MONOGRÁFICO

Explicación de los sistemas de ciberdefensa

Cómo el nuevo modelo de ciberdefensa proporciona resiliencia para la era de la IA agéntica.

SOPHOS

Resumen ejecutivo

Sobre el papel, la cobertura de seguridad para la mayoría de las organizaciones parece sólida. Con el paso de los años, han acumulado docenas de productos de seguridad. Sin embargo, según Gartner: "Por término medio, las organizaciones cuentan con 45 herramientas de seguridad que a menudo funcionan de forma aislada, lo que genera complejidad, puntos ciegos y exposiciones no identificadas que los adversarios atacan".[1] Por lo tanto, si bien no faltan herramientas, sí existe una falta de conectividad entre ellas.

Los atacantes ya están aprovechando las brechas entre las herramientas, moviéndose a través del correo electrónico, la identidad, los endpoints y la red en cuestión de minutos. La IA está aumentando la velocidad, la escala y el alcance de las ciberamenazas a un ritmo sin precedentes, lo que permite ejecutar ataques multicapa sofisticados a gran escala.

Los auditores, los organismos reguladores y las ciberaseguradoras exigen ahora un conjunto de pruebas que los productos de ciberseguridad fragmentados tienen dificultades para proporcionar. La mayoría de las organizaciones siguen teniendo dificultades para responder a tres preguntas básicas: ¿estamos protegidos?, ¿dónde radica nuestro mayor riesgo? y ¿están funcionando nuestras inversiones?

Un nuevo modelo de ciberdefensa está tomando forma para garantizar la seguridad en la era de la IA. La plataforma de seguridad está evolucionando para convertirse en el sistema de ciberdefensa. Estas son sus características distintivas:

- **Una única vista del entorno en tiempo real** alimentada por todos los puntos de control de cualquier proveedor.
- **Las respuestas se coordinan automáticamente** entre los distintos puntos de control: correo electrónico, identidad, endpoints, red y mucho más.
- **La IA agéntica responde a la velocidad y al volumen de los ataques modernos**, mientras que los expertos humanos establecen los límites y asumen la responsabilidad de los resultados.
- **Aprendizaje continuo**: cada nueva información y cada amenaza detenida en toda la base de usuarios refuerzan automáticamente las defensas en todas partes.
- **La unidad de defensa deja de ser cada producto individual para convertirse en una arquitectura que los conecta**, incluida tanto la arquitectura tecnológica como una red de expertos humanos.

Las amenazas de la era de la IA agéntica ya son una realidad

A finales de 2025, unos investigadores documentaron la primera campaña de ciberespionaje conocida ejecutada principalmente por IA, en lugar de por personas. La IA llevó a cabo por sí sola aproximadamente entre el 80 % y el 90 % de la operación, a una velocidad y una escala que ningún equipo humano podría igualar.

Fuente: Anthropic, noviembre de 2025

Un sistema de ciberdefensa es...

Una arquitectura de seguridad unificada en la que todos los puntos de control comparten una vista en tiempo real, responden como un todo, aprenden continuamente y actúan a velocidad de máquina bajo supervisión humana.

1. *Gartner, «Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System». Neil MacDonald. 12 de diciembre de 2025*

SOPHOS

Sus retos de seguridad en la era de la IA

Años de decisiones razonables de adquisición para hacer frente a cada amenaza han dado lugar a un entorno tan complejo que la propia complejidad se ha convertido en una exposición. Ahora, esa pila de productos sin coordinar se enfrenta a atacantes que actúan a la velocidad de la IA y no consigue seguirles el ritmo. ¿Cómo hemos llegado hasta aquí?

Limitaciones del enfoque basado en plataformas

Prácticamente todos los grandes proveedores de ciberseguridad afirman que su plataforma puede hacer todo lo que necesita. Venden soluciones individuales destinadas a quienes compran en función de cada amenaza y que, supuestamente, funcionan conjuntamente como una única plataforma.

La filosofía de crear un sistema unificado mediante una plataforma iba por buen camino, pero lo que suelen vender es un conjunto de herramientas desarrolladas o adquiridas precipitadamente para aprovechar ciclos de expectación anteriores o inflar el precio de las acciones. Las promesas no se cumplen:

- **Prometen un "panel único"**, pero, cuando se ponen a prueba en situaciones reales, los responsables de la respuesta siguen teniendo que pasar de una consola a otra.
- **Prometen datos compartidos**, pero los productos de la plataforma no pueden analizar esos datos conjuntamente para detectar un ataque que abarque la identidad, la nube y los endpoints.
- **Prometen integración**, pero cada producto conserva su propio modelo de datos y las acciones de respuesta permanecen aisladas en los distintos dominios.

Todo el trabajo relacionado con la plataforma, como la configuración, la personalización y la creación de un flujo de trabajo que utilice conjuntamente todos sus componentes, queda en manos del cliente.

Según Gartner®: «Limitarse a añadir más herramientas a la pila no proporcionará la estructura inteligente de ciberdefensa que necesitan las organizaciones para mitigar ataques coordinados mediante IA como el identificado recientemente por Anthropic».

Neil MacDonald
Gartner | VP, Distinguished Analyst and Gartner Fellow Emeritus

Gartner, «Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System». Neil MacDonald. 12 de diciembre de 2025. GARTNER es una marca registrada de Gartner, Inc. y/o sus filiales

Los ataques que abarcan varios dominios superan a las defensas fragmentadas

La fragmentación de los modelos de datos y los análisis de los productos de las plataformas resulta muy ventajosa para un atacante. En el siguiente escenario de ataque se muestra el motivo:

- **Paso 1:** Un correo electrónico convincente llega a una bandeja de entrada sin ser detectado.
- **Paso 2:** El destinatario introduce su contraseña en una página de inicio de sesión falsa.
- **Paso 3:** El atacante inicia sesión desde una ubicación desconocida.
- **Paso 4:** El atacante añade discretamente una regla de buzón de correo para supervisar el tráfico.
- **Paso 5:** El atacante utiliza su acceso para llegar a un recurso compartido de archivos y exfiltrar datos.

Cinco pasos, cada uno de ellos en un dominio diferente.

- **La protección del correo electrónico** detecta el mensaje.
- **La solución de identidad** detecta el inicio de sesión inusual.
- **La protección para endpoints** registra una pequeña anomalía.
- **El firewall** registra la conexión saliente.

Cada producto registra su propia parte y, técnicamente, todos están haciendo su trabajo. Sin embargo, **ninguno de ellos ve el panorama completo**, porque no comparten lo que saben con los demás mientras el ataque sigue en curso. Solo parece ruido, no la narrativa de un único ataque. La cadena solo se hace evidente más tarde, cuando ya es demasiado tarde.

Este tipo de movimiento lateral es habitual en los ataques modernos y también suele pasar desapercibido. El Informe del estado del ransomware 2026 de Sophos reveló que el 55 % de los ciberdelincuentes consiguió cifrar los datos incluso cuando el firewall detectó el ataque.

Ataques a velocidad de máquina, respuesta a velocidad humana

Ahora imagine ese ataque entre dominios y comprima el plazo del ataque de días a minutos. Eso es lo que ha hecho la IA. Una defensa que espera a que una persona detecte una alerta en un producto y la coteje con otro producto ya llega demasiado tarde. El problema no es que los responsables de la seguridad sean lentos, sino que las respuestas herramienta por herramienta lo son. Los flujos de trabajo con un alto grado de intervención manual no pueden seguir el ritmo de un ataque automatizado. Para cuando un operador ha formulado una respuesta, el atacante ya ha pasado a la siguiente fase.

Los conocimientos especializados escasean. El ruido no.

Destinar más personas al problema no es realmente una opción, porque esas personas no están disponibles. La escasez de personal cualificado en ciberseguridad es real y no está disminuyendo. En el estudio de ISC2 sobre profesionales de 2025, el 95 % de los equipos de seguridad señaló al menos una carencia de competencias y el 59 % la calificó de crítica o significativa, frente al 44 % del año anterior.

Al mismo tiempo, el volumen de trabajo sigue aumentando. Un equipo pequeño puede acabar siendo responsable de más productos, alertas y paneles de control de los que razonablemente podría supervisar. La mayoría de esas alertas no son más que ruido, pero alguien debe encontrar la señal que se oculta entre ellas.

Se suponía que la IA aliviaría esa presión, pero en algunos entornos ha provocado el efecto contrario.

Añadir la IA como otro producto incorporado a posteriori genera los mismos problemas: más ruido y más alertas, porque no se diseñó para interactuar de forma nativa con el resto de los productos de la plataforma. Ahora, el equipo de ciberseguridad no solo tiene que examinar falsos positivos, sino también hacer frente a las «alucinaciones» de la IA.

La línea de pobreza en ciberseguridad es real

La línea de pobreza en ciberseguridad es el umbral por debajo del cual una organización no puede protegerse de forma eficaz. No viene determinada por el tamaño o el presupuesto de una organización, ni por si cuenta o no con un CISO. De hecho, muchas organizaciones con una buena financiación se encuentran por debajo de ese umbral.

La línea de pobreza en ciberseguridad es un umbral de capacidad estratégica.

¿Su organización se limita a disponer de tecnología de seguridad o es capaz de gestionarla como un sistema? Los equipos numerosos pueden invertir mucho en herramientas que nadie sabe utilizar, mientras que un fabricante disciplinado con 200 empleados puede gestionar un sistema de defensa que supere a los de organizaciones mucho mayores. Muchas organizaciones se encuentran sin saberlo por debajo de la línea de pobreza porque dan por sentado que ya disponían internamente de la capacidad necesaria para gestionar la seguridad como un sistema.

Para estas organizaciones, la mayor carencia no es una herramienta que falta. Es la ausencia de una estrategia clara y de la orquestación necesaria para que los controles existentes funcionen de forma conjunta frente a las amenazas aceleradas por la IA. Siguen invirtiendo, pero continúan teniendo dificultades para responder a tres preguntas básicas:

- ¿Estamos protegidos?
- ¿Dónde se encuentran nuestros mayores riesgos?
- ¿Están funcionando realmente nuestras inversiones?

Los reguladores exigen más pruebas de resiliencia

A los reguladores y las ciberaseguradoras no les importa que disponga de los productos adecuados. En su lugar, cada vez exigen más que las organizaciones demuestren:

- Control coordinado entre dominios.
- Pruebas conservadas y auditables.
- Informes coherentes y oportunos.
- Resiliencia probada en situaciones reales.

Estas nuevas normativas suponen una pesada carga para las organizaciones cuyo entorno de seguridad sigue repartido entre docenas de productos, cada uno con su propio modelo de datos y periodo de retención. Aportar las pruebas que solicita un auditor o una aseguradora puede convertirse en un trabajo a tiempo completo: exportar registros de sistemas independientes, unirlos manualmente y confiar en que el resultado siga contando una historia coherente. A efectos de cumplimiento, un control que no puede demostrarse es un control que no cuenta.

El denominador común

Ninguno de estos problemas se resuelve añadiendo otro producto o botón a una consola. Todos comparten una única causa fundamental: las defensas que funcionan de forma aislada fracasan cuando las amenazas contra ellas actúan de forma coordinada. Para cerrar esa brecha se necesita algo diferente, no simplemente otro producto nuevo.

Sistemas de ciberdefensa: un enfoque moderno de la seguridad

Si el problema es la fragmentación, la respuesta no consiste en consolidar por el mero hecho de hacerlo. Comprar un producto que intenta hacerlo todo y fracasa no es mejor que disponer de varios buenos productos que no se coordinan correctamente.

En su lugar, las organizaciones deberían buscar un sistema de ciberdefensa: un conjunto de productos y servicios de seguridad diseñados para funcionar como un único sistema unificado. Cada punto de control debe contribuir a una comprensión compartida del entorno y responder como parte de un conjunto coordinado. El sistema debe estar bien conectado, sincronizado, automatizado, ser inteligente y adaptativo. Cinco principios describen cómo funciona esto en la práctica.

1 Puntos de control sincronizados y autónomos

Un sistema de ciberdefensa comienza por los puntos de control. Son las tecnologías y los servicios en los que se observa la telemetría de seguridad y se aplican las reglas de seguridad. Los puntos de control pueden ver lo que sucede en ellos y actuar al respecto. Los endpoints, el firewall, el correo electrónico, la identidad, las herramientas de productividad y otros elementos son puntos de control.

2 Una única vista compartida en tiempo real

Un sistema de defensa se diferencia de una plataforma porque ofrece una comprensión compartida de lo que ocurre en todo el entorno. Cada punto de control transmite en tiempo real lo que observa a una capa de datos común, sin copias ni procesos de conciliación posteriores. Esto proporciona a todo el sistema una vista única y compartida de los eventos en tiempo real. Sin puntos ciegos ni brechas en la respuesta.

3 Respuesta coordinada en todas las capas

Una respuesta coordinada comienza con una detección en una capa que puede desencadenar automáticamente una acción en las demás, sin que un analista tenga que transmitir la señal de una consola a otra.

Un inicio de sesión sospechoso puede provocar un análisis más exhaustivo tanto en la capa de endpoints como en la de correo electrónico. Un archivo malicioso en un dispositivo puede hacer que el firewall o la red bloqueen la conexión que intenta establecer. El sistema responde como uno solo porque ya percibe el ataque como uno solo. Y cuando un ataque se propaga rápidamente, este tipo de coordinación es fundamental.

4 IA agéntica con responsabilidad humana

La velocidad es el factor decisivo. Los ataques que se desarrollan en cuestión de minutos no pueden detenerse con defensas que esperan a que una persona detecte una alerta. Por eso, la IA debe estar en el centro del sistema, no en los extremos.

En un sistema de ciberdefensa, la IA forma parte de la arquitectura: está integrada, no incorporada a posteriori. La IA correlaciona señales en todas las capas, reconoce la forma que va adoptando un ataque e impulsa la detección, la investigación y la respuesta a velocidad de máquina. Este sistema nativo de IA se diferencia de la IA incorporada a posteriori en un único producto, que solo puede ver los datos de ese producto.

La IA integrada en un sistema de defensa puede razonar a partir de todo lo que ve el sistema. Sin embargo, una respuesta a velocidad de máquina sin responsabilidad humana supone un riesgo, no una ventaja. Los sistemas de ciberdefensa no apartan a las personas de la seguridad. En su lugar, las dirigen allí donde el criterio humano es más importante: establecer los límites, tomar decisiones novedosas o de alto riesgo, revisar incidentes y asumir la responsabilidad de los resultados.

La IA se ocupa de la velocidad y el volumen. También de la clasificación rutinaria y las acciones rápidas con un alto grado de confianza.

Los expertos humanos definen los límites de confianza: qué puede decidir la IA por sí sola y cuándo necesita ayuda. Intervienen cuando el contexto no resulta familiar o hay mucho en juego.

A medida que el sistema se gana la confianza, esos límites pueden ampliarse. Pero la responsabilidad siempre recae en los expertos humanos.

La IA se ocupa de la velocidad y el volumen.

Los expertos humanos definen el límite de confianza.

5 Inteligencia acumulativa

Los sistemas de defensa aprenden. Una amenaza detectada en cualquier lugar se convierte en conocimiento en todas partes. El endpoint detecta lo que ha detectado el firewall. La puerta de enlace de correo electrónico comunica a la capa de identidad lo que ha captado. Todas las herramientas aprenden junto con las demás y aprovechan lo aprendido anteriormente. Todo esto sucede sin ninguna configuración manual. La inteligencia del sistema de defensa crece con cada nuevo usuario y cada nuevo patrón observado, lo que permite que el sistema evolucione tan rápidamente como los ataques basados en IA.

De las plataformas a los sistemas de ciberdefensa

En conjunto, estos cinco principios definen una categoría propia. Los sistemas de defensa son la evolución de las plataformas, optimizada para la era de la IA. Por lo general, una plataforma no es más que un conjunto de productos tras una consola compartida, unidos por unas credenciales de acceso y un acuerdo de licencia, no por su diseño.

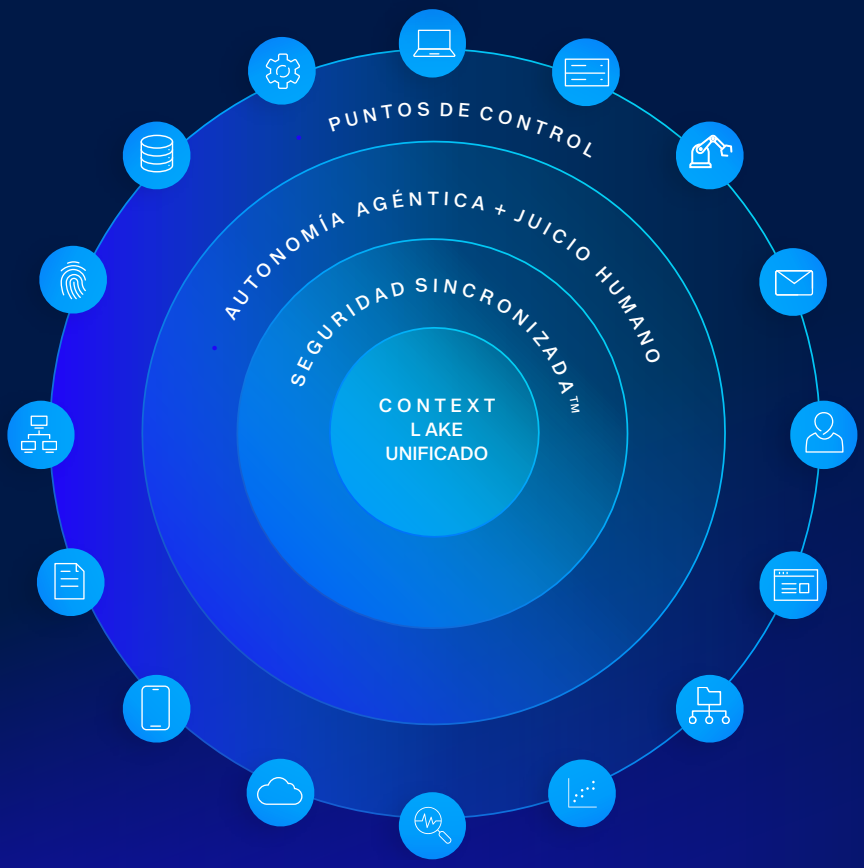
Un sistema de ciberdefensa es diferente. Sus datos se comparten, la IA está integrada, la respuesta está coordinada y los expertos humanos mantienen el control. Es una arquitectura diseñada para funcionar como un único producto, no como una colección de productos dispuestos para parecer uno solo.

Sophos Fusion: el sistema de ciberdefensa de Sophos

Sophos Fusion es el sistema de ciberdefensa más completo del sector, desarrollado para un mundo en el que las amenazas evolucionan a la velocidad de la IA. Gracias a la arquitectura de Sophos AI-Native Cybersecurity Defense System y a más de 500 integraciones de Sophos y de terceros, lo ve todo, lo conecta todo y permite que sus defensas respondan de forma unificada.

Sophos Fusion lleva a la práctica los principios del sistema de ciberdefensa: una arquitectura única y abierta en la que todos los puntos de control funcionan como un todo, con tecnología de IA agéntica y bajo el criterio humano, para proteger a las organizaciones de amenazas basadas en IA cuya velocidad de propagación supera la capacidad de reacción de los responsables de seguridad.

Cuantos más productos de la cartera de Sophos active un cliente, más valor aportará Sophos Fusion.



Puntos de control sincronizados y autónomos

Todos los puntos de control de los que ya dispone proporcionan continuamente información sobre amenazas en tiempo real y ejecutan acciones de respuesta. La arquitectura es totalmente abierta: se integra de forma nativa con los productos de Sophos y con más de 500 tecnologías de terceros, de modo que las inversiones que ya ha realizado pasan a formar parte de una defensa coordinada en lugar de funcionar de forma aislada.

También ofrece la integración de seguridad con Microsoft más completa del mercado, disponible para todos los planes de Microsoft y no solo para los más caros, por lo que incluso las organizaciones con licencias básicas de Microsoft pueden reforzar sus defensas con esa telemetría.

Una única vista compartida en tiempo real

Toda la telemetría de todos los puntos de control fluyen en tiempo real hacia el Context Lake unificado, una única capa de datos compartida. No se producen retrasos en la agregación ni existe un almacén de datos independiente en cada punto de control. Piense en ello como un sistema nervioso compartido: cada punto de control percibe lo mismo que todos los demás en el preciso instante en que sucede. Este contexto compartido es lo que hace posible la coordinación.

Respuesta coordinada en todas las capas: Seguridad Sincronizada

Seguridad Sincronizada es el tejido conectivo que convierte el contexto compartido en acciones coordinadas en todo Sophos Fusion. Permite que los puntos de control de Sophos y de terceros respondan conjuntamente y de forma automática a las amenazas.

Una detección en el endpoint puede desencadenar una respuesta en el firewall. Una identidad vulnerada puede bloquear el acceso en todo el entorno. Un correo electrónico sospechoso puede activar una supervisión más exhaustiva en todas las demás capas. Cuantas más soluciones de Sophos despliegue, más ventajas de Seguridad Sincronizada podrá aprovechar.

Piense en el sistema de extinción de incendios de un edificio moderno: un sensor situado en una estancia no se limita a activar una alarma, sino que cierra las puertas cortafuegos, redirige el flujo de aire y activa los rociadores de las plantas cercanas. Sophos Fusion funciona del mismo modo, como un todo coordinado. Puede hacerlo porque los datos ya están unificados. No se requiere ninguna configuración ni acción adicional.

IA agéntica con responsabilidad humana

Sophos Fusion detecta, investiga y responde a velocidad de máquina, pero siempre bajo supervisión humana. Todas las acciones se mantienen dentro de los límites establecidos y ajustados continuamente por expertos humanos. Eso es lo que la convierte en IA agéntica: una IA capaz de razonar ante situaciones nuevas y no solo de seguir tareas automatizadas predefinidas.

Una analogía útil es el piloto automático de un avión. El sistema puede pilotar el avión, pero el piloto establece los parámetros, supervisa los instrumentos y toma el control cuando la situación es desconocida o presenta un riesgo elevado.

En Sophos Fusion, esta capacidad agéntica la proporciona Fusion AI, la IA agéntica nativa de Sophos. Sophos integra más de 50 modelos de IA en sus defensas, todos ellos perfeccionados continuamente mediante información sobre amenazas en tiempo real. Por ejemplo, Sophos Email utiliza más de 20 modelos, incluidos modelos propios de procesamiento del lenguaje natural (PLN) que analizan el texto, el tono, el contexto y la estructura de los correos electrónicos para identificar ataques de phishing y estafas por correo electrónico corporativo comprometido.

Sophos MDR, un servicio 24/7 en el que los expertos de Sophos supervisan su entorno y responden en su nombre, gestiona el SOC (centro de operaciones de seguridad) agéntico más grande del mundo utilizando Sophos Cyber Defense System Se trata de la mayor operación de detección y respuesta gestionadas del sector y protege a más de 40 000 organizaciones. Resuelve el 52 % de los incidentes de principio a fin mediante IA, con una media de 89 segundos desde la alerta hasta la respuesta automatizada, mientras que los expertos humanos siguen asumiendo la responsabilidad de las decisiones que implican riesgos para la organización.

Inteligencia acumulativa

Sophos Cyber Defense System aprende de todos los ataques, no solo de los dirigidos contra su organización. Cada amenaza detectada en las más de 625 000 organizaciones protegidas por Sophos se incorpora a Sophos Fusion, junto con cada caso excepcional que resuelve un analista y cada nuevo entorno que se conecta. Sophos X-Ops refuerza el sistema con su profundo conocimiento especializado y su información sobre amenazas en tiempo real, que se distribuyen automáticamente a todos los productos de Sophos y a todos los clientes para mejorar sus defensas.

Funciona de forma muy similar al sistema inmunitario de un organismo. Cada amenaza con la que se encuentra el organismo pasa a formar parte de su memoria permanente: queda catalogada, comprendida y lista para cuando vuelva a aparecer. Sophos Fusion funciona del mismo modo. Desde el primer día, un nuevo cliente está protegido frente a amenazas que nunca antes había visto porque el sistema ya las conoce.

Por eso es importante la cifra de más de 625 000 organizaciones. Refleja la amplitud de la experiencia que permite acumular protección e información. Cuanto más observa el sistema, mejor protege a todos los que forman parte del mismo.

Sophos Fusion: donde experimenta un sistema de ciberdefensa

Sophos AI-Native Cybersecurity Defense System es la arquitectura. Sophos Fusion es donde todo esto cobra vida. Un único lugar desde el que gestionar sus puntos de control de Sophos, ver el panorama completo de todos los puntos de control conectados y actuar.

Esto significa que no hay que comprar ni activar nada adicional y que tampoco es necesario cambiar su forma de trabajar actual. Todos los puntos de control de Sophos forman ya parte de Sophos Fusion, por lo que, en cuanto despliega uno, pasa a formar parte de la arquitectura. Y, a medida que añade más puntos de control de Sophos o de terceros, se activa una parte mayor del sistema, lo que alimenta una visión compartida más completa y aporta más valor a todo lo que ya utiliza.

El ataque visto desde Sophos Fusion

Volvamos al ataque de varias fases anterior. Un correo electrónico malicioso, una credencial robada, un inicio de sesión inusual, una regla de reenvío del buzón de correo y un movimiento lateral hacia datos sensibles. En Sophos Fusion, la telemetría de Sophos Email y del entorno Microsoft del cliente converge en el Context Lake unificado. Sophos XDR correlaciona entonces esas señales a medida que llegan y reconoce la secuencia como un único ataque conectado, en lugar de cinco alertas independientes.

A partir de ahí, Seguridad Sincronizada coordina la respuesta en el correo electrónico, la identidad, los endpoints y la red. La IA agéntica actúa a velocidad de máquina, mientras que los analistas de Sophos MDR toman medidas directas y adoptan las decisiones de alto riesgo. El ataque que podría burlar productos aislados es detectado por un sistema que ve el panorama completo.

Qué significa Sophos Fusion para su organización

Sophos Fusion proporciona ciberresiliencia para la era de la IA agéntica en cuatro áreas importantes para la empresa.

- **Protección frente a amenazas aceleradas por IA que avanzan más rápido de lo que pueden responder los responsables de la seguridad.** Los ataques de varias fases se detectan y contienen en una etapa temprana, incluso cuando la IA acelera su velocidad y escala, porque todos los puntos de control comparten contexto y responden conjuntamente, en lugar de actuar por separado.

- **Mayor rendimiento de su personal y sus inversiones.** La IA agéntica se encarga del trabajo rutinario y ruidoso de clasificación y respuesta, de modo que su equipo y sus puntos de control actuales consiguen mejores resultados sin aumentar la plantilla ni la complejidad. Todas las herramientas conectadas, sean o no de Sophos, contribuyen al resultado.

- **Una postura mejorada en materia de cumplimiento y ciberseguros.** La cobertura ininterrumpida, la conservación del contexto entre capas y la respuesta coordinada proporcionan las pruebas que esperan los auditores, los organismos reguladores y las aseguradoras mediante un único registro consultable, en lugar de registros exportados manualmente. La misma arquitectura que mejora la protección mejora también la capacidad de demostrarla.

- **Una estrategia de ciberseguridad alineada con su empresa.** Al conectar y coordinar sus defensas, Sophos Fusion le permite pasar de gestionar paneles de control tácticos a disfrutar de confianza operativa, con una visibilidad clara de dónde se encuentran sus lagunas y mayores riesgos, y de si sus inversiones están funcionando. Así es como las organizaciones de cualquier tamaño, tengan o no un CISO, pueden implantar por fin la estrategia que siempre han deseado.

Todos los clientes de Sophos forman ya parte de Sophos Fusion, el sistema de defensa de Sophos. Se trata de una actualización automática y fluida que protege a los clientes frente a las amenazas de la era de la IA.

Cómo empezar a utilizar Sophos Fusion

Todas las soluciones de Sophos forman parte de Sophos Fusion, por lo que cada una constituye un punto de entrada y no una herramienta independiente. Para empezar, basta con desplegar un producto o servicio de Sophos. Sophos MDR, Sophos XDR, Sophos Endpoint, Sophos Firewall y Sophos Email son puntos de partida habituales. Cuantas más soluciones añada, más capacidades de la arquitectura desbloqueará.

No es necesario cambiar los puntos de control de terceros de los que depende actualmente. Intégrelos en Sophos Fusion para proporcionar información continua sobre amenazas en tiempo real y ejecutar acciones de respuesta. Empiece por el área de mayor riesgo y amplíe el sistema a su propio ritmo.

¿Está preparado para empezar? Hable con un experto de Sophos para determinar el punto de partida adecuado para su entorno u obtenga más información en sophos.com/es-es/fusion.

Conclusión

Durante años, la respuesta predeterminada ante cada nueva amenaza consistía en añadir otro producto, y ese hábito creó la fragmentación que ahora aprovechan los atacantes. La IA no ha hecho más que agravar el problema al ampliar la brecha entre la velocidad a la que avanza un ataque y la capacidad de una respuesta de consola en consola para seguirle el ritmo. Añadir más productos no cerrará esa brecha. Un sistema de ciberdefensa sí lo hará.

Un sistema de ciberdefensa traslada la unidad de defensa desde los productos individuales hasta la arquitectura que los conecta:

- Una vista compartida
- Respuesta coordinada en todas las capas
- IA integrada para actuar a velocidad de máquina
- Expertos humanos que mantienen el criterio y la responsabilidad donde corresponden

Proteger la era de la IA significa conseguir que todo lo que ya posee funcione conjuntamente como un único sistema. Sophos Fusion, el Sophos AI-Native Cybersecurity Defense System, le permite aplicar este modelo sin sustituir lo que ya posee.

¿Está preparado para hablar sobre sus necesidades de ciberdefensa para la era de la IA?

Póngase en contacto con un experto de Sophos hoy mismo.

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

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