SOPHOS

Guía para la adquisición de seguridad para endpoints

A medida que las ciberamenazas se vuelven más complejas, aumenta la presión para dar con la solución para endpoints más adecuada. Sin embargo, el mercado de la seguridad para endpoints se ha visto saturado con tantas soluciones distintas y tantos reclamos de marketing carentes de fundamento que tomar una decisión informada para su organización es cada vez más difícil.

Esta guía confiere claridad al describir las funciones clave de una solución de protección para endpoints y lo que necesita para protegerse contra las amenazas avanzadas actuales. Al disponer de todos estos datos, podrá tomar una decisión más informada para su organización.

Monográficos de Sophos. Junio de 2024

El panorama actual de amenazas a la seguridad

Nuestra encuesta independiente a 3000 responsables de TI/ciberseguridad en 14 países ha revelado que la realidad actual es una carrera de ciberseguridad a dos velocidades en que los adversarios y los encargados de la seguridad se mueven a ritmos distintos. Frenados por múltiples vientos en contra, los responsables de la seguridad se están quedando rezagados mientras los adversarios están acelerando.

La evolución de la economía de la ciberdelincuencia

En los últimos años, uno de los cambios más significativos en el panorama de las amenazas ha sido la transformación de la economía de la ciberdelincuencia en una industria con una red de servicios de apoyo y enfoques operativos consolidados y profesionalizados.

A medida que las empresas tecnológicas se han ido decantando por las soluciones "como servicio", el ecosistema de los ciberdelitos ha hecho lo mismo. Esto ha rebajado las barreras de entrada para los ciberdelincuentes en potencia y les ha permitido multiplicar el volumen, la velocidad y el impacto de sus ataques.

En consecuencia, los adversarios ahora pueden ejecutar una amplia variedad de ataques sofisticados a escala. El 94 % de las organizaciones sufrieron un ciberataque en el último año. Aunque el ransomware fue el ataque más citado, las organizaciones se vieron afectadas por muchos otros tipos de amenazas, entre ellas:[1]

27 %	**27 %**	**26 %**
Correo malicioso	Phishing (incluido el spear phishing)	Exfiltración de datos (por el atacante)
24 %	**24 %**	**21 %**
Ciberextorsión	Estafas por correo electrónico corporativo comprometido	Malware para móviles
18 %	**24 %**	**14 %**
Criptomineros	Denegación de servicio (DDoS)	Wipers

Lea nuestro informe, El estado de la ciberseguridad 2023: el impacto de los adversarios en el negocio,, para obtener más información.

El ransomware sigue asediando a las organizaciones

Por lo que respecta al ransomware, el 59 % de las organizaciones afirman que sufrieron un ataque en el último año.

2020	2021	2022	2023	2024
51 %	37 %	66 %	66 %	59 %

En el último año, ¿se ha visto afectada su organización por el ransomware? Sí. n=5000 (2024), 3000 (2023), 5600 (2022), 5400 (2021), 5000 (2020).

Mientras que el índice de ataques registrados en 2024 se ha reducido en comparación con la cifra de 2023, el cifrado de datos como consecuencia del ransomware sigue en un nivel alto: los adversarios lograron cifrar datos en el 70 % de los ataques.

Por otra parte, el ransomware se ha vuelto más costoso que nunca, ya que las organizaciones afirman que el coste medio de recuperación asciende a 2,73 millones USD, lo que supone un aumento con respecto a los 1,82 millones USD registrados en 2023.[2]

Para conocer la realidad a la que se enfrentan las organizaciones en 2024, incluidos datos como la frecuencia, el coste y la causa raíz de los ataques, lea nuestro estudio anual El estado del ransomware 2024.

1 El estado de la ciberseguridad 2023: el impacto de los adversarios en el negocio, Sophos. Estudio independiente a 3000 responsables de TI/ciberseguridad en 14 países realizado entre enero y febrero de 2023.

2 El estado del ransomware 2024, Sophos. Estudio independiente y desvinculado de cualquier proveedor de 5000 responsables de TI/ciberseguridad en 14 países realizado entre enero y febrero de 2024.

Las estrategias de ciberseguridad antiguas no dan buenos resultados

En los últimos años, el entorno empresarial ha cambiado para muchas organizaciones. Los usuarios finales pueden estar en la oficina, trabajar a distancia o desplazarse continuamente entre clientes y Partners. Los datos de la empresa ya no se almacenan únicamente in situ, sino que pueden guardarse localmente, en la nube y en los dispositivos de los usuarios finales; además, se accede a ellos local y remotamente para atender las necesidades de los empleados geográficamente dispersos. En consecuencia, de seguir aplicando estrategias de ciberseguridad antiguas, los resultados no serán satisfactorios.

Algunos de los problemas más comunes para los equipos de seguridad TI son:

- **Escasez de conocimientos:** sigue siendo difícil contratar a empleados especializados en TI. La falta de experiencia significa que los empleados pueden no tener las habilidades para determinar si una alerta de seguridad es maliciosa o benigna.
- **Exceso de ruido:** el hecho de recibir demasiadas alertas de muchos sistemas diferentes abruma al personal de TI, que a menudo no sabe cómo priorizar qué señales/alertas investigar, con lo que puede pasar por alto indicadores de un ataque.
- **Datos aislados:** las señales/alertas de amenazas se limitan a tecnologías específicas, lo que impide a los equipos de TI obtener una visión de conjunto y remediar las alertas o incidentes maliciosos con prontitud.
- **Falta de integración:** las herramientas de seguridad no se integran entre sí ni con la infraestructura de TI de la empresa, lo que aumenta la complejidad.
- **Procesos manuales:** los equipos de TI dedican muchas horas a correlacionar eventos, registros e información para comprender lo que está ocurriendo. Este esfuerzo retrasa la identificación y la respuesta a los ataques.
- **Respuesta reactiva:** debido a los factores anteriores, muchos equipos de TI se encuentran a la zaga, respondiendo a las amenazas solo después de que hayan causado daños en lugar de detenerlas en una fase más temprana de la cadena de ataque.
- **Centrarse en los imprevistos:** la labor diaria para detener las amenazas impide mejoras a largo plazo. Cuando los equipos de TI están apagando fuegos, a menudo no tienen la ocasión de identificar la causa raíz del incidente, ni de mantener registros precisos del ataque y de las medidas adoptadas. Esto dificulta los intentos de abordar los problemas estructurales.
- **Datos distribuidos:** los usuarios y los dispositivos están en todas partes. En consecuencia, los datos también lo están: en las instalaciones, en la nube y en los dispositivos, además de accederse a ellos localmente y a través de soluciones de acceso remoto.

Una forma de contrarrestar muchos de estos retos es desplegar una solución de protección para endpoints de primera clase.

Aspectos fundamentales de la protección para endpoints

Las soluciones de protección para endpoints deben trabajar con y para usted, adaptando sus defensas en respuesta a un ataque. Cuanto menos, una solución de seguridad para endpoints moderna debe priorizar la prevención para:

Reducir la exposición a las amenazas: bloquea el contenido malicioso y las amenazas web, y controla el acceso a aplicaciones, sitios web, dispositivos periféricos, etc.

Bloquear la actividad maliciosa: previene la explotación y las técnicas que los programadores maliciosos y el ransomware utilizan para lograr sus objetivos, identificando esta actividad específica y deteniéndola antes de que se convierta en un problema.

Proporcionar respuestas adaptativas y automatizadas: sus defensas deben responder automáticamente a las amenazas y adaptarse a los cambios de comportamiento de los atacantes. Esto no solo desestabiliza a un adversario, sino que también puede alertar al equipo de TI de su presencia y proporcionarle un tiempo valioso para que responda.

Facilitar la búsqueda de amenazas (interna o gestionada): las señales de alta calidad mejoradas con datos clave de seguridad pueden agilizar enormemente la detección de amenazas y la respuesta a las mismas. Cuanto mejores sean los datos que se aporten, más rápida será la resolución.

Obtención de resultados de seguridad óptimos

Hemos señalado las funciones que debe cumplir una solución de protección para endpoints, pero es esencial tener una visión más amplia de cómo puede beneficiar a su organización. Una protección para endpoints sólida debe permitir obtener unos resultados óptimos en materia de seguridad.

Reducción del ciberriesgo

Una protección para endpoints sólida reduce su ciberriesgo y le protege de un sinfín de ciberamenazas.

Una estrategia centrada en la prevención

Cuanto antes detenga un ataque, menos trabajo tendrá que hacer después. Una protección para endpoints superior utiliza varias capas de defensa para combatir las ciberamenazas y los ataques dirigidos a ordenadores, portátiles, dispositivos móviles y servidores. La protección para endpoints blinda estos dispositivos y sus datos frente al malware, los virus, el ransomware y otras actividades maliciosas.

Identificación de desviaciones de la postura de seguridad

La postura de seguridad se alterará con el tiempo por una serie de razones. En una reciente encuesta desvinculada de cualquier proveedor, los errores de configuración de las herramientas de seguridad fueron el principal riesgo de seguridad percibido por los responsables de TI en 2023.[2]

Busque soluciones de seguridad para endpoints que evalúen constantemente su postura de seguridad y optimicen su configuración. Este enfoque automatizado es fundamental para lograr una postura de seguridad sólida, reducir su ciberriesgo y mitigar los quebraderos de cabeza que supone hacerlo manualmente.

Gestión optimizada

Una consola de administración centralizada permite a los administradores de TI supervisar y gestionar la configuración de seguridad, las políticas, las exclusiones y las alertas de amenazas en todos los endpoints desde una única ubicación. Esto simplifica la gestión de la seguridad, reduce el riesgo de errores de configuración y garantiza una protección uniforme. Algunas consolas de administración centralizada van un paso más allá: comprueban automáticamente el estado de seguridad de su postura y destacan cualquier actividad o cambio de política que pudiera ponerla en peligro.

Aceleración de la detección y la respuesta

Cada segundo cuenta cuando hay un adversario en su entorno. Una protección para endpoints de alta calidad que parta de un enfoque que priorice la prevención reduce la cantidad de ruido y ofrece alertas de alta fiabilidad. Las tecnologías de detección y respuesta para endpoints (EDR) y de detección y respuesta ampliadas (XDR) pueden utilizarse para investigar estas alertas.

Algunas soluciones van un poco más lejos y aprovechan la inteligencia artificial (IA) y la información sobre amenazas para priorizar automáticamente las detecciones. Estas soluciones garantizan que su equipo sepa dónde concentrar su tiempo y aceleran la respuesta a las amenazas realizada por humanos.

Aumento de la eficiencia de TI

El 64 % de las empresas quiere que sus equipos de TI dediquen menos tiempo a combatir ciberataques y más a cuestiones estratégicas.[3] Una protección para endpoints automatizada y fácil de usar ayuda a los equipos de TI a alcanzar este objetivo.

Las mejores soluciones para endpoints bloquean y limpian automáticamente la mayoría de las amenazas desde el principio. Esto reduce la carga de trabajo de TI, lo que permite a estos equipos priorizar las iniciativas empresariales. Tecnologías como XDR sirven para reducir la fatiga por excesivas señales y así liberar aún más tiempo para proyectos importantes.

En última instancia, este aumento de la eficiencia permite a los equipos de TI pasar de un enfoque reactivo a uno proactivo en materia de ciberseguridad. Da a estos equipos el tiempo necesario para buscar amenazas antes de que causen problemas a largo plazo, lo que a su vez también reduce el ciberriesgo.

2 El estado del ransomware 2024, Sophos. Estudio independiente y desvinculado de cualquier proveedor de 5000 responsables de TI/ciberseguridad en 14 países realizado entre enero y febrero de 2024.

3 El estado de la ciberseguridad 2023: el impacto de los adversarios en el negocio, Sophos. Estudio independiente a 3000 responsables de TI/ciberseguridad en 14 países realizado entre enero y febrero de 2023.

Mejora del retorno de la inversión en ciberseguridad

Una ciberseguridad sólida debe proteger a las organizaciones de las consecuencias financieras y operativas de un incidente de seguridad grave.

Invertir en una protección para endpoints de primer nivel es clave. La prevención, si se hace bien, cuesta mucho menos que la remediación. Una protección para endpoints robusta bloquea la mayoría de las amenazas desde el principio, lo que reduce la posibilidad de sufrir un ataque y tener que hacer frente a los costes que conlleva.

Además, las mejores soluciones de protección para endpoints pueden integrarse y comunicarse con sus actuales inversiones en seguridad para ampliar su protección, reducir la complejidad y hacer que sus tecnologías de protección existentes (correo electrónico, firewall, red, identidad y la nube) funcionen de forma más inteligente y eficaz que nunca.

Todos estos aspectos mejoran el retorno de la inversión en ciberseguridad al tiempo que reducen el coste total de propiedad.

Mejora de la posición frente a las ciberaseguradoras

En los últimos años, las primas de los ciberseguros han aumentado considerablemente y las solicitudes de pólizas se han vuelto más complejas y lentas. Las aseguradoras están exigiendo controles cibernéticos más estrictos; de hecho, el 95 % de las organizaciones que contrataron un seguro el año pasado afirmaron que la calidad de sus defensas afectó directamente a su posición en el mercado asegurador[4].

La clave para optimizar su posición frente a las aseguradoras es minimizar su ciberriesgo. Invertir en defensas sólidas, incluidos servicios de seguridad 24/7 y herramientas punteras de detección y respuesta, aporta múltiples ventajas para el seguro:

1. Facilita la contratación de un ciberseguro (es decir, mejora la asegurabilidad)
2. Ayuda a reducir las primas y a mejorar las condiciones
3. Reduce la probabilidad de una reclamación y el consiguiente aumento de las primas
4. Reduce el riesgo de impago en el caso de una reclamación

Las mejores tecnologías de protección para endpoints sirven de conducto para las capacidades de detección y respuesta; asegúrese de que los proveedores que le interesan las ofrecen. Ahora, la detección y respuesta para endpoints (EDR) es un requisito previo para obtener cobertura en la mayoría de las ciberseguradoras, y las organizaciones sin esta funcionalidad suelen tener dificultades para contratar una póliza.

Los servicios que optimizan la detección y la respuesta y, por tanto, minimizan el riesgo de que se produzca un ciberincidente, son considerados el criterio de referencia por las ciberseguradoras. En concreto, las organizaciones que utilizan servicios de detección y respuesta gestionadas (MDR) suelen ser consideradas clientes de "nivel 1" por las aseguradoras, ya que representan el nivel de riesgo más bajo.

Dicho esto, recomendamos buscar proveedores que ofrezcan la posibilidad de migrar fácilmente de una solución de protección para endpoints a un servicio de búsqueda y detección de amenazas y/o respuesta a incidentes totalmente gestionado 24/7 que se integre con los productos existentes y los controles de seguridad de terceros.

5 La vital importancia de las ciberdefensas de primera línea para la contratación de seguros - Sophos.

Evaluación de la seguridad para endpoints: las 10 principales preguntas que hacer

Ahora que tiene una idea más clara de los elementos que caracterizan a una solución de seguridad para endpoints de primera categoría, le sugerimos una serie de preguntas para plantear a un posible proveedor.

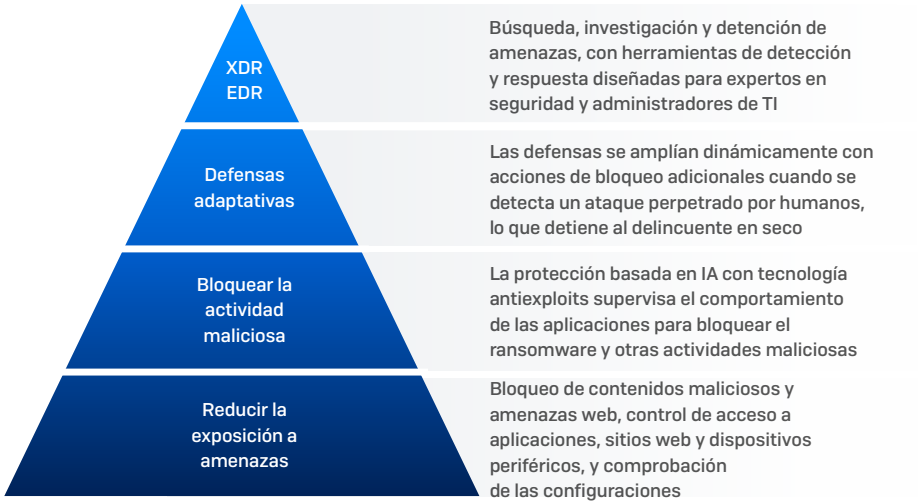
1. ¿El producto utiliza un enfoque multicapa que prioriza la prevención o bien uno que prima la detección? ¿Qué funciones específicas son fundamentales en la tecnología?
2. ¿Dispone de las funcionalidades necesarias para detectar y rectificar automáticamente una desviación de la postura de seguridad? ¿Puede alertar sobre los cambios en la configuración de las políticas que aumentan el riesgo?
3. ¿Responde automáticamente a las amenazas? ¿Puede limpiar una amenaza y responder a un incidente automáticamente?
4. ¿Tiene defensas que se adaptan automáticamente cuando se detecta un ataque manual directo?
5. ¿Ofrece funciones antiransomware y antiexploits sólidas, incluida la protección en tiempo real contra los ataques de ransomware remoto? ¿Están activadas por defecto? ¿Es necesario habilitarlas y entrenarlas para que funcionen en su entorno?
6. ¿Cuántas consolas se necesitan para gestionar el producto? ¿Son consolas alojadas en la nube o requieren una instalación local?
7. ¿Permite una transición fluida a EDR/XDR utilizando la misma consola de administración y el mismo agente en el endpoint/servidor?
8. ¿La funcionalidad XDR integra e incorpora alertas de controles de seguridad nativos y de terceros para ofrecer una visión completa del entorno?
9. ¿Ofrece la posibilidad de migrar fácilmente a un servicio de búsqueda y detección de amenazas y respuesta a incidentes totalmente gestionado 24/7 que se integre con los productos existentes y los controles de seguridad de terceros?
10. ¿Existen testimonios de organizaciones de pruebas de terceros, analistas y clientes que validen el enfoque a la seguridad para endpoints del proveedor?

El enfoque de Sophos

Veamos ahora el enfoque de Sophos a la protección para endpoints. Sophos Endpoint ofrece una protección inigualable frente a los ciberataques avanzados. Gracias a una protección hermética contra el ransomware y a una completa estrategia de defensa exhaustiva, detiene la más amplia variedad de amenazas antes de que afecten a sus sistemas. Nuestras potentes herramientas EDR y XDR permiten a su equipo buscar, investigar y responder a las amenazas con velocidad y precisión.

Estrategia centrada en la prevención

Sophos Endpoint adopta un enfoque integral para proteger todos los endpoints sin depender de una única técnica de seguridad. Al detener más amenazas de manera anticipada, los equipos de TI sobrecargados tienen menos incidentes que investigar y resolver.



Reducción de la exposición a amenazas

Sophos Endpoint reduce su exposición a amenazas y las oportunidades de los atacantes de penetrar en su entorno. Bloquea el contenido web malicioso y las amenazas web y le permite controlar el acceso a aplicaciones, sitios web y dispositivos periféricos.

Bloqueo de amenazas web y control del acceso web

Existen muchas amenazas basadas en la web. Las organizaciones suelen utilizar firewalls next-gen para proteger a los usuarios que trabajan desde la oficina contra el phishing, los sitios web maliciosos y otras amenazas web. Aunque esta medida blinda los endpoints en las redes de oficinas, los dispositivos pueden utilizarse en casa, de viaje, en una cafetería, etc., donde un firewall no puede protegerlos.

Sophos Endpoint bloquea el acceso a sitios web maliciosos y de phishing mediante el análisis de archivos, páginas web y direcciones IP. Garantiza la protección permanente de los endpoints frente a las amenazas, independientemente de su ubicación.

Además, SophosLabs y el equipo de Sophos MDR proporcionan información sobre amenazas en tiempo real para proteger a los clientes de Sophos contra las amenazas emergentes.

Control de la web, los periféricos y las aplicaciones

Sophos le permite restringir las actividades de los endpoints. Estos controles suelen utilizarse con la política de uso aceptable de la organización.

El primer control consiste en supervisar y/o bloquear el acceso a categorías de sitios web (juegos y apuestas, redes sociales, etc.). Sophos Endpoint le permite monitorizar y bloquear categorías de sitios web, aplicando el control dentro y fuera de las redes de la oficina.

Controlar el acceso a los medios extraíbles u otros dispositivos periféricos puede reducir aún más su superficie de ataque. Pensemos en las veces que un usuario conecta una impresora o un dispositivo de almacenamiento USB o carga su teléfono móvil desde un puerto USB. ¿Está permitida alguna de esas acciones? Esta funcionalidad no solo impide que un vector de ataque introduzca código malicioso en un endpoint, sino que también puede ayudar a bloquear la exfiltración de datos de la empresa.

Las aplicaciones son otra categoría que debe tenerse en cuenta. Con el control de aplicaciones, puede bloquear aplicaciones o complementos del navegador para que no se ejecuten en los dispositivos de trabajo. Siguiendo con el tema de la exfiltración de datos, piense en aplicaciones como OneDrive o Google Drive para el almacenamiento en la nube. Por otro lado, considere los programas de torrents, navegadores TOR, etc. y si debe permitir que se utilicen en los endpoints. Existe una gran variedad de complementos para navegadores web. Muchos de ellos tienen usos legítimos y útiles, pero otros no.

Bloqueo de la actividad maliciosa

La siguiente capa de defensa implica el uso de la inteligencia artificial, el análisis de comportamientos, funciones antiransomware y antiexploits y otras tecnologías para detener rápidamente las amenazas antes de que se agraven.

Sophos utiliza una protección centrada en la IA, empezando por la clasificación de ejecutables mediante IA. Utiliza un modelo entrenado con millones de ejecutables benignos y malignos. Este modelo puede identificar de forma rápida y eficaz los ejecutables maliciosos basándose en sus propiedades y no requiere ninguna firma.

Protección hermética contra el ransomware

Sophos Endpoint es la solución de protección de endpoints Zero Touch más sólida contra el ransomware local y remoto. Incluye la avanzada tecnología CryptoGuard, que detecta los indicios del cifrado, independientemente de su origen. Este enfoque universal detiene nuevas variantes y ransomware tanto local como remoto. Inspecciona los cambios en el contenido de los archivos en tiempo real para detectar el cifrado malicioso y bloquea el ransomware remoto que se ejecuta en un dispositivo distinto que intenta cifrar archivos en la red. Los archivos cifrados por el ransomware se revierten automáticamente a su estado no cifrado, independientemente del tamaño o el tipo de archivo. Esto minimiza las posibles repercusiones en la productividad de la empresa. También protege el registro de arranque maestro (MBR) del cifrado utilizado en algunos ataques de ransomware.

Antiexploits

La tecnología antiexploits detiene los comportamientos y las técnicas que usan los atacantes para infiltrarse en dispositivos, robar credenciales y distribuir malware. Sophos despliega innovadores enfoques antiexploits en el dispositivo a escala para todas las aplicaciones. Nada más instalarlo, Sophos amplía la protección básica ofrecida en Microsoft Windows al incorporar por lo menos 60 mitigaciones de exploits preconfiguradas y ajustadas propias. El resultado es que Sophos mantiene su organización segura contra los ataques sin archivos y los exploits de día cero al detener las técnicas utilizadas en toda la cadena de ataque.

Defensas adaptativas

Estas defensas dinámicas adicionales son una iniciativa pionera en el sector que ofrece una protección automatizada progresiva que se adapta al contexto de un ataque. 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.

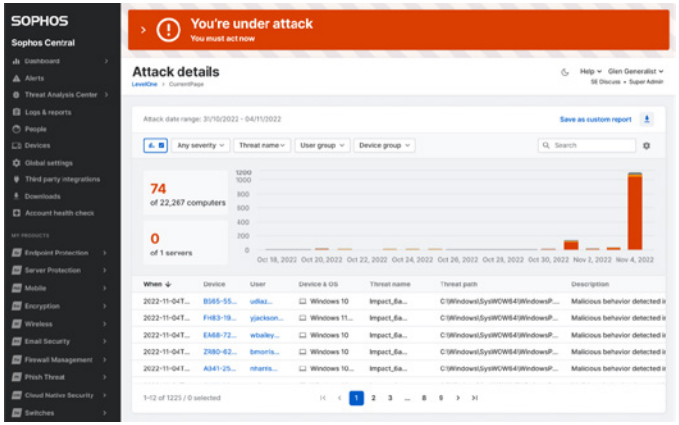
	PROTECCIÓN COMPORTAMENTAL	ADAPTIVE ATTACK PROTECTION	ADVERTENCIA DE ATAQUE CRÍTICO
ALCANCE	DISPOSITIVO INDIVIDUAL	DISPOSITIVO INDIVIDUAL	DISPOSITIVO INDIVIDUAL
VENTAJAS	El motor de comportamientos detiene las primeras fases de los ataques de adversarios activos	Incrementa la sensibilidad de la protección para evitar daños	Alerta al cliente 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!"

Adaptive Attack Protection

Adaptive Attack Protection activa dinámicamente el refuerzo de las defensas en un endpoint cuando se detecta un ataque manual directo. Esto elimina la capacidad del atacante de emprender nuevas acciones, minimiza la superficie de ataque, interrumpe y contiene el ataque y da tiempo a los responsables de la seguridad a responder.

Advertencia de ataque crítico

Una advertencia de ataque crítico le avisa de un ataque grave en toda la infraestructura si se detecta actividad de adversarios en varios endpoints o servidores del entorno con indicadores de gran impacto adicionales. Es una situación de alerta roja: está sufriendo un ataque. La tecnología automatizada le informa de la situación, proporcionándole el contexto y los detalles del ataque. Para responder, puede usar Sophos XDR, solicitar ayuda a su Partner o pedir al equipo de Sophos Incident Response que intervenga y le ayude a responder a la amenaza.



Reducción del coste total de propiedad de la ciberseguridad

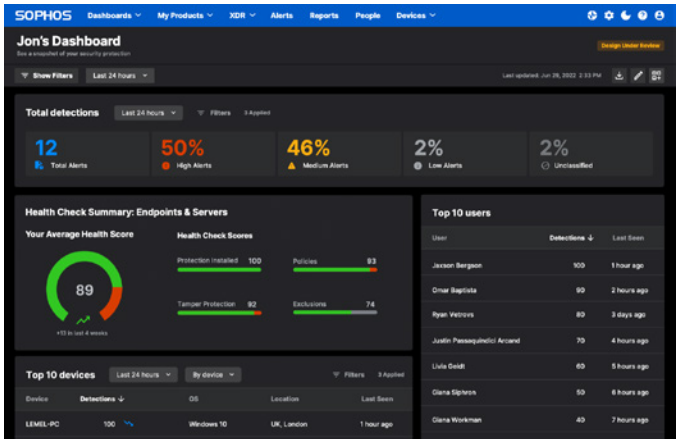
La mayoría de los equipos de TI y seguridad están desbordados. Automatizar y ahorrar tiempo y esfuerzo son cuestiones clave con Sophos Endpoint. Todo lo que pueda automatizarse, reducirse o eliminarse de la carga de trabajo de los equipos de TI y seguridad permite a estos equipos centrarse en otras iniciativas empresariales.

Sophos Central ofrece una plataforma de administración basada en la nube para gestionar sus productos de Sophos (endpoints, servidores, dispositivos móviles, firewalls, switches, puntos de acceso, correo electrónico y la nube), incluido Sophos Endpoint. Desde un mismo lugar, puede crear y gestionar políticas, ver detecciones y alertas, investigar y remediar posibles amenazas y realizar otras acciones en todos sus productos de Sophos.

Todas las tecnologías de protección recomendadas por Sophos están activadas por defecto, lo que garantiza una fácil configuración y que disponga inmediatamente de la máxima protección sin necesidad de realizar ajustes complejos. Si lo necesita, puede disponer de un control granular.

Identificación de desviaciones de la postura de seguridad

Con el tiempo, la postura de seguridad de una organización puede desviarse del cumplimiento o de la configuración óptima. Los parámetros de políticas mal configurados, las exclusiones y otros factores suponen riesgos para su postura de seguridad. La función Verificar estado de cuenta de Sophos 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.

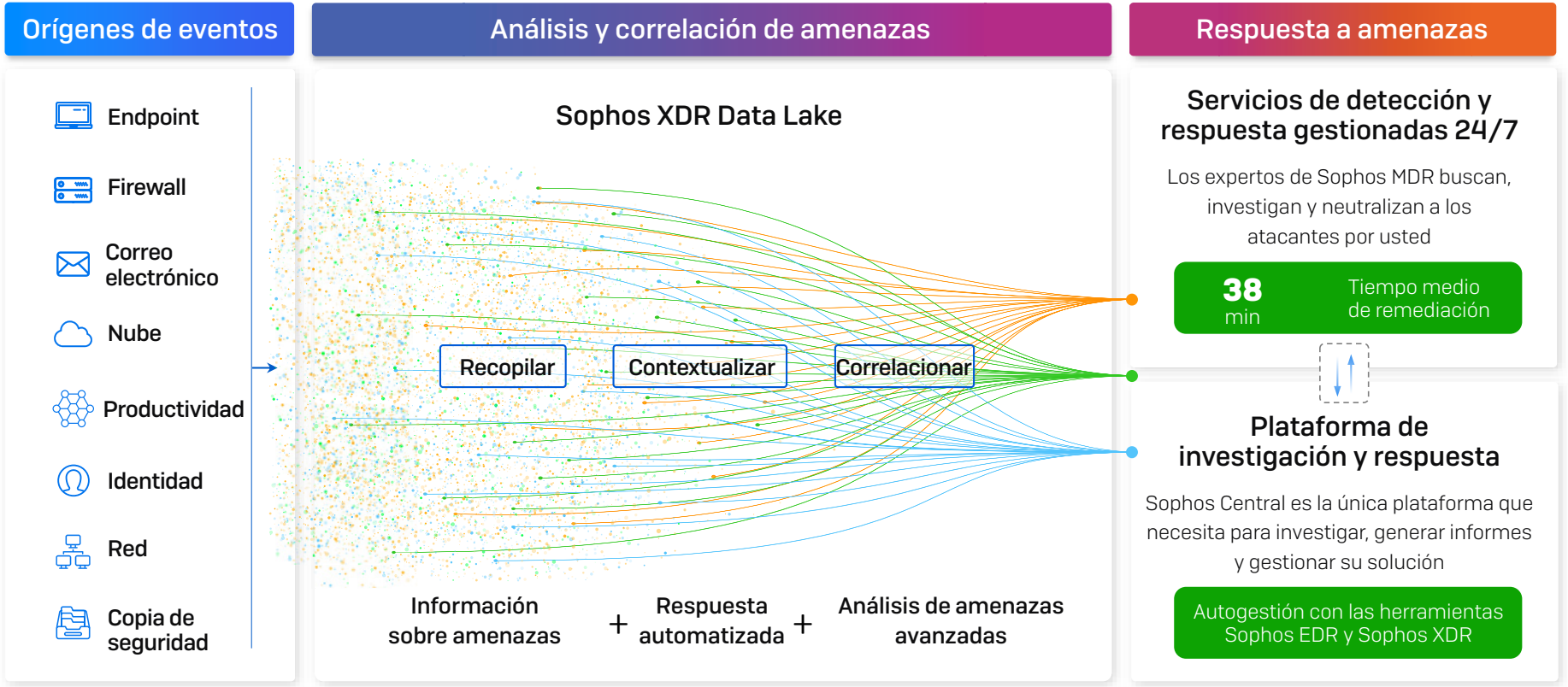


Seguridad Sincronizada

Las soluciones de Sophos funcionan mejor de forma conjunta. Sophos Endpoint comparte información sobre el estado de seguridad con Sophos Firewall, Sophos ZTNA y otros productos para proporcionar más visibilidad sobre las amenazas y el uso de las aplicaciones. La Seguridad Sincronizada aísla automáticamente los dispositivos comprometidos mientras se realiza la limpieza, y les devuelve el acceso a la red una vez neutralizada la amenaza, todo ello sin que intervenga ningún administrador.

Aceleración de la detección y la respuesta: EDR, XDR y MDR

La estrategia centrada en la prevención de Sophos bloquea y limpia automáticamente tantas amenazas como sea posible desde un primer momento, lo que significa que los equipos de TI y seguridad tendrán que investigar menos detecciones de alta fiabilidad más adelante.



El enfoque de Sophos a la prevención, la detección y la respuesta.

Sophos Endpoint Detection and Response (EDR)

Sophos integra potentes funciones de detección y respuesta con el sólido enfoque basado en la prevención de Sophos Endpoint, lo que le permite buscar, investigar y responder a actividades sospechosas en endpoints y servidores. Las detecciones se priorizan con análisis basados en IA, lo que le ayuda a identificar en qué debe invertir más tiempo y energía. Los técnicos pueden acceder a los dispositivos de forma remota para investigar problemas, instalar y desinstalar software y solucionar cualquier problema.

Sophos Extended Detection and Response (XDR)

Para las organizaciones que necesitan funciones más completas de detección y respuesta a amenazas, Sophos XDR les permite buscar, investigar y responder a actividades sospechosas y ataques de varias fases en todo su entorno de seguridad. Diseñada por y para analistas de seguridad, es la única herramienta de operaciones de seguridad del sector que reúne la telemetría de los controles de seguridad nativos de Sophos y de terceros para acelerar la detección y la respuesta. 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.

Sophos Managed Detection and Response (MDR)

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

Tanto Sophos XDR como Sophos MDR se adaptan a sus necesidades y se integran con sus inversiones tecnológicas actuales, como productos de correo electrónico, firewall, red, identidad y la nube, lo que le permite obtener una mayor rentabilidad de las inversiones ya realizadas.

Sophos Incident Response Services Retainer

Sophos Incident Response Services Retainer es una suscripción anual que da a los clientes de Endpoint, EDR y XDR acceso rápido a un equipo de expertos en respuesta a incidentes, con términos de servicio preacordados, para detener rápidamente los ataques activos y volver a la normalidad operativa.

¿Por qué Sophos?

Sophos es una empresa innovadora y líder mundial en soluciones avanzadas de ciberseguridad, que incluyen MDR, respuesta a incidentes y tecnologías de seguridad para endpoints, redes, correo electrónico y la nube que ayudan a las organizaciones a hacer frente a los ciberataques. Como uno de los mayores proveedores especializados en ciberseguridad, Sophos protege a más de 550 000 organizaciones y a más de 100 millones de usuarios de todo el mundo frente a adversarios activos, ransomware, phishing, malware y mucho más. Esta visibilidad sin precedentes del panorama de amenazas proporciona una información sobre amenazas inigualable que se utiliza para mejorar las capacidades defensivas de los productos y servicios de Sophos para todos los clientes.

Pruebas independientes

Las pruebas de terceros fiables son una herramienta importante para ayudar a las organizaciones a tomar decisiones informadas sobre su pila tecnológica e inversiones en seguridad. Sin embargo, a medida que los ataques aumentan en volumen y complejidad, solo se pueden obtener resultados significativos cuando las pruebas reflejan las condiciones reales de las organizaciones.

SE Labs

SE Labs es uno de los pocos especialistas en pruebas de seguridad del sector que simula las herramientas de ataque modernas y las tácticas, técnicas y procedimientos (TTP) que utilizan actualmente los ciberdelincuentes y los especialistas en pruebas de penetración.

En el último informe de pruebas de protección para endpoints de SE Labs (de enero a marzo de 2024), Sophos volvió a situarse como la mejor protección del sector, con calificaciones AAA en todos los apartados de las categorías tanto de grandes empresas como de pymes. Los informes de SE Labs del primer trimestre de 2024 pueden consultarse aquí:

Protección para endpoints: Grandes empresas | Protección para endpoints: Pequeñas empresas

Evaluaciones MITRE Engenuity ATT&CK

Sophos destacó en las evaluaciones MITRE Engenuity ATT&CK 2023 para grandes empresas (Turla). Sophos XDR detectó el 99 % de los comportamientos del adversario en la evaluación: notificó 141 de los 143 subpasos de ataque del adversario. Y, haciendo gala de su capacidad para proporcionar a los equipos de seguridad un amplio contexto sobre el qué, el porqué y el cómo del comportamiento del adversario, Sophos XDR registró una cobertura analítica exhaustiva para el 98 % de los subpasos de la evaluación.

Las evaluaciones de MITRE Engenuity ATT&CK se encuentran entre las pruebas de seguridad independientes más respetadas del mundo, debido en gran parte a la cuidadosa confección y emulación de escenarios de ataque reales, la transparencia de los resultados y la exhaustividad de la información de los participantes.

Premios e informes de analistas

Gartner

- Líder en el Magic Quadrant de Gartner de plataformas de protección de endpoints en 14 informes consecutivos
- Distinción Customers' Choice en los informes Voice of the Customer 2022, 2023 y 2024 de Gartner® Peer Insights™ para plataformas de protección de endpoints (EPP)

IDC

- Líder en el IDC MarketScape 2024 para la seguridad moderna mundial de endpoints para pequeñas y medianas empresas

G2

- Líder global | Suites de protección para endpoints: informes Grid de primavera 2023 y otoño 2023
- Líder global | EDR: informes Grid de primavera 2023 y otoño 2023
- Líder global | XDR: informe Grid de otoño 2023
- Líder global y solución n.º 1 | XDR: informe Grid de primavera 2023

Omdia

- Líder general | Plataformas integrales de detección y respuesta ampliadas (XDR), noviembre de 2022

CRN Tech Innovators Awards 2023

- Sophos Intercept X nombrada la mejor protección para endpoints

ChannelPro Readers' Choice Awards

- Sophos Intercept X es nombrado Gold Winner en Mejor proveedor de seguridad para endpoints

Testimonios de clientes

★★★★★

"La función más valiosa de Sophos Endpoint Protection es su protección contra amenazas avanzadas, ya que Sophos utiliza una combinación de tecnologías de vanguardia, como el Machine Learning, el análisis de comportamientos y la detección basada en firmas, para detectar y bloquear las amenazas maliciosas".

Desarrollador de software | Finanzas (no banca) | Lea la reseña completa en Gartner Peer Insights

★★★★★

"Una solución con un único panel intuitivo para gestionar las amenazas avanzadas de ciberseguridad".

Administrador de redes | Educación | Lea la reseña completa en Gartner Peer Insights

★★★★★

"Mi experiencia fue muy satisfactoria. Reduce la superficie de ataque y evita que los ataques se propaguen por la red de nuestra organización. Con sus funciones antiransomware e IA con Deep Learning, detiene los ataques antes de que afecten al sistema, lo que supone su gran ventaja".

Oficina de seguridad de las TIC | Medios audiovisuales | Lea la reseña completa en G2 Reviews

★★★★★

"Sophos es una solución para endpoints sumamente fácil de usar a la vez que potente".

Director de operaciones de TI | Empresa mediana | Lea la reseña completa en G2 Reviews

★★★★★

"Sophos Endpoint nos ayuda a reducir nuestra vulnerabilidad ante los atacantes y nos da la tranquilidad de que los sistemas de nuestros clientes están protegidos de los delincuentes".

Director de gestión de sistemas y copias de seguridad y recuperación | Gran empresa | Lea la reseña completa en G2 Reviews

Conclusión

La ciberseguridad es un sector que está sujeto a grandes adversidades y evoluciona con rapidez. Los atacantes mejoran continuamente sus técnicas para burlar defensas, y los proveedores de seguridad y las organizaciones deben adaptarse.

Para ello, es fundamental utilizar herramientas de seguridad que apuesten por un enfoque centrado en la prevención. Estas herramientas ofrecen defensas automatizadas y adaptativas para bloquear o ralentizar a los atacantes y ganar tiempo para responder a los ciberataques.

Entretanto, comprender qué debe ofrecer una solución de seguridad para endpoints y en qué consisten unos resultados de seguridad óptimos puede ayudarle a tomar una decisión informada. Además, brindará a su organización la mejor protección contra los ataques de hoy en día.

En Sophos, protegemos a las organizaciones de las amenazas actuales y en evolución. Nuestras soluciones les ayudan a conseguir los mejores resultados de seguridad posibles. Para obtener más información, póngase en contacto con nosotros hoy mismo.

Para obtener más información sobre Sophos Endpoint y cómo ofrece una protección inigualable contra ataques avanzados, visite **es.sophos.com/endpoint**.

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.

2024-06-18 ES-WP (PS)

SOPHOS