

Sophos Endpoint Security and Control 9.7

Guida all'impostazione dei criteri

Data documento: aprile 2011



Sommario

1	Informazioni sulla guida.....	3
2	Consigli generali sui criteri.....	4
3	Impostazione di un criterio di aggiornamento.....	5
4	Impostazione dei criteri antivirus e HIPS.....	7
5	Impostazione del criterio del firewall.....	10
6	Impostazione del criterio di controllo applicazioni.....	14
7	Impostazione del criterio di controllo dispositivi.....	16
8	Impostazione del criterio di controllo dati.....	18
9	Configurazione del criterio del blocco rimozione.....	23
10	Impostazione del criterio di NAC.....	24
11	Consigli sulla scansione.....	26
12	Utilizzo della scansione in accesso.....	27
13	Utilizzo della scansione pianificata.....	28
14	Utilizzo della scansione su richiesta	29
15	Esclusione di oggetti dalla scansione.....	30
16	Supporto tecnico.....	31
17	Note legali.....	32

1 Informazioni sulla guida

Questa guida descrive le linee guida per l'impostazione dei criteri del software Sophos Endpoint Security and Control.

Nello specifico, fornisce consigli per aiutare gli utenti a:

- Comprendere le indicazioni relative ai criteri.
- Impostare e distribuire tutti i criteri in base al tipo.
- Utilizzare le opzioni di scansione per scoprire oggetti.
- Stabilire quali oggetti escludere dalla scansione.

Questa guida sarà utile se:

- Si esegue Enterprise Console.
- Si desiderano consigli sulle migliori opzioni relative all'impostazione e alla distribuzione dei criteri.

Prima di consultare questa guida, leggere la *Guida di avvio rapido* di *Sophos Endpoint Security and Control*.

Tutti i documenti relativi a Enterprise Console sono disponibili su www.sophos.it/support/docs/Enterprise_Console-all.html.

2 Consigli generali sui criteri

Dopo l'installazione di Enterprise Console, vengono creati dei criteri predefiniti. Tali criteri vengono applicati a qualsiasi gruppo creato dall'utente. I criteri predefiniti sono studiati per fornire livelli di protezione efficaci. Se si desidera utilizzare funzioni quali controllo applicazioni, dispositivi, dati, blocco rimozione o accesso alla rete, è necessario creare nuovi criteri o crearne di predefiniti. Quando si impostano criteri, tenere presente quanto riportato di seguito:

- Se possibile, utilizzare impostazioni predefinite all'interno del criterio.
- Tenere presente il ruolo del computer quando si modificano le impostazioni dei criteri predefiniti o se ne creano di nuovi (per es. desktop o server).
- Utilizzare Enterprise Console per tutte le impostazioni dei criteri centrali e, se possibile, impostare le opzioni in Enterprise Console invece che direttamente nel computer.
- Impostare le opzioni direttamente nel computer solo se richiesta una configurazione temporanea di quel determinato computer o per elementi che non possono essere configurati centralmente, quali le opzioni di scansione avanzate.
- Per i computer che richiedono una configurazione speciale a lungo termine, creare un gruppo e criteri a parte.

3 Impostazione di un criterio di aggiornamento

Il criterio di aggiornamento indica in che modo i computer ricevono le definizioni delle nuove minacce e si aggiornano dal software Sophos. La sottoscrizione a un software specifica quali versioni del software del computer vengono scaricate da Sophos per ciascuna piattaforma. Il criterio di aggiornamento predefinito consente di installare e aggiornare il software specificato nella sottoscrizione "consigliata". Quando si imposta il criterio di aggiornamento, prendere in considerazione quanto riportato di seguito:

- Si dovrebbero sottoscrivere le versioni "consigliate" del software per essere sicuri che venga aggiornato automaticamente. Se invece si desidera analizzare le nuove versioni del software prima di distribuirle nella rete principale, si consiglia l'utilizzo delle versioni fisse del software nella rete principale durante il processo di analisi delle nuove versioni. Le versioni fisse vengono aggiornate mensilmente con i nuovi dati relativi al rilevamento delle minacce, ma non con la versione più recente del software.
- Assicurarsi che il numero di gruppi che utilizzano lo stesso criterio di aggiornamento sia gestibile. Non si dovrebbero avere più di 1000 computer che si aggiornano dal medesimo percorso. Il numero ottimale di computer che si aggiornano dallo stesso percorso è 600-700.

Nota: il numero di computer che possono effettuare l'aggiornamento dalla stessa directory dipende dal server sul quale si trova tale directory e dalla connettività di rete.

- Per impostazione predefinita, i computer si aggiornano da un unico percorso primario. Tuttavia, si consiglia di impostare sempre e comunque un percorso secondario alternativo per gli aggiornamenti. Se i computer endpoint non riescono a contattare il proprio percorso primario, cercheranno di aggiornarsi da quello secondario, se ne è stato impostato uno. Per ulteriori informazioni, consultare la Guida in linea di Sophos Enterprise Console.
- Consentire la ricerca automatica di un percorso nel criterio di aggiornamento per gli utenti di laptop aziendali che si collegano a Internet di frequente e spesso dall'estero. Quando è abilitata questa opzione, i laptop in roaming cercheranno di trovare e di aggiornarsi dal percorso più vicino, tramite richiesta ad altri computer endpoint fissi nella stessa rete locale a cui sono connessi, riducendo al minimo i ritardi di aggiornamento e i costi legati alla larghezza di banda. Se vengono restituiti percorsi multipli, il laptop determina quale sia quello più vicino e lo utilizza. Se nessuno di essi funziona, il laptop utilizzerà il percorso primario (e successivamente quello secondario) indicato nei suoi criteri di aggiornamento. La ricerca automatica di un percorso è supportata solamente se si utilizza Sophos Update Manager, e sarà efficace solo se l'endpoint in roaming si aggiorna da un percorso gestito dalla stessa istanza di Enterprise Console che gestisce l'endpoint. Per ulteriori informazioni, consultare la Guida in linea di Sophos Enterprise Console.
- Se preoccupati per il rendimento dei computer a basse specificazioni, è possibile sottoscrivere una versione fissa del software e cambiare manualmente tale sottoscrizione quando pronti ad aggiornare il software di tali computer. Questa opzione garantirà che i computer siano aggiornati con i dati di rilevamento delle minacce più recenti. In alternativa, è possibile effettuare aggiornamenti per i computer a bassa specificazione meno frequentemente (ad esempio due o tre volte al giorno), oppure considerare l'eventualità di eseguire gli aggiornamenti ad orari prestabiliti diversi da quelli tipici di utilizzo degli utenti (come ad esempio di sera o durante il fine settimana).



Attenzione: ricordare che ridurre al minimo gli aggiornamenti aumenta i rischi per la sicurezza.

4 Impostazione dei criteri antivirus e HIPS

4.1 Impostazioni consigliate

Il criterio antivirus e HIPS stabilisce la modalità in cui il software di sicurezza effettua la scansione dei computer alla ricerca di virus, trojan, worm, spyware, adware, applicazioni potenzialmente indesiderate (PUA), comportamenti e file sospetti e come li rimuove. Quando si imposta il criterio antivirus e HIPS, prendere in considerazione quanto riportato di seguito:

- Il criterio predefinito antivirus e HIPS proteggerà i computer da virus e altro malware. È possibile comunque creare nuovi criteri o modificare quelli predefiniti per consentire il rilevamento di altre applicazioni o comportamenti indesiderati.
- Abilita Sophos Live Protection, che utilizza il sistema di ricerca online Sophos per decidere all'istante se un file sospetto è una minaccia e per aggiornare il software Sophos in tempo reale. L'opzione **Attiva Live Protection** è attiva per impostazione predefinita esclusivamente per l'installazione di nuovi software. Per effettuare upgrade del software, è necessario abilitare la relativa opzione. Per sfruttare appieno Sophos Live Protection, si consiglia di selezionare anche l'opzione **Invia automaticamente file campione a Sophos**.
- Utilizzare l'opzione **Notifica solamente** per rilevare solo comportamenti sospetti. Definendo inizialmente il criterio report only, è possibile avere una migliore visione dell'utilizzo in rete del comportamento sospetto. Questa opzione è abilitata per impostazione predefinita e deve essere deselezionata una volta completata la distribuzione del criterio per bloccare programmi e file.

4.2 Distribuzione di un criterio antivirus e HIPS

Si consiglia di distribuire il criterio antivirus e HIPS nel modo seguente:

1. Creare criteri diversi per gruppi diversi.
2. Impostare esclusioni dalla scansione in accesso per directory o computer con database di dimensioni più grandi o file frequentemente modificati; assicurarsi che vengano invece eseguite scansioni pianificate. Si possono, per esempio, escludere determinate directory nei server di Exchange o in altri server in cui si possono avere ripercussioni sul rendimento. Per ulteriori informazioni, consultare l'articolo 12421 in inglese della knowledge base Sophos (<http://www.sophos.com/support/knowledgebase/article/12421.html>, in inglese).

3. Impostare le opzioni di Sophos Live Protection. Questa funzione utilizza il sistema di ricerca online Sophos per decidere all'istante se un file sospetto rappresenta una minaccia e per aggiornare il software Sophos in tempo reale. Sono disponibili le seguenti opzioni:

- **Attiva Live Protection:** se la scansione antivirus di un computer ha identificato un file come sospetto, ma non riesce a determinare se sia malevolo o meno in base ai file di identità delle minacce (IDE) memorizzati nel computer, alcune caratteristiche del file (come il checksum e altri attributi) vengono inviate a Sophos per un'ulteriore analisi. Il servizio di ricerca online Sophos esegue la ricerca istantanea di un file sospetto nel database di SophosLabs. Se il file viene identificato come malevolo o meno, la decisione viene inviata al computer e lo stato del file viene automaticamente aggiornato.

Questa opzione è attiva per impostazione predefinita esclusivamente per l'installazione di nuovi software. Per effettuare upgrade del software, è necessario abilitare questa opzione.

- **Invia automaticamente file campione a Sophos :** se un file viene considerato potenzialmente malevolo, ma non può essere identificato con certezza come tale basandosi solo sulle sue caratteristiche, Sophos Live Protection consente a Sophos di richiedere un campione del file. Se l'opzione "Invia automaticamente file campione a Sophos" è abilitata, e Sophos non possiede ancora un campione del file, il file verrà inviato automaticamente. L'invio di tali campioni permette a Sophos di migliorare costantemente il rilevamento del malware senza il rischio di falsi positivi.

Importante: occorre assicurarsi che il dominio Sophos a cui i dati del file vengono inviati sia considerato fidato nella soluzione di filtraggio web. Per informazioni, consultare l'articolo della knowledge base 62637 in inglese

(<http://www.sophos.com/support/knowledgebase/article/62637.html>, in inglese) Se si utilizza una soluzione di filtraggio web Sophos, come la Web Appliance WS1000, non è necessario svolgere alcuna operazione. I domini Sophos sono già considerati fidati.

4. Rilevare virus e spyware.
 - a) Assicurarsi che la scansione in accesso sia abilitata o pianificare una scansione di tutto il sistema per il rilevamento di virus e spyware. La scansione in accesso è abilitata per impostazione predefinita. Per ulteriori informazioni, consultare la sezione [Utilizzo della scansione in accesso](#) a pagina 27 o [Utilizzo della scansione pianificata](#) a pagina 28.
 - b) Selezionare le opzioni di disinfezione per virus/spyware.
5. Rilevare file sospetti.

I file sospetti hanno determinate caratteristiche comuni al malware, ma tali caratteristiche non sono sufficienti perché tali file possano essere identificati come nuovo malware.

 - a) Abilitare la scansione in accesso o pianificare una scansione completa del sistema per rilevare file sospetti.
 - b) Selezionare l'opzione **File sospetti (HIPS)**.
 - c) Selezionare l'opzione di disinfezione per i file sospetti.
 - d) Se del caso, autorizzare tutti i file di cui è consentito l'utilizzo.

6. Rilevamento di comportamento sospetto e buffer overflow.

Il rilevamento di comportamenti sospetti e buffer overflow consiste nel monitorare costantemente i processi in esecuzione per verificare se un programma presenti comportamenti sospetti. Questi tipi di rilevamento sono utili per bloccare eventuali falle alla sicurezza.

- a) Utilizzare l'opzione **Notifica solamente** solo per rilevare comportamenti sospetti e buffer overflow. Questa opzione è abilitata per impostazione predefinita.
- b) Autorizzare tutti i programmi o file che si desidera continuare ad eseguire anche in futuro.
- c) Configurare il criterio in modo da bloccare i programmi e file rilevati deselezionando l'opzione **Notifica solamente**.

In questo modo evita il blocco dei programmi e dei file di cui gli utenti potrebbero aver bisogno. Per ulteriori informazioni, consultare l'articolo 50160 in inglese della knowledge base Sophos (<http://www.sophos.com/support/knowledgebase/article/50160.html>, in inglese).

7. Rilevare adware e PUA.

Quando si esegue la scansione alla ricerca di adware e PUA per la prima volta, si possono generare molti allarmi relativi ad applicazioni già in esecuzione nella rete. Eseguendo per prima cosa una scansione pianificata, è possibile gestire in sicurezza le applicazioni già in esecuzione nella rete.

- a) Pianificare una scansione di tutto il sistema per rilevare tutti gli adware e PUA.
- b) Autorizzare o disinstallare tutte le applicazioni rilevate dalla scansione.
- c) Selezionare l'opzione scansione in accesso di **Adware e PUA** per poter rilevare, in futuro, adware e PUA.

Per ulteriori informazioni, consultare l'articolo 13815 in inglese della knowledge base Sophos (<http://www.sophos.com/support/knowledgebase/article/13815.html>, in inglese).

8. Rilevare minacce nelle pagine web.

- a) Assicurarsi che l'opzione **Blocca accesso a siti malevoli** sia impostata su **Attiva**, per assicurarsi che i siti web malevoli vengano bloccati. Questa opzione è attiva per impostazione predefinita.
- b) Configurare l'opzione **Scansione download** per **Attiva** o **Come in accesso** per controllare e bloccare il download di dati malevoli. L'impostazione predefinita **Come in accesso**, consente la scansione dei download solo quando è abilitata la scansione in accesso.
- c) A seconda delle proprie necessità, autorizzare i siti web consentiti.

Per informazioni sull'impostazione del criterio antivirus e HIPS, consultare la Guida in linea di Sophos Enterprise Console .

5 Impostazione del criterio del firewall

5.1 Impostazioni consigliate

Il criterio del firewall stabilisce la modalità con la quale il firewall protegge i computer. Quando si imposta il criterio del firewall, prendere in considerazione quanto riportato di seguito:

- Quando viene installato Sophos Client Firewall, vengono disattivate le impostazioni del firewall di Windows; di conseguenza, se si stava eseguendo il firewall di Windows, annotare le configurazioni esistenti e trasferirle a Sophos Client Firewall.
- Utilizzare la modalità **Consenti per impostazione predefinita** per rilevare, ma non bloccare, traffico, applicazioni e processi. Se inizialmente si definisce un criterio report only, ciò consente di avere migliore consapevolezza delle attività della rete.
- Utilizzare il Visualizzatore eventi del firewall per vedere quali tipi di traffico, applicazioni e processi sono in uso. Il Visualizzatore eventi consente anche di creare con facilità regole che permettano o blocchino il traffico, le applicazioni ed i processi rilevati. È possibile accedere al Visualizzatore eventi cliccando su **Visualizza > Eventi Firewall**.
- Nei computer di prova, utilizzare la modalità **Interattiva** per visualizzare finestre di apprendimento, configurare e riconoscere le applicazioni che vengono eseguite e importare/modificare le regole stabilite da quel determinato processo.
- Per la modalità **Interattiva**, si consiglia di deselezionare l'opzione **Visualizza un allarme nella console di gestione se alle regole, applicazioni, processi e checksum globali vengono apportate modifiche a livello locale** per evitare la creazione di allarmi "Diverso dal criterio" ogni qual volta gli utenti rispondano a una finestra di apprendimento.
- Consentire l'utilizzo di browser web, e-mail e condivisione file e stampanti.
- Si consiglia di non modificare le impostazioni predefinite ICMP, le regole globali e le regole delle applicazioni, se non in possesso di un'adeguata conoscenza della rete.
- Si consiglia, quando possibile, la creazione di regole delle applicazioni, piuttosto che di regole globali.

5.2 Configurazione del firewall per percorso doppio

L'opzione relativa al percorso singolo è pensata per computer che si trovano sempre su una rete singola, quali computer desktop. L'opzione relativa al percorso doppio è disponibile se si desidera che il firewall utilizzi impostazioni diverse a seconda del percorso da cui vengono eseguiti i computer, per es. in ufficio e fuori ufficio. È possibile impostare un percorso doppio per i laptop.

Se si seleziona il percorso doppio, si consiglia di impostare le opzioni di configurazione del percorso primario e secondario secondo quanto riportato di seguito:

- Impostare il percorso primario in modo tale che coincida con la rete che si controlla (per es. la rete aziendale) e quello secondario in modo tale che coincida con percorsi esterni.
- Impostare il percorso primario in modo tale che abbia maggiore libertà di accesso e quello secondario in modo tale che abbia accesso più ristretto.

- Quando si configurano le opzioni di rilevamento per il percorso primario, si consiglia solitamente il rilevamento DNS per reti più ampie e complesse e il rilevamento gateway per quelle più piccole e semplici. Il rilevamento DNS richiede il server DNS, ma è di solito più semplice da mantenere rispetto al rilevamento gateway. Se gli hardware utilizzati per il rilevamento gateway non funzionano, è necessario riconfigurare gli indirizzi MAC; inoltre il percorso secondario dei computer potrebbe venire configurato in modo errato se non viene risolto il problema relativo alla configurazione degli hardware.
- Se si utilizza il rilevamento DNS, si consiglia di aggiungere una voce DNS specifica per il server DNS che abbia un nome insolito e che restituisca un indirizzo IP localhost, anche chiamato indirizzo loopback (per es. 127.x.x.x). Questa opzione impedisce che altre reti a cui ci si connette siano rilevate erroneamente come rete primaria.
- Nella configurazione avanzata del criterio firewall, nella sezione "Percorso applicato", selezionare la configurazione del firewall che si desidera applicare al computer. Se si desidera che la configurazione applicata dipenda dal percorso del computer, selezionare l'opzione **Applica la configurazione al percorso rilevato**. Se si desidera applicare manualmente la configurazione primaria o secondaria, selezionare le relative opzioni.



Attenzione: si consiglia vivamente di usare cautela quando si utilizzano le regole di sottorete locale come parte di configurazioni secondarie. Se il computer è un laptop, e viene utilizzato all'esterno dell'ufficio, esiste la possibilità che si colleghi ad una sottorete sconosciuta. In tale evenienza, le regole del firewall nella configurazione secondaria che utilizzano la sottorete locale come indirizzo possono inavvertitamente consentire traffico sconosciuto.

5.3 Quando bloccare o consentire traffico, applicazioni e processi

Si consiglia di bloccare o consentire traffico, applicazioni e processi nel modo seguente:

- Se il firewall utilizza la modalità **Interattiva**, spiegare agli utenti quale tipo di traffico, applicazioni o processi bloccare o consentire.
- Se il firewall utilizza la modalità **Blocca per impostazione predefinita**, l'utente non viene informato dalle finestre di apprendimento; al contrario, è l'amministratore ad essere responsabile del blocco o consenso di tutto il traffico, le applicazioni o i processi da Enterprise Console.
- Nel computer le opzioni **Blocca...solo questa volta** dovrebbero essere utilizzate solo se l'utente non è sicuro di bloccare o meno il traffico. Nel computer queste opzioni sono disponibili solo quando il criterio si trova in modalità **Interattiva**.
- In alcuni casi il traffico **non** deve essere bloccato. Tra questi casi sono incluse le regole del checksum e delle applicazioni relative a browser web, e-mail, condivisione file e stampanti e tutti i programmi che richiedono accesso a Internet.
- Una volta che il computer è impostato con le applicazioni consentite, gli utenti verranno informati solo quando verranno installate nuove applicazioni o patch per applicazioni esistenti (se ci si trova in modalità **Interattiva**).

5.4 Distribuzione del criterio del firewall

Per impostazione predefinita il firewall è attivato e blocca tutto il traffico della rete non essenziale. Deve essere quindi configurato per consentire il traffico, le applicazioni e i processi che si desidera utilizzare; si consiglia inoltre di testarlo prima di installarlo ed eseguirlo su tutti i computer. Si consiglia di impostare il criterio del firewall secondo quanto descritto di seguito:

1. Pensare al criterio e a quali funzioni dovrà svolgere, prima di creare o modificare le regole del firewall (globale, applicazione o altro).
2. Utilizzare la modalità **Consenti per impostazione predefinita** per rilevare, ma non bloccare, traffico, applicazioni e processi comuni.
3. Utilizzare il Visualizzatore eventi del firewall per vedere quali tipi di traffico, applicazioni e processi sono in uso. Il Visualizzatore eventi consente anche di creare con facilità regole che permettano o blocchino il traffico, le applicazioni ed i processi rilevati. È possibile accedere al Visualizzatore eventi cliccando su **Visualizza > Eventi Firewall**.
4. Se necessario, creare regole globali o applicazioni personalizzate.

Nota: in alternativa ai passaggi 1-4, è possibile configurare un computer di prova in modalità **Interattiva** per poi importare e modificare le regole stabilite dal processo. Per ulteriori informazioni, consultare la Guida in linea di Sophos Endpoint Security and Control.

5. Eseguire una distribuzione in fasi di Sophos Client Firewall nella rete. Ciò eviterà che, nelle fasi iniziali, venga sovraccaricato il traffico della rete. Per prima cosa distribuire Sophos Client Firewall a un numero limitato di computer facili da monitorare. Tali computer devono essere rappresentativi dei diversi ruoli presenti nella rete.



Attenzione: non eseguire la distribuzione in tutta la rete prima di avere testato e controllato accuratamente la configurazione.

- a) Installare e configurare Sophos Client Firewall nei computer di prova.
 - b) Su tali computer eseguire tutti i programmi e procedure abituali.
 - c) Ricercare eventuali punti deboli della configurazione di prova (per es. troppa libertà di accesso a determinati utenti).
 - d) Se le necessità sono diverse, suddividere il gruppo e creare configurazioni extra a seconda delle necessità.
 - e) Una volta testate le regole, cambiare la modalità del criterio in **Blocca per impostazione predefinita**; se non si compie questa operazione, i computer rimarranno esposti.
6. Completata la prima fase della distribuzione, pianificare la distribuzione completa in tutta la rete di Sophos Client Firewall.

È importante evitare il sovraccarico della rete con un eccesso di traffico in una volta sola. Non eseguire la distribuzione in tutta la rete in una volta sola.

- Dividere il resto della rete in gruppi gestibili, per esempio composti da 100 computer alla volta.
- In tali gruppi, eseguire la distribuzione a livelli.

Per ulteriori informazioni sull'impostazione del criterio del firewall, consultare la Guida in linea di Sophos Enterprise Console. Per informazioni sulle impostazioni predefinite del firewall, consultare l'articolo 14464 in inglese della knowledge base Sophos (<http://www.sophos.com/support/knowledgebase/article/14464.html>, in inglese).

Per informazioni sulle nuove funzioni del firewall in Enterprise Console 4.0, consultare l'articolo 54750 in inglese della knowledge base Sophos (<http://www.sophos.com/support/knowledgebase/article/54750.html>, in inglese).

6 Impostazione del criterio di controllo applicazioni

6.1 Impostazioni consigliate

I criteri del controllo applicazioni stabiliscono quali applicazioni vengono bloccate e quali consentite sui computer. Quando si imposta il criterio del controllo applicazioni, prendere in considerazione quanto riportato di seguito:

- Utilizzare l'opzione **Rileva ma consenti l'esecuzione** per rilevare, ma non bloccare, le applicazioni controllate. Se inizialmente si definisce il criterio report only, ciò consente di avere migliore consapevolezza dell'utilizzo delle applicazioni nella rete.
- Utilizzare il Visualizzatore eventi del controllo applicazioni per verificare l'utilizzo delle applicazioni all'interno della rete. È possibile accedere al Visualizzatore eventi cliccando su **Visualizza > Eventi controllo applicazioni**.
- Utilizzare Report Manager per creare, tramite computer o utente, i report dei trend relativi agli eventi del controllo applicazioni.
- Prendere in considerazione l'utilizzo dell'opzione "Tutti quelli aggiunti da Sophos in futuro" per bloccare tutte le applicazioni nuove appartenenti a una determinata tipologia e che Sophos aggiunge di volta in volta; in questo modo non si dovrà continuamente aggiornare il criterio. Per esempio, se al momento si stanno bloccando tutte le applicazioni di messaggistica istantanea, perché non bloccare tutte le nuove applicazioni di messaggistica istantanea?

6.2 Distribuzione del criterio di controllo applicazioni

Per impostazione predefinita, sono consentite tutte le applicazioni e i tipi di applicazione. Si consiglia di impostare il controllo applicazioni come segue:

1. Pensare a quali applicazioni si desidera controllare.
2. Abilitare la scansione in accesso e selezionare l'opzione **Rileva ma consenti l'esecuzione** per rilevare, ma non bloccare, le applicazioni.
A questo punto si dispone di un solo criterio del controllo applicazioni per l'intera rete.
3. Utilizzare il Visualizzatore eventi del controllo applicazioni per vedere quali applicazioni sono in esecuzione e stabilire le applicazioni o tipi di applicazione che si desidera bloccare. È possibile accedere al Visualizzatore eventi cliccando su **Visualizza > Eventi controllo applicazioni**.
4. Per garantire l'accesso alle applicazioni in maniera diversa in base ai gruppi di computer, creare criteri diversi per gruppi diversi. Per esempio, si potrebbe decidere di non consentire il VoIP per i computer situati in ufficio, ma autorizzarne l'uso per i computer in remoto.
5. Stabilire le applicazioni o tipi di applicazione che si desidera bloccare e spostarli nell'elenco Applicazioni bloccate.
6. Configurare il criterio in modo tale da bloccare le applicazioni controllate che vengono rilevate, deselezionando l'opzione **Rileva ma consenti l'esecuzione**.

Adottando questo metodo, si evita di generare un elevato numero di allarmi e di bloccare le applicazioni necessarie agli utenti. Per ulteriori informazioni sull'impostazione del criterio di controllo applicazioni, consultare la Guida in linea di Sophos Enterprise Console.

7 Impostazione del criterio di controllo dispositivi

7.1 Impostazioni consigliate

Il criterio del controllo dispositivi specifica quali dispositivi di archiviazione e di rete sono autorizzati nei computer. Quando si imposta il criterio del controllo dispositivi, prendere in considerazione quanto riportato di seguito:

- Utilizzare l'opzione **Rileva, ma non bloccare i dispositivi** per rilevare, ma non bloccare, i dispositivi controllati. Per fare ciò, occorre prima impostare lo status su **Bloccato** per ogni tipo di dispositivo che si desidera rilevare. Il software non rileverà i tipi di dispositivi non specificati. Se inizialmente si definisce il criterio report only, ciò consente di avere migliore consapevolezza dell'utilizzo dei dispositivi nella rete.
- Utilizzare il Visualizzatore eventi del controllo dispositivi per bloccare rapidamente tramite filtri gli eventi su cui investigare. È possibile accedere al Visualizzatore eventi cliccando su **Visualizza > Eventi Controllo Dispositivi**.
- Utilizzare il Report Manager per creare i report dei trend relativi agli eventi del controllo dispositivi per computer o utente.
- Prendere in considerazione la restrizione dell'accesso alla rete da parte di computer i cui utenti hanno accesso a informazioni sensibili.
- Prima di distribuire un criterio che blocca i dispositivi, creare un elenco di esenzioni per dispositivi. Si potrebbe, per esempio, voler consentire l'utilizzo di unità ottiche all'interno di un team di creativi.
- La categoria "Dispositivo di memorizzazione rimovibile sicuro" può essere utilizzata per autorizzare automaticamente i dispositivi di memorizzazione USB con hardware cifrato di vari rivenditori supportati. Un elenco completo di rivenditori supportati è disponibile nel sito web Sophos. Per un elenco dei dispositivi di memoria rimovibili sicuri supportati, consultare l'articolo 63102 in inglese della knowledge base del supporto tecnico Sophos (<http://www.sophos.com/support/knowledgebase/article/63102.html>, in inglese).
- Quando si aggiungono al criterio del controllo dispositivi esenzioni per dispositivi, nel campo **Commento** indicare la ragione dell'esenzione o chi l'ha richiesta.
- Utilizzare le opzioni di messaggistica desktop personalizzate per fornire agli utenti maggiore supporto ogni qual volta venga scoperto un dispositivo controllato. Si potrebbe, per esempio, fornire un link al criterio aziendale relativo all'utilizzo dei dispositivi.
- Se si vuole abilitare un dispositivo di rete (per es. adattatori Wi-Fi) quando il computer è fisicamente disconnesso dalla rete, selezionare l'opzione **Blocca bridging** quando si impostano i livelli di accesso per i dispositivi di rete.

Nota: la modalità Blocca bridging riduce significativamente il rischio di bridging di rete tra una rete aziendale e una non aziendale. Questa modalità è disponibile sia per i dispositivi wireless che per i modem. La modalità funziona disabilitando le schede di rete wireless o modem quando un computer è collegato a una rete fisica (solitamente, mediante una connessione Ethernet). Quando il computer è scollegato dalla rete fisica, le schede di rete wireless o modem vengono riabilite direttamente.

- È bene essere assolutamente sicuri di voler bloccare un dispositivo, prima di distribuire il relativo criterio. Occorre essere a conoscenza di tutte le esigenze degli utenti, soprattutto in relazione a dispositivi WiFi e di rete.



Attenzione: le modifiche al criterio vengono apportate dal server di Enterprise Console al computer attraverso la rete; di conseguenza, una volta bloccata, la rete non potrà essere sbloccata da Enterprise Console, in quanto il computer non potrà accettare alcuna configurazione aggiuntiva dal server.

7.2 Distribuzione del criterio di controllo dispositivi

Per impostazione predefinita, il controllo dispositivi è disattivato e tutti i dispositivi sono consentiti. Si consiglia di impostare il controllo dispositivi come segue:

1. Pensare a quali dispositivi si desidera controllare.
2. Abilitare la scansione del controllo dispositivi e selezionare l'opzione **Rileva, ma non bloccare i dispositivi** per rilevare, ma non bloccare, il controllo dispositivi. Per fare ciò, occorre prima impostare lo status su **Bloccato** per ogni tipo di dispositivo che si desidera rilevare. Il software non rileverà i tipi di dispositivi non specificati.
A questo punto si dispone di un unico criterio del controllo dispositivi per l'intera rete.
3. Utilizzare il Visualizzatore eventi del controllo dispositivi per vedere quali dispositivi sono in esecuzione e stabilire quali tipi di dispositivi si desidera bloccare. È possibile accedere al Visualizzatore eventi cliccando su **Visualizza > Eventi Controllo Dispositivi**.
4. Per garantire l'accesso ai dispositivi in maniera differente in base ai vari gruppi di computer, creare criteri diversi per gruppi diversi. È per esempio possibile non autorizzare l'utilizzo di dispositivi di memorizzazione rimovibili per i dipartimenti di risorse umane e finanza, e consentirlo invece per IT e commerciale.
5. Esentare le istanze o i tipi di modello che non si desidera bloccare. È possibile esentare una specifica chiave USB (istanza) o tutti i modem Vodafone 3G (tipo di modello).
6. Stabilire quali dispositivi si desidera bloccare e cambiare il loro stato in **Bloccato**. È anche possibile consentire l'accesso in sola lettura per determinati tipi di dispositivi di memorizzazione.
7. Configurare il criterio per bloccare i dispositivi controllati rilevati deselegnando l'opzione **Rileva, ma non bloccare i dispositivi**.

Adottando questo metodo, si evita di generare un elevato numero di allarmi e di bloccare i dispositivi necessari agli utenti. Per ulteriori informazioni sull'impostazione del criterio di controllo dispositivi, consultare la Guida in linea di Sophos Enterprise Console.

8 Impostazione del criterio di controllo dati

8.1 Definizione del criterio di controllo dati

Il criterio del controllo dati consente di gestire i rischi legati al trasferimento accidentale di dati sensibili dai computer.

Ogni azienda ha una propria definizione di dati sensibili. Tra i più comuni esempi:

- Record di clienti contenenti dati che possono portare all'identificazione personale.
- Dati finanziari, quali numeri di carte di credito.
- Documenti confidenziali.

Una volta abilitato il criterio di controllo dati, Sophos monitora le azioni degli utenti negli exit point dei dati comuni:

- Trasferimento di file in dispositivi di memorizzazione (dispositivi rimovibili, unità disco ottico e supporti basati su disco).
- Caricamento di file nelle applicazioni (browser web aziendali, client di posta elettronica e client IM).

Una regola del controllo dati è composta da tre elementi:

- Elementi da far coincidere: le opzioni includono contenuto, tipo e nome dei file.
- Punti da monitorare: includono tipi di archiviazione e applicazioni.
- Azioni da intraprendere: le azioni disponibili comprendono "Consenti il trasferimento dei file e crea il log evento" (modalità monitor), "Consenti il trasferimento su accettazione da parte dell'utente e crea il log evento" (modalità training), "Blocca il trasferimento e crea il log evento" (modalità limitata)

Per esempio, le regole del controllo dati possono essere definite in modo da registrare il caricamento di tutti i fogli elettronici tramite Internet Explorer o da consentire il trasferimento degli indirizzi dei clienti su DVD, una volta che tale trasferimento è confermato dall'utente.

La definizione di dati sensibili in base al contenuto può essere complessa. Sophos ha semplificato questa operazione fornendo una libreria precostituita di definizioni di dati sensibili, chiamata Content Control List. Questa libreria comprende una vasta gamma di formati di dati che possono portare all'identificazione personale e finanziaria ed è tenuta aggiornata da Sophos. A seconda delle proprie necessità, è anche possibile definire Content Control List personalizzate.

Come per tutti i criteri Sophos, il criterio del controllo dati continua ad essere attuato nei computer anche quando disconnessi dalla rete aziendale.

8.2 Impostazioni consigliate

Quando si imposta il criterio del controllo dati, prendere in considerazione quanto riportato di seguito:

- Utilizzare l'azione **Consenti trasferimento del file e l'accesso all'evento** per rilevare, ma non bloccare, dati controllati. Se inizialmente si definisce il criterio report only, ciò consente di avere migliore consapevolezza dell'utilizzo dei dati nella rete.
- Utilizzare l'azione **Consenti il trasferimento se l'utente ha accettato e accedi all'evento** per avvertire gli utenti dei rischi legati al trasferimento di documenti potenzialmente contenenti dati sensibili. Ciò può ridurre il rischio di perdita di dati senza avere ripercussioni di rilievo sulle operazioni informatiche.
- All'interno delle regole dei contenuti, utilizzare l'impostazione "quantità" per configurare il volume di dati sensibili che si desidera trovare prima che una regola venga applicata. Per esempio, una regola configurata per il rilevamento di un solo indirizzo di posta all'interno di un documento genererà più eventi del controllo dati di una regola configurata per rilevare 50 o più indirizzi.

Nota: Sophos fornisce impostazioni della quantità predefinite per tutti i Content Control List.

- Utilizzare il Visualizzatore eventi del controllo dati per filtrare rapidamente gli eventi su cui investigare. Tutti gli eventi e le azioni del controllo dati vengono registrati centralmente in Enterprise Console. È possibile accedere al Visualizzatore eventi cliccando su **Visualizza > Eventi controllo dati**.
- Utilizzare Report Manager per creare i report dei trend relativi agli eventi del controllo dati per regole, computer o utenti.
- Utilizzare le opzioni di messaggistica desktop personalizzate per fornire agli utenti maggiore supporto quando viene avviata un'azione. Si potrebbe, per esempio, fornire un link al criterio aziendale relativo alla sicurezza dei dati.
- Utilizzare la modalità di log dettagliata per ottenere maggiori informazioni sull'esattezza delle regole del controllo dati. Una volta portata a termine la valutazione di tali regole, disabilitare il log dettagliato.

Nota: il log dettagliato deve essere attivato su tutti i computer. Tutti i dati generati vengono memorizzati nel log del controllo dati locale del computer. Una volta che la modalità di log dettagliato è attiva, tutte le stringhe di un documento che corrispondono ai dati specificati nella regola vengono registrate. I dati aggiuntivi contenuti all'interno del log possono essere utilizzati per identificare frasi o stringhe di un determinato documento che hanno dato inizio all'evento del controllo dati.

8.3 Distribuzione del criterio di controllo dati

Per impostazione predefinita, il controllo dati è disattivato e non è specificata alcuna regola che monitori o limiti il trasferimento di file nei dispositivi di memorizzazione o nelle applicazioni. Si consiglia di impostare il controllo dati come segue:

1. Comprendere il funzionamento del controllo dati nei computer:

- **Dispositivi di memorizzazione** : il controllo dati intercetta tutti i file copiati su dispositivi di memorizzazione monitorati utilizzando Esplora risorse (incluso il desktop di Windows). Tuttavia, i salvataggi diretti effettuati dall'interno di applicazioni come Microsoft Word, o i trasferimenti eseguiti utilizzando il prompt di comando, non sono intercettati.

È possibile forzare tutti i trasferimenti su dispositivi di memorizzazione monitorati da eseguire usando Esplora risorse, mediante l'azione "Consenti il trasferimento se l'utente ha accettato e accedi all'evento" o l'azione "Blocca trasferimento e l'accesso all'evento". In ogni caso, qualsiasi tentativo di salvare direttamente dall'interno di un'applicazione o di trasferire i file utilizzando il prompt di comando viene bloccato dal controllo dati e sul desktop è visualizzato un allarme per l'utente, il quale richiede l'utilizzo di Esplora risorse per completare il trasferimento.

Quando un criterio del controllo dati contiene solo regole con l'azione "Consenti trasferimento del file e l'accesso all'evento", i salvataggi diretti dall'interno delle applicazioni e i trasferimenti mediante il prompt di comando non sono intercettati. Questo comportamento consente agli utenti di utilizzare dispositivi di memorizzazione senza limitazioni. Tuttavia, gli eventi di controllo dati sono comunque registrati per i trasferimenti effettuati utilizzando Esplora risorse.

Nota: questa limitazione non si applica al monitoraggio dell'applicazione.

- **Applicazioni:** il controllo dati intercetta file e documenti caricati sulle applicazioni monitorate. Per assicurarsi che vengano monitorati solo i file caricati dagli utenti, alcuni percorsi dei file di sistema vengono esclusi dal monitoraggio del controllo dati. Per maggiori informazioni sul contenuto e sulle azioni all'interno delle applicazioni sottoposte o non sottoposte a scansione, vedere [Comprensione della scansione del controllo dati all'interno delle applicazioni](#) a pagina 21.

Nota: se si stanno monitorando i client e-mail, il controllo dati esamina tutti gli allegati dei file ma non il contenuto della posta elettronica. Se si vuole analizzare il contenuto della posta elettronica, si può usare la soluzione Sophos Email Security and Data Protection.

2. Considerare quali tipi di informazioni si desidera identificare e per cui si desidera creare nuove regole. Sophos fornisce esempi di regole utilizzabili per creare il criterio di controllo dati.

Importante: la scansione del contenuto può essere un processo laborioso e questo è un elemento da prendere in considerazione quando si creano regole di contenuto. È importante testare l'impatto della regola di contenuto prima di distribuirla a un numero elevato di computer.

Nota: quando si crea il primo criterio, si consiglia di concentrarsi sul rilevamento di ampie raccolte di dati che possono portare all'identificazione personale all'interno dei documenti. Sophos fornisce esempi di regole per poter soddisfare tale requisito.

3. Abilitare la scansione del controllo dati e selezionare, nella regola, l'azione **Consenti trasferimento dei file e l'accesso all'evento** per rilevare, ma non bloccare, il controllo dati.
Importante: si consiglia di configurare tutte le regole in modo tale che utilizzino questa azione per la distribuzione iniziale. Ciò consente di verificare l'efficacia delle regole senza avere ripercussioni sulla produttività dell'utente.
4. Attuare il criterio del controllo dati in un piccolo gruppo di computer per rendere più semplice l'analisi degli eventi del controllo dati innescati dal criterio.
5. Utilizzare il Visualizzatore eventi del controllo dati per visualizzare i dati in uso, ricercare eventuali punti deboli della configurazione di prova (per es. una regola troppo sensibile che genera un numero di eventi più alto di quanto ci si aspettasse). È possibile accedere al Visualizzatore eventi cliccando su **Visualizza > Eventi controllo dati**.
6. Una volta testato il criterio, è possibile apportare le dovute correzioni e distribuirlo a un numero più elevato di computer all'interno dell'azienda. A questo punto si può decidere di:
 - Cambiare le azioni relative ad alcune regole in modo da **Consenti il trasferimento se l'utente ha accettato e accedi all'evento** oppure **Blocca trasferimento e l'accesso all'evento**.
 - Creare criteri diversi per gruppi diversi. Per esempio, si potrebbe desiderare di permettere ai computer nel dipartimento risorse umane di trasferire informazioni strettamente personali, ma impedire ciò a tutti gli altri gruppi.

Per ulteriori informazioni sull'impostazione del criterio di controllo dati, consultare la Guida in linea di Sophos Enterprise Console.

8.4 Comprensione della scansione del controllo dati all'interno delle applicazioni

Il seguente elenco comprende contenuti ed azioni presi in esame o meno dalla scansione eseguita all'interno delle applicazioni supportate.

Per un elenco completo di limitazioni note rispetto al controllo dati, consultare l'articolo 63016 in inglese della knowledge base del supporto Sophos (<http://www.sophos.com/support/knowledgebase/article/63016.html>, in inglese).

Applicazioni	Azioni di scansione del controllo dati
Browser web	Esaminati: <ul style="list-style-type: none"> ■ File caricati ■ Allegati webmail ■ Upload di Microsoft SharePoint Non esaminati <ul style="list-style-type: none"> ■ Contenuto messaggi Webmail ■ Voci del blog

Applicazioni	Azioni di scansione del controllo dati
	<ul style="list-style-type: none"> ■ File scaricati <p>Nota: in una piccola percentuale di casi, la scansione dei file può essere eseguita durante il download.</p>
Client e-mail	<p>Esaminati</p> <ul style="list-style-type: none"> ■ Allegati e-mail <p>Non esaminati</p> <ul style="list-style-type: none"> ■ Contenuto messaggi e-mail ■ Allegati inoltrati ■ Allegati fatti utilizzando l'opzione e-mail "Invia" all'interno delle applicazioni (es. Windows Explorer e Microsoft Office) ■ Allegati svolti utilizzando l'opzione "invia file via e-mail" all'interno di Windows Explorer ■ Allegati copiati da un'e-mail all'altra ■ Allegati salvati <p>Nota: in una piccola percentuale di casi, è possibile eseguire la scansione dei file durante il salvataggio.</p>
Client di messaggistica istantanea (IM)	<p>Esaminati</p> <ul style="list-style-type: none"> ■ Trasferimenti di file <p>Nota: è possibile che un file venga sottoposto a scansione due volte: la prima durante l'upload sul client IM, e poi di nuovo su accettazione del destinatario. Entrambe le scansioni hanno luogo sul computer del mittente.</p> <p>Non esaminati</p> <ul style="list-style-type: none"> ■ Contenuto messaggi IM ■ File inviati

9 Configurazione del criterio del blocco rimozione

9.1 Impostazioni consigliate

Il criterio del blocco rimozione vi consente di impedire ad utenti non autorizzati (amministratori locali con limitate conoscenze tecniche) di riconfigurare, disabilitare o disinstallare il software di sicurezza Sophos. Per utenti non autorizzati s'intendono quegli utenti che non dispongono della password del blocco rimozione.

Nota: il blocco rimozione non è pensato per offrire protezione contro utenti con vaste conoscenze tecniche. Non offre protezione contro malware appositamente studiato per sabotare il rilevamento da parte del sistema operativo. Tale tipo di malware può essere rilevato solamente eseguendo una scansione alla ricerca di minacce e comportamenti sospetti. Per ulteriori informazioni, consultare la sezione [Impostazione dei criteri antivirus e HIPS](#) a pagina 7.

Dopo aver abilitato il blocco rimozione e aver creato una password, un utente che non conosce la stessa non sarà in grado di: riconfigurare la scansione in accesso o il rilevamento di comportamenti sospetti in Sophos Endpoint Security and Control; disattivare il blocco rimozione; disinstallare i componenti di Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate o Sophos Remote Management System) o Sophos SafeGuard Disk Encryption dal Pannello di controllo.

Quando si imposta il criterio del blocco rimozione, prendere in considerazione quanto riportato di seguito:

- Usare il Visualizzatore eventi del blocco rimozione per verificare l'utilizzo della password del blocco rimozione e monitorare il tasso di tentativi di manomissione nella vostra azienda. È possibile visualizzare sia gli eventi di autenticazione del blocco rimozione conclusi con successo (utenti autorizzati che aggirano la protezione) che i tentativi falliti di disattivare il software di sicurezza Sophos. È possibile accedere al Visualizzatore eventi cliccando su **Visualizza > Eventi blocco rimozione**.

9.2 Distribuzione del criterio del blocco rimozione

Per impostazione predefinita, il blocco rimozione è disattivato. Si consiglia di impostare il blocco rimozione come segue:

1. Abilitare il blocco rimozione e creare una password del blocco rimozione sicura.
La password consente solo agli utenti autorizzati di riconfigurare, disattivare o disinstallare il software di sicurezza Sophos.
Nota: il blocco rimozione non influisce sui gruppi SophosUsers e SophosPowerUsers. Quando il blocco rimozione è attivo, tali utenti possono ancora eseguire tutti i compiti a cui sono normalmente autorizzati, senza bisogno di immettere la password del blocco rimozione
2. Se si richiede la facoltà di attivare o disattivare il blocco rimozione, o creare password diverse per vari gruppi, creare criteri diversi per gruppi diversi.

Per ulteriori informazioni su come impostare il criterio del blocco rimozione, consultare la Guida in linea di Sophos Enterprise Console.

10 Impostazione del criterio di NAC

10.1 Quando utilizzare criteri di NAC predefiniti

I criteri di NAC stabiliscono le condizioni alle quali i computer devono conformarsi prima di poter accedere alla rete. Per impostazione predefinita, Sophos NAC consente l'accesso alla rete a tutti i computer. È necessario configurare un criterio di NAC in modo tale da controllare l'accesso.

Utilizzare i criteri predefiniti per supportare la conformità ai criteri di protezione per computer gestiti e non. È possibile modificare i criteri predefiniti in NAC Manager per cambiare la modalità del criterio, i profili nel criterio o i modelli di accesso alla rete applicati al criterio.

Sono disponibili i seguenti criteri:

- **Default:** questo criterio viene utilizzato se in un computer è installato Compliance Agent, ma non è stato assegnato alcun criterio. Per impostazione predefinita, il criterio è in modalità Report Only. Se il criterio è impostato su Remediate o Enforce, tale criterio svolgerà azioni correttive sul computer.
- **Managed:** questo criterio può essere utilizzato nei computer gestiti con Enterprise Console e in cui è installato Compliance Agent. Per impostazione predefinita, il criterio è in modalità Report Only. Se il criterio è impostato su Remediate o Enforce, tale criterio svolgerà azioni correttive sul computer.
- **Unmanaged:** questo criterio può essere utilizzato per i computer esterni all'azienda. Non svolge attività correttive nel computer. Compliance Dissolvable Agent utilizza il criterio Unmanaged.

Per ulteriori informazioni sui criteri predefiniti, consultare la Guida in linea di Sophos NAC Manager.

10.2 Distribuzione del criterio di NAC

Inizialmente, il criterio di NAC "predefinito" viene applicato a tutti i computer. Se si desidera modificare le impostazioni del criterio o utilizzare un criterio differente, si può utilizzare Sophos NAC Manager per modificare il criterio e Enterprise Console per applicarlo ai computer. Si consiglia di impostare il criterio di NAC secondo quanto descritto di seguito:

1. In Enterprise Console, creare o importare gruppi e applicare Sophos Compliance Agent ai computer tramite la procedura guidata di protezione dei computer.
2. In NAC Manager, assicurarsi che i criteri di NAC contengano le impostazioni, i profili e i modelli di accesso che si desidera utilizzare.
3. Utilizzare Enterprise Console per applicare il criterio Managed di NAC a tutti i gruppi gestiti in Enterprise Console.

Gli agenti cominceranno a verificare la conformità nella modalità del criterio Report Only.

4. Utilizzare i report in NAC Manager per stabilire l'attuale stato di conformità degli utenti.

I report offrono una rappresentazione realistica di quanto gli utenti siano conformi ai criteri NAC.

5. Utilizzare NAC Manager per aggiornare il criterio Managed di NAC. Cambiare la modalità del criterio da Report Only a Remediate.
6. Utilizzare i report in NAC Manager per stabilire lo stato di conformità corrente degli utenti.
Col passare del tempo, i computer conformi o parzialmente conformi vengono corretti automaticamente per migliorare lo stato di conformità generale.
7. Utilizzare NAC Manager per aggiornare il criterio Managed di NAC. Cambiare la modalità del criterio da Remediate a Enforce.
8. Utilizzare i report in NAC Manager per stabilire lo stato di conformità corrente degli utenti.
I computer non conformi devono essere sottoposti ad azioni correttive, in caso contrario agli utenti verrà negato l'accesso alle risorse di rete.

Per informazioni sulla configurazione di NAC, consultare la Guida in linea di Sophos NAC Manager.

11 Consigli sulla scansione

Le opzioni di scansione presentate nelle seguenti sezioni si trovano all'interno del criterio antivirus e HIPS, anche se alcune di queste opzioni (per es. estensioni ed esclusioni) sono applicabili anche al criterio di controllo applicazioni. Quando si impostano le opzioni di scansione, tenere presente quanto riportato di seguito:

- Se possibile, utilizzare le impostazioni predefinite.
- Se possibile, impostare la scansione in Enterprise Console e non nel computer.
- Tenere presente il ruolo del computer (per es. desktop o server).
- L'opzione **Scansiona tutti i file** non è solitamente necessaria, né viene consigliata. Utilizzare invece l'opzione **Scansiona solo eseguibili e altri tipi di file vulnerabili** per eseguire la scansione delle minacce rilevate da SophosLabs. Eseguire la scansione di tutti i file solo se consigliata dal supporto tecnico.
- L'opzione **Scansione di tutti i file** rallenta la scansione ed è raramente necessaria. Quando si cerca di accedere ai contenuti di un file di archivio, la scansione di tale file viene eseguita automaticamente. Per tanto, si sconsiglia di selezionare questa opzione, a meno che non si faccia un uso frequente dei file di archivio.
- Si consiglia di effettuare la scansione della memoria di sistema di un computer, alla ricerca di eventuali minacce. La memoria di sistema viene utilizzata dal sistema operativo. La scansione della memoria di sistema può venire effettuata periodicamente senza che l'utente se ne accorga, quando è abilitata la scansione in accesso. È inoltre possibile includere la scansione della memoria di sistema come parte di una scansione pianificata. L'opzione **Esegui scansione della memoria di sistema** è attiva per impostazione predefinita esclusivamente per nuovi criteri ed installazioni di software. Per effettuare l'upgrade del software, è necessario abilitare questa opzione.

12 Utilizzo della scansione in accesso

Quando si utilizza la scansione in accesso, considerare quanto riportato di seguito:

- Se possibile, utilizzare le impostazioni predefinite.
- Utilizzare l'opzione della scansione in accesso **Lettura**. Le opzioni della scansione in accesso **Scrittura** e **Rinomina** non sono di solito necessarie, ma vengono fornite per ottenere sicurezza massima. Queste opzioni possono rivelarsi utili per le infezioni dovute a malware.
- La scansione in accesso potrebbe non rilevare i virus, se sono installati determinati software di cifratura. Modificare i processi di avvio per assicurarsi che i file vengano decifrati quando inizia la scansione in accesso. Per ulteriori informazioni su come utilizzare criteri antivirus e HIPS con software di cifratura, consultare l'articolo 12790 della knowledge base Sophos (<http://www.sophos.com/support/knowledgebase/article/12790.html>, in inglese).
- Quando non si seleziona la scansione in accesso, assicurarsi che i computer utilizzino scansioni pianificate. Per ulteriori informazioni, consultare la sezione [Utilizzo della scansione pianificata](#) a pagina 28.



Attenzione: ricordare che la disabilitazione della scansione in accesso aumenta i rischi per la sicurezza.

13 Utilizzo della scansione pianificata

Quando si utilizza la scansione pianificata, tenere presente quanto riportato di seguito:

- Se possibile, utilizzare le impostazioni predefinite.
- Utilizzare la scansione pianificata come strumento di verifica delle minacce e per tracciare una stima della preponderanza di applicazioni indesiderate o controllate.
- Utilizzare la scansione pianificata nelle directory dei server, in cui la scansione in accesso potrebbe avere ripercussioni sul rendimento. Per esempio, si potrebbe essere in possesso di un gruppo di server di Exchange che utilizzano la scansione pianificata su determinate directory. Per ulteriori informazioni, consultare l'articolo 12421 in inglese della knowledge base Sophos (<http://www.sophos.com/support/knowledgebase/article/12421.html>, in inglese).
- Quando non si seleziona la scansione in accesso, assicurarsi che i computer utilizzino scansioni pianificate. Mettere i computer in un gruppo e definire la scansione pianificata.
- Ricordare che il rendimento potrebbe essere compromesso quando si pianificano scansioni. Se, per esempio, si esegue la scansione di un server che legge e scrive costantemente sui database, considerare il momento in cui il suo rendimento verrà influenzato il meno possibile.
- Per i server, considerare le operazioni che stanno eseguendo. Se è in esecuzione un'operazione di back up, non eseguire la scansione pianificata contemporaneamente all'operazione di back up.
- Eseguire la scansione a orari prestabiliti. Assicurarsi che in tutti i computer venga eseguita una scansione pianificata al giorno, per esempio alle 9 PM. Le scansioni pianificate devono essere eseguite su tutti i computer con la cadenza minima di una volta a settimana.
- L'opzione **Esegui scansione a priorità più bassa** permette a sistemi operativi Windows Vista o successivi di effettuare una scansione pianificata a priorità meno elevata, in modo da minimizzare il suo impatto sulle applicazioni dell'utente. Questa è un'opzione consigliata; tuttavia, la durata della scansione sarà maggiore rispetto a quella delle scansioni eseguite senza tale opzione.

14 Utilizzo della scansione su richiesta

Quando si utilizza la scansione su richiesta, considerare quanto riportato di seguito:

- Utilizzare la scansione su richiesta quando è necessaria la verifica o la disinfezione manuale.

15 Esclusione di oggetti dalla scansione

Per escludere oggetti dalla scansione, procedere come segue:

- Per escludere dalla scansione determinati tipi di file, utilizzare le relative estensioni.
- Per escludere dalla scansione oggetti o unità specifiche, utilizzare le esclusioni. È possibile creare esclusioni a livello di driver (X:), directory (X:\Programmi\Exchsrvr\) o file (X:\Programmi\SomeApp\SomeApp.exe).
- Escludere dalla scansione in accesso le unità disco per utenti specifici che le utilizzano molto frequentemente. Queste unità leggono e scrivono su file temporanei; tutti questi file vengono intercettati e scansionati ogni volta che vengono utilizzati, rallentando il processo di scansione.
- Utilizzare l'opzione **Escludi file remoti** quando non si desidera che i file remoti (nelle risorse di rete) vengano sottoposti a scansione. Si consiglia di impostare tutti i computer in modo tale che eseguano la scansione dei file remoti quando vi accedono; tuttavia, potrebbe essere utile selezionare questa opzione per file server o in casi particolari di accesso in remoto a file di grandi dimensioni o continuamente modificati.



Attenzione: ricordare che l'esclusione di oggetti dalla scansione aumenta i rischi per la sicurezza.

16 Supporto tecnico

È possibile ricevere supporto tecnico per i prodotti Sophos in uno dei seguenti modi:

- Visitando la community SophosTalk su <http://community.sophos.com/> e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su <http://www.sophos.com/support/>.
- Scaricando la documentazione del prodotto su <http://www.sophos.com/support/docs/>.
- Inviando un'e-mail a support@sophos.com, indicando il o i numeri di versione del software Sophos in vostro possesso, i sistemi operativi e relativi livelli di patch, ed il testo di ogni messaggio di errore.

17 Note legali

Copyright © 2011 Sophos Limited. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la registrazione e altri mezzi, salvo che da un licenziatario autorizzato a riprodurre la documentazione in conformità con i termini della licenza, oppure previa autorizzazione scritta del titolare dei diritti d'autore.

Sophos e Sophos Anti-Virus sono marchi registrati di Sophos Limited. Tutti gli altri nomi citati di società e prodotti sono marchi o marchi registrati dei rispettivi titolari.

Common Public License

Il software Sophos descritto in questo documento comprende o può comprendere programmi di software concessi in licenza (o sottolicensing) all'utente secondo i termini della Common Public License (CPL), la quale, tra gli altri diritti, permette all'utente di avere accesso al codice sorgente. La CPL richiede, per qualsiasi software concesso in licenza secondo i termini della stessa, e distribuito in formato codice oggetto, che il codice sorgente di tale software venga messo a disposizione anche degli altri utenti del formato codice oggetto. Per qualsiasi software che rientri nei termini della CPL, il codice sorgente è disponibile tramite ordine postale inviandone richiesta a Sophos; per e-mail a support@sophos.com o tramite internet su <http://www.sophos.com/support/queries/enterprise.html>. Una copia dei termini per tali software è reperibile all'indirizzo <http://opensource.org/licenses/cpl1.0.php>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.