SOPHOS

Security made simple.

Sophos Enterprise Console
Guida all'impostazione dei criteri

Versione prodotto: 5.5

Sommario

1 Informazioni sulla guida

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

Nota: Se non incluse nella licenza, alcune funzioni potrebbero non essere disponibili.

Nello specifico, fornisce consigli per aiutare gli utenti a:

- 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 alla distribuzione dei criteri.

Prima di consultare questa guida, leggere la *guida di avvio rapido di Sophos Enterprise Console*.

La documentazione completa di Enterprise Console è reperibile al link http://www.sophos.com/it-it/support/documentation/enterprise-console.aspx.

2 Consigli generali sui criteri

Dopo l'installazione di Enterprise Console, vengono automaticamente creati criteri predefiniti. Tali criteri vengono applicati a tutti i gruppi creati dall'utente. I criteri predefiniti sono studiati per fornire livelli di protezione efficaci. Se si desidera utilizzare funzioni quali controllo dell'accesso alla rete, patch, controllo applicazioni dispositivi, dati o blocco rimozione, è necessario creare nuovi criteri o modificare quelli 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, ove possibile, impostare le opzioni in Enterprise Console, piuttosto che sul 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 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 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.

- 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, sezione *Aggiornamento computer* > *Configurazione criterio di aggiornamento*.

- La ricerca automatica di un percorso va consentita in un criterio per utenti dotati di laptop che navigano frequentemente o internazionalmente all'interno di un'organizzazione 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, minimizzando i ritardi di aggiornamento e i costi legati alla larghezza di banda. Se vengono restituiti percorsi multipli, il laptop determina quale sia quello più prossimo 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 del percorso funziona solo se sia i laptop in roaming sia gli endpoint fissi sono gestiti dalla stessa istanza di Enterprise Console e utilizzano la medesima sottoscrizione al software. Gli eventuali firewall di terze parti devono essere configurati per consentire query e risposte relative al percorso degli aggiornamenti. La porta utilizzata per impostazione predefinita è la 51235, ma è possibile cambiarla.

  Per ulteriori informazioni, consultare la Guida in linea di Sophos Enterprise Console, sezione *Aggiornamento computer* > *Configurazione criterio di aggiornamento* > *Configurazione dei percorsi del server per gli aggiornamenti*. Per le domande più frequenti relative alla ricerca automatica di un percorso, leggere l'articolo 112830 della knowledge base del supporto tecnico Sophos (http://www.sophos.com/it-it/support/knowledgebase/112830.aspx).

- 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 in maniera meno frequente (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.
- Per sfruttare appieno la funzionalità Sophos Live Protection, attivata per impostazione predefinita, si consiglia di selezionare anche l'opzione **Invia automaticamente file campione a Sophos**.
- Abilitare il rilevamento del traffico malevolo, che consente di rilevare le comunicazioni fra computer endpoint e server command and control coinvolti in attacchi botnet o di altro malware. L'opzione **Rileva traffico malevolo** è abilitata per impostazione predefinita nelle nuove installazioni di Enterprise Console versione 5.3 o successive. Se si è effettuato l'upgrade da una versione precedente di Enterprise Console, sarà necessario abilitare questa opzione per poter usufruire di tale funzionalità.

  Nota: Il rilevamento del traffico malevolo è al momento supportato da sistemi operativi non-server Windows 7 e successivi. Richiede Sophos Live Protection.

- Utilizzare l'opzione **Notifica solamente** per rilevare solo il comportamento sospetto. Se inizialmente si definisce il criterio report only, ciò consente di avere migliore consapevolezza 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.

Per ulteriori informazioni, consultare l'articolo 114345 della knowledge base del supporto tecnico Sophos (http://www.sophos.com/it-it/support/knowledgebase/114345.aspx).

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. 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 vostro software Sophos in tempo reale. Sophos Live Protection è richiesta dalle funzionalità di Rilevamento del traffico malevolo e Reputazione del download.

- Verificare che le opzioni **Abilita Live Protection per la scansione in accesso** e **Abilita Live Protection per la scansione su richiesta** siano selezionate. Se la scansione antivirus su un computer ha identificato un file come sospetto, ma non riesce poi a determinare se sia pulito o malevolo, in base ai file di identità delle minacce (IDE) memorizzati nel computer, alcune caratteristiche del file (come il checksum e altri attributi) vengono inviati 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 pulito o malevolo, la decisione viene inviata al computer e lo stato del file viene automaticamente aggiornato.
- Selezionare l'opzione **Invio automatico di file campione a Sophos**. Se un file viene considerato potenzialmente malevolo, ma non può essere identificato con certezza come malevolo solo in base alle caratteristiche del file, Sophos Live Protection consente a Sophos di richiedere un campione del file. Quando è abilitata Live Protection, se l'opzione **Invia automaticamente file campione a Sophos** è attiva e Sophos non detiene ancora un campione del file, l'invio del file avverrà in maniera automatica. L'invio di tali campioni permette a Sophos di migliorare continuamente 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 vostra soluzione di filtraggio web. Per informazioni, consultare l'articolo della knowledge base 62637 (http://www.sophos.com/it-it/support/knowledgebase/62637.aspx). Se si utilizza una soluzione di filtraggio web Sophos, come la Web Appliance WS1000, non c'è bisogno di fare nulla. I domini Sophos sono già considerati fidati.

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. Per ulteriori informazioni, vedere Utilizzo della scansione in accesso a pagina 34 o Utilizzo della scansione pianificata a pagina 35.
   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 **File sospetti** nelle impostazioni di scansione.
   c) Selezionare l'opzione di disinfezione per i file sospetti.
   d) Se del caso, autorizzare tutti i file di cui è consentito l'utilizzo.
5. Rilevare comportamenti malevoli e sospetti, buffer overflow, oltre che traffico malevolo (monitoraggio del comportamento).

Queste opzioni monitorano costantemente i processi in esecuzione per stabilire se un determinato programma abbia comportamenti malevoli o sospetti. Sono utili per bloccare eventuali falle alla sicurezza.

a) Accertarsi che il monitoraggio del comportamento sia abilitato per la scansione in accesso. Dovrebbe essere abilitato per impostazione predefinita.

b) Verificare che l'opzione **Rilevamento di traffico malevolo** sia selezionata.

c) Utilizzare l'opzione **Avvisa solamente** solo per rilevare comportamenti sospetti e buffer overflow. Questa opzione è abilitata per impostazione predefinita.

d) Autorizzare tutti i programmi o file che si desidera continuare ad eseguire anche in futuro.

e) 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 di Sophos (http://www.sophos.com/it-it/support/knowledgebase/50160.aspx).

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.

   c) Selezionare l'opzione **scansione in accesso di Adware e PUA** per rilevare adware e PUA in futuro.

   Per ulteriori informazioni, consultare l'articolo 13815 della knowledge base di Sophos (http://www.sophos.com/it-it/support/knowledgebase/13815.aspx).

7. Rilevare minacce nelle pagine web.

   Questa opzione blocca i siti web noti per ospitare contenuti malevoli, esegue la scansione dei download alla ricerca di contenuti malevoli.

   a) Assicurarsi che l'opzione **Blocca l'accesso ai siti web malevoli** sia impostata su **On**, per assicurarsi che i siti web malevoli vengano bloccati. Questa opzione è attiva per impostazione predefinita.

   b) Impostare l'opzione **Scansione dei contenuti** su **Attiva** o **Come in accesso**, per effettuare la scansione e bloccare il download di dati malevoli. **Come in accesso**, impostazione predefinita, consente la scansione dei download solo quando è abilitata la scansione in accesso.

   c) A seconda delle proprie necessità, autorizzare i siti web consentiti.

   d) Controllare che la verifica della reputazione dei file sia abilitata.

   Nota: È inoltre possibile utilizzare il criterio di controllo web per controllare l'utilizzo di Internet grazie all'opzione di filtro dei siti web inclusi nelle 14 categorie di siti web inappropriati. Per informazioni su come impostare un criterio di controllo web, consultare la sezione Impostazione dei criteri per il controllo web a pagina 28.

Per ulteriori informazioni su come impostare i criteri di controllo antivirus e HIPS, consultare la Sophos Enterprise Console di Guida in linea.

5 Impostazione dei criteri del firewall

5.1 Criterio del firewall

Il criterio del firewall stabilisce la modalità con la quale il firewall protegge i computer. Solo le applicazioni o classi di applicazioni menzionate possono accedere alla rete aziendale o a internet.

Nota: Sophos Client Firewall non è supportato nei sistemi operativi del server. Per i requisiti di hardware e sistema operativo, consultare la pagina corrispondente del sito web di Sophos (http://www.sophos.com/it-it/products/all-system-requirements).

Attenzione: Configurare il criterio del firewall prima di utilizzarlo. Distribuire, in un gruppo, un criterio predefinito non modificato utilizzando Enterprise Console provocherà problemi di comunicazione di rete.

Il criterio del firewall predefinito non deve essere distribuito "così com'è" e non è adatto a uso normale. Si tratta della base su cui costruire criteri propri.

Per impostazione predefinita il firewall è attivato e blocca tutto il traffico della rete non essenziale. Ciò che va oltre il networking di base, per esempio software di posta elettronica, browser web e qualsiasi accesso del database di rete, non funzionerà correttamente se è attivo il criterio predefinito che blocca le connessioni non essenziali. 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.

5.2 Pianificazione dei criteri firewall

Pianificare i criteri firewall e stabilire quali funzioni dovranno svolgere, prima di creare o modificare le regole del firewall (globale, applicazione o altro).

Quando si pianificano i criteri firewall, considerare:

- Quali computer debbano avere Sophos Client Firewall.
- Se si tratti di computer desktop o laptop. È possibile impostare un percorso doppio per i laptop.
- Quale metodo di rilevamento del percorso eseguire, vale a dire ricerca DNS o gateway MAC.
- Sistemi e protocolli di rete.
- Le connessioni remote.

In base ai diritti di accesso delle applicazione e della rete richiesti dai diversi gruppi di utenti, decidere quanti criteri firewall sarà necessario creare. I criteri si riferiranno a diverse applicazioni e varieranno in restrittività. Ricordare che in Enterprise Console, quando è presente un maggior numero di criteri occorre impostare più gruppi.

- Evitare di utilizzare un solo criterio di Sophos Client Firewall. Se si utilizza un solo criterio, si potrebbe essere costretti ad aggiungere regole per uno o due computer (per es. la workstation dell'amministratore), ma queste regole resterebbero presenti in tutta la rete e ciò potrebbe costituire un rischio alla sicurezza.

- Viceversa, utilizzando molte configurazioni viene richiesto più tempo per il monitoraggio e la manutenzione.

Sistemi e protocolli di rete

Tenere presente i servizi su cui si fonda la rete. Per esempio:

- DHCP
- DNS
- RIP
- NTP
- GRE

Nella configurazione predefinita del firewall sono presenti regole per amministrare la maggior parte di questi servizi. È tuttavia necessario sapere quali consentire e quali no.

Accesso remoto ai computer

Se si utilizza un software di accesso remoto per monitorare i computer, è necessario creare regole nella propria configurazione per poter lavorare in questo modo.

Identificare le tecnologie utilizzate per accedere ai computer nella rete. Per esempio:

- RDP
- VPN client/server
- SSH/SCP
- Servizi terminal
- Citrix

Verificare quale tipo di accesso sia richiesto e, in base a questo, creare le proprie regole.

5.3 Impostazioni consigliate

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

- Quando è installato Sophos Client Firewall, Windows Firewall viene disattivato. Di conseguenza, se si utilizza Windows Firewall, prendere nota delle 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 **Eventi** > **Eventi firewall**.
- Rivedere le regole create utilizzando il Visualizzatore eventi. Un'applicazione può generare più eventi del firewall (eventi diversi per azioni diverse eseguite dall'applicazione), ma una regola dell'applicazione deve includere tutte le azioni dell'applicazione. Per esempio, un client di posta elettronica potrebbe generare due diversi eventi relativi all'invio e alla ricezione di un'e-mail, ma una regola dell'applicazione per tale client deve includere entrambe le azioni sopra citate.

- 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 competenza di rete.
- Si consiglia, quando possibile, la creazione di regole delle applicazioni, piuttosto che di regole globali.
- In un criterio in cui è impostato un percorso doppio, non utilizzare la modalità **Interattiva**.
- Non utilizzare la modalità **Interattiva** in reti di medie o grandi dimensioni, oltre che in ambienti di dominio. La modalità **Interattiva** può essere utilizzata per la creazione di regole del firewall in tutte le reti di piccole dimensioni (per es. fino a 10 computer), in ambienti di gruppo di lavoro e in computer autonomi.

5.4 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 scheda **Generale**, sotto **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 esercitare 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.

5.5 Implementazione di un criterio firewall

Implementazione di un criterio che consente di monitorare tutto il traffico nella rete. I report sul traffico di rete verranno riportati nel Visualizzatore eventi del firewall. Utilizzare queste informazioni per impostare un criterio di base.

Si consiglia di eseguire un'implementazione in fasi di Sophos Client Firewall nella rete, vale a dire, implementare Sophos Client Firewall in un gruppo alla volta. Ciò eviterà che, nelle fasi iniziali, venga sovraccaricato il traffico della rete.

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

1. Implementare Sophos Client Firewall su un gruppo di computer di prova che includa i diversi ruoli presenti nella rete.
2. Configurare un criterio firewall perché si utilizzi la modalità **Consenti per impostazione predefinita** per rilevare, ma non bloccare, il traffico ordinario, applicazioni e processi, quindi assegnare il criterio al gruppo di test.
   a) Creare un nuovo criterio firewall. In Enterprise Console, nel pannello **Criteri**, cliccare con il tasto destro del mouse su **Firewall** e selezionare l'opzione **Crea criterio**. Attribuire un nome a questo criterio e cliccarvi due volte.

      Si avvia la procedura guidata di **configurazione dei criteri del Firewall**.

   b) Scegliere se utilizzare la procedura guidata cliccando su **Avanti**, oppure eseguire la configurazione manualmente cliccando su **Criteri avanzati firewall**.
      - Se si utilizza la procedura guidata: Cliccare su **Avanti**. Scegliere **Percorso singolo** e cliccare su **Avanti**. Selezionare **Monitora**, cliccare su **Avanti** quindi su **Avanti** di nuovo, poi su **Fine**.
      - Se si utilizza l'opzione **Criteri avanzati firewall**: Nella casella di dialogo **Criterio firewall**, vicino a **Percorso primario**, cliccare su **Configura**. Nella scheda **Generale**, impostare la modalità di lavoro su **Consenti per impostazione predefinita**. Cliccare su **OK** e quindi su **OK** ancora.

   c) Attribuire il nuovo criterio firewall al gruppo di test.
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 **Eventi** > **Eventi firewall**.
4. Monitorare gli eventi firewall e creare il proprio criterio che sia per esempio valido per alcune settimane.
   a) Creare regole dal Visualizzatore eventi. Cliccare col tasto destro del mouse sull'evento per cui creare la relativa regola. Per ulteriori informazioni sulla creazione delle regole firewall, consultare la Guida in linea di Sophos Enterprise Console, nella sezione *Configurazione criteri > Criterio firewall*.
   b) Ricercare eventuali punti deboli nel criterio (per es. troppa libertà di accesso a determinati utenti).
   c) Se le necessità sono diverse, suddividere il gruppo e creare criteri e regole extra a seconda delle necessità.

5. Rivedere le regole create utilizzando il Visualizzatore eventi. Un'applicazione può generare più eventi del firewall (eventi diversi per azioni diverse eseguite dall'applicazione), ma una regola dell'applicazione deve includere tutte le azioni dell'applicazione. Per esempio, un client di posta elettronica potrebbe generare due diversi eventi relativi all'invio e alla ricezione di un'e-mail, ma una regola dell'applicazione per tale client deve includere entrambe le azioni sopra citate.
6. Dividere il resto della rete in gruppi gestibili e rappresentativi dei diversi ruoli presenti in rete, per es. le workstation degli addetti alle vendite, quelle degli amministratori IT ecc.
7. Dopo avere incluso tutti i ruoli, per es. quando si è ridotto il numero degli eventi del firewall per cui non sussistono regole, creare criteri basati sulle regole ed assegnarli secondo necessità. Se nella rete è presente un numero elevato di computer, si consiglia di eseguire la distribuzione di Sophos Client Firewall in un gruppo alla volta.
8. 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.

Per ulteriori informazioni su come impostare i criteri del firewall, consultare la Guida in linea di Sophos Enterprise Console, sezione *Configurazione criteri > Criterio firewall*.

Nota: Come alternativa al monitoraggio del traffico di rete e alla creazione di regole utilizzando il Visualizzatore eventi del Firewall, in reti molto piccole o computer autonomi che eseguono Windows 7 o precedenti, è possibile installare Sophos Client Firewall in un computer di prova e configurarlo in modalità **Interattiva**. Utilizzare il maggior numero possibile di applicazioni eseguite nella rete, inclusi i browser web. Quindi importare e modificare la configurazione del firewall contenenti le regole stabilite da tale processo. Per ulteriori informazioni, consultare la Guida in linea di Sophos Endpoint Security and Control.

6 Impostazione dei criteri del 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 **Eventi** > **Eventi del 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 di un criterio del 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 **Eventi** > **Eventi del 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 desiderare 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, 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 su come impostare un criterio del controllo applicazioni, consultare la Guida in linea di Sophos Enterprise Console.

Nota: Il controllo applicazioni può essere configurato per bloccare il file CScript.exe utilizzato da Patch. Se si utilizzano contemporaneamente il controllo applicazioni e patch, accertarsi di non bloccare **Microsoft WSH CScript**, nella categoria **tool di programmazione/scrip**. Per impostazione predefinita, i tool di programmazione e script sono consentiti.

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 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.

7.2 Impostazioni consigliate

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

- Utilizzare l'azione **Consenti trasferimento file e registra 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 registra 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 rilevarne 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 **Eventi** > **Eventi del 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 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 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.

7.3 Distribuzione di un criterio del 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 registra evento" o l'azione "Blocca trasferimento e registra 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, in cui si richiede l'utilizzo di Esplora risorse per completare il trasferimento.

     Quando un criterio del controllo dati contiene solo regole con l'azione "Consenti trasferimento file e registra 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 i file e i 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 concentrasi 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 file e registra 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 datti 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 **Eventi** > **Eventi del 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 **Permettere il trasferimento dietro accettazione dell'utente e connettersi all'evento** oppure **Bloccare il trasferimento e connettersi all'evento**.
   - Creare criteri diversi per gruppi diversi. Per esempio, si potrebbe voler autorizzare i computer nel reparto Risorse umane a trasferire informazioni che possono portare all'identificazione personale, ma impedire questa azione a tutti gli altri gruppi.

Per ulteriori informazioni su come impostare un criterio di controllo dati, consultare la Guida in linea di Sophos Enterprise Console.

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

Il seguente elenco comprende contenuti ed azioni esaminati o non esaminati dalla scansione all'interno delle applicazioni supportate

Per un elenco completo di limitazioni note del controllo dati, consultare l'articolo 63016 della knowledge base del supporto tecnico Sophos (http://www.sophos.com/it-it/support/knowledgebase/63016.aspx).

Applicazioni	Azioni di scansione del controllo dati
Browser web	**Esaminati:** ▪ File caricati ▪ Allegati webmail ▪ Upload di Microsoft SharePoint **Non esaminati** ▪ Contenuto messaggi Webmail ▪ Voci del blog ▪ File scaricati **Nota:** In una piccola percentuale di casi, la scansione dei file può essere eseguita durante il download.

Applicazioni	Azioni di scansione del controllo dati
Client e-mail	**Esaminati** ▪ Allegati e-mail **Non esaminati** ▪ Contenuto messaggi e-mail ▪ Allegati inoltrati ▪ Allegati fatti utilizzando l'opzione e-mail "Send" 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 **Nota:** In una piccola percentuale di casi, è possibile eseguire la scansione dei file durante il salvataggio.
Client di messaggistica istantanea (IM)	**Esaminati** ▪ Trasferimenti di file **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. **Non esaminati** ▪ Contenuto messaggi IM ▪ File inviati

8 Impostazione dei criteri del controllo dispositivi

8.1 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 **Eventi** > **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 della knowledge base del supporto tecnico Sophos (http://www.sophos.com/it-it/support/knowledgebase/63102.aspx).
- 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 riabilitate 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 sarà in grado di accettare alcuna configurazione aggiuntiva dal server.

8.2 Distribuzione di un criterio del 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 **Eventi** > **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 deselezionando 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 su come impostare un criterio del controllo dispositivi, consultare la Guida in linea di Sophos Enterprise Console.

9 Configurazione dei criteri del blocco rimozione

9.1 Criterio del blocco rimozione

Il blocco rimozione impedisce agli utenti (amministratori locali con limitate conoscenze tecniche) di riconfigurare, disabilitare o disinstallare il software di sicurezza Sophos. Gli utenti che non conoscono la password del blocco rimozione non potranno eseguire queste operazioni.

Nota: Il blocco rimozione non è pensato per offrire protezione contro utenti con vaste conoscenze tecniche. Non offre protezione contro malware appositamente studiato per sovvertire il funzionamento del sistema operativo in modo tale da non essere rilevato. 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 8.

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 (ad es. Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, o Sophos Remote Management System) 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 **Eventi** > **Eventi blocco rimozione**.

9.2 Distribuzione di un 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 ha alcuna ripercussione 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 un criterio del blocco rimozione, consultare la Guida in linea di Sophos Enterprise Console.

10 Configurazione dei criteri patch

Nota: Questa funzione non è inclusa in tutte le licenze. Se la si desidera utilizzare potrebbe essere necessario personalizzare la propria licenza. Per ulteriori informazioni, vedere https://www.sophos.com/it-it/products/endpoint-antivirus/how-to-buy.aspx.

10.1 Criterio patch

I criteri patch consentono di verificare che i computer abbiano sempre installate le patch più aggiornate.

SophosLabs fornisce livelli di valutazione delle minacce che consentono di determinare i problemi critici relativi alle patch, per poterli risolvere il più rapidamente possibile. I livelli di minaccia forniti da SophosLabs prendono in considerazione i fenomeni più recenti e possono quindi non corrispondere ai livelli di pericolosità stabiliti dai fornitori.

Quando si imposta il criterio patch, considerare l'utilizzo del Visualizzatore eventi per controllare le patch mancanti nei computer aziendali. Fornisce informazioni sulle patch di protezione e i risultati della verifica delle patch. Dopo avere abilitato la verifica patch nel criterio patch, è possibile visualizzare lo stato delle patch per computer, gruppo o minaccia. È possibile accedere al Visualizzatore eventi cliccando su **Eventi** > **Eventi verifica patch**.

Nota: Patch utilizza il file CScript.exe che può essere bloccato dal controllo applicazioni. Se si utilizzano contemporaneamente il controllo applicazioni e patch, accertarsi di non bloccare **Microsoft WSH CScript**, nella categoria **tool di programmazione/scrip** nel criterio del **Controllo applicazioni**. Per impostazione predefinita, i tool di programmazione e script sono consentiti dal controllo applicazioni.

10.2 Implementazione di un criterio patch

Inizialmente, il criterio patch "predefinito" viene applicato a tutti i computer. Nel criterio predefinito la verifica patch è disabilitata.

Una volta abilitata la verifica delle patch, i computer daranno inizio a tale operazione. Possono essere necessari diversi minuti. Le verifiche successive verranno eseguite in base all'intervallo impostato nel criterio, per impostazione predefinita con cadenza giornaliera.

Nota: Se i computer eseguono una verifica prima che Enterprise Console abbia scaricato per la prima volta i dati sulle patch da Sophos, il Visualizzatore eventi patch non restituirà alcun risultato. Il download può richiedere molte ore. Per verificare che sia concluso, controllare il campo relativo agli **aggiornamenti delle patch** nel **Visualizzatore eventi - Verifica patch**.

Si consiglia di impostare il criterio patch secondo quanto descritto qui di seguito:

1. Distribuire l'agente delle patch nei computer tramite la procedura guidata di protezione dei computer (nella pagina **Seleziona funzionalità** della procedura guidata, scegliere **Patch**).

   Nota: Se i computer eseguono già Endpoint Security and Control ma non dispongono del patch agent, dovranno essere nuovamente protetti eseguendo la procedura guidata per la protezione dei computer.

2. Abilitare le verifiche patch nel criterio patch predefinito.

   A questo punto si dispone di un unico criterio patch per l'intera rete.

3. Utilizzare il Visualizzatore eventi della verifica patch per vedere quali computer non dispongono di tutte le patch e quali invece sono aggiornati. È possibile accedere al Visualizzatore eventi cliccando su **Eventi** > **Eventi verifica patch**.

   Nota: Installare manualmente le patch mancanti nei computer.

4. Se si richiede la facoltà di attivare o disattivare il criterio patch o di assegnare intervalli di verifica patch diversi per vari gruppi, creare criteri diversi per gruppi diversi.

Per ulteriori informazioni su come impostare un criterio patch, consultare la Guida in linea di Sophos Enterprise Console.

11 Impostazione dei criteri per il controllo web

Nota: Questa funzione non è inclusa in tutte le licenze. Se la si desidera utilizzare potrebbe essere necessario personalizzare la propria licenza. Per ulteriori informazioni, vedere https://www.sophos.com/it-it/products/endpoint-antivirus/how-to-buy.aspx.

Il criterio di controllo web specifica i siti web a cui gli utenti possono accedere tramite browser web.

Per impostazione predefinita, il controllo web è disattivato e gli utenti possono visitare tutti i siti web il cui accesso non sia stato interdetto dalla protezione web di Enterprise Console. È possibile utilizzare il criterio per applicazioni potenzialmente indesiderate o quello per controllo web completo. Entrambi i criteri vengono descritti nelle sezioni di seguito.

11.1 Impostazioni consigliate

Per configurare il controllo web è possibile scegliere fra due criteri: Controllo siti web inappropriati e Controllo web completo. A seconda del criterio selezionato sono applicabili soluzioni differenti. Durante l'impostazione del criterio del controllo web, tenere presente quanto riportato di seguito:

Controllo siti web inappropriati

- Rivedere le azioni selezionate per ogni categoria di siti web e aggiornarle in base alle esigenze della propria organizzazione o gruppo. Per garantire l'accesso al web secondo modalità diverse a seconda dei diversi gruppi di computer, creare criteri diversi per gruppi diversi. Per esempio, può essere necessario rendere disponibili alcuni siti web, quali Facebook, alle risorse umane
- Prima di distribuire un criterio creare un elenco di esenzioni dei siti web. È possibile inserire manualmente i siti web che si desidera escludere dal criterio utilizzando la scheda **Esenzioni siti web**. È per esempio possibile avere una serie di indirizzi web locali che non richiedono filtro, o bloccare alcuni siti web che fanno parte di una categoria altrimenti consentita.
- Utilizzare il Visualizzatore eventi del controllo web per filtrare rapidamente gli eventi su cui investigare. È possibile accedere al Visualizzatore eventi cliccando su **Eventi** > **Eventi web**. È possibile modificare le impostazioni delle categorie dei siti web in base alle azioni visualizzate.

Controllo web completo

Importante: per eseguire il criterio di Controllo web completo è necessario essere in possesso di una Sophos Web Appliance o una Appliance di gestione della sicurezza.

- Le Guide alla configurazione di Sophos Web Appliance e Appliance di gestione della sicurezza contengono linee guida generali per impostare l'appliance. L'appliance include una procedura guidata per l'installazione che accompagna nella scelta delle impostazioni può adatte alla propria organizzazione.

- Nel caso si desideri configurare criteri diversi per diversi tipi di utenti. Per informazioni consultare la documentazione del prodotto relativa alla Appliance Web, reperibile dal web.

  La documentazione relativa alla Sophos Web Appliance è disponibile alla pagina web http://wsa.sophos.it/docs/wsa/.

- Prima di distribuire un criterio, pianificare le eventuali eccezioni al criterio di controllo web. È per esempio possibile utilizzare la funzione "fasce orarie specifiche" per garantire l'accesso a tutti o alcuni siti web al di fuori degli orari lavorativi, per esempio durante la pausa pranzo. È anche possibile creare "Criteri aggiuntivi" applicabili solo a determinati utenti e che rappresentano eccezioni al Criterio predefinito e a quello per Fasce orarie specifiche.
- Stabilire quale azione (se alcuna) la Web Appliance debba intraprendere nel caso in cui non si possano categorizzare le informazioni relative ad un determinato sito web. La casella di spunta **Bloccare navigazione se non può essere determinata alcuna categoria web *non*** è selezionata per impostazione predefinita. Ciò permette agli utenti di continuare a usare Internet, nel caso il servizio di categorizzazione non funzioni. Quando viene selezionata la casella di spunta, le URL non categorizzate verranno bloccate in attesa del ripristino del servizio.

Per ulteriori informazioni, consultare la documentazione relativa a Sophos Enterprise Console e Sophos Web Appliance.

11.2 Distribuzione di un criterio del controllo web

Decidere in primo luogo quale modalità di filtraggio web si desidera utilizzare: Controllo siti web inappropriati, oppure Controllo web completo. Per distribuire tutte le funzionalità del criterio del controllo web, è necessario essere in possesso di una Sophos Web Appliance o una Appliance di gestione della sicurezza.

Per ulteriori informazioni su come impostare un criterio del controllo web, consultare la Sophos Enterprise Console di Guida in linea.

11.2.1 Distribuzione di un criterio di controllo dei siti web inappropriati

Si tratta di un'opzione del controllo web di base che include 14 categorie di siti web essenziali. È pensata per evitare che utenti visitino siti web inappropriati. Tenere in considerazione quanto riportato qui di seguito durante l'implementazione di un criterio di controllo web. Per istruzioni specifiche, consultare la documentazione relativa a Enterprise Console.

1. Assicurarsi che il criterio di controllo web sia abilitato.
2. Se l'organizzazione ha già in atto criteri di utilizzo adeguati, scegliere le impostazioni in modo tale da supportare tali criteri, così da evitare che gli utenti accedano a siti web ritenuti inappropriati.
3. Se si desidera garantire l'accesso differenziato ai siti web da parte di gruppi di computer diversi, creare criteri diversi per gruppi diversi.
4. Decidere quali gruppi di computer debbano essere sottoposti al controllo web e quale tipo di criterio si addica a ciascun gruppo.
5. Prendere visione dell'azione predefinita relativa a ciascuna categoria di siti web. Se si desidera applicare un'azione diversa, selezionarla da un elenco a discesa. Scegliere le categorie per cui si desidera bloccare l'accesso, quelle per cui lo si desidera consentire, e quelle per cui si desidera allertare agli utenti.

6. Scegliere quali siti web escludere dall'azione di filtro e aggiungerli all'elenco **Siti web da consentire** o **Siti web da bloccare**.

   Nota: Nel caso di elementi in conflitto o sovrapponibili, presenti sia nell'elenco "Blocca" sia nell'elenco "Consenti", quelli presenti nell'elenco Blocca avranno sempre priorità. Per esempio, se lo stesso indirizzo IP è incluso sia nell'elenco Blocca che Consenti, il sito web viene bloccato. Inoltre, se nell'elenco Blocca è incluso un dominio, mentre un sottodominio di quello stesso dominio fa parte dell'elenco Consenti, la voce presente nell'elenco Consenti viene ignorata e tutto il dominio, inclusi i sottodomini, viene bloccato.

7. Utilizzare il Visualizzatore eventi del controllo web per prendere in esame i risultati dell'azione di filtro. È possibile accedere al Visualizzatore eventi cliccando su **Eventi** > **Eventi web**. Utilizzare il Visualizzatore eventi per visionate gli eventi web. In base a questi risultati è possibile apportare le necessarie modifiche e correzioni.

Per ulteriori informazioni, consultare la documentazione relativa a Enterprise Console.

11.2.2 Implementazione di un criterio del controllo web completo

Questa modalità utilizza un criterio web completo. Consente l'utilizzo di un criterio del controllo web completo e fornisce reportistica dettagliata sul traffico web. Per poter utilizzare questa opzione è necessaria una Sophos Web Appliance o unaAppliance di gestione della sicurezza.

1. Configurare la Sophos Web Appliance o Appliance di gestione della sicurezza seguendo le istruzioni riportate nella documentazione relativa all'appliance e assicurandosi che **Endpoint Web Control** sia attivo.
2. Assicurarsi che il controllo web sia abilitato in Enterprise Console.
3. Se l'organizzazione ha già in atto criteri di utilizzo adeguati, scegliere le impostazioni in modo tale da supportare tali criteri, così da evitare che gli utenti accedano a siti web ritenuti inappropriati.
4. Se si desidera garantire l'accesso differenziato ai siti web da parte di gruppi di utenti diversi, creare criteri diversi per i gruppi di uetnti diversi.
5. Pensare a quali siti web si desidera controllare. A quali categorie di siti web si desidera bloccare l'accesso da parte degli utenti? Quali saranno invece accessibili? Per quali categorie di siti web si desidera avvertire gli utenti?
6. Stabilire quali siti web si desidera esentare e aggiungerli all'elenco dei siti dell'appliance.
7. Con il Controllo completo del web, si ha la possibilità di utilizzare Sophos LiveConnect. È possibile configurare l'appliance in modo tale che utilizzi LiveConnect; ciò consente la distribuzione agli utenti degli aggiornamenti ai criteri e il caricamento dei dati sulla reportistica provenienti dai computer degli utenti anche quando non in rete.

Per ulteriori informazioni, consultare la documentazione relativa a Sophos Enterprise Console e Sophos Web Appliance.

12 Impostazione di criteri di prevenzione degli exploit

Nota: Questa funzione non è inclusa in tutte le licenze. Se la si desidera utilizzare potrebbe essere necessario personalizzare la propria licenza. Per ulteriori informazioni, vedere https://www.sophos.com/it-it/products/endpoint-antivirus/how-to-buy.aspx.

Il criterio di prevenzione degli exploit definisce il livello di protezione contro il ransomware e altre forme di exploit generati dal malware.

- Protezione dei file di documento contro il ransomware (CryptoGuard).
- Protezione delle funzioni critiche nei browser web (Safe Browsing).
- Attenuazione degli exploit. Questa opzione difende le applicazioni più vulnerabili agli exploit da parte del malware, come ad es. le applicazioni Java.
- Protezione contro gli attacchi di process hollowing.
- Protezione contro il caricamento di file .DLL da cartelle non attendibili.
- Protezione contro il branch tracing del processore.

12.1 Impostazioni consigliate

Il criterio di prevenzione degli exploit definisce il modo in cui il software di sicurezza protegge i sistemi contro ransomware e altri exploit generati dal malware.

Nota: Per impostazione predefinita, sono abilitate tutte le opzioni di prevenzione degli exploit.

Si consiglia di utilizzare le impostazioni predefinite.

12.2 Implementazione di un criterio di prevenzione degli exploit

Per implementare un criterio di prevenzione degli exploit, si consiglia di procedere come segue:

1. Tutte le opzioni di prevenzione degli exploit sono abilitate per impostazione predefinita. Si consiglia di utilizzare le impostazioni predefinite. Prima di modificare le impostazioni, monitorare gli eventi di prevenzione degli exploit per un periodo di tempo prestabilito.
2. Utilizzare il Visualizzatore eventi della prevenzione degli exploit per monitorare gli eventi di prevenzione degli exploit. È possibile accedere al Visualizzatore eventi cliccando su **Eventi** > **Eventi prevenzione degli exploit**.
3. Modificare il criterio di prevenzione degli exploit in base ai risultati del monitoraggio. Si può, ad esempio, decidere di escludere alcune applicazioni dalla mitigazione degli exploit. Per ulteriori informazioni, consultare la Guida in linea di Sophos Enterprise Console, alla sezione *Configurazione criteri* > *Criterio di prevenzione degli exploit*.

   Importante: Le applicazioni vulnerabili sono protette per impostazione predefinita. Occorre esercitare la dovuta cautela quando si escludono applicazioni dalla prevenzione degli

exploit. Continueranno infatti a essere protette da CryptoGuard e Safe Browsing (Navigazione sicura).

a) Creare un nuovo criterio o modificare il criterio predefinito.

b) Verificare se il criterio presenti punti deboli.

c) Se vi dovessero essere necessità diverse, dividere il gruppo e creare criteri aggiuntivi, secondo necessità.

4. Assegnare i criteri come richiesto.

Per ulteriori informazioni su come impostare criteri di prevenzione degli exploit, consultare la Guida in linea di Sophos Enterprise Console.

13 Consigli sulla scansione

Le impostazione della scansione in questa sezione possono essere selezionate nel criterio antivirus e HIPS. 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).

Estensioni

Per accedere alle opzioni relative all'estensione per la scansione in accesso, nella finestra di dialogo **Criterio antivirus e HIPS**, cliccare sul pulsante **Configura** di fianco a **Abilita scansione in accesso** e passare alla scheda **Estensioni**.

Per le scansioni pianificate, nella finestra di dialogo **Criterio antivirus e HIPS**, sotto **Scansione pianificata**, cliccare su **Estensioni ed esclusioni**.

- L'opzione **Scansiona tutti i file** è di solito non necessaria o sconsigliata. 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.

Altre opzioni di scansione

Per accedere alle altre opzioni della scansione in accesso, nella finestra di dialogo **Criterio antivirus e HIPS**, cliccare sul pulsante **Configura** di fianco a **Abilita scansione in accesso**.

Per le scansioni pianificate, nella finestra di dialogo **Criterio antivirus e HIPS**, sotto **Scansione pianificata**, scegliere un tipo di scansione e cliccare su **Modifica**. Nella finestra di dialogo **Impostazioni scansione pianificat**a, cliccare su **Configura**.

- 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 in maniera inosservabile, 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 **Scansione della memoria di sistema** è abilitata per impostazione predefinita.

14 Utilizzo della scansione in accesso

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

- Se possibile, utilizzare le impostazioni predefinite.
- La scansione in accesso per le opzioni **Lettura**, **Scrittura** e **Rinomina** è abilitata per impostazione predefinita, solo per le installazioni di software nuovi. Per effettuare l'upgrade del software, è necessario abilitarle.
- 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 del supporto tecnico Sophos (http://www.sophos.com/it-it/support/knowledgebase/12790.aspx).
- 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 35.

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

15 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.
- 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.

16 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.

17 Esclusione di oggetti dalla scansione

Per escludere oggetti dalla scansione, procedere come segue:

- 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. 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.

18 Supporto tecnico

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

- Visitare la Sophos Community su community.sophos.com/ e cercare altri utenti che hanno riscontrato lo stesso problema.
- Visitare la knowledge base del supporto Sophos su www.sophos.com/it-it/support.aspx.
- Scaricando la documentazione del prodotto su www.sophos.com/it-it/support/documentation.aspx.
- Aprendo un ticket per il nostro supporto tecnico alla pagina https://secure2.sophos.com/it-it/support/contact-support/support-query.aspx.

19 Note legali

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at http://www.apache.org/licenses/LICENSE-2.0

Boost Software License

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Common Public License

The Sophos software that is referenced 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.it or via the web at https://www.sophos.com/it-it/support/contact-support.aspx. A copy of the license agreement for any such included software can be found at 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.

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Microsoft Public License (MS-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

   The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

   A "contribution" is the original software, or any additions or changes to the software.

   A "contributor" is any person that distributes its contribution under this license.

   "Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

   (A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

   (B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

   (A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

   (B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

   (C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

   (D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

   (E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

A copy of the MS-PL terms can be found at https://opensource.org/licenses/MS-PL.

OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2016 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

   The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Windows Template Library (WTL)

Copyright © Microsoft Corporation. All rights reserved.

The use and distribution terms for this software are covered by the Common Public License. Source code for this component is available here: https://sourceforge.net/projects/wtl/files/

zlib data compression library

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu