

Folleto de la solución

Sophos Endpoint

Con Intercept Intercept X



La solución de seguridad para endpoints con IA más sofisticada del sector

Sophos Endpoint, que cuenta con la tecnología de Intercept X, proporciona una protección inigualable, ya que detiene los ataques avanzados antes de que afecten a sus sistemas. Las potentes herramientas de detección y respuesta para endpoints y de detección y respuesta ampliadas (EDR/XDR) permiten a su organización buscar, investigar y responder a actividades sospechosas e indicadores de ataque.

Enfoque a la seguridad centrado en la prevención

Sophos Endpoint adopta un enfoque integral de la seguridad centrado en la prevención para bloquear las amenazas sin depender de una única técnica. Múltiples modelos de IA con Deep Learning protegen frente a ataques conocidos y desconocidos. Controles web, de aplicaciones y de periféricos reducen la superficie de amenazas y bloquean vectores de ataque comunes. Análisis de comportamientos, herramientas antiransomware y antiexploits y otras tecnologías avanzadas detienen las amenazas rápidamente antes de que se agraven, de modo que los equipos de TI sobrecargados tienen menos incidentes para investigar y resolver.

Protección hermética contra el ransomware

Sophos Endpoint es la solución más robusta del sector para la protección Zero Touch de endpoints frente al ransomware avanzado. La tecnología CryptoGuard detiene el cifrado malicioso en tiempo real y revierte automáticamente los archivos afectados a su estado original, lo que minimiza el impacto en la empresa.

Defensas adaptativas

Nuestras defensas dinámicas pioneras en el sector se adaptan en respuesta a los adversarios activos y los ataques manuales directos. Esto elimina la capacidad operativa del adversario, interrumpiendo y conteniendo el ataque y dando tiempo adicional a los responsables de la seguridad para responder.

Fácil de configurar y gestionar

Sophos Central es una potente plataforma de gestión de ciberseguridad basada en la nube que unifica todas las soluciones de seguridad next-gen de Sophos. Las tecnologías y funciones recomendadas están activadas por defecto para que disponga inmediatamente de la máxima protección sin necesidad de realizar ajustes.

Un líder de confianza en seguridad para endpoints

Sophos Endpoint recibe de forma continuada el máximo reconocimiento por parte de clientes, analistas y organizaciones de pruebas independientes. Sophos ha sido nombrado líder 15 veces en el Magic Quadrant™ de Gartner® de plataformas de protección de endpoints y Suite de protección para endpoints n.º 1 en los informes G2 Grid® de invierno de 2025.

Aspectos destacados

- Múltiples modelos de IA con Deep Learning le protegen frente a ataques conocidos y desconocidos.
- Reduzca su superficie de ataque y bloquee vectores de ataque comunes con controles web, de aplicaciones y de periféricos.
- Detenga rápidamente las amenazas antes de que se agraven con análisis de comportamientos, herramientas antiransomware y antiexploits y otras tecnologías.
- Proteja sus datos frente a ataques de ransomware locales y remotos con la mejor protección de su clase.
- Benefíciese de unas defensas dinámicas pioneras en el sector que se adaptan automáticamente en respuesta a los adversarios activos y los ataques manuales directos.
- Busque, investigue y responda a la actividad sospechosa con potentes herramientas EDR y XDR.

Reduzca su superficie de ataque con un enfoque centrado en la prevención

Detener los ataques en una fase temprana consume menos recursos que monitorizarlos y subsanarlos más adelante en la cadena de ataque. Las sofisticadas tecnologías de protección de Sophos Endpoint bloquean la más amplia variedad de ataques. Se sirve de controles web, de aplicaciones y de periféricos para reducir su superficie de ataque y bloquear vectores de ataque comunes, lo que reduce las oportunidades para los atacantes de penetrar en su entorno.

Protección web

Bloquea el tráfico saliente del navegador a sitios web maliciosos, lo que frena las amenazas en la fase de distribución y evita los sitios de phishing o malware.

Control web

Bloquea el acceso a contenido inapropiado y no deseable. Aplique políticas de uso web aceptable a toda su organización y protéjase de la pérdida de datos.

Reputación de descarga

Analiza los archivos descargados utilizando la información sobre amenazas global de SophosLabs para emitir un veredicto basado en la frecuencia, la antigüedad y el origen, e instar a los usuarios a bloquear los archivos con reputación baja o desconocida.

Control de aplicaciones

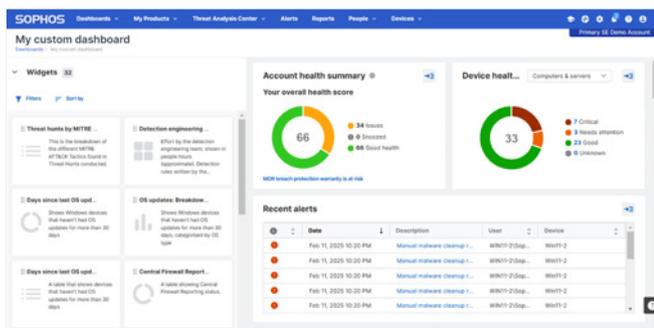
Bloquea aplicaciones vulnerables o inapropiadas mediante categorías predefinidas, por lo que deja de ser necesario bloquear las aplicaciones individualmente por hash.

Control de periféricos (dispositivos)

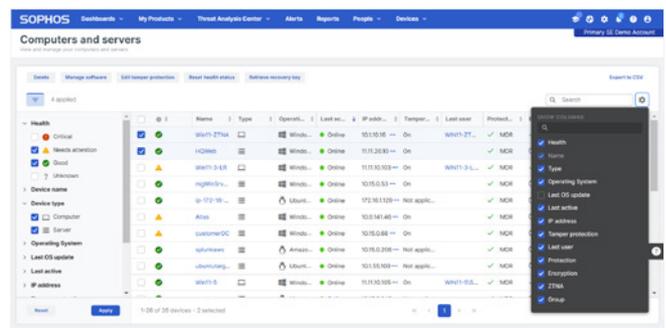
Supervisa y bloquea el acceso a medios extraíbles, Bluetooth y dispositivos móviles para impedir que determinado hardware se conecte a la red.

Prevención de fugas de datos

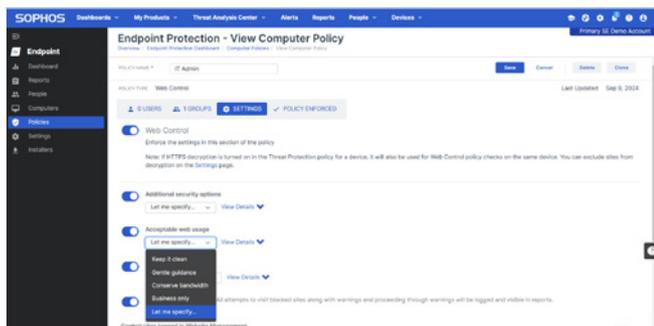
Supervise o restrinja la transferencia de archivos que contienen datos confidenciales. Por ejemplo, puede impedir que un usuario envíe un archivo confidencial utilizando el correo electrónico basado en la web.



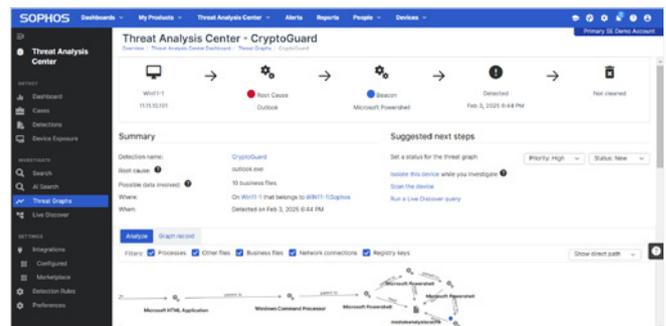
Cree paneles de control personalizados para cubrir sus necesidades.



Una protección para endpoints que es fácil de configurar y gestionar.



Políticas configurables con opciones recomendadas activadas por defecto.



Analice amenazas para establecer la causa raíz.

Un enfoque centrado en la prevención detiene las amenazas rápidamente

Detectar y remediar amenazas lo antes posible reduce el riesgo. Sophos Endpoint detiene las amenazas rápidamente antes de que se agraven, de modo que los equipos de TI sobrecargados tienen menos incidentes que investigar y resolver. Sophos ofrece unas sólidas funciones de prevención de amenazas, validadas por los mejores resultados obtenidos sistemáticamente en pruebas de seguridad independientes.



Protección hermética contra el ransomware

Según el Informe de protección digital de Microsoft de 2024, el cifrado remoto ya se observa en el 70 % de los ataques consumados, y el 92 % se originan en dispositivos no gestionados de la red. Sophos Endpoint ofrece la protección Zero Touch para endpoints más robusta frente al ransomware local y remoto, sirviéndose de la avanzada tecnología CryptoGuard para detectar intentos de cifrado, sea cual sea el origen.

- Bloquea variantes de ransomware nuevas.
- Inspecciona los cambios en los archivos en tiempo real para detectar el cifrado malicioso.
- Impide que el ransomware remoto cifre archivos de forma remota a través de la red.
- Revierte automáticamente los archivos cifrados a su estado original no cifrado utilizando una tecnología patentada que no depende del servicio de instantáneas de volumen de Windows.
- Protege archivos de todos los tipos y tamaños con un impacto mínimo sobre el rendimiento.
- Protege el registro de arranque maestro (MBR) de ataques avanzados dirigidos al disco duro.

Prevención de malware con Deep Learning con IA

Detecta y bloquea el malware tanto conocido como desconocido analizando los atributos de los archivos y utilizando el razonamiento predictivo para identificar amenazas.

Antiexploits

Protege la integridad de los procesos con refuerzo de memoria y más de 60 técnicas antiexploits, sin necesidad de ajustes y superando las capacidades nativas de Windows y otras soluciones de seguridad.

Protección comportamental

Supervisa procesos, archivos y eventos del registro para detectar y detener la actividad maliciosa. Escanea la memoria, examina los procesos en ejecución en busca de amenazas ocultas y detecta a los atacantes que inyectan código malicioso para eludir la detección.

Seguridad sincronizada

Sophos Endpoint comparte información sobre el estado de seguridad con Sophos Firewall, Sophos Zero Trust Network Access (ZTNA) y otros productos de Sophos para proporcionar más visibilidad sobre las amenazas y el uso de las aplicaciones, además de aislar los dispositivos comprometidos automáticamente.

Protección activa

Amplía nuestra sólida protección en el dispositivo con consultas en tiempo real de la información sobre amenazas global de SophosLabs para obtener contexto adicional de archivos, verificación de decisiones, reputación de archivos y supresión de falsos positivos.

Bloqueo de aplicaciones

Evita el uso indebido de navegadores y aplicaciones al bloquear acciones que no suelen asociarse a esos procesos.

Interfaz de análisis antimalware (AMSI)

La interfaz de análisis antimalware (AMSI) de Windows bloquea los ataques sin archivos en que el malware se carga directamente desde la memoria. Sophos Endpoint también incluye una mitigación exclusiva contra la evasión de la detección de AMSI.

Detección de tráfico malicioso

Detecta dispositivos que se comunican con servidores de comando y control (C2) interceptando y analizando el tráfico no relacionado con navegadores para identificar destinos maliciosos.

Defensas adaptativas

Sophos Endpoint se sirve de unas defensas dinámicas pioneras en el sector que automatizan la protección adaptándose en tiempo real en respuesta a los adversarios activos y los ataques manuales directos. Sophos Endpoint bloquea las acciones que no son intrínsecamente maliciosas en un contexto cotidiano pero que son peligrosas en el contexto de un ataque. Esta funcionalidad responde dinámicamente a los ataques activos y los interrumpe cuando los delincuentes pueden haberse afianzado sin levantar sospechas ni utilizar código malicioso.

Protección adaptativa contra ataques

Activa dinámicamente el refuerzo de las defensas en el endpoint cuando se detecta un ataque manual directo, lo que interrumpe al adversario y le da a usted más tiempo para responder.

Advertencia de ataque crítico

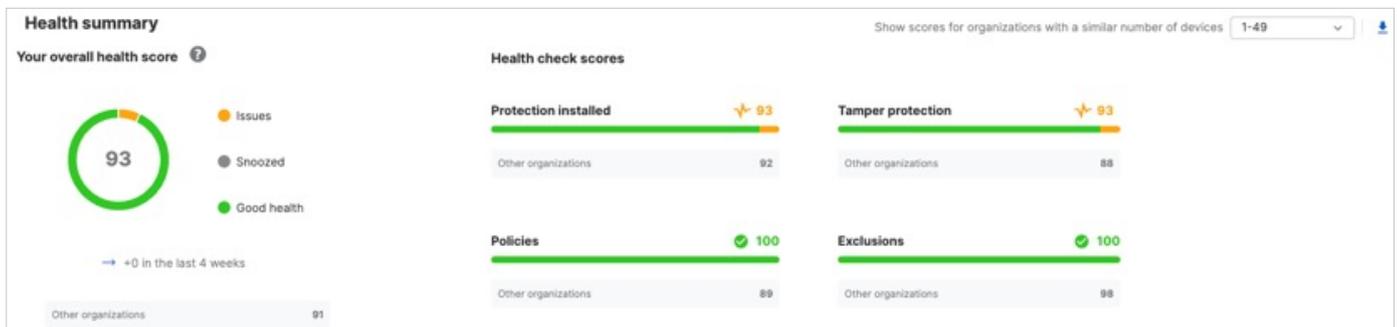
Notifica a los administradores sobre actividades en curso graves por parte de los adversarios a través de múltiples endpoints, basándose en detecciones de amenazas en toda la organización.

| | PROTECCIÓN COMPORAMENTAL | ADAPTIVE ATTACK PROTECTION | ADVERTENCIA DE ATAQUE CRÍTICO |
|-----------------------|--|--|--|
| ALCANCE | DISPOSITIVO INDIVIDUAL | DISPOSITIVO INDIVIDUAL | TODO EL ENTORNO |
| VENTAJAS | El motor de comportamientos detiene las primeras fases de los ataques de adversarios activos | Incrementa la sensibilidad de la protección para evitar ataques | Le avisa de un ataque que requiere una respuesta inmediata al incidente |
| DESENCADENANTE | Reglas de comportamiento | Detección de conjuntos de herramientas de hacking | Indicadores de adversarios activos de gran impacto, incluidos umbrales y correlaciones a nivel de organización |
| ANALOGÍA |  "¡ESCUDOS PREPARADOS!" |  "¡ESCUDOS ARRIBA!" |  "¡ALERTA ROJA!" |

Defensas adaptativas de Sophos Endpoint

Identifique desviaciones de la postura de seguridad

Los parámetros de políticas mal configurados, las exclusiones y otros factores pueden comprometer su postura de seguridad. La función de comprobación del estado de seguridad de la cuenta identifica las desviaciones de la postura de seguridad y los errores de configuración de alto riesgo, lo que le permite solucionar los problemas con un solo clic.



Verificar estado de cuenta

Capas de protección adicional (complementos)

Sophos ZTNA

Permita que sus usuarios se conecten de forma segura a sus aplicaciones con el sustituto definitivo de la VPN. Sophos ZTNA es la única solución Zero Trust Network Access que se integra perfectamente con la protección para endpoints next-gen.

Device Encryption

Teniendo en cuenta que todos los días se pierden o roban dispositivos, el cifrado completo de disco es esencial. El cifrado de archivos integrado en Sophos Endpoint permite gestionar BitLocker (Windows) y FileVault (macOS) con eficacia.

Acelere la detección, la investigación y la respuesta

Sophos Endpoint bloquea automáticamente la mayoría de las amenazas desde un principio, lo que reduce el número de eventos que deben investigarse. Para las actividades sospechosas y amenazas que requieren un análisis realizado por humanos, Sophos ofrece soluciones potentes para detectar, investigar y responder rápidamente en todos los vectores de ataque claves.

Sophos XDR

Sophos Extended Detection and Response (XDR) permite buscar, investigar y responder a actividades sospechosas y ataques de varias fases en todo su entorno de seguridad. Diseñadas por analistas de seguridad para usuarios de todos los niveles, nuestras potentes herramientas con IA generativa permiten a todo el mundo (desde técnicos informáticos hasta analistas SOC de nivel superior) investigar rápidamente las amenazas y neutralizar a los adversarios.

Sophos XDR ofrece integraciones preconfiguradas con un amplio ecosistema de soluciones para endpoints, firewalls, redes, correo electrónico, identidad, productividad, la nube y copias de seguridad, lo que le permite obtener más rentabilidad de sus herramientas de seguridad existentes.

Más información en [Sophos.com/XDR](https://sophos.com/XDR)

Sophos MDR

Para aquellas organizaciones que no dispongan de los recursos necesarios para gestionar la detección y respuesta a amenazas de forma interna, Sophos Managed Detection and Response (MDR) es un servicio 24/7 prestado por un equipo de élite de analistas de seguridad, cazadores de amenazas y expertos en respuesta a incidentes. Sophos MDR se sirve de la telemetría tanto de las tecnologías de seguridad de Sophos como de terceros para detectar y neutralizar incluso las amenazas más sofisticadas.

Sophos MDR se adapta a usted, con múltiples niveles de servicio y modos de respuesta para cubrir las necesidades de su organización y compatibilidad con sus herramientas y tecnologías actuales.

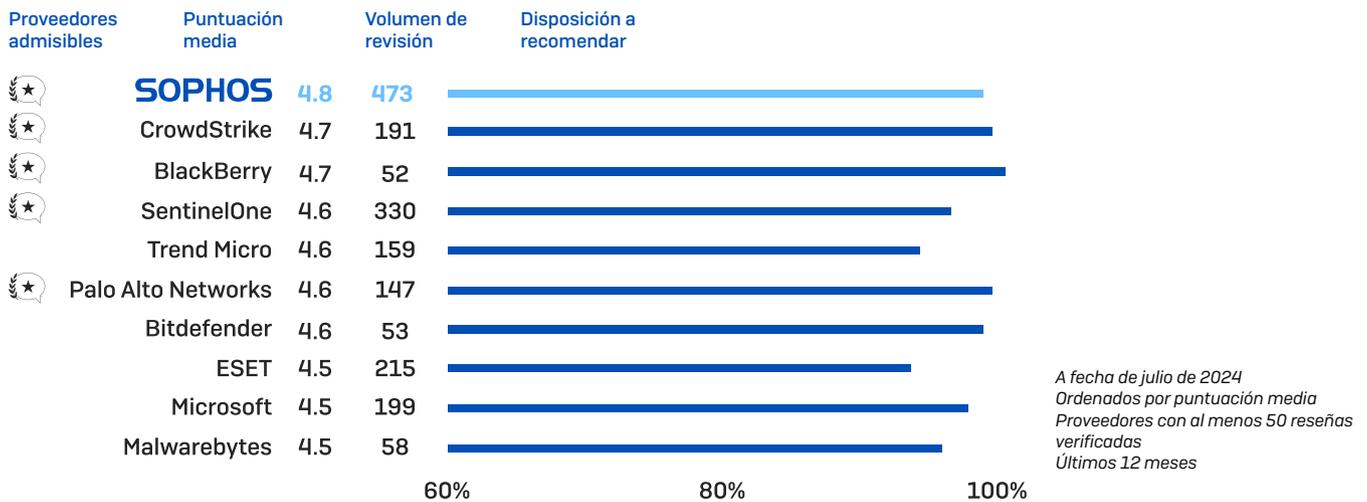
Más información en [Sophos.com/MDR](https://sophos.com/MDR)

| | Sophos Endpoint | Sophos XDR | Sophos MDR |
|---|-----------------|------------|------------|
| Protección contra amenazas next-gen Protección web y antimalware con Deep Learning con IA | ✓ | ✓ | ✓ |
| Bloqueo de actividad maliciosa Antiransomware, antiexploits, defensas adaptativas | ✓ | ✓ | ✓ |
| Reducción de la exposición a amenazas Funciones de control de aplicaciones, periféricos, web, DLP | ✓ | ✓ | ✓ |
| Detección y respuesta Potentes herramientas de investigación y respuesta a amenazas | | ✓ | ✓ |
| Visibilidad en todas las superficies de ataque claves Integraciones con tecnología de Sophos y terceros | | ✓ | ✓ |
| Detección y respuesta gestionadas Supervisión de amenazas y respuesta a incidentes 24/7 a cargo de expertos | | | ✓ |

El proveedor con la solución de protección para endpoints mejor valorada y con más reseñas

En el informe Voice of the Customer de Gartner de 2024 de plataformas de protección de endpoints, Sophos recibió el número más alto de reseñas de todos los proveedores del estudio y una puntuación de 4,8 sobre 5. Sophos también fue nombrado proveedor Customers' Choice 2024 en los 11 sectores incluidos en el informe.

Plataformas de protección de endpoints



Descubra por qué los clientes eligen Sophos Endpoint

Sophos es un líder consolidado en seguridad para endpoints, con el reconocimiento del sector que lo sustentan.

Gartner

Sophos fue nombrado líder en el Magic Quadrant™ de Gartner® 2024 de plataformas de protección de endpoints en 15 informes consecutivos.

SE Labs

Sophos obtiene sistemáticamente los mejores resultados de protección del sector en pruebas independientes de seguridad para endpoints.

G2 Leader

Sophos es nombrado líder en los informes G2 Grid® de invierno de 2025 para suites de protección de endpoints, EDR, XDR, software para firewalls y MDR.

IDC

Sophos es nombrado líder en el IDC MarketScape 2024 para la seguridad moderna mundial de endpoints para pequeñas y medianas empresas.

Pruébelo gratis hoy mismo

Regístrese para una evaluación gratuita de 30 días en es.sophos.com/endpoint

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com