

SOPHOS

Sophos Endpoint Security and Control Guida all'impostazione dei criteri

Versione prodotto: 9.0

Data documento: agosto 2009



Sommario

1	Informazioni sulla guida.....	3
2	Consigli sui criteri generali.....	4
3	Impostazione del criterio di aggiornamento.....	5
4	Impostazione dei criteri antivirus e HIPS.....	6
5	Impostazione dei criteri del controllo applicazioni.....	8
6	Impostazione dei criteri del controllo dispositivi.....	9
7	Impostazione dei criteri del controllo dati.....	11
8	Impostazione dei criteri firewall.....	15
9	Impostazione dei criteri di NAC.....	18
10	Consigli sulla scansione.....	20
11	Utilizzo della scansione in accesso.....	21
12	Utilizzo della scansione pianificata.....	22
13	Utilizzo della scansione su richiesta	23
14	Esclusione degli oggetti dalla scansione.....	24
15	Supporto tecnico.....	25
16	Copyright.....	26

1 Informazioni sulla guida

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

Nello specifico, fornisce consigli per supportare gli utenti nel:

- Comprendere le raccomandazioni 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 utilizza Enterprise Console.
- Si desiderano consigli sulle migliori opzioni relative all'impostazione e 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 in www.sophos.it/support/docs/Enterprise_Console-all.html.

2 Consigli sui criteri generali

Dopo l'installazione di Enterprise Console, vengono creati dei criteri predefiniti. Tali criteri vengono quindi 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 e accesso alla rete, è necessario creare nuovi criteri o crearne di predefiniti. Quando si impostano i 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 gruppo e criteri a parte.

3 Impostazione del 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 dalla stessa posizione 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.

- Se in possesso di computer non sempre connessi alla rete (come laptop), impostare una fonte di aggiornamento alternativa. Se i computer non riescono a contattare la fonte consueta, tenteranno di eseguire l'aggiornamento da questa fonte alternativa. Per ulteriori informazioni, consultare la Guida in linea di Sophos Enterprise Console .
- Se preoccupati per il rendimento dei computer a basse specifiche, 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 più recenti relativi al rilevamento delle minacce. È, altrimenti, possibile eseguire l'aggiornamento dei computer a basse specifiche meno frequentemente (due o tre volte al giorno) o a orari fissi al di fuori degli orari di lavoro degli utenti (la sera o durante i weekend).



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

I criteri antivirus e HIPS stabiliscono come 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.
- Utilizzare l'opzione **Notifica solamente** per rilevare solo il comportamento in fase di esecuzione HIPS. Se inizialmente si definisce il criterio report only, ciò consente di avere migliore consapevolezza dell'utilizzo in rete del comportamento in fase di esecuzione. 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 del criterio antivirus e HIPS

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

1. Creare diversi criteri per diversi gruppi.
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 della knowledge base (<http://www.sophos.it/support/knowledgebase/article/12421.html>).
3. 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.
 - b) Selezionare le opzioni di disinfezione per virus/spyware.
4. 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 **Cerca file sospetti (HIPS)**.
 - c) Selezionare l'opzioni di disinfezione per i file sospetti.
 - d) Se del caso, autorizzare tutti i file di cui è consentito l'utilizzo.

5. Rilevare comportamento sospetto e buffer overflow (comportamento in fase di esecuzione HIPS).

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 **Avvisa 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 eliminando l'opzione **Avvisa solamente**.

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

6. 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.

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

7. Abilitare la scansione in accesso per proteggere i computer in futuro. Per ulteriori informazioni, consultare la sezione *Utilizzo della scansione in accesso* a pagina 21.

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

5 Impostazione dei criteri del controllo applicazioni

5.1 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.
- Utilizzare il 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?

5.2 Distribuzione del criterio di controllo applicazioni

Per impostazione predefinita, sono consentite tutte le applicazioni e i tipi di applicazione. Sophos consiglia di impostare il controllo delle 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.
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.
4. Creare diversi criteri per diversi gruppi.
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, cancellando 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.

6 Impostazione dei criteri del controllo dispositivi

6.1 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. 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.
- 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.
- 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.
- Essere assolutamente sicuri di voler bloccare un dispositivo, prima di distribuire il relativo criterio. 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, se la rete è bloccata, non potrà essere sbloccata da Enterprise Console, dal momento che il computer non potrà accettare alcuna configurazione aggiuntiva dal server.

6.2 Distribuzione del criterio di controllo dispositivi

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

Nota: se il controllo dispositivi veniva utilizzato con Enterprise Console 3.1, le impostazioni del controllo dispositivi si trovano nel criterio di controllo applicazioni. Per trasferirle al nuovo criterio del controllo dispositivi, utilizzare il tool DeviceControlMigration. Per ulteriori informazioni, consultare la Guida all'upgrade avanzata di Sophos Endpoint Security and Control.

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.
3. Utilizzare il Visualizzatore eventi del controllo dispositivi per vedere quali dispositivi sono in esecuzione e stabilire quali tipi di dispositivi si desidera bloccare.
4. Creare diversi criteri per diversi gruppi. È per esempio possibile non autorizza l'utilizzo di dispositivi di memorizzazione rimovibili per i dipartimenti di risorse umane e finanza e invece consentirlo 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 cancellando 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.

7 Impostazione dei criteri del controllo dati

7.1 Definizione del criterio del 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 a disposizione includono "Consenti il trasferimento del file" (modalità monitor), "Consenti il trasferimento se l'utente ha accettato" (modalità training) e "Blocca il trasferimento".

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.

7.2 Impostazioni consigliate

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

- Utilizzare l'azione **Consenti il trasferimento del file** 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** 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 rilevarne 50 o più indirizzi.

Nota: Sophos fornisce impostazioni della quantità predefinite per tutti i Content Control List. Per evitare che si generino troppi eventi del controllo dati, Sophos consiglia di utilizzare una quantità minima pari a tre o più corrispondenze.

- 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.
- 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 dettagliato per ottenere maggiori dettagli 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 dettagliata 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.

7.3 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. Sophos consiglia di impostare il controllo dati come segue:

1. Comprendere il funzionamento del controllo dati nei computer:

- **Dispositivi di memorizzazione:** tutti i trasferimenti su dispositivi di memorizzazione monitorati devono avvenire tramite Windows Explorer. Ciò garantisce che venga eseguita la scansione di tutti i file prima che vengano copiati nel dispositivo di memorizzazione. Verrà bloccato qualsiasi tentativo di creare file in o di salvarli direttamente su un dispositivo di memorizzazione. Quando si verifica questo tipo di blocco, per poter completare il trasferimento l'utente dovrà utilizzare Windows Explorer. Questa restrizione è attuata per tutte le azioni relative al controllo dati.
- **Applicazioni:** per assicurarsi che vengano monitorati solo i file caricati dagli utenti, alcuni percorsi dei file di sistema vengono esclusi dal monitoraggio del controllo dati. Ciò consente di ridurre in modo rilevante il rischio che si generino eventi del controllo dati dovuti ad applicazioni che aprono file di configurazione, piuttosto che a utenti che caricano file.

Importante: se si verificano eventi errati generati da un'applicazione che apre file di configurazione, tale problema può essere risolto aggiungendo esclusioni di percorsi personalizzate o configurando una regola del controllo dati in modo tale che sia meno sensibile. Per ulteriori informazioni, consultare l'articolo 57630 della knowledge base (<http://www.sophos.it/support/knowledgebase/article/57630.htm>).

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, Sophos 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 il trasferimento del file** per rilevare, ma non bloccare, il controllo dati.

Importante: Sophos 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).

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 reattive ad alcune regole per **Consenti il trasferimento se l'utente ha accettato** o **Blocca il trasferimento**. Se si utilizzano queste azioni, trovare il giusto equilibrio fra la riduzione del rischio di perdita dei dati e il tentativo di non interrompere i normali processi aziendali.
 - Creare diversi criteri per diversi gruppi. Per esempio, si può voler consentire ai computer del dipartimento delle risorse umane di accedere a dati che possono portare all'identificazione personale, ma bloccare l'accesso a tutti gli altri computer del gruppo.

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

8 Impostazione dei criteri firewall

8.1 Impostazioni consigliate

I criteri Firewall stabiliscono 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 il 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.
- 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 cancellare l'opzione **Visualizza un allarme nella console di gestione se sono apportati cambiamenti a regole globali, applicazioni, processi o checksum** 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.
- Sophos consiglia di non modificare le impostazioni predefinite ICMP, le regole globali e le regole delle applicazioni, se non in possesso di una competenza della rete adeguata.
- Sophos consiglia, quando possibile, la creazione di regole di applicazione piuttosto che di regole globali.

8.2 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, Sophos 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, Sophos consiglia 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, Sophos consiglia di aggiungere una voce DNS specifica per il server DNS che abbia un nome inusuale 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.

8.3 Quando bloccare o consentire traffico, applicazioni e processi

Sophos 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 da Enterprise Console di tutto il traffico, applicazioni o processi.
- 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 avvertiti solo quando verranno installate nuove applicazioni o patch per applicazioni esistenti (se ci si trova in modalità **Interattiva**).

8.4 Distribuzione del criterio 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 in tutti i computer. Sophos 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 quale tipo di traffico, applicazioni e processi sono in uso. Il Visualizzatore eventi consente anche di creare con facilità regole che consentano o blocchino il traffico, le applicazioni ed i processi rilevati.
4. Se necessario, creare regole globali o delle 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 non saranno messi in sicurezza.
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 della knowledge base (<http://www.sophos.it/support/knowledgebase/article/14464.html>).

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

9 Impostazione dei criteri di NAC

9.1 Quando utilizzare criteri di NAC predefiniti

I criteri NAC stabiliscono le condizioni alle quali i computer devono conformarsi prima di poter accedere alla rete. Per impostazione predefinita, Sophos NAC consente a tutti i computer di accedere alla rete. È necessario configurare un criterio 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 il Compliance Agent, ma non gli è stato attribuito nessun 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 viene utilizzato per i computer gestiti con Enterprise Console e che hanno il Compliance Agent installato. 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. Il Compliance Dissolvable Agent utilizza il criterio Unmanaged.

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

9.2 Distribuzione del criterio di NAC

Quando si installa NAC per la prima volta, il criterio "Predefinito" di NAC 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. Sophos consiglia di impostare il criterio di NAC secondo quanto descritto di seguito:

1. In Enterprise Console, creare o importare gruppi e applicare i 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 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 lo stato di conformità corrente degli utenti.
I report offrono una rappresentazione realistica di quanto gli utenti siano conformi al criterio di NAC.
5. Utilizzare NAC Manager per aggiornare il criterio Managed 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 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.

10 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 impostazioni predefinite all'interno del criterio.
- Se possibile impostare la scansione in Enterprise Console e non nel computer.
- Tenere presente il ruolo del computer (per es. desktop o server).
- La scansione **Normale** è preferibile a quella **Completa**. La scansione normale esegue la scansione delle parti infettabili dei file, mentre quella completa esegue la scansione di tutti i contenuti del file apportando un aumento minimo della sicurezza. Utilizzare la scansione completa solo se consigliata dal supporto tecnico.
- L'opzione **Scansione di tutti i file** non è solitamente necessaria né viene consigliata. Utilizzare invece l'opzione **Scansione dei file eseguibili e infettabili** per ricercare le minacce trovate 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, Sophos sconsiglia di selezionare questa opzione, a meno che non si faccia un uso frequente dei file di archivio.

11 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 **In lettura**. Le opzioni della scansione in accesso **In scrittura** e **Se rinominati** 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 i criteri antivirus e HIPS con software di cifratura, consultare l'articolo 12790 della knowledge base (<http://www.sophos.it/support/knowledgebase/article/12790.html>).
- 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 22.



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

12 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 della knowledge base (<http://www.sophos.it/support/knowledgebase/article/12421.html>).
- 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.

13 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.

14 Esclusione degli oggetti dalla scansione

Per escludere oggetti dalla scansione fare quanto riportato di seguito:

- Per escludere dalla scansione determinati tipi di file, utilizzare le estensioni.
- Per escludere dalla scansione oggetti o driver specifici, 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 sono 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. Sophos consiglia che tutti i computer eseguano la scansione dei file remoti quando vi accedono, anche se questa opzione viene selezionata solo per i file server o in casi particolari in cui si accede 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.

15 Supporto tecnico

Per ricevere assistenza tecnica, visitare il sito <http://www.sophos.it/support>.

Se si contatta il supporto tecnico, fornire più informazioni possibile, fra le quali

- il o i numeri di versione del software Sophos
- i sistemi operativi e relativi livelli di patch
- il testo esatto di ogni messaggio di errore visualizzato.

16 Copyright

Copyright © 2009 Sophos Group. 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 Plc e Sophos Group. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at <http://www.sophos.com/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>