SOPHOS

Cybersecurity made simple.

Sophos Endpoint per Mac

Guida in linea

Sommario

1 Sophos Endpoint

Nota
È possibile che non si disponga di tutte le funzionalità descritte in questa guida in linea. Dipendono infatti dalla licenza.

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

Le operazioni che possono essere eseguite su Mac sono le seguenti:

- Verificare lo Stato (pagina 2) del Mac.
- Effettuare la Scansione di un file (pagina 9) o la Scansione del Mac (pagina 9) alla ricerca di minacce.
- Visualizzare dettagli degli Eventi (pagina 4) nel Mac, come ad esempio le minacce rilevate.
- Rimozione di una minaccia (pagina 9).
- Modifica delle impostazioni di sicurezza (pagina 9). È ad esempio possibile disattivare alcune funzionalità a scopo di risoluzione dei problemi.
- Aggiorna ora (pagina 10).
- Troubleshooting (pagina 10).

Nota
Per rimuovere le minacce o modificare le impostazioni, occorre utilizzare l'**Accesso amministratore** e immettere la password del Blocco rimozione.

2 Stato

Nota
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 Mac.
- Effettuare la scansione del Mac alla ricerca di eventuali minacce.
- Vedere le funzionalità installate e il relativo stato di protezione.

Nota
Il link **Info** permette di aggiornare le definizioni dei virus e di risolvere eventuali problemi del prodotto.

Stato di sicurezza

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

 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 indicate tutte le funzionalità installate, insieme al rispettivo stato di protezione.

Scansione del Mac

Cliccare su **Effettua scansione ora** per sottoporre a scansione tutti i file sul Mac alla ricerca di eventuali minacce.

Nota
Se viene rilevata una minaccia, l'opzione **Effettua scansione ora** non sarà disponibile. Sarà invece possibile cliccare su **Visualizza dettagli** per ottenere ulteriori informazioni sulla minaccia.

Una volta completata la scansione, verrà visualizzato un riepilogo contenente i risultati della scansione. Se sono state rilevate minacce, sarà possibile cliccare su **Visualizza dettagli** o su **Eventi** per maggiori informazioni.

3 Eventi

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

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

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 Eventi mostra quanto segue:

- La gravità. Un'icona indica se un evento ha priorità alta, media, oppure se è una notifica.
- L'origine. Un'icona 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). Il link è disponibile solamente se è stato effettuato l'accesso con il ruolo di amministratore.

Per visualizzare i dettagli di un evento, cliccare sulla voce corrispondente all'interno dell'elenco.

Le azioni che possono essere intraprese sono le stesse che sono disponibili nella console di amministrazione di Sophos Central. Vedere l'elenco nella pagina **Notifiche** della guida in linea di Sophos Central.

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.

Minacce web

Le minacce web includono siti web malevoli 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.

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 Mac (attacco di "comando e controllo").

Ransomware

I ransomware sono software malevoli che impediscono l’accesso ai documenti personali fino a quando non viene pagato un riscatto (ransom).

4 Rilevamenti

È possibile eseguire la scansione del Mac per individuare eventuali minacce rilevate e neutralizzate da Sophos.

Scansione del computer

Cliccare su **Effettua scansione ora** per sottoporre a scansione tutti i file sul Mac 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.

Cronologia eventi per malware e PUA

Mostra la cronologia di malware e PUA rilevati. Cliccare sulla freccia per visualizzare i dettagli nella pagina **Eventi**.

Cronologia dei rilevamenti

Mostra la quantità di minacce di un tipo specifico che sono state rilevate. Cliccare su un tipo di minaccia per visualizzare nella pagina **Eventi** i dettagli relativi alle minacce appartenenti alla tipologia selezionata.

Ripristina riepilogo

Cliccare su **Ripristina riepilogo** per azzerare i contatori della cronologia visualizzati nella pagina **Rilevamenti**.

5 impostazioni

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

La pagina **Impostazioni** è disponibile solamente se si utilizza l'**Accesso amministratore** e si immette la password del Blocco rimozione (che può essere richiesta all'amministratore di Sophos Central).

È possibile modificare temporaneamente le impostazioni di sicurezza su questo Mac.

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

Come modificare le impostazioni

Attivare l'impostazione **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 che voi (o un altro amministratore) avete implementato dalla console di amministrazione di Sophos Central.

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

Nota
È possibile ripristinare le impostazioni originarie anche prima, se lo si desidera. Tuttavia, questa operazione non può essere eseguita per le singole funzionalità. Occorre disattivare l'impostazione **Ignora il criterio di Sophos Central per un massimo di 4 ore per consentire la risoluzione dei problemi**, che viene applicata a tutte le funzionalità.

Scansioni in tempo reale

Le scansioni in tempo reale analizzano gli elementi a cui gli utenti cercano di accedere, concedendo l'accesso solo se 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 delle periferiche**. Consente di controllare l'accesso a periferiche e supporti removibili.
- **Controllo delle applicazioni**. Permette di rilevare e bloccare le applicazioni che non costituiscono una minaccia di sicurezza, ma che sono ritenute inappropriate per l'utilizzo nell'ambiente lavorativo.

- **Controllo del 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.

Protezione per runtime

Difende i sistemi dalle minacce, rilevando comportamenti e traffico sospetti o malevoli sui Mac. È possibile selezionare:

- **Rilevamento del traffico malevolo**. Questa opzione rileva se il traffico tra un Mac e un server mostri comportamenti che possono indicare un tentativo di assumere il controllo del Mac.
- **Rilevamento del ransomware (CryptoGuard)**. 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.

6 Come effettuare ...

6.1 Scansione di un file

Per effettuare la scansione di singoli file:

Dal Finder, cliccare con il tasto destro del mouse sul file e selezionare **Esegui scansione con Sophos Endpoint**.

Si aprirà la finestra di dialogo **Scansione elementi del Finder**, che permette di monitorare il progresso e i risultati della scansione.

6.2 Scansione del Mac

Per effettuare la scansione di tutti i file nel Mac:

1. Aprire la pagina **Stato** o la pagina **Rilevamenti**.
2. Cliccare su **Scansione immediata**.
   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

Per rimuovere una minaccia che è stata rilevata:

1. Cliccare su **Accesso amministratore** e immettere la password del Blocco rimozione (che può essere richiesta all'amministratore di Sophos Central).
   Il link **Impostazioni** nella barra dei menu è ora attivo.
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 nella console di amministrazione di Sophos Central. Vedere l'elenco nella pagina **Notifiche** della Guida in linea di Sophos Central.

6.4 Modifica delle impostazioni di sicurezza

Per modificare le impostazioni di sicurezza:

1. Cliccare su **Accesso amministratore** e immettere la password del Blocco rimozione (che può essere richiesta all'amministratore di Sophos Central).
   Il link **Impostazioni** nella barra dei menu è ora attivo.
2. Caricare la pagina **Impostazioni**.
3. Attivare l'impostazione **Ignora il criterio di Sophos Central per un massimo di 4 ore per consentire la risoluzione dei problemi**.

4. Utilizzare i comandi della pagina per attivare o disattivare le varie funzionalità di sicurezza.

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

Nota
È possibile ripristinare le impostazioni originarie anche prima, se lo si desidera. Tuttavia, questa operazione non può essere eseguita per le singole funzionalità. Occorre disattivare l'impostazione **Ignora il criterio di Sophos Central per un massimo di 4 ore per consentire la risoluzione dei problemi**, che viene applicata a tutte le funzionalità.

6.5 Aggiorna ora

Per effettuare l'aggiornamento:

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

6.6 Troubleshooting

Per il troubleshooting dei problemi:

1. Cliccare su **Informazioni**.
2. Cliccare su **Esegui strumento di diagnostica** per raccogliere dati sul problema.

Per ulteriori informazioni, cliccare su **Forum della Community**.

6.7 Cifratura del Mac

La funzionalità Device Encryption cifra il disco rigido del Mac utilizzando la tecnologia FileVault 2. Quando l'amministratore attiva la funzionalità **Device Encryption**, viene visualizzata la finestra di dialogo **Sophos Device Encryption**.

1. Nella finestra di dialogo **Sophos Device Encryption**, immettere la password di accesso e cliccare su **Cifra**.
   Questa operazione attiva Device Encryption. In alternativa, cliccare su **Posponi** per avviare il processo in un secondo momento.
2. La chiave di ripristino verrà automaticamente memorizzata in Sophos Central.

Quando viene cifrato il disco di sistema, i volumi di dati interni saranno automaticamente cifrati. I dischi cifrati vengono automaticamente sbloccati al riavvio del Mac. I volumi di dati rimovibili, quali le chiavi USB, non vengono cifrati.

6.8 Accesso al Mac in caso di password dimenticata

Se non si è in grado di accedere al proprio Mac perché si è dimenticata la password di accesso, occorre 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 di Sophos Central.
- Chiedere all'amministratore di recuperare la chiave di ripristino, come indicato in Uso del Ripristino di FileVault (pagina 11). Servirsi di questa opzione nel caso in cui non fosse possibile adoperare il portale self-service.

6.8.1 Uso del Ripristino di FileVault

Per richiedere a un amministratore di recuperare una chiave di ripristino, procedere come segue.

1. Riavviare il Mac e attendere che venga visualizzato 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 Mac.
2. Contattare l'amministratore e fornire l'**ID chiave di ripristino**.
   L'amministratore deve quindi individuare la chiave di ripristino del Mac in Sophos Central e fornirla all'utente.
3. Cliccare sull'icona a forma di punto interrogativo nel campo **Password**.
   Verrà visualizzato un messaggio.
4. Cliccare sulla freccia accanto al messaggio per passare al campo delle chiave di ripristino.
5. Inserire la chiave di ripristino.
6. Seguire le istruzioni visualizzate sullo schermo per creare una nuova password.
   Se l'account utente è stato importato da Active Directory, cliccare su **Annulla** nella finestra di dialogo **Reimposta Password** e chiedere all'amministratore di reimpostare la password.
7. Se richiesto, cliccare su **Crea nuovo portachiavi**.

È ora possibile accedere nuovamente al Mac.

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.

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 Ulteriore assistenza

È possibile ricevere supporto tecnico come segue:

- 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.

9 Note legali