Folleto de la solución

Sophos Managed Detection and Response

Detección y respuesta a amenazas 24/7

Sophos MDR es un servicio 24/7 totalmente gestionado prestado por expertos que detectan y responden a ciberataques dirigidos contra sus ordenadores, servidores, redes, cargas de trabajo en la nube, cuentas de correo electrónico, copias de seguridad y más.

Servicios de prevención de ransomware y filtraciones

La necesidad de mantener las operaciones de seguridad siempre activas es ahora imperiosa. Sin embargo, la complejidad de los entornos operativos modernos y la velocidad de las ciberamenazas hacen que sea cada vez más difícil para la mayoría de las organizaciones gestionar con éxito la detección y la respuesta por su cuenta.

Con Sophos MDR, nuestro equipo de expertos detiene ataques avanzados perpetrados por humanos. Podemos tomar medidas para neutralizar las amenazas antes de que afecten a sus operaciones empresariales o que pongan en peligro sus datos confidenciales. Sophos MDR puede personalizarse con varios niveles de servicio y prestarse a través de nuestra tecnología propia o de sus actuales inversiones tecnológicas en ciberseguridad.

La ciberseguridad prestada como servicio

Mediante funciones de detección y respuesta gestionadas (MDR) que proporcionan una completa cobertura de seguridad independientemente de dónde residan sus datos, Sophos MDR puede:

- **Detectar más ciberamenazas de las que pueden identificar las herramientas de seguridad por sí solas**
  Nuestras herramientas bloquean el 99,98 % de las amenazas, lo que permite a nuestros analistas centrarse en perseguir a los atacantes más sofisticados a quienes solo puede detectar y detener un humano altamente cualificado.

- **Tomar medidas en su nombre para impedir que las amenazas afecten a su negocio**
  Nuestros analistas detectan, investigan y responden a las amenazas en minutos, tanto si necesita una respuesta a incidentes integral como si prefiere recibir ayuda para tomar decisiones más acertadas.

- **Identificar la causa raíz de las amenazas para evitar futuros incidentes**
  Tomamos medidas y ofrecemos recomendaciones de forma proactiva a fin de reducir los riesgos para su organización. Menos incidentes significan menos interrupciones para sus equipos de TI y seguridad, sus empleados y sus clientes.

Compatible con las herramientas de ciberseguridad que ya tiene

Podemos proporcionarle la tecnología que necesita de nuestro galardonado catálogo, o también tiene la opción de que nuestros analistas utilicen sus actuales tecnologías de seguridad para detectar amenazas y responder a ellas.

La plataforma abierta y nativa de IA de Sophos es compatible con una amplia gama de soluciones de identidad, redes, firewall, correo electrónico, la nube, productividad, copia de seguridad y protección de endpoints, con integraciones de Microsoft y Google Workspace incluidas sin coste adicional.

Aspectos destacados

- Detenga el ransomware y otros ataques avanzados perpetrados por humanos con un equipo 24/7 de expertos en respuesta a amenazas
- Maximice el ROI de sus tecnologías de ciberseguridad existentes
- Deje que Sophos MDR ejecute una respuesta a incidentes integral, que trabaje con usted para gestionar incidentes de seguridad o que ofrezca notificaciones de amenazas detalladas y orientación
- Mejore su elegibilidad para obtener cobertura de ciberseguridad con las funciones de supervisión 24/7 y detección y respuesta para endpoints (EDR)
- Libere a su personal de TI y seguridad interno para que puedan centrarse en impulsar el negocio

Una MDR que se adapta a sus necesidades

Sophos MDR se puede personalizar con diferentes niveles de servicio y opciones de respuesta a las amenazas. Deje que el equipo de operaciones de Sophos MDR ejecute una respuesta a incidentes integral, que trabaje con usted para gestionar las ciberamenazas o que notifique a sus equipos de operaciones de seguridad internos en cuanto se detecten amenazas. Nuestro equipo aprende rápidamente el quién, qué, cuándo y cómo de un ataque. Podemos responder a las amenazas en cuestión de minutos.

Funciones clave

Supervisión y respuesta a amenazas 24/7

Detectamos y respondemos a las amenazas antes de que puedan poner en peligro sus datos o provocar interrupciones. Con el respaldo de siete centros de operaciones de seguridad (SOC) globales, Sophos MDR ofrece cobertura las 24 horas.

Compatible con herramientas de seguridad de otros proveedores

Sophos MDR puede integrar la telemetría de soluciones de terceros para endpoints, firewalls, redes, identidades, correo electrónico, copia de seguridad y restauración y otras tecnologías.

Respuesta a incidentes integral

Cuando detectamos una amenaza activa, el equipo de operaciones de Sophos MDR puede ejecutar un gran número de acciones de respuesta en su nombre para interrumpir, contener y neutralizar por completo al adversario de forma remota. Con una licencia de Sophos MDR Complete, se beneficiará de una respuesta a incidentes integral ilimitada, sin topes ni costes adicionales.

Datos exhaustivos e informes del servicio

Sophos Central es el único panel de control que necesitará para recibir alertas en tiempo real, generar informes y gestionar su solución. Los informes detallados y los paneles de control le ofrecen un análisis pormenorizado de las investigaciones de seguridad, las ciberamenazas y su postura de seguridad.

Protección de endpoints y cargas de trabajo incluida

Los analistas de Sophos MDR pueden utilizar la telemetría de su solución de protección de endpoints existente para detectar y responder a las amenazas que tienen como objetivo sus ordenadores y servidores. Si lo prefiere, puede pasarse a Sophos Endpoint para disfrutar de una protección superior, incluida sin coste adicional.

Búsqueda de amenazas a cargo de expertos

Analistas altamente cualificados buscan amenazas de forma proactiva para detectar y eliminar rápidamente más amenazas de las que pueden detectar los productos de seguridad por sí solos. El equipo de operaciones de Sophos MDR también puede utilizar telemetría de otros proveedores para realizar búsquedas de amenazas e identificar comportamientos de atacantes que han eludido la detección de las herramientas desplegadas.

Soporte telefónico directo

Su equipo tiene acceso telefónico directo a nuestro centro de operaciones de seguridad (SOC) para revisar posibles amenazas e incidentes activos. El equipo de operaciones de Sophos MDR está disponible 24/7/365 y cuenta con el apoyo de equipos de soporte en 26 lugares de todo el mundo.

Responsable de respuesta a incidentes dedicado

Le proporcionamos un responsable de respuesta a incidentes dedicado que colabora con su equipo interno y Partners externos en cuanto identificamos un incidente y que trabaja con usted hasta que este queda resuelto.

Análisis de causa raíz

Además de proporcionarle recomendaciones proactivas para mejorar su postura de seguridad, realizamos análisis de causa raíz para identificar los problemas subyacentes que han provocado el incidente. Le ofrecemos orientación prescriptiva para resolver vulnerabilidades de seguridad a fin de que no puedan ser explotadas en el futuro.

Función Verificar estado de cuenta

Revisamos continuamente los ajustes y las configuraciones de los endpoints gestionados por Sophos MDR y nos aseguramos de que mantengan su máximo rendimiento.

Contención de amenazas

En el caso de las organizaciones que deciden no optar por la respuesta a incidentes integral de Sophos MDR, el equipo de operaciones de Sophos MDR puede ejecutar acciones de contención para interrumpir la amenaza y evitar su propagación. Esto reduce la carga de trabajo de los equipos de seguridad internos y les permite aplicar medidas de remediación rápidamente.

Sesiones informativas

Los boletines semanales ThreatBrief y los webinars mensuales en directo ThreatCast de Sophos MDR, exclusivos para los clientes de Sophos MDR, ofrecen información sobre las últimas amenazas y las prácticas recomendadas de seguridad.

Breach Protection Warranty

Esta garantía, incluida con todas las licencias anuales (de uno a cinco años) y mensuales de Sophos MDR Complete, cubre hasta 1 millón USD en gastos de respuesta. No hay niveles de garantía, ni condiciones mínimas de contrato ni requisitos de compra adicionales.

Con el respaldo de Sophos X-Ops

Sophos X-Ops reúne una amplia experiencia en el ámbito del entorno de ataque. Nuestros equipos de élite proporcionan una información sobre amenazas inigualable, y crean y despliegan continuamente nuevas reglas de detección en su nombre, para protegerle contra adversarios activos a medida que sus tácticas evolucionan.

Integraciones incluidas

Los datos de seguridad de las siguientes fuentes se pueden integrar para que pueda usarlos el equipo de operaciones de Sophos MDR 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 MDR

Workload Protection

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

Producto incluido en el precio de Sophos MDR

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; requiere suscripción a la protección Xstream; 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 Optix

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

Integraciones incluidas:

- Broadcom Symantec
- CrowdStrike
- Cylance
- Jamf
- Microsoft
- SentinelOne
- Trend Micro

Compatible con otras soluciones de protección de endpoints con el agente "XDR Sensor" de Sophos

Herramientas de seguridad de Microsoft

- Defender para punto de conexión
- Defender para Office 365
- Defender for Cloud Apps
- Defender for Identity
- Entra ID Protection
- Microsoft 365 Defender
- Microsoft Purview DLP

Retención de datos de 90 días

Retiene los datos de detección en Sophos Data Lake durante 90 días de serie

Actividad de administración de Microsoft Office 365

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

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

Integraciones de complementos

Los datos de seguridad de las siguientes fuentes de terceros se pueden integrar para que los use el equipo de operaciones de Sophos MDR 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.

Sophos NDR

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

Compatible con cualquier red mediante el reflejo de puertos SPAN

Firewall

Integraciones incluidas:

- Barracuda
- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- F5
- Forcepoint
- Palo Alto Networks
- SonicWall
- Ubiquiti
- WatchGuard

Red

Integraciones incluidas:

- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary
- Vectra
- Zscaler

Identidad

Integraciones incluidas:

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

Integración con Microsoft incluida sin cargo adicional

Correo electrónico

Integraciones incluidas:

- Mimecast
- Proofpoint
- Trend Micro

Integraciones de Microsoft 365 y Google Workspace incluidas sin cargo adicional

Nube:

Integraciones incluidas:

- Orca Security

Integraciones de AWS, Azure y GCP incluidas con el producto Sophos Cloud Optix, que se vende por separado.

Copia de seguridad y recuperación

Integraciones incluidas:

- Acronis
- Rubrik
- Veeam

Retención de datos de 1 año

Retiene los datos de detección en Sophos Data Lake durante 1 año

Servicio complementario

Sophos Managed Risk, con la tecnología de Tenable

Reduzca los riesgos de ciberseguridad gracias a la gestión proactiva como servicio de las vulnerabilidades en la superficie de ataque. Sophos Managed Risk identifica vulnerabilidades de alta prioridad, de forma que se puedan tomar medidas para evitar ataques antes de que afecten a su negocio. Disponible como complemento de Sophos MDR.

Niveles de servicio de Sophos MDR

	Sophos MDR Essentials	Sophos MDR Complete
Supervisión y respuesta a amenazas 24/7 a cargo de expertos	✓	✓
Sophos Endpoint y Sophos Workload Protection Incluidos	✓	✓
Compatible con productos de seguridad de otros proveedores	✓	✓
Datos exhaustivos e informes del servicio	✓	✓
Sesiones informativas sobre amenazas de Sophos	✓	✓
Función Verificar estado de cuenta	✓	✓
Búsqueda de amenazas a cargo de expertos	✓	✓
Contención de amenazas: se interrumpen los ataques y se impide su propagación Utilice el agente Sophos XDR completo o el agente "XDR Sensor" de Sophos	✓	✓
Soporte telefónico directo durante incidentes activos	✓	✓
Respuesta a incidentes integral: se eliminan las amenazas por completo Requiere el agente Sophos XDR completo	Servicio IR complementario*	✓
Responsable de respuesta a incidentes dedicado	Servicio IR complementario*	✓
Análisis de causa raíz	Servicio IR complementario*	✓
Breach Protection Warranty		✓
Integraciones de Microsoft y Google Workspace incluidas	✓	✓
Integraciones con soluciones de terceros: firewall, red, correo electrónico, nube, identidad y copia de seguridad	Complemento	Complemento
Sophos Network Detection and Response (NDR)	Complemento	Complemento
Sophos Managed Risk, con la tecnología de Tenable	Complemento	Complemento

*Una suscripción anual a Sophos IR Services Retainer ofrece descuentos en los servicios de respuesta a incidentes. Benefíciese un equipo de élite de expertos en respuesta a incidentes que le ayude a volver a la normalidad rápidamente en caso de ataque.

Incorporación guiada (opcional)

Sophos MDR Guided Onboarding puede adquirirse por separado para obtener asistencia remota con la incorporación. Este servicio proporciona ayuda práctica para conseguir un despliegue fluido y eficiente, garantiza el uso de las configuraciones recomendadas y ofrece formación para maximizar el valor de su inversión en el servicio MDR. Se le asignará un contacto dedicado de la organización de servicios profesionales de Sophos que le guiará durante los primeros 90 días para garantizar el éxito de su implementación. Sophos MDR Guided Onboarding incluye:

Día 1: Implementación

- Inicio del proyecto
- Configurar Sophos Central y revisar funciones
- Crear y probar el proceso de despliegue
- Configurar integraciones de MDR
- Configurar sensores de Sophos NDR
- Despliegue en toda la empresa

Día 30: Formación de MDR

- Aprender a pensar y actuar como un SOC
- Entender cómo identificar indicadores de peligro
- Entender cómo utilizar nuestra plataforma MDR para tareas administrativas
- Aprender a crear consultas para investigaciones futuras

Día 90: Evaluación de la postura de seguridad

- Revisar políticas actuales para recibir recomendaciones de mejores prácticas
- Analizar funciones no utilizadas que podrían ofrecer una protección adicional
- Evaluación de seguridad siguiendo el marco del NIST
- Recibir informe de resumen con recomendaciones tras nuestra revisión

Descubra por qué los clientes eligen Sophos MDR

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

IDC

Líder en el IDC MarketScape 2024 para los servicios de detección y respuesta gestionadas globales

Gartner peerinsights™

Customers' Choice en el informe Voice of the Customer 2024 de Gartner® de detección y respuesta gestionadas

G2 Leader

Nombrado líder global para la detección y respuesta gestionadas por los clientes en el informe G2 Grid® de invierno de 2025

FROST & SULLIVAN

Líder en el informe Frost Radar 2024 para la detección y respuesta gestionadas globales

MITRE | ATT&CK® Evaluations

Sólidos resultados en las evaluaciones de MITRE ATT&CK para servicios administrados

Para obtener más información, visite

es.sophos.com/mdr

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

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

2025-02-03 BRES (PS)

SOPHOS