System Center

Endpoint Protection per Mac

Manuale di installazione e Guida utente

Microsoft

Contenuti

System Center Endpoint Protection

Come conseguenza della sempre crescente diffusione dei sistemi operativi basati su Unix, i creatori di malware stanno sviluppando nuove minacce per colpire gli utenti Mac. System Center Endpoint Protection offre una protezione potente ed efficace contro queste minacce emergenti. System Center Endpoint Protection consente anche di allontanare le minacce di Windows, proteggendo gli utenti Mac durante le loro interazioni con gli utenti Windows e viceversa. Sebbene i malware Windows non rappresentino una minaccia diretta per il Mac, la disattivazione dei malware che hanno determinato l'infezione di una macchina Mac consentirà di evitarne la diffusione su computer Windows attraverso una rete locale o Internet.

Requisiti di sistema

Per un funzionamento ottimale di System Center Endpoint Protection, il sistema deve soddisfare i seguenti requisiti hardware e software:

System Center Endpoint Protection:

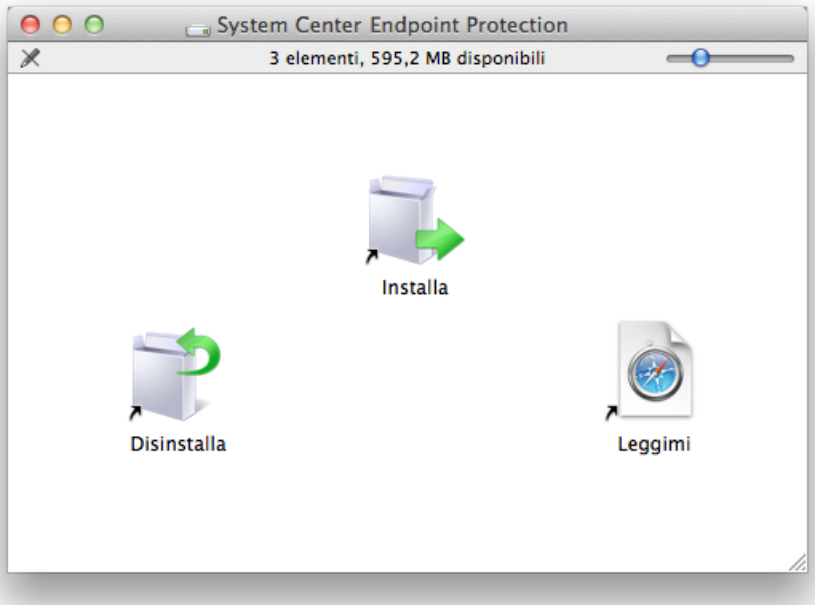
	Requisiti di sistema
Architettura processore	32 bit, 64 bit Intel®
Sistema operativo	Mac OS X 10.6 e versioni successive
Memoria	512 MB
Spazio libero su disco	100 MB

Installazione

Prima di cominciare la procedura di installazione, chiudere tutti i programmi aperti sul computer. In System Center Endpoint Protection sono contenuti componenti che possono creare conflitto con altri programmi antivirus già installati nel computer. Si raccomanda vivamente di rimuovere eventuali altri programmi antivirus per evitare potenziali problemi. È possibile installare System Center Endpoint Protection tramite il CD/DVD di installazione o mediante un file che è possibile scaricare dal nostro sito web.

Per avviare la procedura guidata di installazione, procedere in uno dei modi descritti di seguito:

- Se si utilizza il CD/DVD di installazione, inserirlo nel computer, aprirlo dal desktop o dalla finestra Finder e fare doppio clic sull'icona **Installa**.
- Se si utilizza un file scaricato, aprirlo e fare doppio clic sull'icona **Installa**.



Dopo aver avviato il programma di installazione, l'installazione guidata condurrà l'utente attraverso le fasi di configurazione di base. Dopo aver accettato i termini dell'Accordo di licenza del software e aver letto l'Informativa sulla privacy, è possibile scegliere uno dei seguenti tipi di installazione:

- Tipica 4
- Personalizzata 5

Installazione tipica

La modalità installazione tipica comprende le opzioni di configurazione adatte alla maggior parte degli utenti. Queste impostazioni garantiscono livelli massimi di sicurezza, nonché prestazioni ottimali del sistema. L'installazione tipica rappresenta l'opzione predefinita consigliata nel caso in cui gli utenti non abbiano particolari necessità relative a impostazioni specifiche.

Dopo aver selezionato la modalità di installazione **Tipica**, configurare il **Rilevamento delle applicazioni potenzialmente indesiderate** . Le applicazioni potenzialmente indesiderate non sono necessariamente dannose. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Applicazioni di questo tipo sono spesso legate all'installazione di altri programmi e potrebbe essere difficile rilevarle durante il processo di installazione. Sebbene tali applicazioni consentano di visualizzare una notifica durante il processo di installazione, esse possono essere installate facilmente senza il consenso dell'utente.

Dopo aver installato System Center Endpoint Protection, sarà necessario eseguire un controllo del computer per ricercare eventuali codici dannosi. Nella finestra principale del programma, fare clic su **Scansione computer**, quindi fare clic su **Controllo smart**. Per ulteriori informazioni sul Controllo del computer su richiesta, si rimanda alla sezione Controllo del computer su richiesta 10.

Installazione personalizzata

La modalità di installazione personalizzata è indicata per utenti esperti che desiderano modificare le impostazioni avanzate durante il processo di installazione.

Dopo aver selezionato la modalità di installazione **Personalizzata**, verrà richiesto di configurare le impostazioni del **Server proxy**. In caso di utilizzo di un server proxy, è possibile definirne i parametri selezionando l'opzione **Utilizzo un server proxy**. Immettere l'indirizzo IP o l'URL del server proxy nel campo **Indirizzo**. Nel campo porta, specificare la porta sulla quale il server proxy accetta le connessioni (per impostazione predefinita, la porta 3128). Nel caso in cui il server proxy richieda l'autenticazione, sarà necessario immettere un **Nome utente** e una **Password** validi per consentire l'accesso al server proxy. Se si è certi di non utilizzare un server proxy, scegliere l'opzione **Non utilizzo un server proxy**. In caso di dubbi, è possibile utilizzare le impostazioni di sistema correnti selezionando **Utilizza le impostazioni di sistema (scelta consigliata)**.

Nella fase successiva è possibile **Definire gli utenti con privilegi** che saranno in grado di modificare la configurazione del programma. Dalla lista di utenti sulla sinistra, è possibile scegliere gli utenti e l'opzione **Aggiungi** alla lista degli **Utenti con privilegi**. Per visualizzare tutti gli utenti del sistema, selezionare l'opzione **Mostra tutti gli utenti**.

Il passaggio successivo del processo di installazione consiste nella configurazione dell'opzione di **Rilevamento delle applicazioni potenzialmente indesiderate**. Le applicazioni potenzialmente indesiderate non sono necessariamente dannose. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Applicazioni di questo tipo sono spesso legate all'installazione di altri programmi e potrebbe essere difficile rilevarle durante il processo di installazione. Sebbene tali applicazioni consentano di visualizzare una notifica durante il processo di installazione, esse possono essere installate facilmente senza il consenso dell'utente.

Dopo aver installato System Center Endpoint Protection, sarà necessario eseguire un controllo del computer per ricercare eventuali codici dannosi. Nella finestra principale del programma, fare clic su **Scansione computer**, quindi fare clic su **Controllo smart**. Per ulteriori informazioni sulle scansioni del computer su richiesta, si rimanda alla sezione Scansione del computer su richiesta 10.

Disinstallazione

Se si desidera disinstallare System Center Endpoint Protection dal computer, procedere in uno dei modi descritti di seguito:

- inserire il CD/DVD di installazione System Center Endpoint Protection nel computer, aprirlo dal desktop o dalla finestra Finder e fare doppio clic sull'icona **Disinstalla**,
- aprire il file di installazione System Center Endpoint Protection (*.dmg*) e fare doppio clic sull'icona **Disinstalla** oppure
- lanciare il **Finder**, aprire la cartella **Applicazioni** sul disco rigido, premere ctrl e fare clic sull'icona System Center Endpoint Protection, quindi selezionare l'opzione **Mostra contenuti pacchetto**. Aprire la cartella **Contents > Helpers** e fare doppio clic sull'icona **Uninstaller**.

Guida introduttiva

In questo capitolo viene fornita una panoramica su System Center Endpoint Protection e sulle configurazioni di base.

Interfaccia utente

La finestra principale di System Center Endpoint Protection è suddivisa in due sezioni principali. La finestra principale sulla destra contiene informazioni corrispondenti all'opzione selezionata dal menu principale sulla sinistra.

Di seguito è riportata una descrizione delle opzioni del menu principale:

- **Stato protezione** - Fornisce informazioni relative allo stato di protezione di System Center Endpoint Protection. Se è attivata la **Modalità avanzata** verrà visualizzato il sottomenu **Statistiche**.
- **Scansione computer** - Questa opzione consente di configurare e avviare la Scansione del computer su richiesta.
- **Aggiorna** - Consente di visualizzare informazioni relative agli aggiornamenti del database delle firme antivirali.
- **Configurazione** - Selezionare questa opzione per regolare il livello di protezione del computer. Se è attivata la **Modalità avanzata** verrà visualizzato il sottomenu **Antivirus e antispyware**.
- **Strumenti** - Consente di accedere ai **File di registro**, alla **Quarantena** e alla **Pianificazione attività**. Questa opzione può essere visualizzata esclusivamente in **Modalità avanzata**.
- **Guida** - Fornisce le informazioni sul programma e consente di accedere ai file della guida.

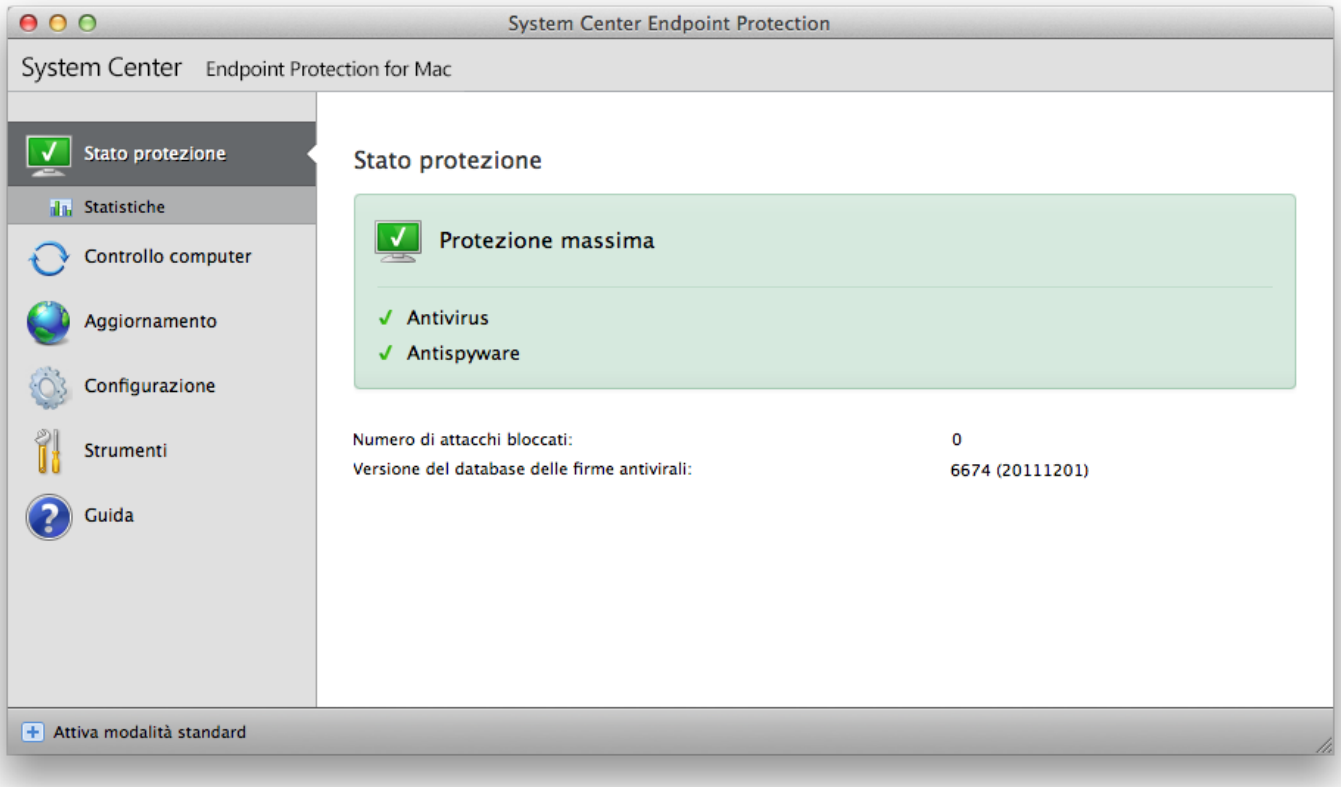
L'interfaccia utente System Center Endpoint Protection consente agli utenti di alternare le modalità Standard e Avanzata. La modalità standard consente l'accesso alle funzioni necessarie per le normali operazioni. Tale modalità non consente di visualizzare opzioni avanzate. Per passare da una modalità all'altra, fare clic sull'icona "più" (**+**) accanto a **Attiva modalità avanzata/Attiva modalità standard** nell'angolo in basso a sinistra della finestra principale del programma oppure premere cmd+M.

Quando si passa alla modalità avanzata, viene aggiunta l'opzione **Strumenti** al menu principale. L'opzione **Strumenti** consente di accedere ai sottomenu per i **File di registro**, la **Quarantena** e la **Pianificazione attività**.

NOTA: Tutte le istruzioni rimanenti della guida si riferiscono alla **Modalità avanzata**.

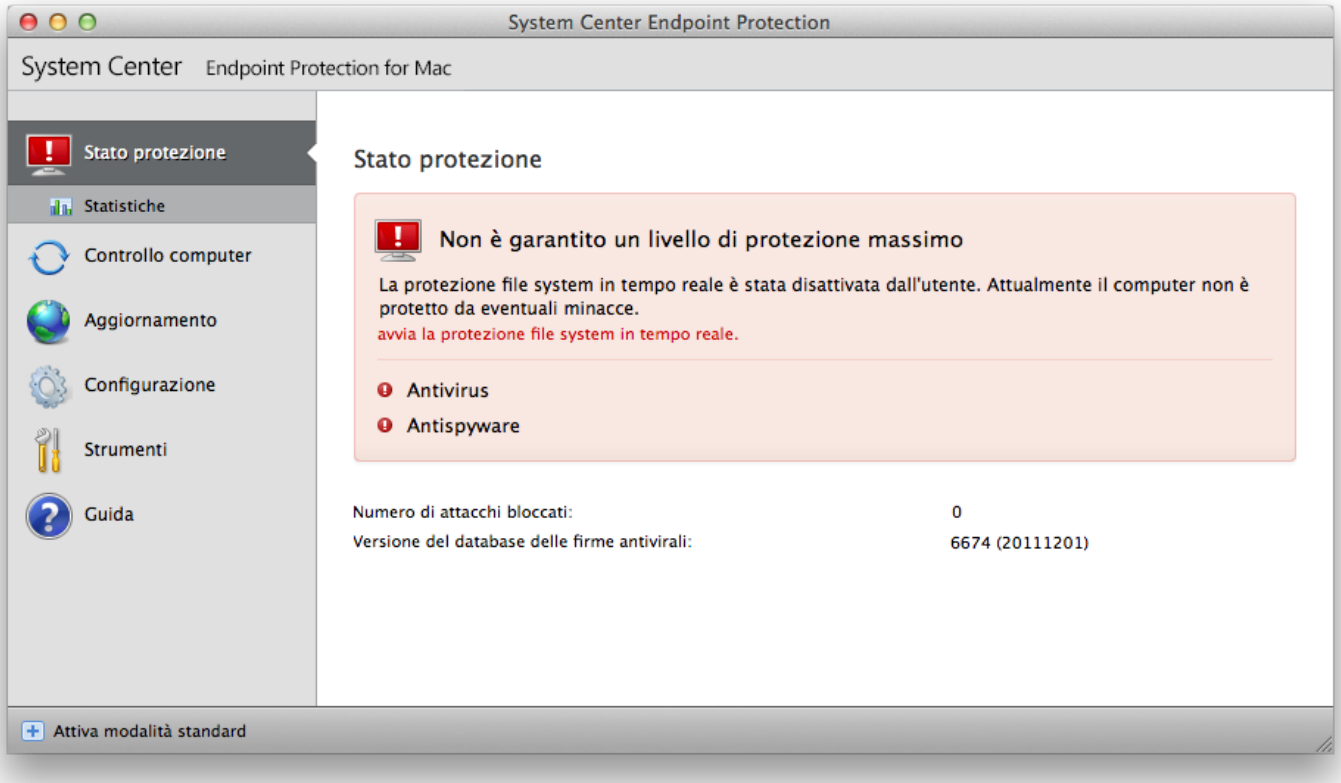
Verifica del funzionamento del sistema

Per visualizzare lo **Stato protezione**, fare clic sull'opzione in alto nel menu principale. Nel rapporto di funzionamento di System Center Endpoint Protection è possibile visualizzare la finestra principale, nonché un sottomenu con le **Statistiche**. Selezionarlo per visualizzare informazioni più dettagliate e statistiche relative ai controlli del computer eseguiti sul sistema. La finestra Statistiche è disponibile esclusivamente in modalità avanzata.



Cosa fare se il programma non funziona correttamente

Se i moduli attivati funzionano correttamente, verrà visualizzata un'icona di controllo verde. In caso contrario, verrà visualizzato un punto esclamativo rosso o un'icona di notifica arancione e, nella parte superiore della finestra, verranno visualizzate ulteriori informazioni sul modulo. Verrà inoltre visualizzata una soluzione consigliata per la riparazione del modulo. Per modificare lo stato dei singoli moduli, scegliere **Configurazione** dal menu principale e fare clic sul modulo desiderato.



Utilizzo di System Center Endpoint Protection

Protezione antivirus e antispyware

La protezione antivirus difende il sistema da attacchi dannosi, modificando i file che rappresentano minacce potenziali. In caso di rilevamento di una minaccia costituita da codice dannoso, il modulo antivirus è in grado di eliminarla bloccandola e pulendola, eliminandola o mettendola in quarantena.

Protezione file system in tempo reale

La funzione di Protezione file system in tempo reale consente di controllare tutti gli eventi correlati all'antivirus nel sistema. Tutti i file vengono sottoposti a scansione per la ricerca di codici dannosi al momento dell'apertura, creazione o esecuzione sul computer. La funzione Protezione file system in tempo reale viene attivata all'avvio del sistema.

Impostazione protezione in tempo reale

La protezione file system in tempo reale controlla tutti i tipi di supporto e attiva una scansione quando si verificano determinati eventi. La protezione file system in tempo reale potrebbe variare rispetto ai file appena creati o a quelli esistenti. Nel caso di file appena creati, è possibile applicare un livello di controllo maggiore.

In base alle impostazioni predefinite, la protezione in tempo reale viene attivata automaticamente all'avvio del sistema operativo e fornisce un controllo ininterrotto. In casi speciali, ad esempio in caso di conflitto con un altro scanner in tempo reale, la protezione in tempo reale può essere interrotta facendo clic sull'icona System Center Endpoint Protection sulla barra dei menu (sulla parte superiore dello schermo) e selezionando quindi l'opzione **Disattiva la protezione file system in tempo reale**. La protezione in tempo reale può anche essere interrotta dalla finestra del programma principale (**Configurazione** > **Antivirus e antispyware** > **Disattiva**).

Per modificare le impostazioni avanzate della protezione in tempo reale, fare clic su **Configurazione** > **Inserisci preferenze applicazione ...** > **Protezione** > **Protezione in tempo reale** e fare clic sul pulsante **Configurazione...** vicino a **Opzioni avanzate** (descritte nella sezione intitolata Opzioni avanzate di scansione 8).

Scansione al verificarsi di un evento

In base alle impostazioni predefinite, il controllo viene effettuato all'**Apertura dei file**, durante la **Creazione dei file** o l'**Esecuzione dei file**. È consigliabile mantenere le impostazioni predefinite che offrono il massimo livello di protezione in tempo reale per il computer.

Opzioni avanzate di scansione

In questa finestra è possibile definire le tipologie di oggetti da sottoporre a scansione da parte del motore di scansione e attivare/disattivare l'opzione di **Euristica avanzata** nonché modificare le impostazioni degli archivi e della cache file.

Si consiglia di non modificare i valori predefiniti nella sezione **Impostazioni predefinite archivi** salvo nel caso in cui fosse necessario risolvere un problema specifico, poiché livelli di ricerca degli archivi troppo elevati possono ostacolare le prestazioni del sistema.

È possibile passare alla scansione euristica avanzata per i file eseguiti, creati e modificati separatamente facendo clic sulla casella di controllo **Euristica avanzata** nelle rispettive sezioni dei parametri del motore.

Al fine di determinare un impatto minimo sul sistema durante l'utilizzo della protezione in tempo reale, è possibile definire le dimensioni della cache di ottimizzazione. Tale comportamento è attivo nel momento in cui si sceglie l'opzione **Attiva pulisci cache file**. Quando questa funzione è disattivata, tutti i file vengono controllati a ogni accesso. I file non verranno sottoposti a scansione ripetutamente dopo essere stati memorizzati nella cache (salvo il caso in cui siano stati modificati) fino alle dimensioni definite della cache. I file vengono controllati nuovamente subito dopo ogni aggiornamento del database delle firme antivirali.

Fare clic su **Attiva pulisci cache file** per attivare/disattivare questa funzione. Per impostare il numero di file da memorizzare nella cache, basta indicare il valore desiderato nel campo di inserimento accanto alla voce **Dimensioni cache**.

È possibile impostare ulteriori parametri di scansione nella finestra **Configurazione motore**. È possibile definire il tipo di **Oggetti** da sottoporre a scansione, le **Opzioni** da utilizzare e il livello di **Pulizia**, nonché definire le **Estensioni** e i **Limiti** delle dimensioni dei file per la protezione file system in tempo reale. È possibile accedere alla finestra di configurazione del motore facendo clic sul pulsante **Configurazione...** vicino a**Motore** nella finestra di Configurazione avanzata. Per ulteriori informazioni relative ai parametri del motore si rimanda alla sezione Configurazione parametri motore 13.

Esclusioni da scansione

Questa sezione consente di escludere alcuni file e cartelle dalla scansione.

- **Percorso** - percorso dei file e delle cartelle esclusi
- **Minaccia** - se è presente il nome di una minaccia accanto a un file escluso, significa che il file viene escluso solo per la minaccia indicata e non per tutte. Pertanto, se il file si infetta successivamente con altri malware, esso verrà rilevato dal modulo antivirus.
- **Aggiungi...**- esclude gli oggetti dal rilevamento. Inserire il percorso a un oggetto (è anche possibile utilizzare i caratteri jolly * e ?) o selezionare la cartella o il file dalla struttura ad albero.
- **Modifica...** - consente di modificare le voci selezionate
- **Elimina** - rimuove le voci selezionate
- **Predefinito** - annulla tutte le esclusioni.

Quando modificare la configurazione della protezione in tempo reale

La protezione in tempo reale è il componente più importante per la sicurezza di un sistema. Agire con prudenza nel momento in cui si modificano i parametri della protezione in tempo reale. È consigliabile modificarli solo in casi specifici, come ad esempio il caso in cui. si verifichi un conflitto con una determinata applicazione o con lo scanner in tempo reale di un altro programma antivirus.

Dopo l'installazione di System Center Endpoint Protection, tutte le impostazioni sono ottimizzate al fine di offrire il massimo livello di protezione del sistema agli utenti. Per ripristinare le impostazioni predefinite, fare clic sul pulsante **Predefinito** posizionato nell'angolo in basso a sinistra della finestra **Protezione in tempo reale** (**Configurazione** > **Inserisci preferenze applicazione ...** > **Protezione** > **Protezione in tempo reale**).

Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare il file di test eicar.com. Questo file di test è un file innocuo, speciale, rilevabile da tutti i programmi antivirus. Il file è stato creato da EICAR (European Institute for Computer Antivirus Research) per testare la funzionalità dei programmi antivirus.

Per controllare lo stato della Protezione in tempo reale da remoto, effettuare la connessione al computer client utilizzando il **Terminale** ed eseguire il seguente comando:
`/Applications/.scep/Contents/MacOS/scep_daemon --status`

Lo stato del Controllo in tempo reale verrà visualizzato come `RTPStatus=Enabled` o `RTPStatus=Disabled`.

L'output del bash del Terminale include anche i seguenti stati:

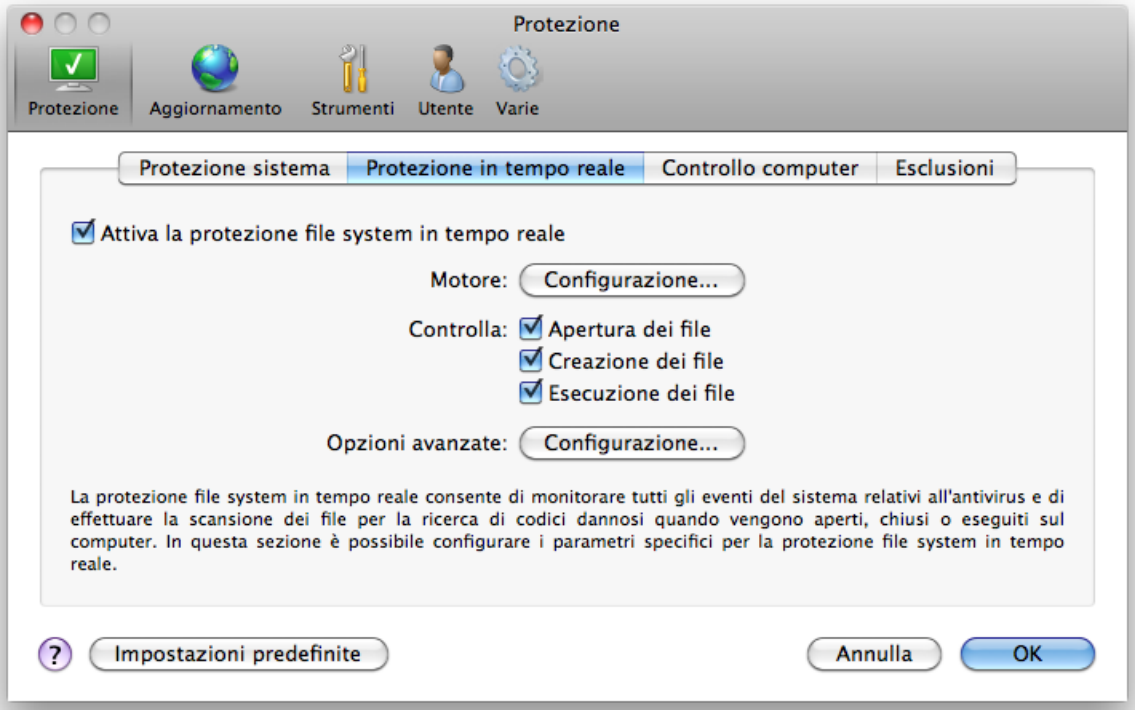
- versione di System Center Endpoint Protection installata sul computer client
- data e versione del database delle firme antivirali
- percorso al server di aggiornamento

NOTA: l'utilizzo del Terminale è consigliato esclusivamente agli utenti avanzati.

Cosa fare se la protezione in tempo reale non funziona

Nel prossimo capitolo verranno illustrate situazioni problematiche che si possono verificare quando si utilizza la protezione in tempo reale e verranno descritte le relative modalità di risoluzione.

La protezione in tempo reale è disattivata
Se la protezione in tempo reale è stata inavvertitamente disattivata da un utente, sarà necessario riattivarla. Per riattivare la protezione in tempo reale, selezionare **Configurazione** > **Antivirus e antispyware** e fare clic sul collegamento **Attiva la protezione file system in tempo reale** (sulla destra) nella finestra principale del programma. In alternativa, è possibile attivare la protezione file system in tempo reale nella finestra Configurazione avanzata in **Protezione** > **Protezione in tempo reale** selezionando l'opzione **Attiva protezione file system in tempo reale**.



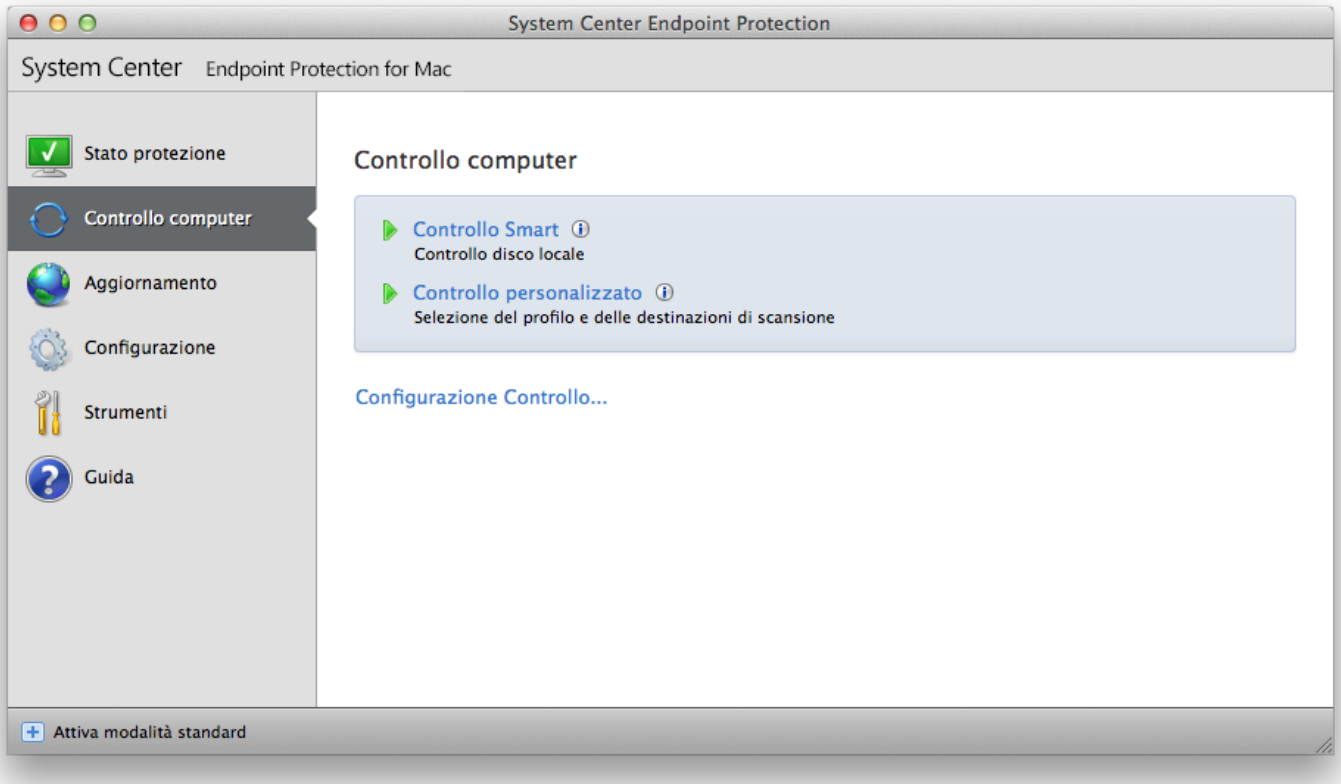
La protezione in tempo reale non rileva né pulisce le infiltrazioni
Assicurarsi che nel computer non siano installati altri programmi antivirus. Se sono attivati contemporaneamente due scudi di protezione in tempo reale, essi possono entrare in conflitto. È consigliabile disinstallare gli altri programmi antivirus che potrebbero essere presenti nel sistema.

La protezione in tempo reale non viene avviata
Se la protezione in tempo reale non si attiva all'avvio del sistema, ciò potrebbe dipendere da conflitti con altri programmi. In questo caso, consultare i propri specialisti dell'Assistenza tecnica.

Scansione del computer su richiesta

Se si sospetta che il computer sia infetto perché non funziona normalmente, eseguire una **Scansione computer** > **Controllo smart** per cercare eventuali infiltrazioni nel computer. Per garantire un livello massimo di protezione, è necessario eseguire regolarmente controlli del computer come parte delle misure di sicurezza di routine, anziché limitarsi ad eseguirle in caso di infezioni sospette. Una scansione regolare consente di rilevare infiltrazioni non rilevate dallo scanner in tempo reale se salvate su disco. Ciò accade se, al momento dell'infezione, lo scanner in tempo reale è stato disattivato o quando il database di firme antivirali è obsoleto.

È consigliabile eseguire una scansione del computer su richiesta almeno una volta al mese. Il controllo può essere configurato come attività pianificata in **Strumenti** > **Pianificazione attività**.



È inoltre possibile trascinare i file e le cartelle selezionati dal desktop o dalla finestra del Finder sulla schermata principale di System Center Endpoint Protection, sull'icona del dock, sull'icona della barra dei menu (parte superiore della schermata) o sull'icona dell'applicazione (collocata nella cartella */Applicazioni*).

Tipo di scansione

Sono disponibili due tipologie di scansione del computer su richiesta. **Controllo smart**, che consente di eseguire rapidamente la scansione del sistema senza che sia necessario configurare ulteriori parametri. **Controllo personalizzato**, che consente di selezionare uno dei profili di controllo predefiniti, nonché di scegliere destinazioni di controllo specifiche.

Controllo Smart

La funzione controllo Smart consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. Il vantaggio principale è la semplicità della procedura, che non richiede una configurazione di scansione dettagliata. Il controllo Smart consente di effettuare un controllo di tutti i file presenti nelle cartelle, nonché una pulizia o un'eliminazione automatica delle infiltrazioni rilevate. Il livello di disinfezione viene impostato automaticamente sul valore predefinito. Per ulteriori informazioni sui tipi di disinfezione, si rimanda alla sezione dedicata alla Pulizia 14.

Controllo personalizzato

Il **Controllo personalizzato** rappresenta una soluzione ottimale se si desidera specificare parametri di scansione quali destinazioni e metodi di scansione. Il vantaggio del controllo personalizzato consiste nella possibilità di configurare i parametri in dettaglio. È possibile salvare diverse configurazioni come profili di scansione definiti dagli utenti. Questi sono particolarmente utili se la scansione viene eseguita più volte con gli stessi parametri.

Per scegliere le destinazioni di scansione, selezionare **Controllo computer** > **Controllo personalizzato** quindi selezionare **Destinazioni di scansione** specifiche dalla struttura ad albero. Una destinazione di scansione può anche essere specificata in modo più preciso, immettendo il percorso alla cartella dei file che si desidera includere nel controllo. Se si desidera controllare solo il sistema senza ulteriori azioni di pulizia, selezionare l'opzione **Scansione senza rimozione**. È inoltre possibile scegliere tra tre livelli di disinfezione selezionando **Configurazione...** > **Pulizia**.

L'esecuzione di scansioni del computer attraverso il controllo personalizzato è un'operazione raccomandata per gli utenti avanzati con precedenti esperienze di utilizzo di programmi antivirus.

Destinazioni di scansione

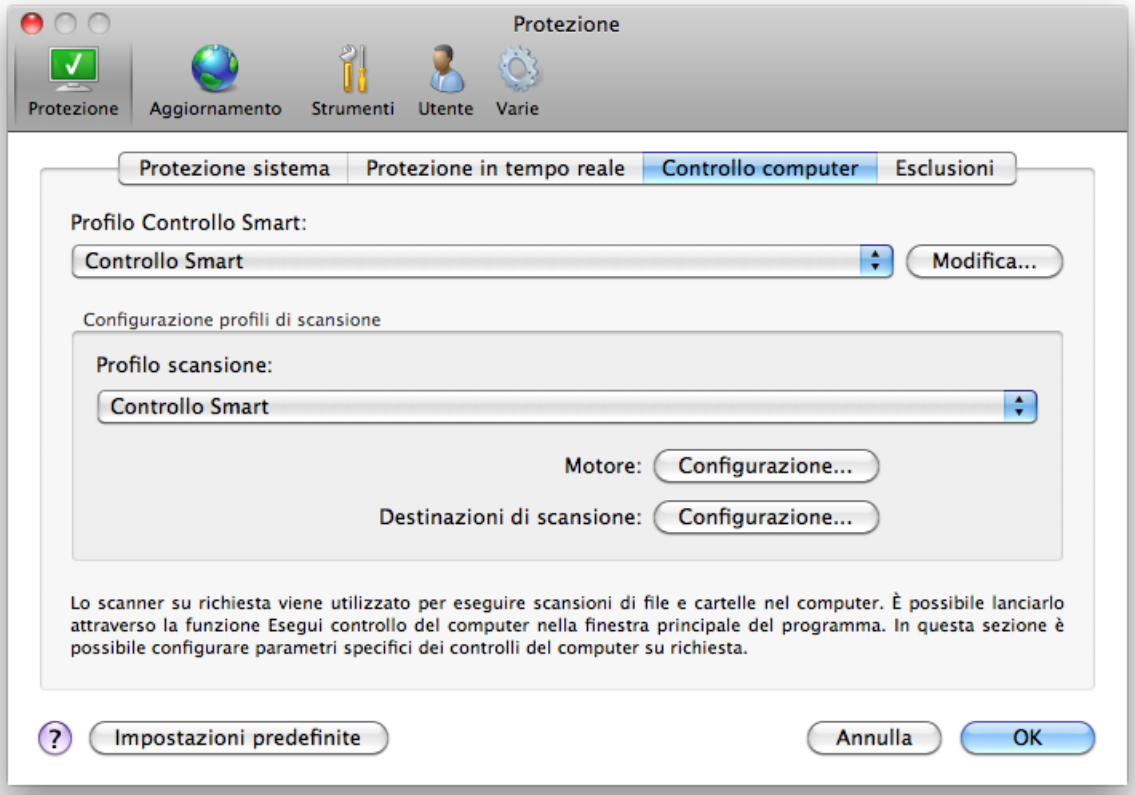
La struttura ad albero delle destinazioni di scansione consente di selezionare i file e le cartelle da sottoporre a scansione anti-virus. È altresì possibile selezionare le cartelle in base alle impostazioni di un determinato profilo.

Una destinazione di scansione può essere definita in modo più preciso, immettendo il percorso alla cartella dei file che si desidera includere nel controllo. Selezionare le destinazioni dalla struttura ad albero contenente una lista di tutte le cartelle presenti nel computer.

Profili di scansione

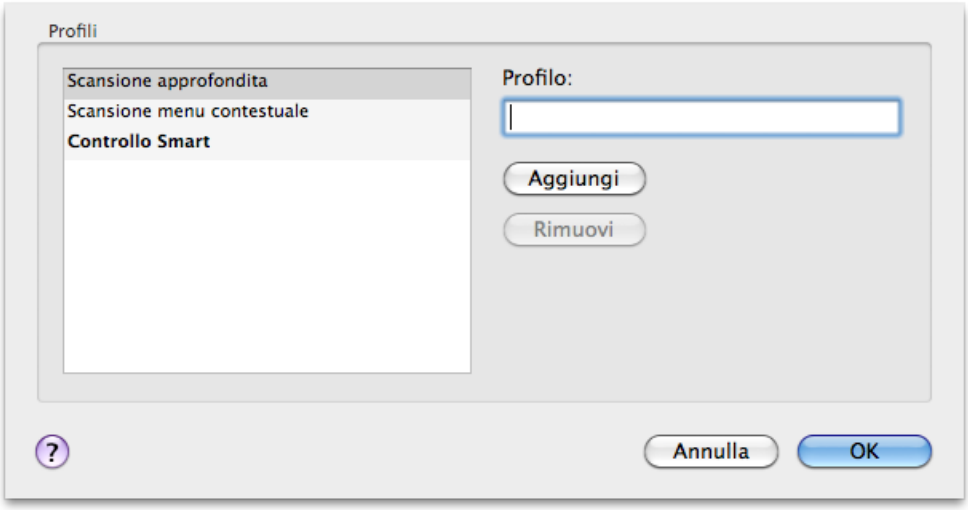
È possibile salvare le impostazioni di scansione preferite per scansioni future. È consigliabile creare un profilo di scansione differente (con diverse destinazioni di scansione, metodi di scansione e altri parametri) per ciascuna scansione utilizzata abitualmente.

Per creare un nuovo profilo, accedere alla sezione **Configurazione** > **Inserisci preferenze applicazione ...** > **Protezione** > **Scansione computer** e fare clic su **Modifica...** vicino alla lista dei profili correnti.



Per ricevere assistenza nella creazione di un profilo di scansione adatto alle proprie esigenze, si rimanda alla sezione Configurazione parametri motore 13 contenente una descrizione di ciascun parametro di configurazione della scansione.

Esempio: Si supponga di voler creare il proprio profilo di scansione e che la configurazione della Controllo smart sia appropriata solo in parte, in quanto non si desidera eseguire la scansione di eseguibili compressi o di applicazioni potenzialmente pericolose, bensì si intende applicare l'opzione di Massima pulitura. Nella finestra **Lista profili scanner su richiesta**, digitare il nome del profilo, fare clic sul pulsante **Aggiungi** e confermare facendo clic su **OK**. Specificare quindi i parametri in base alle proprie esigenze impostando **Motore** e **Destinazioni di scansione**.



Configurazione parametri motore

La tecnologia di scansione utilizzata in System Center Endpoint Protection è proattiva, ovvero fornisce protezione anche durante le prime ore di diffusione di una nuova minaccia. Essa utilizza una combinazione di diversi metodi (analisi del codice, emulazione del codice, firme generiche, firme antivirali) che operano in modo integrato per potenziare in modo significativo la protezione del sistema. Il motore di scansione è in grado di controllare contemporaneamente diversi flussi di dati, ottimizzando l'efficienza e la percentuale di rilevamento. Questa tecnologia è inoltre in grado di bloccare i rootkit.

Le opzioni di configurazione della tecnologia del motore consentono di specificare vari parametri di scansione:
- Tipi ed estensioni dei file da controllare
- Combinazione di diversi metodi di rilevamento
- Livelli di pulizia e così via.

Per aprire la finestra di configurazione, fare clic su **Configurazione** > **Antivirus e antispyware** > **Configurazione avanzata protezione antivirus e antispyware** quindi fare clic sul pulsante **Configurazione...** posizionato nei caratteri jolly **Protezione sistema**, **Protezione in tempo reale** e **Controllo computer**. Scenari di protezione diversi possono richiedere configurazioni diverse. Ciò detto, i parametri del motore sono configurabili singolarmente per i seguenti moduli di protezione:
- **Protezione sistema** > Controllo automatico file di avvio
- **Protezione file system in tempo reale** > Protezione file system in tempo reale
- **Controllo computer** > Scansione del computer su richiesta

I parametri del motore sono ottimizzati per ciascun modulo e la relativa modifica può influire in modo significativo sul funzionamento del sistema. Ad esempio, la modifica delle impostazioni per la scansione degli eseguibili compressi o per l'attivazione della scansione euristica avanzata nel modulo di protezione del file system in tempo reale potrebbe condurre a un rallentamento del sistema. È quindi consigliabile non modificare i parametri predefiniti del motore per tutti i moduli, con l'eccezione di Scansione computer.

Oggetti

Nella sezione **Oggetti** è possibile definire i file del computer che saranno sottoposti a scansione per la ricerca di infiltrazioni.

- **File** - consente di eseguire il controllo di tutti i tipi di file più comuni (programmi, immagini, file audio, file video, database e così via).
- **Collegamenti simbolici** - (Solo per scansione su richiesta): consentono di effettuare la scansione di tipologie speciali di file contenenti una stringa di testo interpretata e seguita dal sistema operativo come percorso a un altro file o directory.
- **File di e-mail** - (non disponibile nel caso della protezione in tempo reale): consente di effettuare la scansione di file speciali contenenti messaggi di posta elettronica.
- **Caselle di posta** - (non disponibile nel caso della protezione in tempo reale): consente di effettuare la scansione delle caselle di posta del sistema. Un uso scorretto di questa opzione potrebbe determinare un conflitto con il client e-mail.
- **Archivi** - (non disponibile nel caso della protezione in tempo reale) consente di eseguire il controllo dei file compressi in archivi (.rar, .zip, .arj, .tar e così via).
- **Archivi autoestraenti** - (non disponibile nel caso della protezione in tempo reale): consente di effettuare la scansione dei file contenuti in archivi autoestraenti.
- **Eseguibili compressi** - a differenza dei file di archivio standard, i file eseguibili compressi vengono decompressi in memoria, in aggiunta agli eseguibili statici standard (UPX, yoda, ASPack, FGS e così via).

Opzioni

Nella sezione **Opzioni**, è possibile selezionare i metodi utilizzati durante una scansione del sistema per il rilevamento di eventuali infiltrazioni. Sono disponibili le seguenti opzioni:

- **Euristica** - L'euristica è un algoritmo che analizza le attività (dannose) dei programmi. Il vantaggio principale del rilevamento euristico consiste nella possibilità di rilevare un nuovo software dannoso che in precedenza non esisteva o che non era incluso nell'elenco dei virus conosciuti (database di firme antivirali).
- **Euristica avanzata** - L'euristica avanzata comprende un algoritmo di euristica unico ottimizzato per il rilevamento di worm e trojan horse scritto in linguaggi di programmazione di alto livello. Grazie all'euristica avanzata, la capacità di rilevamento del programma è decisamente più elevata.
- **Applicazioni potenzialmente indesiderate** - Si tratta di applicazioni non necessariamente dannose. Tuttavia, esse potrebbero influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. I cambiamenti più significativi comprendono finestre popup indesiderate, attivazione ed esecuzione di processi nascosti, aumento dell'utilizzo delle risorse di sistema, modifiche dei risultati delle ricerche e applicazioni che comunicano con server remoti.
- **Applicazioni potenzialmente pericolose** - tali applicazioni si riferiscono a software commerciali e legali che possono essere sfruttati dagli aggressori informatici se installati all'insaputa dell'utente. Tale classificazione comprende programmi quali strumenti di accesso remoto. Pertanto, questa opzione è disattivata per impostazione predefinita.

Pulizia

Le impostazioni di pulizia determinano il comportamento dello scanner durante la disinfezione di file infetti. Sono disponibili 3 livelli di disinfezione:

- **Nessuna pulizia** - I file infetti non vengono puliti automaticamente. Il programma consentirà di visualizzare una finestra di avviso per consentire all'utente di scegliere un'azione.
- **Pulizia standard** - Il programma tenterà di pulire o eliminare automaticamente un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma proporrà una serie di azioni di follow-up. La scelta tra queste azioni verrà visualizzata anche nel caso in cui non possa essere completata un'azione predefinita.
- **Massima pulizia** - Il programma pulirà o eliminerà tutti i file infetti (inclusi gli archivi). Le uniche eccezioni sono rappresentate dai file di sistema. Nel caso in cui non fosse possibile pulirli, l'utente potrà intraprendere un'azione all'interno di una finestra di avviso.

Attenzione: Nella modalità di pulizia standard, viene eliminato l'intero file di archivio solo se tutti i file contenuti sono infetti. Nel caso in cui fossero presenti anche file non infetti, esso non verrà eliminato. Se nella modalità di Massima pulizia viene rilevato un file di archivio infetto, verrà eliminato l'intero file, anche se sono presenti file puliti.

Estensioni

Un'estensione è la parte del nome di un file delimitata da un punto. L'estensione definisce il tipo e il contenuto del file. Questa sezione della configurazione dei parametri del motore consente di definire i tipi di file da escludere dalla scansione.

Per impostazione predefinita, tutti i file vengono sottoposti a scansione indipendentemente dall'estensione. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dalla scansione. I pulsanti **Aggiungi** e **Rimuovi** consentono di attivare o impedire la scansione delle estensioni desiderate.

L'esclusione di file dalla scansione è talvolta utile nel caso in cui il controllo di determinati tipi di file impedisca il corretto funzionamento del programma. Ad esempio, è consigliabile escludere le estensioni *.log*, *.cfg* e *.tmp*.

Limiti

La sezione **Limiti** consente di specificare la dimensione massima degli oggetti e i livelli degli archivi nidificati sui quali eseguire la scansione:

- **Dimensioni massime:** Consente di definire la dimensione massima degli oggetti da sottoporre a scansione. Il modulo antivirus eseguirà unicamente la scansione degli oggetti di dimensioni inferiori a quelle specificate. Si consiglia di non modificare il valore predefinito, poiché di norma non sussiste alcun motivo per farlo. Questa opzione dovrebbe essere modificata solo da utenti esperti che abbiano ragioni particolari per escludere oggetti di dimensioni maggiori dalla scansione.
- **Durata massima controllo:** Consente di definire il valore massimo di tempo destinato alla scansione di un oggetto. Se è stato immesso un valore definito dall'utente, il modulo antivirus interromperà la scansione di un oggetto una volta raggiunto tale valore temporale, indipendentemente dal fatto che la scansione sia stata completata.
- **Massimo livello di nidificazione:** Consente di specificare il livello massimo di scansione degli archivi. Si consiglia di non modificare il valore predefinito di 10; in circostanze normali non sussiste alcun motivo per farlo. Se la scansione termina prima del tempo a causa del numero di archivi nidificati, l'archivio non verrà controllato.

- **Dimensione massima file:**Questa opzione consente di specificare le dimensioni massime dei file contenuti all'interno degli archivi da sottoporre a scansione una volta estratti. Se, a causa di tale limite, la scansione termina prima del tempo, l'archivio non verrà controllato.

Altri

Al fine di garantire il miglior livello di scansione, l'attivazione dell'ottimizzazione intelligente consente l'utilizzo delle impostazioni più efficienti alla velocità di scansione più elevata. I vari moduli di protezione eseguono la scansione in modo intelligente, utilizzando metodi di scansione differenti e applicandoli a tipi di file specifici. L'ottimizzazione Smart non è definita in modo rigido all'interno del prodotto. Il nostro team di sviluppo provvede costantemente all'implementazione di nuove modifiche che vengono successivamente integrate in System Center Endpoint Protection attraverso aggiornamenti regolari. Se l'opzione ottimizzazione Smart non è attivata, durante la scansione vengono applicate solo le impostazioni definite dall'utente di moduli specifici nell'architettura del motore.

Esegui scansione flussi dati alternativi (Solo per scansione su richiesta)
I flussi di dati alternativi (fork risorsa/dati) utilizzati dal file system sono associazioni di file e cartelle invisibili alle tecniche di scansione standard. Numerose infiltrazioni tentano di eludere le rilevazioni presentandosi come flussi di dati alternativi.

Rilevamento di un'infiltrazione

Le infiltrazioni possono raggiungere il sistema da diversi accessi: pagine web, cartelle condivise, messaggi e-mail o periferiche rimovibili (USB, dischi esterni, CD, DVD, dischetti e così via).

Se il computer mostra segnali di infezione da malware (ad esempio appare più lento, si blocca spesso e così via), è consigliabile seguire le seguenti istruzioni:

1. Aprire System Center Endpoint Protection e fare clic su **Scansione computer**.
2. Fare clic su **Controllo Smart** (per ulteriori informazioni, vedere la sezione Controllo Smart 11).
3. Al termine della scansione, controllare nel registro il numero di file sottoposti a scansione, di file infetti e di file puliti.

Se si desidera effettuare la scansione solo di una parte del disco, scegliere **Scansione personalizzata** e selezionare gli oggetti da controllare alla ricerca di virus.

Per avere un'idea generale di come System Center Endpoint Protection gestisce le infiltrazioni, si supponga che il monitoraggio del file system in tempo reale, che utilizza il livello di pulizia predefinito, rilevi un'infiltrazione. Verrà eseguito il tentativo di pulire o eliminare il file. In assenza di azioni predefinite disponibili per il modulo di protezione in tempo reale, verrà chiesto all'utente di selezionare un'opzione in una finestra di avviso. Le opzioni generalmente disponibili sono **Pulisci**, **Elimina** e **Nessuna azione**. Non è consigliabile selezionare **Nessuna azione**, poiché con tale opzione si lasciano i file infetti inalterati. È opportuno selezionare questa opzione solo quando si è certi che il file non è pericoloso e che si tratta di un errore di rilevamento.

Pulizia ed eliminazione - Applicare la pulizia nel caso in cui un file sia stato attaccato da un virus che ha aggiunto al file pulito un codice dannoso. In tal caso, tentare in primo luogo di pulire il file infetto per ripristinarne lo stato originale. Nel caso in cui il file sia composto esclusivamente da codici dannosi, verrà eliminato.

Eliminazione dei file negli archivi In modalità di pulizia predefinita, l'intero archivio verrà eliminato solo nel caso in cui contenga file infetti e nessun file pulito. In pratica, gli archivi non vengono eliminati nel caso in cui dovessero contenere anche file puliti non dannosi. È tuttavia consigliabile essere prudenti durante l'esecuzione di una scansione di **Massima pulizia**, poiché in questa modalità l'archivio viene eliminato anche se contiene un solo file infetto, indipendentemente dallo stato degli altri file dell'archivio.

Aggiornamento del programma

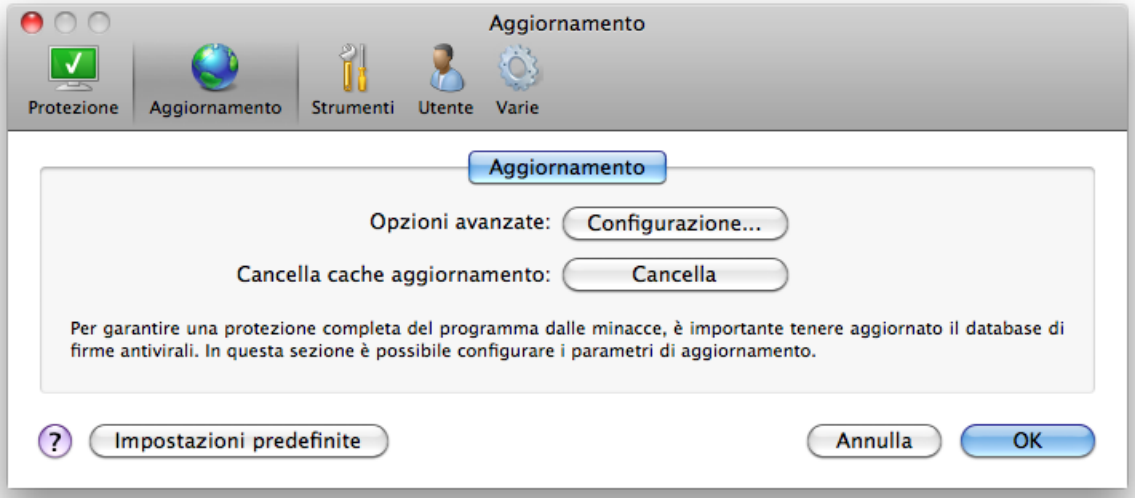
Per garantire il massimo livello di sicurezza, è necessario aggiornare regolarmente System Center Endpoint Protection. Il modulo di aggiornamento garantisce l'aggiornamento costante del programma grazie alla possibilità di scaricare il database delle firme antivirali più recente.

Facendo clic su **Aggiorna** nel menu principale, è possibile visualizzare lo stato corrente degli aggiornamenti, comprese la data e l'ora dell'ultimo aggiornamento eseguito correttamente e valutare se sia necessario un aggiornamento. Per avviare manualmente il processo di aggiornamento, fare clic su **Aggiorna database delle firme antivirali**.

In circostanze normali, ovvero in caso di download corretto degli aggiornamenti, verrà visualizzato il messaggio *Non sono necessari aggiornamenti - il database delle firme antivirali installato è aggiornato* nella finestra Aggiornamento.

La finestra di aggiornamento contiene anche informazioni relative alla versione del database di firme antivirali. Questo indicatore numerico rappresenta un collegamento attivo al sito web in cui vengono riportate tutte le firme aggiunte nel corso dell'aggiornamento in questione.

Impostazione dell'aggiornamento



Per attivare l'utilizzo della modalità test (download degli aggiornamenti pre-rilascio), fare clic sul pulsante **Configurazione...** accanto a **Opzioni avanzate**, quindi selezionare la casella di controllo **Attiva aggiornamenti pre-rilascio**. Per disattivare la visualizzazione delle notifiche sulla barra delle applicazioni al completamento dell'aggiornamento eseguito con successo, selezionare la casella di controllo **Non visualizzare notifiche relative agli aggiornamenti avvenuti con successo**.

Per eliminare tutti i dati di aggiornamento archiviati temporaneamente, fare clic sul pulsante **Cancella** accanto a **Cancella cache aggiornamento**. Utilizzare questa opzione in caso di problemi relativi all'aggiornamento.

Come creare attività di aggiornamento

È possibile avviare gli aggiornamenti manualmente, selezionando l'opzione **Aggiorna database delle firme antivirali** nella finestra principale visualizzata dopo aver selezionato l'opzione **Aggiorna** dal menu principale.

Gli aggiornamenti possono essere eseguiti anche come attività programmate. Per configurare un'attività programmata, fare clic su **Strumenti** > **Pianificazione attività**. Per impostazione predefinita, in System Center Endpoint Protection sono attivate le seguenti attività:

- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo l'accesso dell'utente**

È possibile modificare ciascuna di queste attività di aggiornamento in base alle proprie esigenze. Oltre alle attività di aggiornamento predefinite, è possibile creare nuove attività di aggiornamento con una configurazione definita dall'utente. Per ulteriori dettagli sulla creazione e sulla configurazione delle attività di aggiornamento, vedere la sezione Pianificazione attività 18.

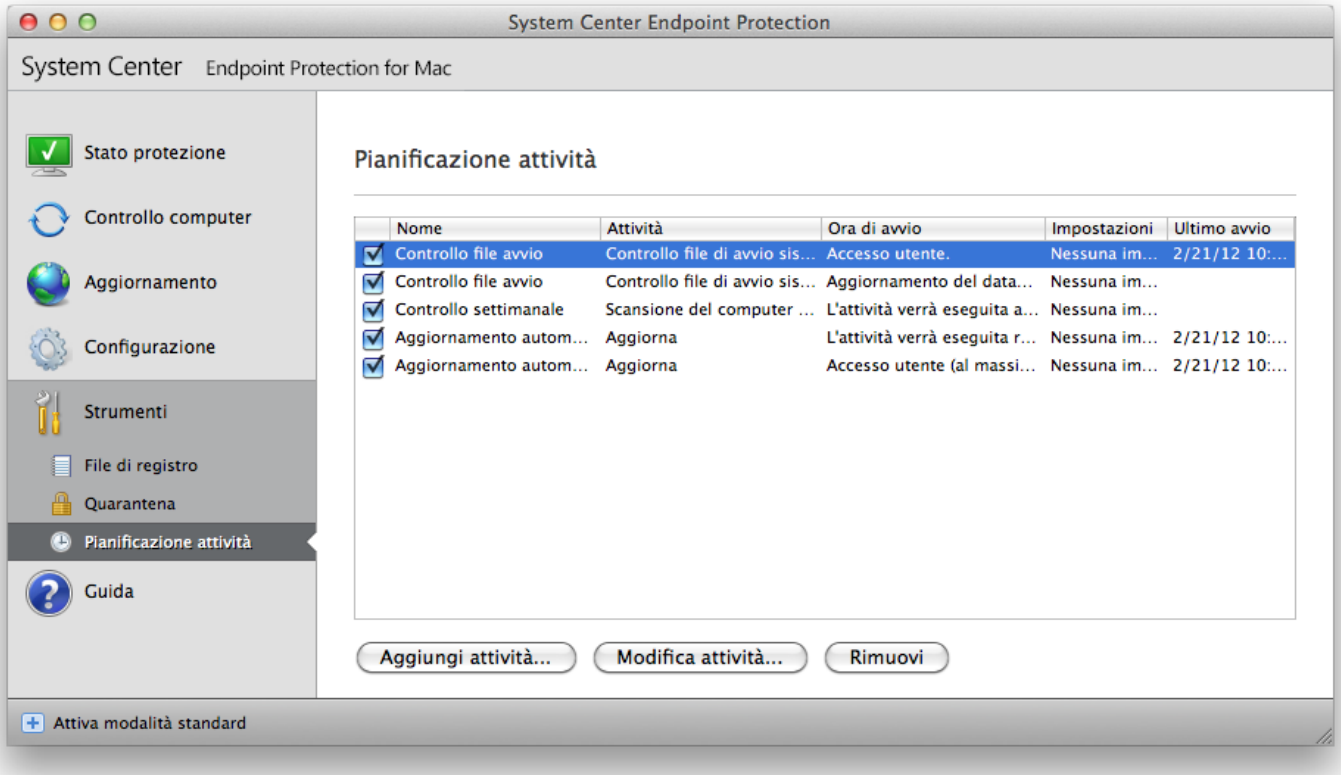
Passaggio a una nuova build

Per assicurare la massima protezione, è importante utilizzare la build più recente di System Center Endpoint Protection. Per verificare la disponibilità di una nuova versione, fare clic su **Aggiorna** dal menu principale a sinistra. Se è disponibile una nuova build, sulla parte inferiore della finestra verrà visualizzato il messaggio *È disponibile una nuova versione del prodotto*. Fare clic su **Per saperne di più...** per visualizzare una nuova finestra contenente il numero di versione della nuova build e il ChangeLog.

Fare clic su **Download** per scaricare la build più recente. Fare clic su **Chiudi** per chiudere la finestra e scaricare l'upgrade in seguito.

Pianificazione attività

La **Pianificazione attività** è disponibile se viene attivata la Modalità avanzata in System Center Endpoint Protection. È possibile trovare la Pianificazione attività nel menu principale di System Center Endpoint Protection in **Strumenti**. La **Pianificazione attività** contiene un elenco di tutte le attività pianificate e delle relative proprietà di configurazione, come data, ora e profilo di scansione predefiniti utilizzati.



Per impostazione predefinita, in Pianificazione attività vengono visualizzate le attività pianificate seguenti:

- Aggiornamento automatico regolare
- Aggiornamento automatico dopo l'accesso dell'utente
- Controllo file di avvio dopo l'accesso dell'utente
- Controllo file di avvio dopo il completamento dell'aggiornamento del database delle firme antivirali
- Manutenzione registro (dopo aver attivato l'opzione **Mostra attività di sistema** nella configurazione della pianificazione attività)
- Controllo settimanale

Per modificare la configurazione di un'attività pianificata esistente (predefinita o definita dall'utente), premere il pulsante ctrl, fare clic sull'attività che si desidera modificare e selezionare **Modifica...** oppure selezionare l'attività e fare clic sul pulsante **Modifica attività...**.

Scopo della pianificazione attività

La Pianificazione attività consente di gestire e avviare attività pianificate con le configurazioni e le proprietà predefinite. La configurazione e le proprietà contengono informazioni quali la data e l'ora, oltre ai profili specificati da utilizzare durante l'esecuzione dell'attività.

Creazione di nuove attività

Per creare una nuova attività in Pianificazione attività, fare clic sul pulsante **Aggiungi attività...** oppure premere il pulsante ctrl, fare clic nel campo vuoto e selezionare **Aggiungi...** dal menu contestuale. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione**
- **Aggiornamento**
- **Manutenzione registro**
- **Scansione del computer su richiesta**
- **Controllo del file di avvio del sistema**

Poiché gli aggiornamenti rappresentano le attività pianificate utilizzate con maggiore frequenza, di seguito verranno illustrate le

modalità in cui è possibile aggiungere una nuova attività di aggiornamento.

Dal menu a discesa **Attività pianificata**, selezionare **Aggiorna**. Inserire il nome dell'attività nel campo **Nome attività**. Selezionare la frequenza dell'attività dal menu a tendina **Esegui attività**. Sono disponibili le seguenti opzioni: **Definito dall'utente**, **Una volta**, **Ripetutamente**, **Ogni giorno**, **Ogni settimana** e **Quando si verifica un evento**. In base alla frequenza selezionata, verrà richiesto di specificare i diversi parametri di aggiornamento.

Selezionando **Definito dall'utente**, verrà richiesto di specificare la data/l'ora in formato cronologico (per ulteriori informazioni, consultare la sezione Creazione di un'attività definita dall'utente 19).

Nella fase successiva, è quindi possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati. Sono disponibili le tre opzioni riportate di seguito:

- **Attendi l'ora pianificata successiva**
- **Esegui l'attività appena possibile**
- **Esegui subito l'attività se il periodo trascorso dall'ultima esecuzione supera l'intervallo specificato** (è possibile definire l'intervallo utilizzando l'opzione **Intervallo minimo di attività**)

Nel passaggio successivo viene visualizzata una finestra contenente un riepilogo delle informazioni relative all'attività corrente pianificata. Fare clic sul pulsante **Fine**.

La nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate correnti.

Per impostazione predefinita, il sistema contiene attività pianificate essenziali per garantire il corretto funzionamento del sistema. Poiché tali attività non devono essere modificate, sono nascoste per impostazione predefinita. Per modificare tale opzione e rendere visibili tali attività, accedere alla sezione **Configurazione** > **Immettere preferenze applicazione ...** > **Strumenti** > **Pianificazione attività** e selezionare l'opzione **Mostra attività di sistema**.

Creazione di un'attività definita dall'utente

È necessario inserire la data e l'ora dell'attività **Definita dall'utente** in formato cronologico con l'anno esteso (stringa che comprende 6 campi separati da uno spazio bianco):

```
minuto(0-59) ora(0-23) giorno del mese(1-31) mese(1-12) anno(1970-2099) giorno della settimana(0-7)(domenica
```

Esempio:

```
30 6 22 3 2012 4
```

Caratteri speciali supportati nelle espressioni cronologiche:

- asterisco (`*`) - l'espressione corrisponderà a tutti i valori del campo, es. l'asterisco nel 3° campo (giorno del mese) indica ogni giorno
- trattino (`-`) - definisce gli intervalli, es. `3-9`
- virgola (`,`) - separa gli elementi di un elenco, es. `1,3,7,8`
- barra (`/`) - definisce gli incrementi degli intervalli, es. `3-28/5` nel 3° campo (giorno del mese) indica il 3° giorno del mese e successivamente ogni 5 giorni.

I nomi dei giorni (lunedì-domenica) e dei mesi (gennaio-dicembre) non sono supportati.

NOTA: Se si definiscono sia il giorno del mese sia il giorno della settimana, il comando verrà eseguito sono in caso di corrispondenza di entrambi i campi.

Quarantena

Lo scopo principale della quarantena è archiviare i file infetti in modo sicuro. I file devono essere messi in quarantena se non è possibile pulirli, se non è sicuro o consigliabile eliminarli o, infine, se vengono erroneamente rilevati come minacce da System Center Endpoint Protection.

È possibile mettere in quarantena qualsiasi tipo di file. È una procedura consigliata nel caso in cui un file si comporti in modo sospetto ma non viene rilevato dallo scanner antivirus.

I file salvati nella cartella di quarantena possono essere visualizzati in una tabella contenente la data e l'ora della quarantena, il percorso originale del file infetto, la dimensione in byte, il motivo (ad esempio, aggiunto dall'utente...) e il numero di minacce (ad esempio, se si tratta di un archivio contenente più infiltrazioni). La cartella di quarantena contenente i file in quarantena (*/Libreria/Assistenza applicazione/Microsoft/scep/cache/quarantena*) rimane nel sistema anche in seguito alla disinstallazione di System Center Endpoint Protection. I file in quarantena sono archiviati in un formato sicuro criptato e possono essere ripristinati dopo l'installazione di System Center Endpoint Protection.

Mettere file in quarantena

System Center Endpoint Protection mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto ad annullare questa opzione nella finestra di avviso). Se necessario, è possibile mettere manualmente in quarantena i file sospetti selezionando il pulsante **Quarantena**. Per questa operazione è possibile utilizzare anche il menu contestuale: premere il pulsante ctrl, fare clic nel campo vuoto, selezionare **Quarantena...**, scegliere il file che si desidera mettere in quarantena, quindi fare clic sul pulsante **Apri**.

Ripristino dalla quarantena

È possibile ripristinare nella posizione di origine i file messi in quarantena. Per questa operazione, utilizzare il pulsante **Ripristina**. L'operazione di ripristino è anche disponibile dal menu contestuale premendo il pulsante ctrl, facendo clic sul file specificato nella finestra **Quarantena**, quindi su **Ripristina**. Il menu contestuale contiene anche l'opzione **Ripristina in...**, che consente di ripristinare i file in una posizione diversa da quella di origine da cui sono stati eliminati.

File di registro

I file di registro contengono informazioni relative a tutti gli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate. La registrazione rappresenta uno strumento essenziale per l'analisi del sistema, il rilevamento delle minacce e la risoluzione dei problemi. La registrazione viene eseguita attivamente in background, senza che sia richiesto l'intervento da parte dell'utente. Le informazioni vengono registrate in base alle impostazioni del livello di dettaglio di registro correnti. È possibile visualizzare i messaggi di testo e i registri direttamente dall'ambiente di System Center Endpoint Protection, nonché dai registri di archivio.

È possibile accedere ai file di registro dal menu principale di System Center Endpoint Protection facendo clic su **Strumenti** > **File di registro**. Selezionare il tipo di registro desiderato dal menu a discesa **Registro** nella parte superiore della finestra. Sono disponibili i registri seguenti:

1. **Minacce rilevate** - Scegliere questa opzione per visualizzare tutte le informazioni sugli eventi relativi al rilevamento delle infiltrazioni.
2. **Eventi** - Questa opzione è utile agli amministratori del sistema e agli utenti per risolvere i problemi. Tutte le azioni importanti eseguite da System Center Endpoint Protection vengono registrate nei registri degli eventi.
3. **Scansione computer** - In questa finestra vengono visualizzati i risultati di tutte le scansioni completate. Fare doppio clic su una voce per visualizzare i dettagli della rispettiva scansione del computer su richiesta.

In ciascuna sezione, le informazioni visualizzate possono essere copiate direttamente negli Appunti, selezionando la voce desiderata e facendo clic sul pulsante **Copia**.

Manutenzione registro

La configurazione della registrazione di System Center Endpoint Protection è accessibile dalla finestra principale del programma. Fare clic su **Configurazione** > **Inserisci preferenze applicazione ...** > **Strumenti** > **File di registro**. Per i file di registro è possibile specificare le opzioni seguenti:

- **Elimina automaticamente i file di rapporto** - le voci del registro con data precedente al numero di giorni specificato vengono automaticamente eliminate.
- **Ottimizza automaticamente i file di rapporto** - i file di registro vengono automaticamente deframmentati se viene superata la percentuale specificata di record inutilizzati.

È possibile salvare tutte le informazioni rilevanti visualizzate nell'interfaccia grafica utente, nonché i messaggi relativi alle minacce e agli eventi, in formati di testo leggibili, come testo normale o CSV (valori separati da virgola). Se si desidera elaborare questi file mediante strumenti di terze parti, selezionare la casella di controllo accanto a **Attiva registrazione a file di testo**.

Per definire la cartella di destinazione in cui verranno salvati i file di rapporto, fare clic su **Configurazione...** accanto a **Configurazione avanzata**.

Le opzioni presenti nella sezione **File di testo dei rapporti:** sono: **Modifica**, che consente di salvare i rapporti inserendo le seguenti informazioni:

- le minacce rilevate dal Controllo all'avvio, dalla Protezione in tempo reale o dal Controllo computer sono salvate nel file chiamato threatslog.txt.
- Alcuni eventi tra cui *Nome utente e password non validi, Non è possibile aggiornare il database delle firme antivirali*, ecc. sono indicati nel file eventslog.txt.
- I risultati di tutti i controlli completati vengono salvati nel formato scanlog.NUMERO.txt.

Per configurare i filtri dei **Record predefiniti rapporti controllo computer**, fare clic sul pulsante **Modifica...** accanto a questa opzione e selezionare/deselezionare i tipi di rapporto appropriati. Per ulteriori informazioni su questi tipi di rapporto, consultare questo capitolo 21.

Filtraggio registri

I registri memorizzano le informazioni relative a eventi importanti di sistema. La funzione di filtraggio del registro consente di visualizzare i record di un determinato tipo di evento.

I tipi di registro utilizzati più spesso sono elencati di seguito:

- **Allarmi critici** - errori critici di sistema (es. Impossibile avviare la protezione antivirus)
- **Errori** - messaggi di errore come "*Errore durante il download del file*" ed errori critici
- **Allarmi** - messaggi di allarme
- **Record informativi**- messaggi informativi che includono gli aggiornamenti riusciti, gli avvisi e così via.
- **Record di diagnostica** - informazioni necessarie per la sincronizzazione ottimale del programma nonché di tutti i record riportati sopra.

Interfaccia utente

Le opzioni di configurazione dell'interfaccia utente in System Center Endpoint Protection consentono di modificare l'ambiente di lavoro per adattarlo alle esigenze specifiche dell'utente. È possibile accedere a tali opzioni di configurazione dalla sezione **Configurazione** > **Inserisci preferenze applicazione ...** > **Utente** > **Interfaccia**.

In questa sezione, l'opzione relativa alla modalità avanzata consente agli utenti di passare alla Modalità avanzata. La Modalità avanzata consente di visualizzare impostazioni più dettagliate e controlli aggiuntivi per System Center Endpoint Protection.

Per avviare la funzionalità relativa alla schermata iniziale, selezionare l'opzione **Mostra schermata iniziale all'avvio**.

Nella sezione **Utilizza menu standard** è possibile selezionare le opzioni **In modalità standard/In modalità avanzata** per consentire l'utilizzo del menu standard nella finestra principale del programma nelle rispettive modalità di visualizzazione.

Per attivare le descrizioni dei comandi, selezionare l'opzione **Mostra descrizioni comandi**. L'opzione **Mostra file nascosti** consente di visualizzare e selezionare i file nascosti nella configurazione **Destinazioni di scansione** di una **Scansione computer**.

Avvisi e notifiche

La sezione **Avvisi e notifiche** consente di configurare la gestione dei messaggi di avviso e delle notifiche di sistema in System Center Endpoint Protection.

La disattivazione dell'opzione **Visualizza avvisi** annullerà tutte le finestre di avviso ed è pertanto adatta solo a situazioni specifiche. Nella maggior parte dei casi, è consigliabile non modificare l'opzione predefinita (attivata).

La selezione dell'opzione **Visualizza notifiche sul desktop** consentirà di attivare le finestre di avviso che non richiedono l'interazione da parte dell'utente per poterle visualizzare sul desktop (per impostazione predefinita, l'angolo in alto a destra dello schermo). È possibile definire il periodo durante il quale verrà visualizzata una notifica modificando il valore **Chiudi automaticamente notifiche dopo** X **secondi**.

Configurazione avanzata avvisi e notifiche

Visualizza solo le notifiche che richiedono l'interazione dell'utente
Questa opzione consente di alternare la visualizzazione dei messaggi che richiedono l'interazione dell'utente.

Visualizza solo le notifiche che richiedono l'interazione dell'utente durante l'esecuzione delle applicazioni in modalità schermo intero
Questa opzione è utile nel caso di presentazioni o altre attività che richiedono la visualizzazione a schermo intero.

Privilegi

Le impostazioni di System Center Endpoint Protection rivestono un ruolo fondamentale dal punto di vista dei criteri di sicurezza dell'organizzazione di appartenenza. Modifiche non autorizzate potrebbero mettere a rischio la stabilità e la protezione del sistema. Di conseguenza, è possibile scegliere quali utenti potranno modificare la configurazione del programma.

Per specificare gli utenti con privilegi, accedere alla sezione **Configurazione** > **Inserisci preferenze applicazione ...** > **Utente** > **Privilegi** .

Per garantire la massima sicurezza del sistema, è necessario configurare correttamente il programma. Qualsiasi modifica non autorizzata può provocare la perdita di dati importanti. Per definire una lista di utenti con privilegi, selezionarli dalla lista **Utenti** sul lato sinistro e fare clic sul pulsante **Aggiungi** . Per rimuovere un utente, selezionarne il nome nella lista **Utenti con privilegi** sulla destra e fare clic su **Rimuovi**.

NOTA: Se la lista di utenti con privilegi è vuota, tutti gli utenti del sistema saranno autorizzati a modificare le impostazioni del programma.

Menu contestuale

È possibile attivare l'integrazione del menu contestuale nella sezione **Configurazione** > **Inserisci preferenze applicazione ...** > **Utente** > **Menu contestuale** attivando la casella di controllo **Integra nel menu contestuale**.

Utente avanzato

Importa ed esporta impostazioni

Le configurazioni di importazione ed esportazione di System Center Endpoint Protection sono disponibili in modalità avanzata in **Configurazione**.

Sia l'importazione che l'esportazione utilizzano i file di archivio per memorizzare la configurazione. Le opzioni di importazione e di esportazione sono utili nel caso in cui si desideri effettuare il backup della configurazione corrente di System Center Endpoint Protection per poterlo utilizzare in un secondo momento. L'opzione di esportazione delle impostazioni è utile anche per quegli utenti che desiderino utilizzare la configurazione preferita di System Center Endpoint Protection su più sistemi. In tal modo, infatti, sarà possibile importare facilmente il file di configurazione per il trasferimento delle impostazioni desiderate.

Importa impostazioni

L'importazione della configurazione è molto semplice. Nel menu principale, fare clic su **Configurazione** > **Importa ed esporta impostazioni ...** quindi selezionare l'opzione **Importa impostazioni**. Inserire il nome del file di configurazione o fare clic sul pulsante **Sfoglia...** per ricercare il file di configurazione che si desidera importare.

Esporta impostazioni

Le operazioni per esportare una configurazione sono molto simili. Nel menu principale, fare clic su **Configurazione** > **Importa ed esporta impostazioni ...** Selezionare l'opzione **Esporta impostazioni** e immettere il nome del file di configurazione. Utilizzare il browser per selezionare un percorso sul computer in cui salvare il file di configurazione.

Configurazione del server proxy

È possibile configurare le impostazioni del server proxy in **Varie** > **Server Proxy**. Specificando il server proxy a questo livello, si definiscono le impostazioni globali del server proxy per tutte le funzioni di System Center Endpoint Protection. Questi parametri vengono utilizzati da tutti i moduli che richiedono una connessione a Internet.

Per specificare le impostazioni del server proxy per questo livello, selezionare la casella di controllo **Utilizza server proxy** e l'indirizzo IP o URL del server proxy nel campo **Server proxy**. Nel campo porta, specificare la porta sulla quale il server proxy accetta le connessioni (per impostazione predefinita, la porta 3128). Se per la comunicazione con il server proxy è necessaria l'autenticazione, selezionare la casella di controllo **Il server proxy richiede l'autenticazione** e inserire un **Nome utente** e una **Password** validi nei rispettivi campi.

Blocco supporti rimovibili

I supporti rimovibili (ad esempio, CD o chiavette USB) potrebbero contenere codici dannosi e mettere a rischio il computer. Per bloccare i supporti rimovibili, selezionare la casella di controllo accanto a **Attiva blocco supporti rimovibili**. Per consentire l'accesso ad alcuni tipi di supporto, deselezionare le rispettive caselle di controllo.

Selezionare la casella di controllo accanto a **Altro** se si desidera applicare queste impostazioni a tipi di supporto diversi da CD, DVD, FireWire o USB. Questa impostazione riguarda nello specifico le eventuali periferiche collegate al computer in uso mediante l'interfaccia Thunderbolt.

Glossario

Tipi di infiltrazioni

Un'infiltrazione è una parte di software dannoso che tenta di entrare e/o danneggiare il computer di un utente.

Virus

Un virus è un'infiltrazione che danneggia i file esistenti sul computer. I virus prendono il nome dai virus biologici, poiché utilizzano tecniche simili per diffondersi da un computer all'altro.

I virus attaccano principalmente i file eseguibili, gli script e i documenti. Per replicarsi, un virus allega il suo "corpo" alla fine di un file di destinazione. In breve, un virus funziona nel seguente modo: dopo l'esecuzione del file infetto, il virus si attiva (prima dell'applicazione originale) ed esegue la sua attività predefinita. L'applicazione originale viene eseguita solo dopo questa operazione. Un virus non può infettare un computer a meno che un utente (accidentalmente o deliberatamente) esegua o apra il programma dannoso.

I virus possono essere classificati in base agli scopi e ai diversi livelli di gravità. Alcuni di essi sono estremamente dannosi poiché dispongono della capacità di eliminare di proposito i file da un disco rigido. Altri, invece, non causano veri e propri danni, poiché il loro scopo consiste esclusivamente nell'infastidire l'utente e dimostrare le competenze tecniche dei rispettivi autori.

È importante tenere presente che i virus (se paragonati a trojan o spyware) sono sempre più rari, poiché non sono commercialmente allettanti per gli autori di software dannosi. Inoltre, il termine "virus" è spesso utilizzato in modo errato per indicare tutti i tipi di infiltrazioni. Attualmente, l'utilizzo di questo termine è stato superato e sostituito dalla nuova e più accurata definizione di "malware" (software dannoso).

Se il computer in uso è infettato da un virus, è necessario ripristinare lo stato originale dei file infetti, ovvero pulirli utilizzando un programma antivirus.

Tra i virus più noti si segnalano: *OneHalf*, *Tenga* e *Yankee Doodle*.

Worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite una rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di replicarsi e di viaggiare autonomamente, in quanto non dipendono da file host (o settori di avvio). I worm si diffondono attraverso indirizzi e-mail all'interno della lista dei contatti degli utenti oppure sfruttano le vulnerabilità delle applicazioni di rete.

I worm sono pertanto molto più attivi rispetto ai virus. Grazie all'ampia disponibilità di connessioni Internet, essi possono espandersi in tutto il mondo entro poche ore dal rilascio e, in taluni casi, perfino entro pochi minuti. Questa capacità di replicarsi in modo indipendente e rapido li rende molto più pericolosi rispetto ad altri tipi di malware.

Un worm attivato in un sistema può provocare diversi inconvenienti: può eliminare file, ridurre le prestazioni del sistema e perfino disattivare programmi. La sua natura lo qualifica come "mezzo di trasporto" per altri tipi di infiltrazioni.

Se il computer è infettato da un worm, si consiglia di eliminare i file infetti poiché è probabile che contengano codice dannoso.

Tra i worm più noti si segnalano: *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* e *Netsky*.

Trojan horse

Storicamente, i trojan horse sono stati definiti come una classe di infiltrazioni che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli a eseguirli. Oggigiorno, tali programmi non hanno più la necessità di camuffarsi. Il loro unico scopo è quello di infiltrarsi il più facilmente possibile e portare a termine i loro obiettivi dannosi. Il termine "Trojan horse" ("cavallo di Troia") ha assunto un'accezione molto generale che indica un'infiltrazione che non rientra in una classe specifica di infiltrazioni.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie:

- Downloader: un programma dannoso in grado di scaricare altre infiltrazioni da Internet.
- Dropper: un tipo di trojan horse concepito per installare sui computer compromessi altri tipi di malware.
- Backdoor: un'applicazione che comunica con gli aggressori remoti, consentendo loro di ottenere l'accesso a un sistema e prenderne il controllo.
- Keylogger (registratore delle battute dei tasti): un programma che registra ogni battuta di tasto effettuata da un utente e che invia le informazioni agli aggressori remoti.

- Dialer - i dialer sono programmi progettati per connettersi a numeri con tariffe telefoniche molto elevate. È quasi impossibile che un utente noti la creazione di una nuova connessione. I dialer possono causare danni solo agli utenti che dispongono di una connessione remota, utilizzata oramai sempre più di rado.
- Solitamente, i Trojan horse assumono la forma di file eseguibili. Se sul computer in uso viene rilevato un file classificato come Trojan horse, si consiglia di eliminarlo, poiché contiene probabilmente un codice dannoso.

Tra i trojan più noti si segnalano: *NetBus, Trojandownloader.Small.ZL, Slapper.*

Adware

Adware è l'abbreviazione di software supportato dalla pubblicità ("advertising-supported software"). Rientrano in questa categoria i programmi che consentono di visualizzare materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra popup contenente pubblicità all'interno di un browser Internet oppure ne modificano la pagina iniziale. I programmi adware vengono spesso caricati insieme a programmi freeware, che consentono agli sviluppatori di freeware di coprire i costi di sviluppo delle proprie applicazioni (in genere utili).

L'adware di per sé non è pericoloso, ma gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo sta nel fatto che l'adware può svolgere anche funzioni di rilevamento, allo stesso modo dei programmi spyware.

Se si decide di utilizzare un prodotto freeware, è opportuno prestare particolare attenzione al programma di installazione. Nei programmi di installazione viene in genere visualizzata una notifica dell'installazione di un programma adware aggiuntivo. Spesso è possibile annullarla e installare il programma senza adware.

Alcuni programmi non vengono installati senza adware. In caso contrario, le rispettive funzionalità saranno limitate. Ciò significa che l'adware potrebbe accedere di frequente al sistema in modo "legale", poiché l'utente ne ha dato il consenso. In questi casi, vale il proverbio secondo il quale la prudenza non è mai troppa. Se in un computer viene rilevato un file adware, l'operazione più appropriata è l'eliminazione dello stesso, in quanto esistono elevate probabilità che il file contenga codice dannoso.

Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso/la consapevolezza dell'utente. Gli spyware si avvalgono di funzioni di monitoraggio per inviare dati statistici di vario tipo, tra cui un elenco dei siti Web visitati, indirizzi e-mail della rubrica dell'utente o un elenco dei tasti digitati.

Gli autori di spyware affermano che lo scopo di tali tecniche è raccogliere informazioni aggiuntive sulle esigenze e sugli interessi degli utenti per l'invio di pubblicità più mirate. Il problema è che non esiste una distinzione chiara tra applicazioni utili e dannose e che nessuno può essere sicuro del fatto che le informazioni raccolte verranno utilizzate correttamente. I dati ottenuti dalle applicazioni spyware possono contenere codici di sicurezza, PIN, numeri di conti bancari e così via. I programmi spyware spesso sono associati a versioni gratuite di un programma dal relativo autore per generare profitti o per offrire un incentivo all'acquisto del software. Spesso, gli utenti sono informati della presenza di un'applicazione spyware durante l'installazione di un programma che li esorta a eseguire il passaggio a una versione a pagamento che non lo contiene.

Esempi di prodotti freeware noti associati a programmi spyware sono le applicazioni client delle reti P2P (peer-to-peer). Spyfalcon o Spy Sheriff (e molti altri ancora) appartengono a una sottocategoria di spyware specifica, poiché si fanno passare per programmi antispyware ma in realtà sono essi stessi applicazioni spyware.

Se in un computer viene rilevato un file spyware, l'operazione più appropriata è l'eliminazione dello stesso, in quanto esistono elevate probabilità che il file contenga codice dannoso.

Applicazioni potenzialmente pericolose

Esistono molti programmi legali utili per semplificare l'amministrazione dei computer in rete. Tuttavia, nelle mani sbagliate, possono essere utilizzati per scopi illegittimi. System Center Endpoint Protection offre la possibilità di rilevare tali minacce.

"Applicazioni potenzialmente pericolose" è la classificazione utilizzata per il software legale e commerciale. Questa classificazione include programmi quali strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente).

Se si rileva la presenza di un'applicazione potenzialmente pericolosa in esecuzione sul computer (che non è stata installata dall'utente), si prega di rivolgersi all'amministratore di rete o di rimuovere l'applicazione.

Applicazioni potenzialmente indesiderate

Le applicazioni potenzialmente indesiderate non sono necessariamente dannose. Tuttavia, potrebbero influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative sono:

- apertura di nuove finestre mai viste in precedenza
- attivazione ed esecuzione di processi nascosti
- maggiore utilizzo delle risorse del sistema
- modifiche dei risultati di ricerca
- applicazioni che comunicano con server remoti.