SOPHOS
Cybersecurity evolved.

Sophos Adaptive Cybersecurity Ecosystem

Sophos Adaptive Cybersecurity Ecosystem (ACE), o ecosistema de ciberseguridad adaptativa de Sophos, es un sistema integral diseñado para optimizar la prevención, la detección y la respuesta. Protege la nueva realidad de los sistemas empresariales interconectados, y sirve como defensa frente al cambiante panorama de la ciberseguridad que ahora combina la automatización con el hacking humano en vivo.

Sophos ACE emplea automatización y analistas, además de la aportación colectiva de los productos, partners, clientes y desarrolladores de Sophos, para crear una protección que mejora de forma continua, un ciclo virtuoso de aprendizaje y avance constantes. Y lo mejor es que se puede comenzar con lo básico y crecer. Empiece con la tecnología para endpoints y firewalls de Sophos y avance a partir de esa base.

Monográficos de Sophos. Mayo 2021

Un panorama cambiante

El panorama en el que opera la ciberseguridad está en constante evolución, y se han producido cambios importantes tanto en los entornos empresariales como en la naturaleza de los ataques durante los últimos años.

Cambio en la empresa: interconectividad

En su incesante búsqueda de formas de mejorar la productividad y la eficiencia, las empresas han creado una cadena de suministro muy interconectada, además de la infraestructura y la tecnología para respaldarla. La migración de datos y aplicaciones a la nube ha reportado numerosos beneficios, como la capacidad de trabajar desde cualquier lugar, unos costes de operación menores y la mejora del rendimiento y la escalabilidad, al tiempo que ha catalizado el crecimiento de la cadena de suministro digital global.

Paralelamente, la COVID-19 aceleró enormemente el cambio al teletrabajo y, con ello, terminó de echar por tierra el mito de un perímetro organizativo. Es necesario asumir que las personas, las aplicaciones, los dispositivos y los datos pueden encontrarse en cualquier lugar.

Si bien estos sistemas interconectados y dispersos nos dan un gran servicio, también han creado nuevos retos de seguridad. A muchas empresas les cuesta trazar el alcance de su red, y ya no digamos proteger todos los sistemas conectados a ella.

Los adversarios inteligentes y adaptativos atacan persistentemente estos sistemas, atraídos por la oportunidad de la dimensión que ofrecen. Un ejemplo reciente, aunque no el único, de esto fue el ataque a SolarWinds en diciembre de 2020, que afectó a víctimas que incluían desde destacados proveedores de tecnología y empresas más pequeñas hasta entidades del sector público del más alto nivel.

CAMBIO EN LA EMPRESA

Cadena de suministro interconectada

Migración a la nube de aplicaciones y datos

Entornos de teletrabajo

Cambio en el ataque: de automatizado a operativo

Cuando se trabaja en ciberseguridad, es fácil perder de vista un hecho importante pero que se subestima: en la batalla por nuestros sistemas y datos críticos, los defensores están ganando.

Las noticias diarias que informan de nuevas filtraciones de seguridad tienen un importante propósito como ejemplos admonitorios que nos recuerdan que debemos tomar medidas preventivas y mantenernos alerta. Pero estos casos son la excepción de la regla. No se escriben titulares sobre las empresas que consiguen defenderse de miles de intentos de infiltración todos los días.

No solo ha mejorado drásticamente la efectividad de la ciberseguridad, sino que las herramientas más recientes y los servicios de seguridad administrada también son más accesibles y asequibles que nunca. Las tecnologías antiransomware, de prevención de exploits, de detección de comportamientos y antiphishing están al alcance de todos.

Estas capacidades, que son favorecidas, mejoradas y aceleradas por la inteligencia artificial y el Machine Learning, están abordando las tácticas, las técnicas y los procedimientos de adversarios conocidos documentados en la plataforma MITRE ATT&CK, además de ataques nuevos y modernos nunca antes observados en circulación. Al cubrir carencias, cerrar rutas y bloquear técnicas, estas mejoras han conseguido que algunos ataques tengan unos costes tan prohibitivos que los atacantes han tenido que

CAMBIO EN EL ATAQUE

Los defensores están ganando

Automatización y operación del atacante

Mayores costes de infiltración

adaptarse. Estas mejoras en seguridad son tan significativas que la antigua idea de que bastaba con que el atacante acertara una única vez ya no se corresponde con la realidad. A fin de ganar dinero, los atacantes deben acertar muchas veces durante un ataque.

De hecho, ha cambiado su enfoque del malware automatizado por un enfoque más exhaustivo que combina la automatización con el hacking manual. El principal objetivo de los adversarios es seguir pasando inadvertidos, y la mejor forma de hacerlo es actuar como un empleado, es decir, utilizando herramientas locales, dispositivos locales y patrones de tráfico típicos.

Estos ataques sofisticados, que requieren una sustanciosa inversión humana, son incluso más costosos para las víctimas. Los atacantes pueden aprovechar sus conocimientos en profundidad del entorno de la víctima para provocar el máximo daño y exigir la máxima rentabilidad.

El cambio de la seguridad TI a las operaciones de seguridad

Estos cambios en las empresas y en los ataques requieren de una evolución en la seguridad TI. Las empresas se enfrentan a adversarios inteligentes que mueven continuamente el objetivo a medida que se acercan a él, lo que requiere que los equipos de seguridad TI desarrollen medidas defensivas que mejoren sus posibilidades de ganar.

En primer lugar, se necesita un cambio sustancial de **la gestión de la seguridad a las operaciones de seguridad**. Atrás quedaron los días de las políticas de seguridad de "configurar y olvidarse"; a medida que los atacantes se pasan a los ataques manuales directos, la seguridad TI necesita hacer lo mismo para buscar y detectar comportamientos y eventos sospechosos antes de que se conviertan en una infiltración.

Los equipos de seguridad deben detectar actividad sospechosa lo antes posible en la cadena de ataque a fin de que puedan responder antes de que se produzcan daños. Incluso los atacantes sigilosos dejan pistas, y los equipos de seguridad han de encontrarlas y seguirlas para detener el ataque en las fases iniciales del proceso. Ya no es solo cuestión de detectar los indicios entre el ruido, sino de identificar los indicios débiles críticos antes de que se conviertan en indicios evidentes. Cuando más evidente es el indicio, más cerca se encuentra la infiltración. Con las herramientas correctas, los problemas de TI pueden detectarse y corregirse de forma proactiva antes de que el adversario pueda descubrirlos y utilizarlos en un ataque.

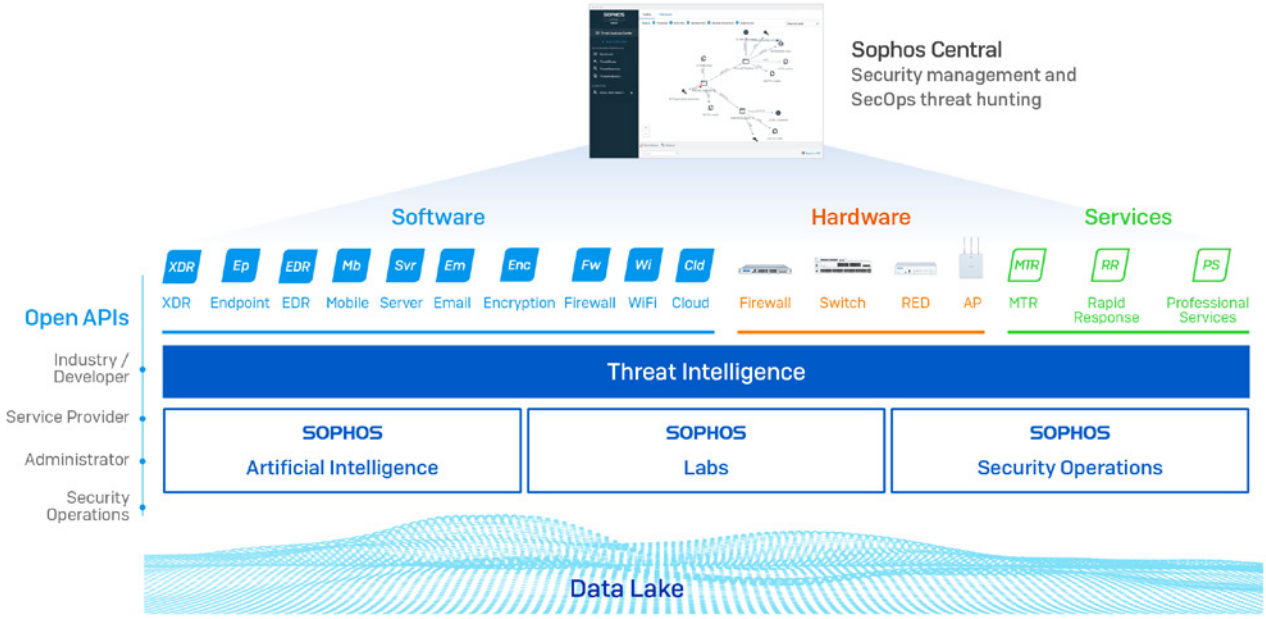
Ahora que las empresas están tan interconectadas, es necesario que la seguridad siga el mismo camino. Los equipos de seguridad TI deben pasarse de los productos independientes de seguridad no integrados a un **sistema de seguridad adaptativa** que ofrezca la máxima prevención posible de forma automática, y que a la vez permita a los operadores buscar y detectar indicios más débiles, como comportamientos y eventos sospechosos, e impedir que se conviertan en infiltraciones.

Los entornos empresariales y los ataques están en constante evolución. El futuro de la seguridad TI pasa por un sistema que permita un bucle de retroalimentación único para que pueda **aprender y mejorar constantemente**. La información y los eventos nuevos detectados por el equipo de operaciones pueden automatizarse, lo que mejora la prevención y reduce el número de ataques nuevos que entran en el sistema. De forma similar, a medida que mejora el software de automatización, los operadores pueden detectar comportamientos y eventos sospechosos más rápido, lo que reduce todavía más los incidentes. Este ciclo virtuoso mejora constantemente la seguridad general de la empresa y su negocio conectado.

Sophos Adaptive Cybersecurity Ecosystem

La buena noticia es que este sistema ya existe. Sophos Adaptive Cybersecurity Ecosystem (ACE) hace frente a esta nueva realidad. Utiliza el poder de la automatización y analistas para posibilitar el cambio de la gestión de la seguridad a las operaciones de seguridad. La automatización puede analizar y reaccionar más rápido a los comportamientos y eventos, mientras que los analistas humanos son mejores a la hora de correlacionar múltiples indicios sospechosos e interpretar su significado.

Sophos ACE ha sido diseñado para proteger la interconexión de nuestros negocios y el mundo online. Protege los sistemas y los datos estén donde estén, y aprende y mejora constantemente para protegerse frente a futuros cambios en la tecnología y los ataques.



Sophos ACE parte de la **información sobre amenazas** colectiva de SophosLabs, las operaciones de seguridad de Sophos (analistas humanos que realizan búsquedas de amenazas avanzadas en miles de entornos de clientes a través de nuestro servicio Managed Threat Response) y el grupo de inteligencia artificial de Sophos. Estas capacidades de información en tiempo real mejoran constantemente las tecnologías next-gen de nuestras soluciones de **software** y **hardware** líderes a escala mundial.

Un único **lago de datos** integrado extrae información de todos nuestros productos y las fuentes de información sobre amenazas, con un análisis en tiempo real que permite a los encargados de la seguridad detectar de forma proactiva los indicios sospechosos entre el ruido. De forma paralela, las **API abiertas** permiten a los clientes, partners y desarrolladores crear herramientas y soluciones que interactúan con el sistema. Todo se gestiona a través de la **plataforma de administración de Sophos Central**. Tendrá toda su seguridad en una única ubicación para beneficiarse de una eficiencia sin precedentes.

Estos cinco elementos (información sobre amenazas, tecnologías next-gen, lago de datos, API y administración centralizada) funcionan de manera conjunta para crear un ecosistema de ciberseguridad adaptativa que aprende y mejora de forma constante. Y si bien la potencia del ecosistema integral es amplia, puede aprovecharla tanto o tan poco como necesite. Muchos clientes empiezan con nuestra protección para endpoints o firewalls, y luego la amplían al ritmo que les convenga.

El último año ha convertido muchos centros de operaciones de seguridad en SOC virtuales. Sophos ACE puede ser gestionado por expertos en seguridad desde cualquier ubicación, lo que da a las empresas la oportunidad de contratar a los mejores profesionales del mundo. Como alternativa, nuestros expertos pueden gestionar la detección y respuesta a amenazas como servicio en su nombre.

La evolución de la Seguridad Sincronizada

La Seguridad Sincronizada, la capacidad de los productos de Sophos de compartir información en tiempo real a través de Security Heartbeat™ y automatizar la respuesta a incidentes, ha sido la piedra angular de nuestra protección durante muchos años. Cuando la lanzamos en 2015, la Seguridad Sincronizada era una propuesta única en el mercado, y seguimos ofreciendo la integración más amplia de todos los proveedores de seguridad, con información entre productos más detallada.

"Sophos sigue liderando el mercado con sus funciones de XDR entre productos de seguridad para endpoints y firewalls".

Gartner
Cuadrante mágico de Gartner de firewalls de redes empresariales,
Analistas: Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 9 de noviembre de 2020

Sophos Adaptive Cybersecurity Ecosystem parte de la automatización y la integración de la Seguridad Sincronizada, y amplía aún más el sistema de ciberseguridad de Sophos.

Más visibilidad

Nadie sabe de dónde procederá el siguiente ataque, y es sencillamente imposible que los operadores humanos lo supervisen todo. En lugar de esto, necesita un sistema que lo monitorice todo y que le permita reaccionar rápidamente a las amenazas emergentes. Por esto hemos ampliado el ecosistema para incluir una gama aún más amplia de tecnologías, como la nueva detección y respuesta ampliadas (XDR) de Sophos y nuestras API. Los productos de Sophos ven y registran todos los eventos, comportamientos y detecciones sospechosos en todo su entorno para que tenga siempre a mano la información que necesita.

Más datos

El lago de datos combina y correlaciona información de todos estos sensores para ofrecer datos más detallados de todos los productos. Los operadores pueden consultar el lago de datos directamente con Sophos Intercept X with EDR y Sophos XDR, lo que permite la identificación de comportamientos y eventos sospechosos en todo su entorno e impedir que los problemas se conviertan en infiltraciones.

Más inteligencia

Con el rápido crecimiento de nuestro servicio Managed Threat Response (MTR), podemos añadir datos en tiempo real de nuestros cazadores de amenazas expertos para complementar los datos de detección. De forma paralela, seguimos desarrollando nuestros modelos de IA y aportaciones de detección de amenazas de SophosLabs.

Más integración

SophosLabs, la IA de Sophos y las operaciones de seguridad de Sophos funcionan de manera conjunta, integrando sus conocimientos para beneficiar a todos los clientes en un ciclo virtuoso. Por ejemplo, PowerShell es una herramienta legítima de gran utilidad para muchos usos, pero también es frecuentemente explotada por los atacantes. Los operadores de MTR entrenan nuestros modelos de IA para distinguir entre los usos "benignos" y "malignos" de PowerShell en función de experiencias del mundo real. Después todo el sistema se actualiza con este aprendizaje de IA, lo que amplifica la protección de los clientes.

Sophos Adaptive Cybersecurity Ecosystem en acción

Sophos ACE es un sistema activo que ya está ampliando y mejorando la protección en escenarios del mundo real. En marzo de 2021, un grupo de adversarios llamado Hafnium explotó la vulnerabilidad ProxyLogon de Microsoft Exchange. Esta es una vulnerabilidad de día cero, y los atacantes aprovecharon deficiencias intrínsecas de la forma en que Exchange había sido diseñado para evitar la activación de detecciones inmediatas.

Tan pronto como se conoció la vulnerabilidad, el servicio Sophos Managed Threat Response (MTR) actualizó al instante la monitorización de los sensores para incluir comportamientos asociados con ProxyLogon. Con la información ya en el lago de datos, Sophos MTR obtuvo acceso instantáneo a todos los datos necesarios para identificar y remediar cualquier actividad maliciosa relacionada con esta vulnerabilidad.

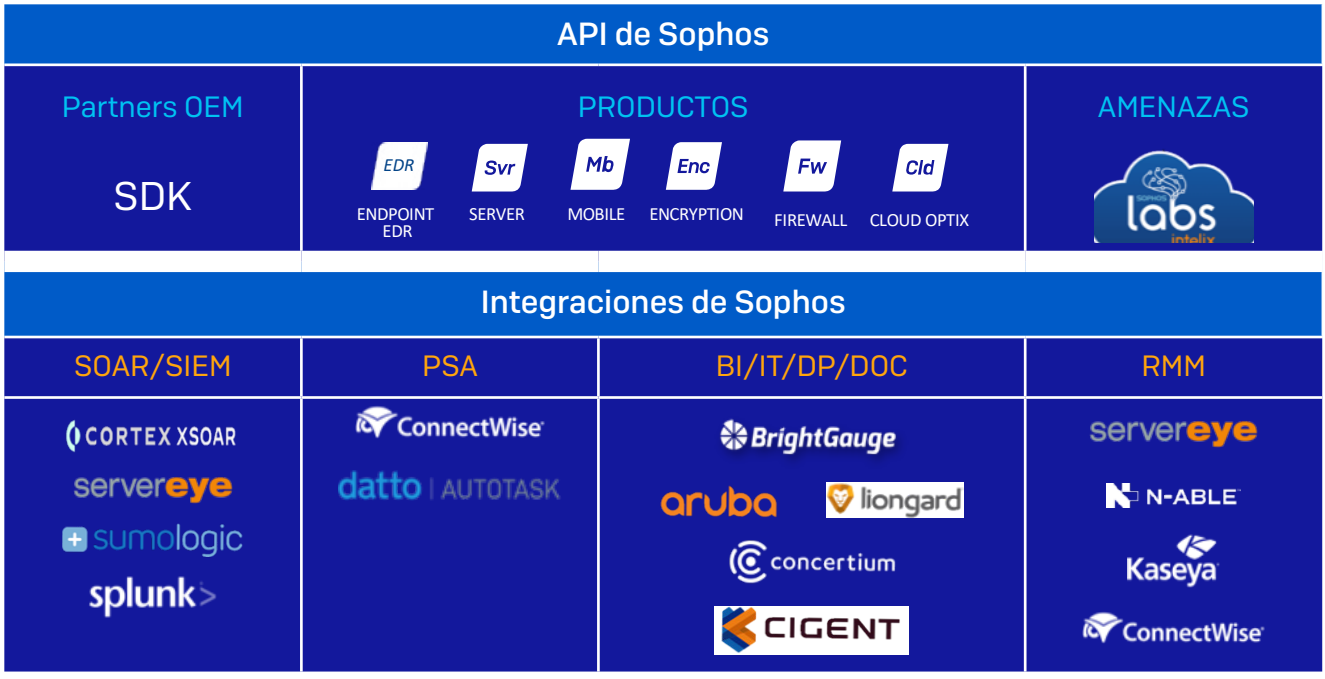
Además, el equipo combinó sus capacidades de búsqueda de amenazas con la tecnología EDR de Sophos para detectar nuevos artefactos o indicadores de peligro (IOC) relacionados con el ataque. Estos indicadores se compartieron directamente con SophosLabs, quienes los utilizaron para publicar IOC adicionales relacionados con la vulnerabilidad de Exchange, lo que aportó aún más protección a todos los clientes de Sophos.

Una plataforma abierta con potentes integraciones y API abiertas

En nuestro mundo interconectado, es fundamental que la ciberseguridad pueda integrarse con la totalidad del entorno empresarial. La ciberseguridad tiene múltiples facetas, y Sophos Adaptive Cybersecurity Ecosystem cubre una amplia gama de necesidades de seguridad, entre ellas:

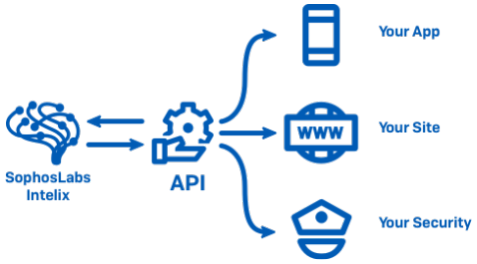
- MSSP: soporte para la prestación de soluciones de ciberdefensa avanzadas a sus clientes
- Partners de canal: agilización de sus procesos empresariales
- ISP: asistencia para garantizar la seguridad de los servicios de Internet que prestan
- Pymes: soporte para la creación de herramientas personalizadas para controlar y posibilitar la seguridad

Ya tenemos implementadas numerosas API e integraciones y aún hay más en camino, y Sophos ACE ya está gestionando más de cinco millones de solicitudes de API todos los días.



Presentación de API: SophosLabs Intelix™

Intelix es un conjunto de API RESTful sencillas y de rápida respuesta que permiten a las apps identificar, clasificar y evitar amenazas, lo que incrementa su seguridad. Los clientes, partners y desarrolladores del ecosistema de Sophos pueden utilizar estas API para realizar búsquedas de amenazas en la nube, análisis de archivos estáticos y análisis de archivos dinámicos. Encontrará más información sobre las API de SophosLabs Intelix en https://www.sophos.com/es-es/labs/intelix.aspx.



Sophos ACE: para un impacto empresarial real

Los beneficios de Sophos Adaptive Cybersecurity Ecosystem son acumulativos. La combinación de tecnologías next-gen (información sobre amenazas de SophosLabs, la IA de Sophos y las operaciones de seguridad de Sophos), un sistema integrado adaptativo que aprende constantemente y la administración centralizada a través de la plataforma de Sophos Central tiene un enorme impacto tanto sobre la protección como sobre la eficiencia.

Tecnologías next-gen	**+**	**Información sobre amenazas**	**+**	**Sistema integrado adaptativo**	**+**	**Gestión centralizada**

Los clientes que utilizan Sophos Firewall y Sophos Intercept X juntos ya nos dicen que necesitarían duplicar su plantilla de seguridad para mantener el mismo nivel de protección si no contaran con un sistema de ciberseguridad de Sophos. También nos comentan que experimentan menos incidentes de seguridad y que pueden identificar y responder más rápido a los problemas que se producen. Sophos ACE parte de este punto, y transforma aún más el coste total de propiedad de la ciberseguridad, así como la protección.

Introducción

Sophos Adaptive Cybersecurity Ecosystem es muy flexible, y ponerse en marcha es tan sencillo como desplegar uno de los productos o servicios de protección de Sophos. Las empresas se benefician inmediatamente de la experiencia en información sobre amenazas combinada de la IA de Sophos, SophosLabs y las operaciones de seguridad de Sophos. Puede ampliar su ecosistema en cualquier momento para alinearlo con las necesidades de su negocio. Los puntos de partida más populares son:

Sophos Intercept X para sus endpoints o servidores (con la opción de añadir la funcionalidad EDR o XDR)

Sophos Firewall, hardware, software o virtual

Servicio Sophos Managed Threat Response (MTR)

Para obtener más información, hable con su representante de Sophos, consulte nuestro sitio web o inicie una evaluación gratuita.

Cuadrante mágico de Gartner de firewalls de redes empresariales,
Analistas: Rajpreet Kaur | Adam Hils | Jeremy D'Hoinne | 9 de noviembre de 2020

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.

Obtenga más información sobre el ransomware y cómo Sophos puede ayudarle a proteger su empresa.

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 funciones next-gen probadas, los datos de su empresa estarán protegidos de forma eficaz por productos basados en la IA y el Machine Learning.

2021-04-26 (SB-NP)

SOPHOS