SOPHOS

Cybersecurity made simple.

# Sophos Endpoint para Mac

## Ayuda

# Contenido

# 1 Sophos Endpoint

**Nota**
Es posible que no disponga de todas las funciones descritas en esta ayuda. Depende de su licencia.

Sophos Endpoint se configura y administra de forma centralizada desde la Sophos Central Admin.

Las tareas que se pueden realizar en el Mac son las siguientes:

- Comprobar el Estado (página 2) del Mac.
- Escanear un archivo (página 8) o Escanear el Mac (página 8) en busca de amenazas.
- Consultar los detalles de los Eventos (página 3) en el Mac, como las amenazas detectadas.
- Limpiar una amenaza (página 8).
- Cambiar la configuración de seguridad (página 8). Por ejemplo, puede desactivar funciones para solucionar problemas.
- Actualizar ahora (página 9).
- Solucionar problemas (página 9).

**Nota**
Para limpiar amenazas o cambiar la configuración, debe utilizar **Inicio de sesión de administrador** e introducir la contraseña de protección contra manipulaciones.

# 2 Estado

**Nota**
Es posible que no disponga de todas las funciones descritas aquí. Depende de su licencia.

La página **Estado** le permite:

- Comprobar el estado de seguridad del Mac.
- Escanear el Mac en busca de amenazas.
- Consultar las funciones instaladas y su estado de seguridad.

**Nota**
El enlace **Acerca de** le permite actualizar las definiciones de virus o solucionar problemas con el producto.

## Estado de seguridad

Un icono en la parte superior de la página muestra el estado.

 Verde. No hay alertas o solo alertas de prioridad baja.

 Rojo. Hay alertas de prioridad alta.

 Amarillo. Hay alertas de prioridad media.

 Gris. Se desconoce el estado.

Debajo, se muestran todas las funciones instaladas con su estado de seguridad individual.

## Escanear el Mac

Haga clic en **Escanear ahora** para escanear todos los archivos del Mac en busca de amenazas.

**Nota**
Si se detecta una amenaza, **Escanear ahora** no está disponible. En su lugar, puede hacer clic en **Ver detalles** para obtener más información sobre la amenaza.

Tras completarse el escaneado, verá un resumen de los resultados. Si se detectan amenazas, puede hacer clic en **Ver detalles** o **Eventos** para obtener más información.

# 3 Eventos

**Nota**
Es posible que no disponga de todas las funciones descritas aquí. Depende de su licencia.

La página **Eventos** muestra los eventos que tienen lugar en el Mac, como las amenazas que se detectan.

Puede filtrar los eventos, por ejemplo para mostrar solo los que requieran alguna medida, o buscar tipos de eventos específicos.

## Lista Eventos

La lista Eventos muestra:

- La gravedad. Un icono muestra si el evento tiene prioridad alta, prioridad media o es una notificación.
- El origen. Una lista de iconos indica la función de Sophos que ha informado del evento.
- La fecha y la hora en que ha tenido lugar el evento.
- Una descripción del evento.
- Un enlace que le permite tomar medidas (si se necesita tomar alguna medida). Solo lo verá si ha iniciado sesión como administrador.

Para ver los detalles de un evento, haga clic en su entrada en la lista.

Las medidas que puede tomar son las mismas que las disponibles en la consola de Sophos Central Admin. Consulte la lista en la página **Alertas** de la ayuda de Sophos Central.

## Programas maliciosos y PUAs

El malware es el término genérico utilizado para englobar programas peligrosos como virus, gusanos, troyanos y programas espía.

Las aplicaciones no deseadas (PUA) son programas que no son maliciosos, como marcadores telefónicos, herramientas de administración remota y herramientas de ataque remoto, pero que no se consideran adecuadas en entornos laborales.

## Amenazas web

Las amenazas web incluyen sitios web maliciosos y descargas peligrosas.

Algunos sitios web, como sitios para adultos o redes sociales, también se suelen considerar inapropiados en entornos laborales. Puede bloquearlos.

## Elementos controlados

Esta categoría incluye:

- Aplicaciones que no suponen una amenaza para la seguridad, pero cuyo uso se considera inadecuado en el entorno empresarial.
- Periféricos y medios extraíbles.
- Descargas peligrosas o sitios web que no son apropiados en el entorno laboral.
- Archivos que contienen información confidencial (como datos personales o financieros) que no desea que se filtren.

## Tráfico malicioso

El **tráfico malicioso** es aquel entre ordenadores que indica un posible intento de toma de control del Mac (un ataque de "comando y control").

## Ransomware

Los programas de ransomware son software malicioso que impide acceder a los archivos hasta que se pague un rescate.

# 4 Detecciones

Puede analizar el Mac en busca de amenazas, así como ver las amenazas que Sophos ha detectado y de las que le ha protegido.

## Escanear el ordenador

Haga clic en **Escanear ahora** para escanear todos los archivos del Mac en busca de amenazas.

Tras completarse el escaneado, verá un resumen de los resultados. Si se detectan amenazas, puede ir a la página **Eventos** para ver los detalles.

## Historial de eventos de programas maliciosos y PUA

Muestra el historial de PUA y malware detectados. Haga clic en la flecha para ver los detalles de la página **Eventos**.

## Historial de detecciones

Muestra cuántas amenazas de un tipo específico se han detectado. Haga clic en un tipo para ver los detalles de las amenazas detectadas de ese tipo en la página **Eventos**.

## Restablecer resumen

Haga clic en **Restablecer resumen** para establecer los contadores del historial mostrados en la página **Detecciones** en cero.

# 5 Configuración

**Nota**
Es posible que no disponga de todas las funciones descritas aquí. Depende de su licencia.

La página **Configuración** solo está disponible si utiliza el **Inicio de sesión del administrador** e introduce la contraseña de protección contra manipulaciones (disponible del administrador de Sophos Central).

Puede cambiar temporalmente la configuración de seguridad del Mac.

Es posible que tenga que hacerlo para solucionar problemas. Por ejemplo, puede desactivar una función para ver si está causando problemas en el Mac.

## Cómo cambiar la configuración

Active **Anular política de Sophos Central hasta 4 horas para solucionar problemas**.

Ahora puede realizar cambios en la página. Los cambios anulan temporalmente la política que usted (u otro administrador) haya aplicado desde la consola de Sophos Central Admin.

Tras cuatro horas, la configuración vuelve a cambiar automáticamente a la de las políticas impuestas de forma centralizada.

**Nota**
Si lo desea, puede restaurar la configuración antes. Esto no se puede hacer para funciones individuales. Debe desactivar **Anular política de Sophos Central hasta 4 horas para solucionar problemas**, que se aplica a todas las funciones.

## Escaneado en tiempo real

El escaneado en tiempo real escanea elementos cuando los usuarios intentan acceder y concede acceso solo si están limpios. Puede seleccionar:

- **Archivos**. Esta opción escanea los archivos locales y (si está seleccionado en la política) los recursos compartidos de red.
- **Internet**. Esta opción escanea los recursos de Internet. Puede escanear descargas en curso, bloquear el acceso a sitios web maliciosos y detectar sitios web de baja reputación.

## Controles en usuarios

- **Control de periféricos**. Esta opción permite controlar el acceso a periféricos y medios extraíbles.
- **Control de aplicaciones**. Esta opción permite detectar y bloquear aplicaciones que no suponen una amenaza para la seguridad, pero cuyo uso no considere adecuado en el entorno empresarial.
- **Control web**. Esta opción permite protegerse contra descargas peligrosas, controlar los sitios que pueden visitar los usuarios y evitar las fugas de datos.

## Protección en tiempo de ejecución

La protección en tiempo de ejecución protege contra amenazas detectando tráfico o comportamientos sospechosos o maliciosos en Macs. Puede seleccionar:

- **Detección de tráfico malicioso**. Esto detecta tráfico entre un Mac y un servidor que indica un posible intento de toma de control del Mac.
- **Detección de ransomware (CryptoGuard)**. Esta opción protege contra programas maliciosos que restringen el acceso a los archivos y exigen un pago para recuperarlos.

# 6 Cómo...

## 6.1 Escanear un archivo

Para escanear archivos individuales:

En el Finder, haga clic con el botón derecho en el archivo y seleccione **Escanear con Sophos Endpoint**.

Se muestra el cuadro de diálogo **Escaneado de ítems del Finder** para que pueda ver el progreso y los resultados del escaneado.

## 6.2 Escanear el Mac

Para escanear todos los archivos del Mac:

1. Vaya a la página **Estado** o a la página **Detecciones**.
2. Haga clic en **Escanear ahora**.
   Tras completarse el escaneado, verá un resumen de los resultados.
3. Si se detectan amenazas, puede ir a la página **Eventos** para ver los detalles.

## 6.3 Limpiar una amenaza

Para limpiar una amenaza que se ha detectado:

1. Haga clic en **Inicio de sesión de administrador** e introduzca la contraseña de protección contra manipulaciones (disponible del administrador de Sophos Central).
   Ahora el enlace **Configuración** de la barra de menús está activo.
2. Vaya a la página **Eventos** para ver los detalles de la amenaza que se ha detectado.
3. Busque un enlace de acción junto a los detalles de la amenaza.

Las medidas que puede tomar son las mismas que las disponibles en la consola de Sophos Central Admin. Consulte la lista en la página **Alertas** de la Ayuda de Sophos Central.

## 6.4 Cambiar la configuración de seguridad

Para cambiar la configuración de seguridad:

1. Haga clic en **Inicio de sesión de administrador** e introduzca la contraseña de protección contra manipulaciones (disponible del administrador de Sophos Central).
   Ahora el enlace **Configuración** de la barra de menús está activo.
2. Vaya a la página **Configuración**.
3. Active **Anular política de Sophos Central hasta 4 horas para solucionar problemas**.
4. Utilice los controles de la página para activar o desactivar funciones de seguridad.

Tras cuatro horas, la configuración vuelve a cambiar automáticamente a la de las políticas impuestas de forma centralizada.

**Nota**
Si lo desea, puede restaurar la configuración antes. Esto no se puede hacer para funciones individuales. Debe desactivar **Anular política de Sophos Central hasta 4 horas para solucionar problemas**, que se aplica a todas las funciones.

## 6.5 Actualizar ahora

Para actualizar:

1. Haga clic en **Acerca de**.
2. Haga clic en **Actualizar ahora**.

## 6.6 Solucionar problemas

Para solucionar problemas:

1. Haga clic en **Acerca de**.
2. Haga clic en **Ejecutar herramienta de diagnóstico** para recopilar datos sobre el problema.

También puede hacer clic en **Foro de la comunidad** para obtener más información.

## 6.7 Cifrar el Mac

La función de cifrado del dispositivo cifra el disco duro del Mac utilizando la tecnología de FileVault 2. Cuando el administrador activa la función **Device Encryption**, aparece el cuadro de diálogo **Sophos Device Encryption**.

1. En el cuadro de diálogo **Sophos Device Encryption**, introduzca su contraseña de inicio de sesión y haga clic en **Cifrar**.
   Esto activa el cifrado del dispositivo. Si lo prefiere, haga clic en **Posponer** para iniciar el proceso en otro momento.
2. La clave de recuperación se almacena automáticamente en Sophos Central.

Cuando el disco del sistema está cifrado, los volúmenes de datos internos se cifran de forma automática. Los discos cifrados se desbloquean automáticamente cuando se inicia el Mac. Los volúmenes de datos extraíbles, como las memorias USB, no se cifran.

## 6.8 Acceder a su Mac si se le olvida la contraseña

Si no puede iniciar sesión en su Mac porque ha olvidado la contraseña de inicio de sesión, necesitará una clave de recuperación.

Si utiliza **Sophos Device Encryption**, la clave de recuperación se almacena en Sophos Central. Para obtener su clave de recuperación, escoja una de las opciones siguientes:

- Iniciar sesión en el portal de autoservicio de Sophos y seguir las instrucciones de la ayuda de Sophos Central.

- Pedir al administrador que obtenga la clave de recuperación por usted, tal como se describe en Usar la recuperación de FileVault (página 10). Siga este procedimiento si no puede utilizar el portal de autoservicio.

### 6.8.1 Usar la recuperación de FileVault

Para que un administrador recupere una clave de recuperación por usted, siga estos pasos.

1. Reinicie el Mac y espere hasta que aparezca el **ID de la clave de recuperación**.
   El **ID de la clave de recuperación** se muestra solo unos instantes. Para volver a verlo, es necesario reiniciar el Mac.
2. Póngase en contacto con su administrador y proporciónele el **ID de la clave de recuperación**.
   El administrador debe buscar la clave de recuperación de su Mac en Sophos Central y darle la clave.
3. Haga clic en el signo de interrogación en el campo **Contraseña**.
   Se mostrará un mensaje.
4. Haga clic en la flecha junto al mensaje para cambiar al campo de la clave de recuperación.
5. Introduzca la clave de recuperación.
6. Siga las instrucciones en pantalla para crear una contraseña nueva.
   Si su cuenta de usuario se ha importado de Active Directory, haga clic en **Cancelar** en el cuadro de diálogo **Restablecer contraseña** y pida al administrador que le restablezca la contraseña.
7. Si se le solicita, haga clic en **Crear un nuevo llavero**.

Ya puede acceder a su Mac de nuevo.

# 7 ¿Por qué se bloquea una transferencia de archivos?

Es posible que vea un mensaje para informarle que se ha bloqueado una transferencia de archivos (por ejemplo, al copiar, mover o enviar archivos por correo electrónico).

Esto sucede porque su empresa ha configurado una política para evitar que envíe información confidencial de forma involuntaria a usuarios que no deben acceder a ella.

Hay dos tipos de mensaje.

## Se ha bloqueado la transferencia

Si recibe un mensaje de bloqueo de transferencia de archivos, no puede transferir los archivos. Es posible que el administrador haya incluido algún consejo en el mensaje.

## Se puede permitir la transferencia

Si recibe un mensaje de solicitud de transferencia de archivos bloqueada, puede decidir si se van a transferir los archivos. Es posible que el administrador haya incluido algún consejo en el mensaje. Haga clic en **Permitir** para confirmar que es seguro seguir adelante.

# 8 Obtener más ayuda

Puede encontrar soporte técnico en los siguientes recursos:

- Visitar el foro Sophos Community en community.sophos.com para consultar casos similares.
- Visitar la base de conocimiento de Sophos en www.sophos.com/es-es/support.aspx.

# 9 Aviso legal