SOPHOS

Refuerce Microsoft Defender con Sophos MDR

Reduzca el ciberriesgo, aumente la eficacia y el impacto de las inversiones en seguridad y mejore la asegurabilidad al reforzar Microsoft Defender con la detección y respuesta a amenazas 24/7 realizadas por humanos del proveedor de servicios MDR que más confianza genera en todo el mundo.

Monográficos de Sophos. Julio de 2023

Introducción

La seguridad para endpoints es una capa de protección fundamental, pero no puede detener todas las amenazas. Los sofisticados adversarios de hoy en día despliegan cada vez más tácticas, técnicas y procedimientos (TTP) sigilosos para evitar ser interceptados por las tecnologías de seguridad, como por ejemplo explotar vulnerabilidades sin parchear, utilizar credenciales robadas y abusar de herramientas de TI legítimas.

Para detener los ataques avanzados de ransomware y las filtraciones de seguridad, es crucial complementar Microsoft Defender con una detección y respuesta 24/7 realizadas por humanos. Sin embargo, el enorme volumen de alertas generadas por las tecnologías de seguridad de Microsoft, junto con la complejidad del entorno de amenazas, hacen que las operaciones de seguridad sean una ardua tarea que exige muchos recursos para la mayoría de las empresas.

Por ello, las organizaciones recurren cada vez más a Sophos, el proveedor de detección y respuesta gestionadas (MDR) más fiable y mejor valorado del mundo, para reforzar Microsoft Defender. Los analistas de Sophos monitorizan, priorizan y responden 24/7 a las alertas de seguridad de Microsoft y toman medidas inmediatas para frenar las amenazas confirmadas. También utilizan detecciones propias de Sophos, información sobre amenazas y búsquedas de amenazas realizadas por humanos para detectar y detener las amenazas más allá de Microsoft Defender.

Sophos MDR está diseñado para adaptarse a sus necesidades, ajustándose a sus inversiones actuales en TI y seguridad, y a sus recursos internos. Tanto si desea complementar su equipo interno con conocimientos adicionales, ampliar sus ciberdefensas con una cobertura integral "fuera del horario laboral" o externalizar por completo la detección y respuesta ante amenazas, Sophos MDR puede ayudarle a conseguir resultados de ciberseguridad superiores.

Refuerce Microsoft Defender con Sophos MDR

✓ Reduzca el ciberriesgo

- Detenga los ataques avanzados de ransomware y las filtraciones, incluidos los ataques perpetrados por humanos que burlan Microsoft Defender

✓ Aumente la eficacia y el impacto de las inversiones en seguridad

- Libere recursos de TI para ejecutar programas estratégicos
- Reduzca la probabilidad de incurrir en costes de recuperación de incidentes graves
- Obtenga más rentabilidad de sus inversiones

✓ Mejore la asegurabilidad

- Consiga mejores ofertas de pólizas que reconozcan y premien el hecho de haber reducido sus ciberriesgos

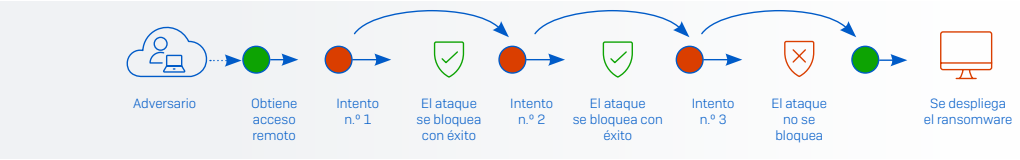
Los adversarios no se cuelan, sino que inician sesión

La realidad es que las soluciones tecnológicas por sí solas, incluida Microsoft Defender, no pueden evitar todos los ciberataques. Los adversarios activos son delincuentes que adaptan sus tácticas, técnicas y procedimientos (TTP) sobre la marcha mediante maniobras manuales en tiempo real en respuesta a las medidas adoptadas por las tecnologías de defensa y los responsables de la seguridad, y como medio para eludir la detección.

Estos ataques, que a menudo desembocan en devastadores incidentes de ransomware y filtración de datos, son de los más difíciles de detener. También se han vuelto muy frecuentes, y es que el 23 % de las pequeñas y medianas empresas afirman que su organización sufrió un ataque perpetrado por un adversario activo en el último año. Reflejo de la posible devastación de estos ataques, el 30 % de los responsables de TI/ciberseguridad consideran que los adversarios activos son una de sus principales preocupaciones para 2023[1].

Bloquear a los adversarios activos con tecnología de seguridad no basta para frustrarlos. Estos hábiles y perseverantes delincuentes despliegan múltiples enfoques innovadores para lograr sus objetivos, entre ellos:

- Explotar las deficiencias de seguridad para penetrar en las organizaciones y moverse lateralmente una vez dentro de la red, incluyendo credenciales robadas, vulnerabilidades no parcheadas y errores de configuración de seguridad.
- Usar indebidamente herramientas de TI legítimas utilizadas por los responsables de la seguridad para evitar que se activen las detecciones, como PowerShell, PsExec y RDP.
- Modificar sus ataques en tiempo real en respuesta a los controles de seguridad, pasando continuamente a nuevas técnicas hasta encontrar la forma de lograr sus objetivos.



Ejemplo de estrategia de ataque de un adversario activo

Al hacerse pasar por usuarios autorizados y explotar los puntos débiles en las defensas de una organización, los ciberdelincuentes pueden evitar la activación de las tecnologías de detección automatizadas que tienen dificultades para diferenciar entre usuarios legítimos y atacantes.

Para complicar aún más la tarea de los encargados de la seguridad, los adversarios actuales, bien financiados, siguen innovando y desarrollando su modelo de negocio. El rápido y reciente crecimiento del modelo de ciberdelincuencia como servicio, que incluye el ransomware como servicio y el phishing como servicio, ha reducido la barrera de entrada para los delincuentes en potencia, al tiempo que facilita la ejecución a escala y aumenta la calidad de los ataques.

Una de las consecuencias de la evolución del panorama de las amenazas es que el índice de cifrado de datos como consecuencia del ransomware ha alcanzado un nivel sin precedentes: los ciberdelincuentes consiguen cifrar los datos en más de tres cuartas partes (76 %) de los ataques[2].

La realidad del ransomware

- El 66 % de las empresas se vieron afectadas por el ransomware en el último año.
- El 76% de los ataques de ransomware comportaron el cifrado de datos
- En el 30 % de los ataques en que se cifraron datos, también se robaron datos
- 1.ª causa raíz de un ataque: explotación de vulnerabilidades (36 %)
- 2.ª causa raíz de un ataque: compromiso de credenciales (29 %)

1 El estado de la ciberseguridad 2023: el impacto de los adversarios en el negocio, Sophos.

2 El estado del ransomware 2023, Sophos.

Detección y respuesta ante amenazas 24/7: un elemento imprescindible de la seguridad moderna

La buena noticia es que combinando expertos humanos y tecnología es posible detener los ataques avanzados perpetrados por humanos. Cada vez que un adversario realiza una acción, se crea una señal. Al combinar la experiencia humana con modelos de Machine Learning con IA avanzados y herramientas de detección y respuesta ampliadas (XDR), los analistas de seguridad pueden sacar partido de las señales de las tecnologías de seguridad y TI para detectar, investigar y neutralizar incluso los ataques más avanzados realizados por humanos, impidiendo así el ransomware y las filtraciones de datos.

Aunque la detección y respuesta a amenazas 24/7 ha pasado a ser una parte fundamental de cualquier pila de ciberseguridad, la mayoría de las organizaciones tiene dificultades para llevarla a cabo con eficacia, lo que las deja expuestas a los ataques. Los dos obstáculos más frecuentes para lograr el éxito son la falta de experiencia y la falta de capacidad.

Reto n.º 1: la falta de experiencia

La detección, investigación y respuesta a las amenazas es una actividad muy especializada que requiere un profundo conocimiento de las técnicas de ataque y las estrategias de investigación, además de un buen dominio de las herramientas usadas por los encargados de la seguridad. Pocas organizaciones disponen internamente de este complejo (y costoso) repertorio de habilidades, y el 93 % admite que realizar las tareas esenciales de las operaciones de seguridad les resulta todo un reto:

- Según el 71 %, es difícil distinguir las señales del ruido (es decir, saber qué señales o alertas hay que investigar)
- Según el 71 %, es difícil obtener datos suficientes para determinar si una señal es maliciosa o benigna
- Según el 75 %, es difícil identificar la causa raíz del incidente (es decir, cómo entró el adversario en la organización)

La magnitud del reto queda patente cuando se observan los datos que los responsables de la defensa reciben de sus herramientas de ciberseguridad. Esta tabla contiene una lista no exhaustiva de eventos de Microsoft Defender, así como la categoría del evento.

Entender las alertas es solo una parte del proceso de detección y respuesta: los equipos de seguridad tienen que aplicar datos contextuales e información sobre las amenazas para poder comprenderlas del todo e identificar la mejor forma de actuar.

TÍTULO DEL EVENTO	TIPO DE EVENTO
URL sospechosa pulsada	Acceso inicial
Archivos maliciosos o conexiones de red asociadas con el proceso 3CXDesktopApp.exe	Malware
Nueva cuenta de usuario creada	Persistencia
TS_BL_Borrado o configuración del registro de eventos sospechosos mediante Wevtutil	Evasión de defensa
Aumento de privilegios de procesos	Aumento de privilegios
Intento de desactivar la protección antivirus de Microsoft Defender	Evasión de defensa
Se ha detectado un archivo o una conexión de red relacionados con el ciberdelincuente Storm-0867	Acceso a credenciales
TS_BL_Motores de script que se conectan a Internet	Comando y control
Posible actividad maliciosa operada por humanos	Actividad sospechosa
TS_BL_Descarga de carga maliciosa a través de binarios de Office	Ejecución
Detectado el grupo de actividad de amenazas emergentes DEV-0867	Acceso a credenciales
Detectado el grupo de actividad de amenazas emergentes Citrine Sleet	Malware

Ejemplo de detecciones de creación de casos de Microsoft Defender

Reto n.º 2: la falta de capacidad

La detección, investigación y respuesta a las amenazas es una actividad que requiere mucho tiempo. Para ilustrar este punto, la mediana de tiempo para detectar, investigar y responder a una alerta es de 9 horas en organizaciones con entre 100 y 3000 empleados, y de 15 horas en las que tienen entre 3001 y 5000 empleados.

Ocuparse de las alertas de seguridad consume una enorme cantidad de horas de TI, y la urgencia del trabajo puede impedir que los equipos se centren en retos más estratégicos. Además, los adversarios ejecutan los ataques a cualquier hora del día o de la noche, por lo que la detección y la respuesta a amenazas deben realizarse 24/7/365 para obtener los mejores resultados. Muchas organizaciones, si no la mayoría, tienen dificultades para disponer de los recursos necesarios.

Solución: complementar las defensas con Managed Detection and Response (MDR)

El 52 % de los responsables de TI/ciberseguridad afirman que las ciberamenazas son demasiado avanzadas para que su organización las gestione por sí sola, por lo que recurren cada vez más a proveedores especializados en detección y respuesta gestionadas, como Sophos, para complementar y ampliar sus capacidades internas.

Qué es la MDR

La detección y respuesta gestionadas (MDR) es un servicio 24/7 totalmente gestionado prestado por expertos especializados en detectar y responder a los ciberataques que las soluciones tecnológicas por sí solas no pueden detener.

La detección y respuesta ampliadas (XDR) es una plataforma que unifica los datos de seguridad procedentes de múltiples fuentes para automatizar y acelerar la detección, investigación y respuesta a las amenazas de formas que no pueden conseguir las soluciones independientes aisladas.

Los analistas de Sophos MDR se sirven de la plataforma Sophos XDR para buscar, investigar y neutralizar amenazas en su nombre. Utilizan señales de toda la pila de TI, incluidas las soluciones de seguridad de firewalls, correo electrónico, la nube y dispositivos móviles, para acelerar la detección y respuesta a las amenazas.

Refuerce Microsoft Defender con Sophos MDR

Sophos MDR ofrece detección y respuesta a amenazas 24/7 para entornos Microsoft Defender. Los analistas de Sophos monitorizan, priorizan y responden 24/7 a las alertas de seguridad de Microsoft y toman medidas inmediatas para frenar las amenazas confirmadas. También utilizan detecciones propias de Sophos, información sobre amenazas y búsquedas de amenazas realizadas por humanos para detectar y detener los ataques perpetrados por humanos más allá de Microsoft Defender.

Cuanto más vemos, más rápido actuamos. Sophos MDR se sirve de los orígenes de eventos de seguridad adicionales de Microsoft incluidos en las licencias E3 y E5, así como de señales de soluciones de firewall, la nube, correo electrónico, identidad y detección y respuesta de red (NDR) de terceros, para optimizar la detección y respuesta a amenazas.

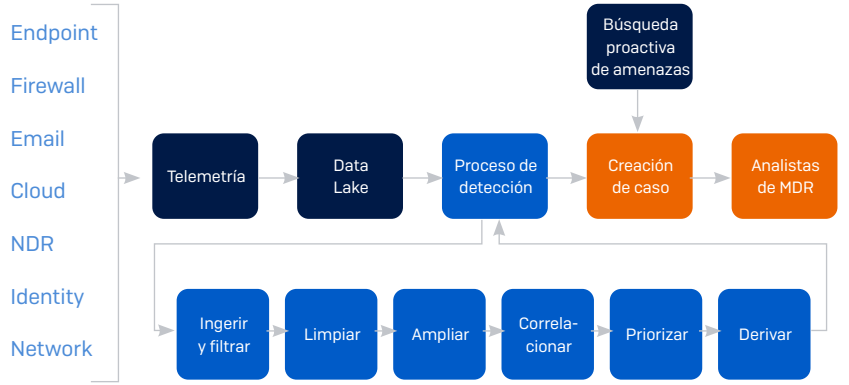
Los usuarios de Microsoft Defender tienen acceso inmediato e ininterrumpido a los expertos en operaciones de seguridad de Sophos por teléfono, así como a informes detallados sobre la actividad de las amenazas en la plataforma Sophos Central.

Sophos MDR para Microsoft Defender es compatible con los orígenes de eventos de seguridad de Microsoft

- Microsoft Defender para punto de conexión
- Microsoft Defender for Identity
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Identity Protection (Azure AD)
- Centro de seguridad y cumplimiento de MS 0365
- Microsoft Azure Sentinel
- Actividad de administración de Office 365 (registro de auditoría unificado)

Sophos MDR Security Event Flow

Nuestro Security Event Flow patentado es un elemento clave del servicio Sophos MDR. La telemetría de todo el entorno de seguridad, incluido Microsoft Defender, llega a Sophos Data Lake, donde se procesa, y los enormes volúmenes de alertas de Microsoft y de terceros se convierten en información útil y priorizada que nos permite investigar y responder con eficacia.



Sophos MDR Security Event Flow

Ingerir y filtrar: se ingiere la telemetría y se filtra el ruido no deseado

Limpiar: los datos se transforman en un esquema normalizado y se asignan a MITRE ATT&CK®

Ampliar: se añade información adicional de terceros sobre amenazas y contexto empresarial

Correlacionar: se agrupan las alertas en función de las entidades, la categorización de MITRE ATT&CK y la hora

Priorizar: se puntúan las alertas y los grupos de alertas para clasificarlos por orden de prioridad

Derivar: se aplica la lógica para derivar grupos de alertas a fin de que se investiguen

Cobertura 24/7 desde siete centros de operaciones de seguridad (SOC)

Las amenazas las investiga y remedia un equipo global de expertos en detección y respuesta a amenazas basados en siete centros de operaciones de seguridad (SOC) globales repartidos por Norteamérica (Indiana, Utah, Hawái), Europa (Reino Unido/Irlanda, Alemania) y Asia-Pacífico (India, Australia). Con más de 500 expertos que abarcan todo el entorno de amenazas, incluidos expertos en malware, automatización, IA y remediación, Sophos MDR tiene una amplia y profunda experiencia que es casi imposible de reproducir internamente.

Tiempos de detección y respuesta líderes en el mundo

Esta combinación única de experiencia humana, tecnológica y en amenazas permite a Sophos MDR ofrecer un tiempo de respuesta a incidentes único en el mundo de tan solo 38 minutos que, a su vez, ofrece resultados superiores en ciberseguridad:

- Tiempo medio de detección (MTTD): 1 minuto
- Tiempo medio de investigación (MTTI): 25 minutos
- Tiempo medio de respuesta (MTTR): 12 minutos

Quién usa Sophos MDR

Miles de organizaciones de todos los sectores utilizan el servicio Sophos MDR, desde pequeñas empresas con recursos de TI limitados hasta grandes compañías con equipos de SOC internos. Los tres modelos de respuesta de Sophos MDR más populares son:

- Sophos MDR gestiona totalmente la respuesta a amenazas en nombre del cliente
- Sophos MDR trabaja en colaboración con el equipo interno para gestionar la respuesta a amenazas
- Sophos MDR da soporte y complementa al equipo interno, alertándoles de incidentes que requieren atención y ofreciendo información sobre amenazas y orientación para remediarlas

Caso de amenaza: uso de Microsoft Defender para detectar un intento de comando y control

SECTOR
Servicios profesionales

SEDE CENTRAL
Estados Unidos

EMPLEADOS
750

NIVEL DE SERVICIO
Sophos MDR para Microsoft Defender

FUENTES DE TELEMETRÍA INTEGRADAS CON SOPHOS MDR

- ✓ Endpoint
- X Identity
- ✓ Firewall
- X Cloud
- X Email
- ✓ Network

¿Qué es comando y control?

El comando y control (también llamado C&C o C2) consiste en técnicas que utilizan los atacantes para comunicarse y enviar comandos a sistemas bajo su control dentro de la red de una víctima.

Los canales de comando y control entre un entorno comprometido y la infraestructura del atacante pueden establecerse de varias formas, por ejemplo, a través de correos electrónicos de phishing, ingeniería social, malware, vulnerabilidades en los complementos de los navegadores, etc. Los ciberdelincuentes suelen utilizar recursos de uso común e imitan el tráfico de red habitual para evitar ser detectados y levantar sospechas.

DETECCIÓN

Microsoft Defender genera una alerta por comunicación a una dirección IP maliciosa.

La alerta de Microsoft se correlaciona automáticamente con los eventos en Sophos XDR Data Lake para determinar si el ataque ha sido bloqueado por el firewall del cliente y si afecta a varios endpoints.

INVESTIGACIÓN

Los analistas de Sophos MDR confirman que la conexión maliciosa asociada a la alerta de Microsoft Defender ha sido bloqueada y la amenaza inmediata está contenida.

Se usa SophosLabs Intelix para identificar la familia de ese ataque, los indicadores de peligro (IOC) y las IP y los dominios conocidos utilizados por el atacante.

La alerta original de Microsoft se enriquece con esta información sobre amenazas para que pueda utilizarse en el análisis de la causa raíz.

RESPUESTA

Se aísla el dispositivo comprometido y se contiene el ataque.

Sophos MDR confirma que el acceso inicial se obtuvo mediante un correo electrónico de phishing. Se lleva a cabo una investigación para identificar la composición del correo electrónico de phishing y garantizar que ninguna otra cuenta de usuario se vea comprometida.

Sophos ofrece recomendaciones para reducir la probabilidad de éxito de los ataques de phishing en el futuro.

Ventajas para los clientes

Tanto si desea complementar y dar soporte a su equipo interno de operaciones de seguridad como si desea beneficiarse de una detección y respuesta 24/7 a cargo de expertos sin la carga operativa de montar su propio SOC, Sophos MDR puede ayudarle. Las organizaciones que refuerzan Microsoft Defender con Sophos MDR consiguen resultados superiores: reducen el ciberriesgo, aumentan la eficacia y el impacto de las inversiones en seguridad y mejoran la asegurabilidad.

Detenga las amenazas avanzadas con Microsoft + Sophos MDR

Monitorización y respuesta 24/7 a cargo de un equipo de expertos
Los analistas de Sophos MDR monitorizan, priorizan y responden a las alertas de Microsoft Defender 24/7 y toman medidas inmediatas para frenar las amenazas confirmadas

Detecte y detenga las amenazas que burlan Microsoft Defender
Las detecciones propias de Sophos, información sobre amenazas y búsquedas de amenazas realizadas por humanos añaden capas adicionales de defensa

Mejore la visibilidad y contextualice las alertas de Microsoft Defender
Integre orígenes de eventos de seguridad de Microsoft adicionales incluidos en su licencia E3 o E5

Obtenga acceso inmediato a expertos en operaciones de seguridad
Los analistas de Sophos MDR están disponibles por teléfono 24/7, y los informes detallados sobre la actividad de las amenazas están disponibles en Sophos Central

Reducir el ciberriesgo

Una de las principales ventajas de reforzar Microsoft Defender con Sophos MDR es una protección superior contra el ransomware y otras ciberamenazas avanzadas.

Los analistas de Sophos tienen una amplia y profunda experiencia, además de un dominio de las herramientas de telemetría y búsqueda de amenazas casi imposible de reproducir internamente. De esta forma, pueden responder con rapidez y precisión en todas las fases del proceso, desde la identificación de señales relevantes hasta la investigación de posibles incidentes y la neutralización de actividades maliciosas.

Sophos MDR protege a más organizaciones que ningún otro proveedor, lo que nos permite ofrecer una "inmunidad comunitaria" sin igual. La información que se obtiene al defender a un cliente se aplica automáticamente a todos los demás con un perfil similar, lo que nos permite prevenir ataques similares de forma proactiva en esa comunidad.

★★★★★

"Los técnicos de pruebas de penetración se sorprendieron enormemente de que no lograron entrar de ninguna manera. En ese punto supimos que podíamos confiar plenamente en el servicio de Sophos".
University of South Queensland, Australia

★★★★★

"Con Sophos MDR, hemos reducido nuestro tiempo de respuesta a amenazas drásticamente".
Tata BlueScope Steel, India

★★★★★

"Recibimos notificaciones de cualquier amenaza en tiempo real".
Bardiani Valvole, Italia

Aumentar la eficacia y el impacto de las inversiones en seguridad

Sophos MDR le permite incrementar la eficacia y el efecto de su personal y sus herramientas de seguridad.

La detección y respuesta a las amenazas consume grandes cantidades de recursos de TI. Sophos MDR asume esta carga, lo que libera valiosos recursos de TI para la ejecución de programas estratégicos. Paralelamente, el acceso telefónico 24/7 a los expertos en operaciones de seguridad de Sophos y los informes detallados sobre la actividad de las amenazas a través de la plataforma Sophos Central agilizan la labor de los equipos internos al permitirles responder con mayor rapidez y precisión a las alertas.

Al utilizar la telemetría de sus herramientas de seguridad existentes de Microsoft y de terceros para acelerar la detección y la respuesta ante amenazas, Sophos MDR eleva sus defensas a la vez que le permite aumentar el rendimiento de sus inversiones actuales.

Además, dado que la factura media para remediar un ataque de ransomware asciende actualmente a 1,85 millones USD y que el 84 % de las víctimas de ransomware afirman que el ataque les ocasionó pérdidas de negocio/ingresos[2], invertir en un servicio como Sophos MDR reduce el coste total de propiedad (TCO) global de la ciberseguridad.

★★★★★

"Desde que implementamos Sophos, hemos logrado liberar un número importante de horas operativas, lo que ha permitido a nuestros equipos centrarse en iniciativas que han incrementado la satisfacción de nuestros estudiantes".

London South Bank University, Reino Unido

★★★★★

"La capacidad de Sophos MDR para remediar o eliminar amenazas de forma rápida y alertarnos sobre ellas nos libera para que podamos centrarnos en tareas de alto valor".

Tomago Aluminium, Australia

2 El estado del ransomware 2023, Sophos.

Mejorar la asegurabilidad

Sophos MDR permite a las organizaciones cumplir muchos de los requisitos de control cibernético esenciales para garantizar la asegurabilidad y mejores ofertas de pólizas, como la detección y respuesta 24/7, la planificación de la respuesta a ciberincidentes, el registro y la supervisión, y mucho más.

Los clientes afirman haber mejorado el acceso a la cobertura de ciberseguridad, así como a pólizas que reconozcan y recompensen el hecho de haber reducido sus ciberriesgos.

★★★★★

"Nuestra decisión de asociarnos con Sophos para XDR y MDR fue un factor importante para conseguir una reducción de las primas de ciberseguridad frente a lo que nos dijeron al principio, que habría supuesto duplicarlas. Es una gran victoria que demuestra un valor real... De hecho, recibí un mensaje del director financiero dando las gracias al equipo por lo que habíamos conseguido, y MDR fue una parte importante de ello".

Bob Pellerin, CISO, The Fresh Market, Estados Unidos

El servicio MDR en el que más confía el mundo

Sophos es el primer proveedor de MDR del mundo, ya que protege a más organizaciones que cualquier otro proveedor contra el ransomware, las filtraciones y otras amenazas que la tecnología por sí sola no puede detener.

Sophos MDR protege a miles de organizaciones de todos los sectores en todo el mundo, lo que nos aporta una experiencia con una profundidad y amplitud sin precedentes sobre las amenazas a las que se enfrentan los distintos sectores. Nos servimos de esta extensa telemetría para generar "inmunidad comunitaria", aplicando lo aprendido al proteger a una organización a todos los demás clientes de un perfil similar, reforzando así las defensas de todos.

Por supuesto, lo que más importa son los resultados de ciberseguridad que ofrecemos a nuestros clientes. Sophos es la solución MDR mejor valorada y con más reseñas en Gartner® Peer Insights™, con una puntuación de 4,8/5 en 300 reseñas a 14 de junio de 2023 y un 97 % de clientes que afirman que nos recomendarían.

Sophos también ha sido nombrado Líder en el informe G2 Grid® de detección y respuesta gestionadas, además de ser nombrado Líder para MDR en los segmentos de G2 General, Medianas empresas y Grandes empresas.

Para obtener más información sobre Sophos MDR y cómo permite a los usuarios de Microsoft Defender reducir los ciberriesgos, aumentar la eficacia y el impacto de las inversiones en seguridad y mejorar la asegurabilidad, visite es.sophos.com/mdr

El más utilizado

Más de 17 000 organizaciones usan Sophos MDR [T2, 2023]

El mejor valorado

Puntuación de clientes independientes de 4,8/5

Con más reseñas

300 reseñas en Gartner Peer Insights en los últimos 12 meses

Explore Sophos Endpoint Protection

Sophos Intercept X Endpoint Protection trabaja para su empresa y con su empresa, adaptando sus defensas en respuesta a un ataque.

Cuenta con una potente protección multicapa que ofrece una protección superior contra el ransomware y las amenazas avanzadas en todas las fases de la cadena de ataque, incluida la reversión del ransomware basada en el comportamiento y 60 mitigaciones de exploits que vienen activadas por defecto, sin necesidad de realizar ajustes.

Nuestra innovadora función Adaptive Attack Protection responde dinámicamente a un ataque perpetrado por humanos, desplegando automáticamente defensas adicionales para frustrar al adversario y dar tiempo a los responsables de la seguridad para responder.

Los usuarios del servicio Sophos MDR que utilicen Microsoft Defender pueden pasarse a Sophos Endpoint Protection en cualquier momento, lo que les ofrece una flexibilidad total a la vez que prepara sus despliegues de seguridad para el futuro.

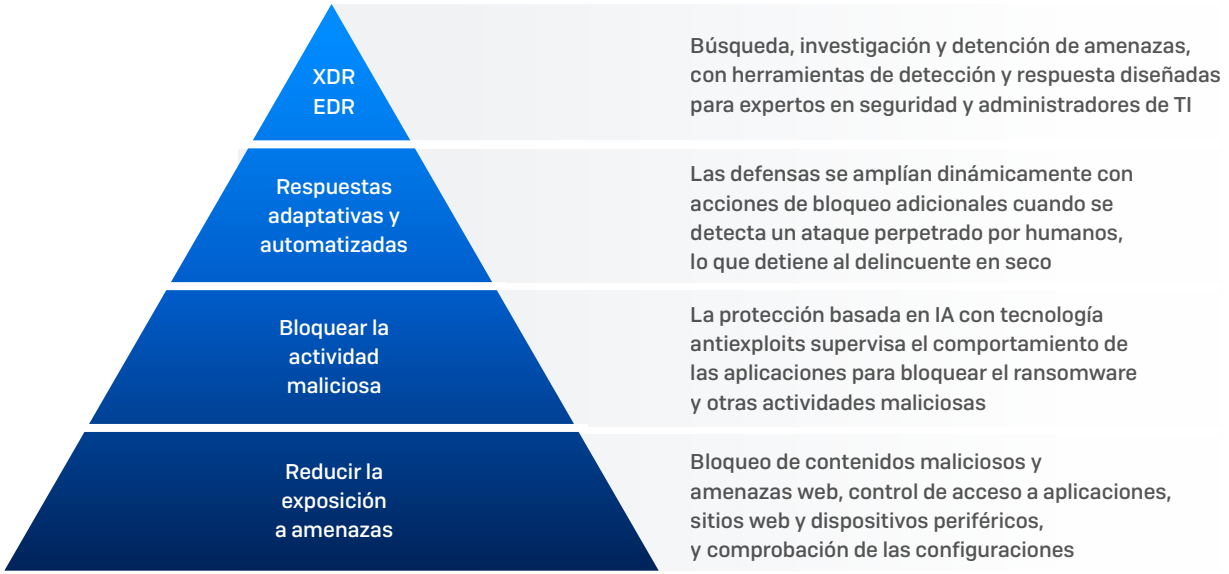
✓ Líder de Gartner en 13 informes consecutivos
Sophos ha sido nombrado líder en el Magic Quadrant de Gartner de plataformas de protección de endpoints en todos los informes desde 2008

✓ Proveedor mejor valorado en Gartner Peer Insights
Puntuación de clientes independientes de 4,8/5

✓ Líder en los informes G2 Grid para grandes empresas, medianas empresas y pymes
Basado exclusivamente en las opiniones de los clientes

✓ Puntuación de protección del 100 % – SE Labs
Calificación AAA en seguridad para grandes empresas y pymes

Para obtener más información o realizar una evaluación gratuita, visite es.sophos.com/endpoint



Gartner, Magic Quadrant de plataformas de protección de endpoints; Peter Firstbrook, Chris Silva, 31 de diciembre de 2022
GARTNER es una marca de servicio y marca registrada de Gartner, Inc. y/o asociados en EE. UU. y en otros países, y Magic Quadrant y PEER INSIGHTS son marcas registradas de Gartner, Inc. y/o asociados y se utilizan aquí con permiso. Reservados todos los derechos. Gartner no apoya a ninguna compañía, producto o servicio mencionado en los estudios publicados y no aconseja a los usuarios de tecnologías que elijan solamente a los proveedores con las clasificaciones más altas. Los estudios publicados por Gartner están compuestos por las opiniones de su equipo de investigaciones y no deben considerarse declaraciones de hecho. Gartner renuncia a todas las responsabilidades, explícitas o implícitas, con respecto a este estudio, incluida cualquier garantía de comercialización o conveniencia para fines particulares.
El contenido de Gartner Peer Insights consiste en las opiniones de usuarios finales individuales basadas en sus propias experiencias; no deben considerarse declaraciones de hecho, ni representan las opiniones de Gartner ni de sus afiliados. Gartner no apoya a ningún proveedor, producto o servicio descrito en este contenido ni ofrece ninguna garantía, expresa o implícita, con respecto a este contenido, sobre su exactitud o integridad, incluida cualquier garantía de comercialización o conveniencia para fines particulares.

Sophos ofrece soluciones de ciberseguridad líderes en el sector a empresas de todos los tamaños, protegiéndolas en tiempo real de amenazas avanzadas como el malware, el ransomware y el phishing. Gracias a nuestras funcionalidades next-gen probadas, los datos de su organización estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.

2023-07-12-ES (WP-NP)

SOPHOS