllo dei programmi, trascinare il dispositivo di scorrimento sull'impostazione desiderata.

Massimo (per le versioni con antivirus) Alto (per le versioni senza antivirus)	Con questa impostazione, saranno visualizzati numerosi avvisi. ◆ I programmi devono richiedere l'accesso a Internet e i diritti di agire da server. ◆ OSFirewall controllerà eventuali comportamenti sospetti. ◆ Il Controllo dei programmi avanzato e il Controllo interazione applicazioni sono attivati. ◆ Per impostazione predefinita, il Controllo dei componenti è disattivato.*
Automatico (per le versioni con antivirus)	Con questa modalità il numero di avvisi è ridotto al minimo. ◆ Questo livello di controllo è meno sicuro nei primi 7-21 giorni. ◆ La rete e OSFirewall controlleranno alcuni programmi.

Medio (per le versioni senza antivirus)	Questa è l'impostazione predefinita. ◆ I programmi devono richiedere l'accesso a Internet e i diritti di agire da server. ◆ OSFirewall controllerà eventuali comportamenti sospetti. ◆ Per impostazione predefinita, il Controllo dei componenti è disattivato.*
Min (per le versioni con antivirus)	◆ OSFirewall è disattivato. ◆ Per impostazione predefinita, il Controllo dei componenti è disattivato.* ◆ Sono disponibili il controllo del server e la modalità invisibile.
Basso (per le versioni senza antivirus)	◆ OSFirewall è disattivato. ◆ Per impostazione predefinita, il Controllo dei componenti è disattivato.* ◆ Il controllo del server e la modalità invisibile non sono disponibili.
Disattivato	Il Controllo dei programmi è disattivato. ◆ I programmi e i componenti non vengono autenticati e non ne viene eseguito l'apprendimento. ◆ Le autorizzazioni per i programmi non sono in vigore. ◆ A tutti i programmi sono concessi diritti di accesso/server. ◆ Viene consentito a tutti i programmi di assumere un comportamento sospetto. ◆ Non vengono visualizzati avvisi relativi ai programmi.

* Il Controllo dei componenti è disattivato per impostazione predefinita. Tuttavia, se il controllo dei componenti è stato attivato, rimarrà attivo fino a quando il Controllo dei programmi è impostato su Alto, Medio o Basso.

Impostazione delle opzioni di sicurezza della rete

Il rilevamento automatico della rete facilita la configurazione della zona attendibile, in modo che le tradizionali attività della rete locale, come la condivisione di file e stampanti, non siano interrotte. Il software di sicurezza Zone Alarm rileva solo le reti a cui si è fisicamente connessi. Le connessioni di rete instradate o virtuali non sono rilevate.

È possibile fare in modo che il software di sicurezza Zone Alarm includa automaticamente nella zona attendibile ogni rete rilevata oppure che chieda ogni volta se aggiungere la rete appena rilevata.

Specificare le impostazioni di rete

1. Selezionare **Firewall|Principale**.
2. Fare clic su **Avanzate**.
3. Nella sezione Impostazioni rete, scegliere le impostazioni di sicurezza.

Includi reti nella zona attendibile dopo il rilevamento	Sposta automaticamente le nuove reti nella zona attendibile. Questa impostazione offre la sicurezza minore.
Escludi reti dalla zona attendibile dopo il rilevamento	Blocca automaticamente l'aggiunta di nuove reti alla zona attendibile e le colloca nella zona Internet. Questa impostazione offre la sicurezza maggiore.
Chiedi in quale zona aggiungere nuove reti durante il rilevamento	Il software di sicurezza Zone Alarm visualizza un avviso di nuova rete o la configurazione guidata Rete, che permette di specificare la zona.
Aggiungi automaticamente nuove reti wireless non protette (WEP o WPA) nella zona Internet	Pone automaticamente le reti wireless non sicure nella zona Internet, impedendo l'accesso non autorizzato ai dati da parte di terzi che accedono alla rete.
Abilita i servizi di rete IPv6	Consenti l'accesso al computer al traffico di rete IPv6.

Correzioni alla documentazione e aggiornamenti

Nelle sezioni seguenti vengono presentate le correzioni e gli aggiornamenti non inclusi nel corpo principale della guida in linea e del manuale utente.

Scansioni alla ricerca di spyware

Nella documentazione delle versioni precedenti di software di sicurezza Zone Alarm si affermava che per avviare la scansione alla ricerca di spyware era necessario aprire un file oppure fare clic col pulsante destro del mouse su un file e selezionare un'opzione di scansione. Questa affermazione non era corretta.

Sono disponibili due metodi per avviare una scansione alla ricerca di spyware:

- È possibile fare clic su **Esegui scansione alla ricerca di spyware** nella sezione Antispyware della scheda Principale nel pannello **Antivirus/Antispyware**.
- È possibile pianificare l'esecuzione di una scansione di sistema una volta o a intervalli regolari. Per informazioni sulla configurazione di questa opzione, consultare la relativa guida in linea.

Esclusione dello spyware dalle scansioni

Nelle versioni precedenti della documentazione, nelle istruzioni relative all'esclusione di programmi specifici dalle scansioni non erano inclusi alcuni dettagli. Ecco la versione corretta.

Sebbene alcuni programmi spyware possano potenzialmente danneggiare il computer o rendere i dati vulnerabili agli hacker, sono presenti molte applicazioni valide che vengono comunque rilevate come spyware durante una scansione. Se si utilizza una di queste applicazioni, per esempio un software di riconoscimento vocale, è possibile escluderlo dalle scansioni di spyware aggiungendolo all'elenco delle eccezioni. Per aggiungere lo spyware all'elenco delle eccezioni fare clic con il pulsante destro del mouse sull'elemento nell'elenco Risultati scansione e scegliere Ignora sempre nel menu.

Risultati delle scansioni alla ricerca di spyware e virus

Nella finestra di dialogo Risultati scansione, che contiene i risultati delle scansioni alla ricerca di spyware e virus, è inclusa ora un'area Dettagli. Per le scansioni alla ricerca di spyware, nell'area Dettagli vengono elencati i percorsi completi di tutte le tracce spyware rilevate (per esempio chiavi di registro, cookies e così via). Queste informazioni sono utili a utenti avanzati che vogliono individuare i programmi spyware che non vengono curati automaticamente da software di sicurezza Zone Alarm. Per i risultati delle scansioni alla ricerca di virus, l'area Dettagli è vuota.

Controllo dei componenti

La documentazione è stata aggiornata per descrivere in modo più accurato l'interazione fra il Controllo dei programmi e il controllo dei componenti. Di seguito viene riportato il testo corretto.

Il controllo dei componenti è disattivato per impostazione predefinita, a prescindere dall'impostazione del Controllo dei programmi. La modifica del livello di Controllo dei programmi non implica l'attivazione automatica del controllo dei componenti. Tuttavia, una volta attivato, il controllo dei componenti rimarrà attivo fino a quando il Controllo dei programmi è impostato su Alto, Medio o Basso.

Nuovo comportamento dell'impostazione Memorizza

Nella versione 6.5, è stato modificato il comportamento della casella di controllo **Memorizza impostazione** negli avvisi Programma. Ecco la nuova descrizione.

Se SmartDefence Advisor è impostato su Automatico, software di sicurezza Zone Labs visualizza i messaggi Programma solo se non è disponibile nessuna impostazione automatica. Se quando si consente o si nega l'accesso a un programma si sceglie **Memorizza impostazione** in un avviso Programma, software di sicurezza Zone Labs mantiene l'impostazione effettuata a meno che SmartDefence Advisor abbia un'impostazione diversa o fino a quando l'utente non cambia l'impostazione manualmente nella scheda Programmi. Se non si sceglie **Memorizza impostazione**, software di sicurezza Zone Labs visualizzerà un altro avviso Programma al successivo tentativo da parte del programma di eseguire la stessa azione.

Modifica di un nome nel pannello Firewall

Una delle impostazioni del livello di sicurezza zona Internet e del livello di sicurezza zona attendibile nella scheda Principale del pannello Firewall è stata rinominata. L'impostazione Basso, infatti, è stata rinominata in Disattivato.

Nuove icone nell'area di notifica del sistema

Nella versione 6.5 sono state aggiunte le seguenti icone nell'area di notifica del sistema:

Icona	Descrizione
	software di sicurezza Zone Alarm sta eseguendo una scansione alla ricerca di spyware e/o virus. Per ulteriori dettagli sulle scansioni alla ricerca di virus e spyware, leggere la relativa guida in linea e le sezioni relative allo spyware nella parte “Correzioni alla documentazione e aggiornamenti", a pagina 8 del presente documento. Se presente, fare clic col pulsante destro del mouse su questa icona e selezionare **Visualizza scansione** per visualizzare la finestra di dialogo Stato scansione.
	La modalità Gioco è attiva e software di sicurezza Zone Alarm ha interrotto gli aggiornamenti, le scansioni e maggior parte degli avvisi. Per ulteriori dettagli sulla modalità Gioco, vedere “Modalità Gioco", a pagina 2.
	software di sicurezza Zone Alarm sta ricevendo un aggiornamento, per esempio l'aggiornamento di nuove definizioni spyware o virus.