

Folleto de la solución

Sophos Extended Detection and Response



Defiéndase de los adversarios activos con completas funciones de EDR y XDR

Detener los ataques rápidamente es fundamental. Sophos XDR ofrece potentes herramientas e información sobre amenazas que le permiten detectar, investigar y responder a actividades sospechosas en todo su entorno de TI.

Basado en la protección más sólida

Cuando se detienen más amenazas desde un principio, los equipos de TI sobrecargados tienen menos incidentes que investigar y resolver. Sophos combina la detección y respuesta ampliadas con la protección para endpoints más sólida del sector para bloquear amenazas antes de que requieran una investigación manual, lo que aligerará su carga de trabajo.

Detección y respuesta para endpoints (EDR) integrada

Sophos XDR incluye completas herramientas de EDR, como potentes funciones de búsqueda personalizables con acceso a 90 días de datos de endpoints y servidores, así como acceso remoto seguro a los dispositivos. Investigue problemas, instale y desinstale software, finalice procesos y mucho más.

Amplíe la visibilidad más allá de los endpoints

Cuanto más vea, más rápido podrá actuar. Los eventos de los productos de Sophos y de terceros se procesan, filtran, correlacionan y priorizan, lo que aumenta la visibilidad en todas las superficies de ataque claves y le permite detectar y detener rápidamente a los adversarios activos.

Amplia cartera de soluciones preparadas para Sophos XDR

Las tecnologías de Sophos se integran a la perfección en la plataforma XDR para ofrecer los mejores resultados de seguridad posibles. Entre las integraciones de soluciones nativas se incluyen Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos NDR, Sophos ZTNA, Sophos Email y Sophos Cloud.

Compatible con sus herramientas y tecnologías actuales

Utilice la telemetría de una amplia gama de herramientas de seguridad de terceros y mejore la rentabilidad de sus inversiones en tecnología existentes al tiempo que acelera las operaciones de seguridad. Las integraciones incluyen tecnologías de protección para endpoints, redes, firewalls, identidad, correo electrónico, la nube y herramientas de productividad.

Aspectos destacados

- ▶ Obtenga visibilidad de la actividad sospechosa en todas las superficies de ataque claves
- ▶ Una plataforma XDR unificada con una amplia gama de soluciones integradas de Sophos
- ▶ Saque partido de sus herramientas e inversiones actuales mediante completas integraciones con tecnologías distintas de Sophos
- ▶ Investigue y responda a las amenazas rápidamente con detecciones priorizadas por IA y flujos de trabajo optimizados
- ▶ Incluye la EDR y la protección para endpoints líderes del sector

Acelere la detección, la investigación y la respuesta

Sophos XDR incluye herramientas y funciones diseñadas para maximizar la eficiencia de los analistas de seguridad y administradores de TI. Las investigaciones guiadas por IA le permiten comprender rápidamente el alcance y la causa de un incidente y minimizar el tiempo de respuesta.



Detecciones priorizadas por IA en todas las superficies de ataque claves

Identifique fácilmente la actividad sospechosa que requiere atención inmediata. Sophos XDR prioriza automáticamente las detecciones en función del riesgo y proporciona todo el contexto.



Asignación a la plataforma MITRE ATT&CK

Las detecciones y los casos se asignan automáticamente a las tácticas de MITRE ATT&CK, lo que le permite identificar fácilmente las lagunas en las defensas y priorizar las mejoras.



Busque e investigue amenazas a toda velocidad

Con potentes opciones de búsqueda y plantillas de consultas predefinidas, podrá encontrar los datos que necesita más rápido sin tener que ser un experto en SQL.



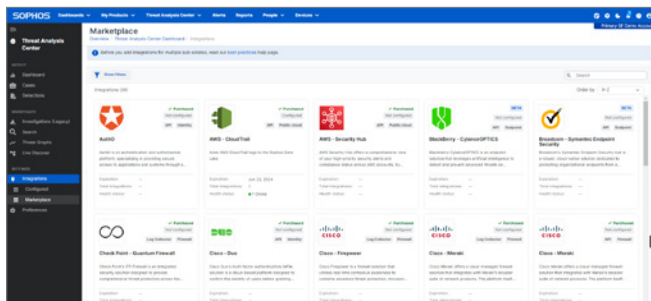
Respuestas automatizadas y aceleradas

Las acciones automatizadas como la finalización de procesos, la reversión del ransomware y el aislamiento de la red frenan las amenazas rápidamente, lo que le ahorrará un tiempo muy valioso.

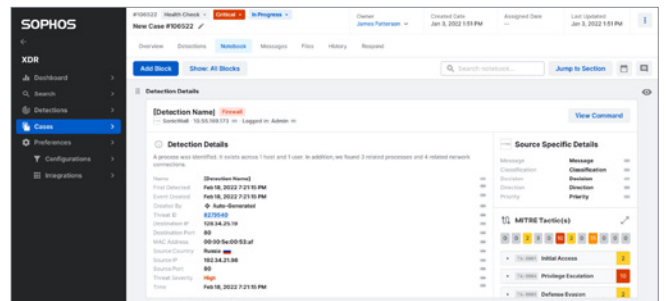


Gestión de casos colaborativa

La creación automática de casos permite una investigación rápida, con completas herramientas de gestión de casos que posibilitan la colaboración con otros miembros del equipo.



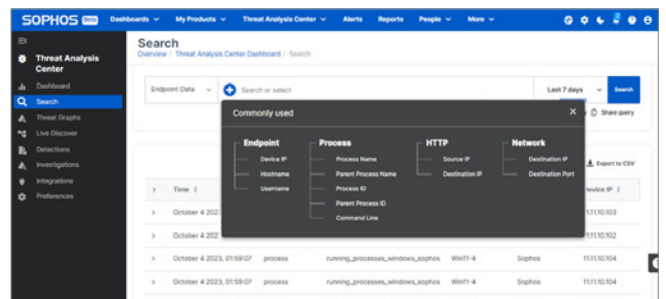
Compatible con soluciones de Sophos y de terceros



Potentes herramientas de gestión de casos y colaboración



Detecciones priorizadas por IA en todas las superficies de ataque claves



Búsqueda sencilla y potente: no se necesitan conocimientos de SQL

Integraciones incluidas con Sophos XDR

Los datos de seguridad de las siguientes fuentes se pueden integrar en la plataforma Sophos XDR sin costes adicionales. Las fuentes de telemetría se utilizan para ampliar la visibilidad de todo su entorno, generar nuevas detecciones de amenazas y mejorar la fidelidad de las detecciones de amenazas existentes, realizar búsquedas de amenazas y habilitar funciones de respuesta adicionales.

Sophos Endpoint

Bloquee las amenazas avanzadas y detecte comportamientos maliciosos en todos los endpoints

Producto incluido en el precio de Sophos XDR

Workload Protection

Protección avanzada y detección de amenazas para servidores y contenedores Windows y Linux

Producto incluido en el precio de Sophos XDR

Sophos Mobile

Mantenga sus dispositivos iOS y Android y sus datos protegidos frente a las amenazas móviles más recientes

Producto vendido por separado; integración sin coste adicional

Sophos Firewall

Supervise y filtre el tráfico de red entrante y saliente para detener amenazas avanzadas antes de que puedan provocar daños

Producto vendido por separado; integración sin coste adicional

Sophos Email

Proteja su bandeja de entrada del malware con una IA avanzada que detiene los ataques de phishing y de suplantación de identidad dirigidos

Producto vendido por separado; integración sin coste adicional

Sophos Cloud

Detenga filtraciones en la nube y obtenga visibilidad de todos sus servicios en la nube críticos, incluidos AWS, Azure y GCP

Producto vendido por separado; integración sin coste adicional

Sophos ZTNA

Sustituya la VPN de acceso remoto por el acceso de mínimo privilegio para conectar de forma segura sus usuarios a sus aplicaciones en red

Producto vendido por separado; integración sin coste adicional

Protección para endpoints de terceros

Compatible con:

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- BlackBerry [Cylance]
- Broadcom [Symantec]

+ compatible con otras soluciones con el agente «XDR Sensor» de Sophos

Herramientas de seguridad de Microsoft

- Defender para punto de conexión
- Defender for Cloud
- Defender for Cloud Apps
- Defender for Identity
- Microsoft Entra ID
- Azure Sentinel
- Office 365 Security and Compliance Center

Retención de datos de 90 días

Conserva los datos de los productos de Sophos y soluciones de terceros (ajenas a Sophos) en Sophos Data Lake

Ampliable a 1 año como complemento opcional

Registros de auditoría de Microsoft









Proporciona información sobre acciones y eventos de usuarios, administradores, sistemas y políticas ingeridos a través de la API de Actividad de administración de Office 365

Google Workspace

Ingiera telemetría de seguridad desde la API del Centro de alertas de Google Workspace

Integraciones de complementos

Los datos de seguridad de las siguientes fuentes se pueden integrar en la plataforma Sophos XDR mediante la compra de paquetes de integración. Las fuentes de telemetría se utilizan para ampliar la visibilidad de todo su entorno, generar nuevas detecciones de amenazas y mejorar la fidelidad de las detecciones de amenazas existentes, realizar búsquedas de amenazas y habilitar funciones de respuesta adicionales.

 <p>Supervise de forma continuada la actividad dentro de su red para detectar acciones sospechosas que tienen lugar entre los dispositivos y que de otra forma no se detectarían</p> <p>Compatible con cualquier red mediante el reflejo de puertos SPAN</p>	 <p>Firewall</p> <p>Compatible con:</p> <ul style="list-style-type: none">• Check Point• Cisco Firepower• Cisco Meraki• Fortinet• Palo Alto Networks• SonicWall• WatchGuard	 <p>Red</p> <p>Compatible con:</p> <ul style="list-style-type: none">• Darktrace• Secutec• Thinkst Canary• Skyhigh Security
 <p>Identidad</p> <p>Compatible con:</p> <ul style="list-style-type: none">• Auth0• Duo• ManageEngine• Okta <p>Integración con Microsoft incluida sin cargo adicional</p>	 <p>Correo electrónico</p> <p>Compatible con:</p> <ul style="list-style-type: none">• Proofpoint• Mimecast <p>Integraciones de Microsoft 365 y Google Workspace incluidas sin cargo adicional</p>	 <p>Nube pública</p> <p>Compatible con:</p> <ul style="list-style-type: none">• AWS Security Hub• AWS CloudTrail• Orca Security <p>Integre datos adicionales de AWS, Azure y GCP mediante el producto Sophos Cloud, que se vende por separado</p>
 <p>Copia de seguridad y recuperación</p> <p>Compatible con:</p> <ul style="list-style-type: none">• Veeam	 <p>Retención de datos de 1 año</p> <p>Conserva los datos de los productos de Sophos y soluciones de terceros (ajenas a Sophos) en Sophos Data Lake</p>	

Basado en la mejor protección para endpoints del mundo

Detenga más filtraciones antes de que comiencen y céntrese en las investigaciones. Con la mayoría de los productos de XDR, los analistas pierden mucho tiempo investigando incidentes que su protección debería haber bloqueado. Sophos combina la XDR con la protección para endpoints más sólida del sector para bloquear amenazas antes de que requieran una investigación manual, lo que aligerará su carga de trabajo.

Las suscripciones a Sophos XDR incluyen Sophos Intercept X Endpoint, que proporciona funciones antiransomware y antiexploits avanzadas, protección contra malware basada en IA y defensas contextuales que adaptan los niveles de protección de forma dinámica.

Encontrará más información en es.sophos.com/endpoint

Beneficiarse de la detección y respuesta como un servicio totalmente gestionado

Opte por detectar e investigar las amenazas por su cuenta con Sophos XDR, o libere a su personal con un completo servicio gestionado 24/7. Con Sophos Managed Detection and Response (MDR), nuestro equipo de analistas y cazadores de amenazas expertos pueden proporcionarle un centro de operaciones de seguridad instantáneo, con una capacidad de respuesta a incidentes integral.

Encontrará más información en es.sophos.com/mdr

Incluido con las suscripciones a Sophos XDR

	Sophos XDR
Detecciones priorizadas por IA e investigaciones guiadas	✓
Gestión de casos, colaboración y acciones de respuesta	✓
Herramientas de búsqueda sencillas y potentes para buscar e investigar amenazas	✓
Soluciones Sophos Endpoint y Workload Protection (Intercept X Advanced)	✓
Herramientas de detección y respuesta para endpoints (EDR)	✓
Retención de datos en la nube	90 días (ampliable a 1 año)
Datos detallados de endpoints y servidores en el dispositivo para EDR	✓
Integraciones con las soluciones de Sophos: Sophos Endpoint, Sophos Workload Protection, Sophos Mobile, Sophos Firewall, Sophos ZTNA, Sophos Email, Sophos Cloud	✓
Sophos Network Detection and Response (NDR)	Complemento opcional
Integraciones con soluciones de protección para endpoints ajenas a Sophos	✓
Integraciones con las soluciones de Microsoft	✓
Integración con la solución de productividad Google Workspace	✓
Integraciones con soluciones de terceros: firewall, red, correo electrónico, nube, identidad y copia de seguridad y recuperación	Complementos opcionales

Descubra por qué los clientes eligen Sophos XDR

Sophos es un líder consolidado en detección y respuesta ampliadas, con reconocimientos del sector que lo sustentan.

Gartner

Sophos ha sido nombrado líder en el Magic Quadrant™ de Gartner® 2023 de plataformas de protección de endpoints en 14 informes consecutivos



Sophos es el único proveedor que ha recibido la distinción Customers' Choice en las categorías de plataformas de protección de endpoints, MDR, firewalls y defensa frente a amenazas móviles

G2 Leader

Líder en protección para endpoints, EDR, XDR, firewall y MDR en los informes de G2 de invierno de 2024

OMDIA

Sophos es el proveedor mejor valorado y único líder en el informe Seleccionar una solución de XDR integral de Omdia Universe de 2023

MITRE ATT&CK

Sophos obtuvo resultados excepcionales en las evaluaciones MITRE Engenuity ATT&CK 2023

SE Labs

Sophos obtiene sistemáticamente los mejores resultados de protección del sector en pruebas independientes

Pruébalo gratis hoy mismo

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

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

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