SOPHOS

Cybersecurity made simple.

Sophos Endpoint per Windows

Guida

Sommario

1 Informazioni su Sophos Endpoint per Windows

Questa guida contiene informazioni su Sophos Endpoint per Windows e ne descrive le procedure passo dopo passo.

2 Sophos Endpoint

Sophos Endpoint si esegue su computer e server per proteggerli.

Restrizione
È possibile che non si disponga di tutte le funzionalità descritte qui di seguito. Dipendono infatti dalla licenza.

Sophos Endpoint è una soluzione configurata e gestita in maniera centralizzata da Sophos Central Admin.

Tuttavia, alcune operazioni possono essere svolte sul computer o sul server:

- Verifica dello stato del computer.
- Scansione di file, computer o server alla ricerca di eventuali minacce.
- Vedere i dettagli degli eventi sul computer o sul server, come ad esempio le minacce rilevate.
- Rimozione di una minaccia.
- Modifica delle impostazioni di sicurezza. È ad esempio possibile disattivare alcune funzionalità a scopo di risoluzione dei problemi.
- Aggiornamento.
- Troubleshooting.

Nota
Occorre utilizzare il **Login** e inserire la password del Blocco rimozione per rimuovere le minacce o modificare le impostazioni.

Concetti correlati

Stato (pagina 3)
È possibile verificare lo stato di sicurezza del proprio computer o server ed eseguirne la scansione.

Eventi (pagina 5)
La pagina **Eventi** mostra gli eventi del computer o del server, come ad esempio le minacce rilevate.

Attività correlate

Scansione di un file (pagina 9)
È possibile eseguire la scansione di singoli file.

Scansione del computer o del server (pagina 9)
Seguire queste istruzioni per eseguire la scansione del computer o del server.

Rimozione di una minaccia (pagina 9)
Seguire queste istruzioni per rimuovere una minaccia che è stata rilevata.

Modifica delle impostazioni di sicurezza (pagina 9)
Seguire queste istruzioni per modificare le impostazioni di sicurezza.

Aggiorna ora (pagina 10)
Seguire queste istruzioni per aggiornare le definizioni dei virus.

Troubleshooting (pagina 10)
Seguire queste istruzioni per risolvere i problemi.

3 Stato

È possibile verificare lo stato di sicurezza del proprio computer o server ed eseguirne la scansione.

Restrizione
È possibile che non si disponga di tutte le funzionalità descritte qui di seguito. Dipendono infatti dalla licenza.

La pagina **Stato** consente di:

- Visualizzare lo stato di sicurezza del computer o del server.
- Effettuare la scansione del computer o del server alla ricerca di eventuali minacce.
- Vedere le funzionalità installate e il relativo stato di protezione.

Nota
Il link **Info** nella parte in basso a destra della pagina permette di aggiornare le definizioni dei virus e di risolvere i problemi del prodotto.

Stato di sicurezza

Un'icona nella parte alta della pagina indica lo stato.

Impostazione	Descrizione
 Verde.	Non sono presenti notifiche, oppure vi sono solamente notifiche di priorità bassa.
 Rosso.	Sono presenti notifiche di priorità alta.
 Giallo.	Sono presenti notifiche di priorità media.
 Grigio.	Lo stato è sconosciuto.

Sotto questa icona vengono visualizzate tutte le funzionalità installate, insieme al relativo stato di protezione individuale.

Scansione del computer

Cliccare su **Esegui scansione** per effettuare la scansione di tutti i file sul computer o sul server alla ricerca di eventuali minacce.

Una volta completata la scansione, verrà visualizzato un riepilogo contenente i risultati della scansione. Se vengono rilevate minacce, è possibile selezionare la pagina **Eventi** per visualizzare informazioni dettagliate.

4 Eventi

La pagina **Eventi** mostra gli eventi del computer o del server, come ad esempio le minacce rilevate.

Restrizione
È possibile che non si disponga di tutte le funzionalità descritte qui di seguito. Dipendono infatti dalla licenza.

È anche possibile filtrare gli eventi, per visualizzare ad esempio solamente gli eventi che richiedono un'azione, oppure per cercare tipi specifici di eventi.

L'elenco Eventi

L'elenco mostra le seguenti informazioni:

- La gravità. Un'icona sul lato sinistro dell'elenco indica se un evento ha priorità alta, media, oppure se è una notifica.
- L'origine. Un'icona sul lato sinistro dell'elenco indica la funzionalità Sophos che ha segnalato l'evento.
- La data e l'ora in cui si è verificato l'evento.
- Una descrizione dell'evento.
- Un link che consente di intraprendere l'azione necessaria (se occorre agire). Viene visualizzato solamente se è stato effettuato l'accesso con il ruolo di amministratore.

Per visualizzare i dettagli di ciascun evento, cliccare sulla freccia sulla destra per espandere le informazioni.

Le azioni che possono essere intraprese sono le stesse che sono disponibili in Sophos Central Admin. Consultare l'elenco nella pagina **Avvisi** dellaGuida in linea di Sophos Central Admin.

È possibile filtrare gli eventi in base ai seguenti tipi:

Tipo di evento	Descrizione
Malware e PUA	Malware è un termine generico utilizzato per indicare software malevolo. Include virus, worm, trojan e spyware. Le applicazioni potenzialmente indesiderate (potentially unwanted application, PUA) sono programmi non malevoli come ad es. dialer, strumenti di amministrazione remota e di hacking, generalmente considerati inadatti alle reti aziendali.

Tipo di evento	Descrizione
Minacce web	Le minacce web includono siti web malevoli, siti web non appartenenti ad alcuna categoria, e download rischiosi. Inoltre, alcuni siti web vengono generalmente considerati come inadeguati per le reti aziendali, come ad esempio siti web per soli adulti o social media. Questi siti possono essere bloccati.
Comportamento malevolo	Il comportamento malevolo è un comportamento sospetto che viene rilevato nei software già in esecuzione sul computer o sul server. I ransomware sono software malevoli che impediscono l'accesso ai documenti personali fino a quando non viene pagato un riscatto (ransom).
Elementi controllati	Questa categoria include: • Applicazioni che non pongono alcuna minaccia alla sicurezza, ma che vengono ritenute inadatte all'utilizzo nell'ambiente di lavoro. • Periferiche e supporti removibili. • Download rischiosi, o siti web che vengono ritenuti inadeguati per l'utilizzo in ufficio. • File contenenti informazioni di natura sensibile (ad esempio dati personali o finanziari) che non devono assolutamente finire nelle mani sbagliate.
Traffico malevolo	Il termine traffico malevolo viene utilizzato per definire il traffico tra computer, quando mostra comportamenti che possono indicare un tentativo di assumere il controllo di un computer o server (attacco di "comando e controllo").
Exploit	Gli exploit che Sophos può prevenire includono l'hijacking delle applicazioni e gli exploit che sfruttano le vulnerabilità di browser, plugin per i browser, applicazioni Java, applicazioni multimediali e applicazioni Microsoft Office.

5 Impostazioni

È possibile modificare temporaneamente le impostazioni di sicurezza sul computer o server utilizzato.

Potrebbe essere necessario per la risoluzione dei problemi. Potrebbe ad esempio essere desiderabile disattivare una funzionalità, qualora quest'ultima causi problemi nel computer.

Restrizione
È possibile che non si disponga di tutte le funzionalità descritte qui di seguito. Dipendono infatti dalla licenza.

Restrizione
La pagina **Impostazioni** è disponibile solamente se è stata inserita la password del Blocco rimozione (che può essere richiesta all'amministratore di Sophos Central).

Come modificare le impostazioni

Spuntare la casella contrassegnata come **Ignora il criterio di Sophos Central per un massimo di 4 ore per consentire la risoluzione dei problemi**.

È ora possibile apportare modifiche in questa pagina. Le modifiche ignorano temporaneamente il criterio applicato da un amministratore in Sophos Central Admin.

Dopo quattro ore le impostazioni verranno automaticamente ripristinate a quelle del criterio che sono state applicate a livello centrale.

È possibile ripristinare le impostazioni originarie anche prima, se lo si desidera. Questa azione non può essere effettuata utilizzando l'indicatore di scorrimento per le funzionalità individuali. Occorre invece disattivare **Ignora il criterio di Sophos Central per un massimo di 4 ore per consentire la risoluzione dei problemi**.

Deep learning

Il deep learning sfrutta tecnologie avanzate di machine learning per rilevare le minacce. È in grado di rilevare malware e applicazioni potenzialmente indesiderate senza utilizzare le firme.

Scansioni in tempo reale

Le scansioni in tempo reale analizzano gli elementi a cui gli utenti cercano di accedere, negando l'accesso se non risultano sicuri. È possibile selezionare:

- **File**: Questa azione avvia la scansione dei file locali e (se selezionato nei criteri) delle condivisioni di rete.
- **Internet**: Questa azione avvia la scansione delle risorse internet. Può analizzare i download in corso, bloccare l'accesso ai siti web malevoli, e rilevare siti web di bassa reputazione.

Controlli per gli utenti

- **Controllo periferiche** consente di controllare l'accesso a periferiche e supporti removibili.
- **Controllo applicazioni** permette di rilevare e bloccare le applicazioni che non costituiscono una minaccia per la sicurezza, ma che sono ritenute inadatte all'utilizzo nell'ambiente lavorativo.
- **Controllo web** consente di proteggere i sistemi dai download rischiosi, imponendo severi controlli sui siti ai quali gli utenti possono accedere, e prevenendo la perdita dei dati.
- **Prevenzione della perdita di dati** consente di monitorare e imporre restrizioni sul trasferimento di file contenenti dati di natura sensibile.
- **Blocco rimozione** consente di limitare le modifiche. Se questa opzione è attivata, un amministratore locale avrà bisogno della password necessaria per modificare le impostazioni di sicurezza o disinstallare Sophos Endpoint.

Protezione per runtime

La Protezione per runtime protegge i sistemi contro le minacce, rilevando comportamenti o traffico sospetti o malevoli nei computer endpoint. È possibile selezionare:

- **Rilevamento del ransomware**: Questa opzione serve a difendere il sistema dalle categorie di malware che agiscono limitando l'accesso ai file ed esigendo il pagamento di un riscatto per il rilascio delle informazioni.
- **Navigazione sicura**: Questa opzione protegge i browser web dagli exploit del malware.
- **Mitigazione degli exploit**: Questa opzione difende le applicazioni più esposte agli exploit da parte del malware, come ad es. le applicazioni Java.
- **Protezione dalle minacce di rete**: Questa opzione rileva se il traffico tra computer endpoint e server mostri comportamenti che possono indicare un tentativo di assumere il controllo di un endpoint. Include l'ispezione dei pacchetti, che analizza le comunicazioni della rete, identificando e bloccando le minacce prima che possano danneggiare sistema operativo o applicazioni.

  Nota
  Disattivando la **Protezione dalle minacce di rete**, verranno disattivate anche le funzionalità Endpoint Detection and Response (EDR), Isolamento e Confinamento.

- **Rilevamento dei comportamenti malevoli**: Questa opzione agisce rilevando e bloccando comportamenti sospetti o noti per essere malevoli.

Controlli del computer

È possibile monitorare Windows Firewall (e altri firewall registrati) sui propri computer e server.

6 Come effettuare ...

6.1 Scansione di un file

È possibile eseguire la scansione di singoli file.

Per eseguire la scansione di un file, procedere come segue:

- Da Esplora risorse, cliccare con il tasto destro del mouse sul file e selezionare **Scansione**.

6.2 Scansione del computer o del server

Seguire queste istruzioni per eseguire la scansione del computer o del server.

Per effettuare la scansione di tutti i file nel computer o nel server:

1. Aprire la pagina **Stato** o la pagina **Rilevamenti**.
2. Cliccare su **Esegui scansione**.
   Una volta completata la scansione, verrà visualizzato un riepilogo contenente i risultati della scansione.
3. Se vengono rilevate minacce, è possibile selezionare la pagina **Eventi** per visualizzare informazioni dettagliate.

6.3 Rimozione di una minaccia

Seguire queste istruzioni per rimuovere una minaccia che è stata rilevata.

Per rimuovere una minaccia, procedere come segue:

1. Cliccare su **Login amministratore** e inserire la password del Blocco rimozione (che può essere richiesta all'amministratore di Sophos Central).
2. Navigare sulla pagina **Eventi** per visualizzare i dettagli della minaccia che è stata rilevata.
3. Cercare un link corrispondente a un'azione, situato vicino ai dettagli della minaccia.

Le azioni che possono essere intraprese sono le stesse che sono disponibili in Sophos Central Admin. Consultare l'elenco nella pagina **Avvisi** dellaGuida in linea di Sophos Central Admin.

6.4 Modifica delle impostazioni di sicurezza

Seguire queste istruzioni per modificare le impostazioni di sicurezza.

Per modificare le impostazioni di sicurezza:

1. Cliccare su **Login** nella parte in alto a destra dell'interfaccia.
2. Inserire la password del Blocco rimozione (che può essere richiesta all'amministratore di Sophos Central).
   Comparirà ora un link **Impostazioni** nella barra dei menù.
3. Caricare la pagina **Impostazioni**.

4. Spuntare la casella contrassegnata come **Ignora il criterio di Sophos Central per un massimo di 4 ore per consentire la risoluzione dei problemi**.
5. Utilizzare gli indicatori di scorrimento presenti nella pagina per disattivare le funzionalità di sicurezza.

Dopo quattro ore le modifiche verranno automaticamente annullate, e saranno nuovamente applicate le impostazioni del criterio implementate centralmente.

Nota
È possibile ripristinare le impostazioni originarie anche prima, se lo si desidera. Questa azione non può essere effettuata utilizzando l'indicatore di scorrimento per le funzionalità individuali. Occorre invece togliere la spunta alla casella **Ignora il criterio di Sophos Central per un massimo di 4 ore per consentire la risoluzione dei problemi**.

6.5 Aggiorna ora

Seguire queste istruzioni per aggiornare le definizioni dei virus.

Per eseguire l'aggiornamento, procedere come segue:

1. Cliccare su **Informazioni**.
2. Cliccare su **Aggiorna ora**.

6.6 Troubleshooting

Seguire queste istruzioni per risolvere i problemi.

Per risolvere i problemi, procedere come segue:

1. Cliccare su **Informazioni**.
2. Cliccare su **Apri strumento Endpoint Self Help** per raccogliere informazioni sul problema, oppure cliccare sul link al **Forum della Community**.

6.7 Cifratura del computer

Seguire queste istruzioni per cifrare il proprio computer.

Restrizione
Device Encryption è disponibile solo sui computer endpoint.

Device Encryption cifra l'hard disk del computer utilizzando la tecnologia Windows BitLocker. L'amministratore stabilisce se si debba o meno effettuare l'autenticazione ogni volta che si accede al computer.

Se non è richiesta alcuna autenticazione, il processo di cifratura dell'hard disk comincerà automaticamente non appena viene riavviato il computer dopo aver ricevuto il criterio di Sophos Central. In tale eventualità, non occorre intraprendere alcuna azione.

Se viene richiesta l'autenticazione, procedere come segue:

1. Quando compare la finestra di dialogo **Sophos Device Encryption**, seguire le istruzioni fornite nella finestra di dialogo. Le istruzioni specifiche dipenderanno dal sistema e dalle impostazioni dei criteri definite dall'amministratore.
   - Se il criterio di Device Encryption richiede un PIN o una password per l'autenticazione, seguire le istruzioni visualizzate sullo schermo per creare un PIN o una password.

     Nota
     Prestare estrema attenzione durante la creazione di un PIN o una password. L'ambiente di preavvio supporta solamente il layout di tastiera EN-US. Se si crea un PIN o una password con caratteri speciali, potrebbe essere necessario utilizzare tasti diversi quando si effettuerà l'accesso in futuro.

   - Se il criterio di Device Encryption richiede una chiave USB per l'autenticazione, occorrerà connettere un'unità flash USB al computer. L'unità flash USB deve essere formattata con NTFS, FAT, o FAT32.
2. Cliccando su **Riavvia e cifra**, il computer si riavvierà e cifrerà gli hard disk. Si potrà procedere con il proprio lavoro come di consueto.

   Nota
   L'utente può selezionare **Rimanda a un altro momento** per chiudere la finestra di dialogo. Tuttavia, verrà visualizzata nuovamente all'accesso successivo.

Una volta completata la cifratura del volume di sistema da parte di Sophos Central, verrà avviata la cifratura dei volumi di dati. I volumi di dati rimovibili, quali le chiavi USB, non vengono cifrati.

Quando si effettua l'accesso al proprio computer, potrebbe essere necessario inserire un PIN, una password o una chiave USB per sbloccare il volume di sistema. I volumi di dati vengono sbloccati automaticamente.

6.8 Accesso al computer in caso di password dimenticata

Per accedere al computer, procedere come segue.

Se non dovesse essere possibile accedere al computer per via di un PIN, una password o una chiave USB dimenticata, occorrerà ottenere una chiave di ripristino.

Se si utilizza Sophos Device Encryption, la chiave di ripristino è memorizzata in Sophos Central. Per ottenere la chiave di ripristino, è possibile procedere in uno dei seguenti modi:

- Accedere al portale self-service Sophos e seguire le istruzioni indicate nella Guida in linea.
- Chiedere all'amministratore di recuperare la chiave di ripristino. Servirsi di questa opzione nel caso in cui non fosse possibile adoperare il portale self-service.

Attività correlate

Uso del Ripristino di BitLocker (pagina 12)
Seguire queste istruzioni per ripristinare il computer.

6.8.1 Uso del Ripristino di BitLocker

Seguire queste istruzioni per ripristinare il computer.

Per eseguire il ripristino del computer, procedere come segue:

1. Riavviare il computer e premere il tasto ESC nella schermata di accesso di **BitLocker**.
2. Nella schermata **Ripristino BitLocker**, cercare l'**ID chiave di ripristino**.
   L'**ID chiave di ripristino** viene visualizzato solamente per un breve periodo di tempo. Per visualizzarlo nuovamente, occorre riavviare il computer.
3. Contattare l'amministratore e fornire l'**ID chiave di ripristino**.
   L'amministratore deve quindi individuare la chiave di ripristino del computer in Sophos Central e fornirla all'utente.
4. Nella schermata **Ripristino BitLocker**, immettere la chiave di ripristino.
   È ora possibile riavviare il computer.
5. Seguire le istruzioni visualizzate sullo schermo per creare, quando richiesto, un nuovo PIN di BitLocker o una nuova password.

   I computer che eseguono Windows 7 non visualizzano istruzioni. La reimpostazione del PIN o della password deve essere effettuata manualmente.

È ora possibile accedere nuovamente al computer.

Nota
Una chiave di ripristino può essere adoperata una sola volta. Se dovesse essere necessario ripristinare nuovamente il computer, occorrerà ottenere una nuova chiave di ripristino.

7 Perché è stato bloccato il trasferimento del file?

È possibile che venga visualizzato un messaggio che indica che il trasferimento di un file (ad esempio, la copia, lo spostamento o l'invio dei file tramite e-mail) è stato bloccato.

Ciò avviene perché l'azienda ha impostato un criterio che impedisce l'invio non intenzionale di informazioni di natura sensibile a utenti non autorizzati a visualizzarle.

I messaggi possono essere di due tipi.

Messaggio	Descrizione
Il trasferimento è bloccato	Se si riceve un messaggio "trasferimento di file bloccato", non è possibile trasferire i file. L'amministratore potrebbe aver aggiunto alcune indicazioni al messaggio.
Il trasferimento può essere autorizzato	Se si riceve un messaggio "richiesta del trasferimento di file bloccata", è possibile decidere se trasferire o meno i file. L'amministratore potrebbe aver aggiunto alcune indicazioni al messaggio. Cliccare su **Autorizza** se si è sicuri che sia possibile procedere senza rischi.

8 Supporto

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

- Visitando la Sophos Community su community.sophos.com/ e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su www.sophos.com/it-it/support.aspx.
- Scaricando la documentazione del prodotto da 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.

9 Note legali