

MONOGRÁFICO

# Seguridad Sincronizada™ Explicador

SOPHOS

# Seguridad Sincronizada

Synchronized Security™ está en el corazón de Sophos Fusion, el sistema de defensa de ciberseguridad nativo de IA líder en la industria de Sophos. Es el tejido conectivo que convierte la información sobre amenazas de todos los puntos de control conectados – Sophos y terceros – en una respuesta coordinada a las amenazas.

En su Tech FutureSight: Protege la superficie de ataque global con un sistema de ciberdefensa autónomo[1], Gartner identificó que "las organizaciones necesitan una capa inteligente que conecte los diferentes elementos de su conjunto de herramientas de ciberseguridad para responder de manera proactiva y reactiva a riesgos y amenazas a velocidades de máquina". La Seguridad Sincronizada es un elemento clave de cómo se entrega esto en Sophos Fusion.

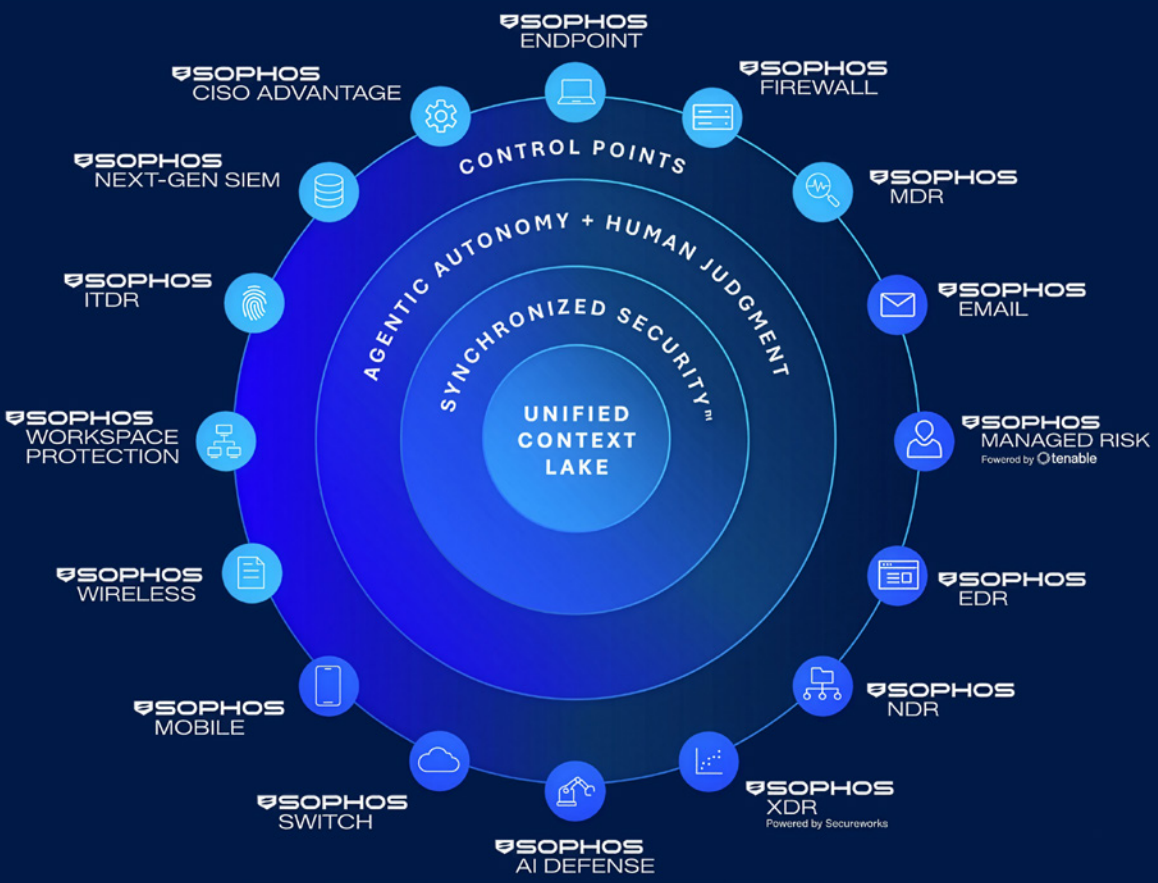
Esta guía explica cómo funciona la Seguridad Sincronizada, los beneficios que ofrece y cómo las organizaciones pueden aprovecharla.

1 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.



# Resumen rápido

- La Seguridad Sincronizada es un elemento central del sistema de defensa Sophos Fusion y se incluye automáticamente – no es necesario adquirir un módulo adicional ni licenciar componentes adicionales.
- Permite una respuesta coordinada a las amenazas en puntos de control conectados. Empezar requiere dos o más puntos de control que trabajen conjuntamente en Sophos Fusion.
- La Seguridad Sincronizada funciona con puntos de control tanto de Sophos como no Sophos. Las acciones de respuesta en entornos de clientes individuales dependen de qué controles están conectados a Sophos Fusion y del nivel de acción autónoma que el cliente otorga sobre cada punto de control.
- Sophos XDR está en el centro de la Seguridad Sincronizada, correlacionando señales de todo el entorno del cliente en una única cadena de ataque y permitiendo acciones de respuesta automatizadas o dirigidas por humanos en todo el sistema de defensa.
- Las soluciones Sophos también pueden funcionar juntas sin Sophos XDR, añadiendo mayor profundidad de Seguridad Sincronizada.
- Seguridad Sincronizada se basa en las capacidades fundamentales probadas en batalla que Sophos lanzó en 2015.



# Por qué importa una respuesta coordinada

Las herramientas de seguridad históricamente se han construido para hacer bien un trabajo. Un agente de estación de trabajo asegura el dispositivo en el que se ejecuta (por ejemplo, escritorio, portátil o servidor). Un Firewall monitorea lo que cruza la red. Un servicio de correo electrónico controla lo que llega a la bandeja de entrada. Cada uno es bueno en su trabajo y ciego a todo lo que está fuera de él.

Los atacantes entendieron esto hace mucho tiempo. Una intrusión moderna no es un evento único en un solo lugar. Cruza identidad, correo electrónico, estaciones de trabajo y red por diseño, porque el espacio entre ellos es exactamente donde se encuentran las brechas, y los atacantes las explotan.

La consecuencia es familiar para cualquiera que haya dirigido un equipo de seguridad. Las soluciones individuales ven solo su propio dominio, identificando anomalías aparentemente dispares. Cada uno parece funcionar de forma independiente. Nadie tiene el tiempo o el contexto para reconocer las anomalías como el mismo ataque hasta que se ha hecho el daño.

La IA ha ampliado las brechas. Los ataques ahora se ejecutan a velocidad de máquina y en volúmenes que la industria no ha visto antes. Sin embargo, la mayoría de las defensas todavía funcionan a velocidad humana, con un analista moviéndose entre consolas y correlacionando a mano.

Añadir otro producto al entorno no cierra esa brecha. En cambio, las organizaciones deberían buscar conectar los productos en los que ya han invertido. Esto es precisamente lo que hace la Seguridad Sincronizada dentro de Sophos Fusion.



# Lo que entrega la Seguridad Sincronizada

La coordinación transforma la velocidad, la escala y el alcance de la respuesta a amenazas, cambiando el resultado de un ataque. Cuando las estaciones de trabajo, la red y otros controles actúan juntos, la contención ocurre en segundos, no después de que alguien se dé cuenta y reaccione. Una estación de trabajo comprometida se aísla inmediatamente antes de que un adversario pueda moverse lateralmente, acceder a datos sensibles o establecer persistencia. Además, dado que la respuesta es automatizada, funciona durante la noche y los fines de semana cuando a menudo hay una cobertura humana reducida.

La coordinación también cierra las brechas en las que se basan los atacantes. Puntos de control de terceros que anteriormente solo generaban alertas ahora contribuyen activamente a la defensa. Las inversiones de seguridad existentes dejan de estar en aislamiento y se convierten en parte de la respuesta coordinada.

El impacto operativo en un equipo de seguridad es inmediato. La contención rutinaria ocurre sin intervención del analista. Cuando se requiere una investigación humana, el analista comienza con el contexto entre capas ya ensamblado, en lugar de armarlo manualmente a través de varias consolas.

La misma coordinación facilita probar la protección. El contexto entre capas se retiene y una respuesta coordinada deja un registro coherente de lo que se encontró y lo que se hizo al respecto. Esa es la narrativa de control que esperan los auditores, reguladores y aseguradoras. La arquitectura que mejora la protección también mejora la capacidad de un cliente para demostrarla.

La defensa también se fortalece a medida que crece. Cada nuevo punto de control conectado a Sophos Fusion envía una señal adicional al lago de contexto unificado y abre otro lugar desde donde responder, sin un aumento correspondiente en el esfuerzo operativo. Más cobertura no significa más trabajo.

Para los proveedores de servicios gestionados, la misma coordinación se ejecuta consistentemente en cada entorno de cliente, incluidos aquellos que mezclan Sophos y puntos de control de terceros. La contención automatizada reduce la sobrecarga de triaje y remediación manual.

# Cómo funciona

La Seguridad Sincronizada comienza con la telemetría. Cada punto de control conectado informa lo que ve en el lago de contexto unificado a medida que sucede. Estaciones de trabajo, Firewall, correo electrónico, nube, red, identidad y herramientas de productividad alimentan el mismo lago. Los puntos de control de terceros lo alimentan junto con los de Sophos. Nada espera en una cola para ser agregado, y no hay un almacén de datos secundario para conciliar más tarde.

Sophos XDR interpreta la imagen compartida y realiza el trabajo que un analista haría manualmente. Vincula eventos relacionados y los resuelve en una única cadena de ataque en lugar de una serie de alertas separadas. La correlación es la parte que importa, porque un único punto de control solo ve un fragmento.

Luego, las acciones de respuesta viajan de vuelta a los puntos de control. Sophos XDR suministra la maquinaria: Automatización SOAR, guías interactivas, gestión de casos y un amplio conjunto de acciones de respuesta. La mayoría se ejecutan automáticamente sin intervención humana. Cuando se necesita criterio, un analista interno puede activar la misma acción manualmente usando Sophos XDR, al igual que un analista de Sophos MDR.

Integración bidireccional con puntos de control de terceros significa que Sophos Fusion puede extraer y enviar datos a través de la integración. Por ejemplo:

- Puede extraer telemetría de un firewall que no es de Sophos y enviar de vuelta una dirección IP para que el firewall la bloquee.
- La integración de ServiceNow abre, actualiza y cierra casos.
- La respuesta a amenazas activas en Sophos Firewall utiliza respuestas activadas por API a feed de amenazas de terceros para expulsar de la red un dispositivo comprometido o no autorizado.

Únicamente, los puntos de control de Sophos también actúan unos sobre otros directamente sin ninguna participación de Sophos XDR. El Security Heartbeat integrado transmite el estado de seguridad de un dispositivo desde Sophos Endpoint a los otros puntos de control de Sophos: un estado Verde está en buen estado, un estado Amarillo está potencialmente comprometido y un estado Rojo está comprometido.

Los otros puntos de control de Sophos están construidos para actuar sobre el estado de seguridad del dispositivo. Una vez que los puntos de control están conectados a la misma cuenta de Sophos Fusion, las respuestas centrales no necesitan configuración adicional. Las capacidades que aprovechan el estado de seguridad, como una regla de Firewall que restringe el acceso a internet o una política de Workspace Protection de Sophos, son configuradas por el cliente antes de que tengan efecto.

**Recopilar**

**Correlacionar**

**Responder**

Sophos Fusion recopila telemetría, Sophos XDR construye contexto y las acciones automatizadas de respuesta restablecen la aplicación de medidas en los puntos de control.

# Una capacidad, múltiples dimensiones de coordinación

Seguridad Sincronizada se lanzó inicialmente en 2015, siendo pionera a nivel mundial en ese momento, y ha ampliado su alcance en más de una década. La profundidad de la coordinación entre los puntos de control difiere de un entorno de cliente a otro dependiendo de la mezcla exacta de puntos de control que tengan implementados.

La coordinación es más profunda entre los puntos de control de Sophos, ya que están diseñados para funcionar juntos desde la base. Los puntos de control de terceros se unen a través de las integraciones en Sophos Fusion, y las acciones de respuesta varían según lo que exponga el otro proveedor.

La profundidad de la coordinación también depende del nivel de control que un cliente entrega a Sophos Fusion en cada punto de control. Esa elección le pertenece al cliente, y el hecho de que exista es el punto más que una deficiencia. Pregunte a la mayoría de las organizaciones si una estación de trabajo infectada debe ser desconectada de la red sin que nadie lo apruebe, y la respuesta es sí. Preguntar si un sistema debe reescribir una política de Firewall para reducir su exposición por sí mismo, y la respuesta varía.

Los cortafuegos son el ejemplo que hace obvia la tensión. Al final, bloquear una estación de trabajo comprometida es un cambio de regla del firewall. Muchas organizaciones desconfían de los cambios automatizados en la configuración del Firewall, y sus procesos de control de cambios existen por una buena razón.

Los clientes pueden escribir sus propias automatizaciones y manuales de estrategias y ejecutarlas junto a las que proporciona Sophos. Un cliente que utiliza Sophos Endpoint decide por sí mismo lo que significa una estación de trabajo comprometida para su firewall Fortinet, cubriendo cómo se comporta ese firewall y cómo está configurado. Una vez creadas, esas automatizaciones se ejecutan dentro de Sophos Fusion como cualquier otra respuesta coordinada.



# La Seguridad Sincronizada en acción

La coordinación es más fácil de reconocer con ejemplos. Los casos de uso a continuación muestran la misma capacidad operando en diferentes profundidades en lugar de una lista de características separadas.

## Coordinación entre productos Sophos

Cuando Sophos Endpoint encuentra una amenaza en una estación de trabajo o servidor, establece el estado de seguridad del Security Heartbeat de ese dispositivo en Rojo. El nuevo estado se comparte automáticamente con los otros puntos de control Sophos conectados a través del Security Heartbeat. Varias respuestas siguen automáticamente:

- Sophos Endpoint intenta remediar la amenaza, lo que puede incluir bloquear y revertir el cifrado por ransomware, o implementar un nivel de control más alto para contener a un adversario activo.
- Sophos Firewall limita el acceso a internet del dispositivo, cortando cualquier conexión a un servidor de comando y control, y evita que llegue a dispositivos sanos.
- Sophos Wireless, Sophos Switches y Sophos Workspace Protection restringen el acceso del dispositivo a los recursos de la red, limitando aún más el impacto de la vulneración.
- A las estaciones de trabajo sanas se les informa del estado de seguridad Rojo y rechazarán las solicitudes de conexión de red del dispositivo afectado.

El mismo mecanismo detecta problemas que nunca se anuncian como una infección. Una estación de trabajo o servidor que envía grandes volúmenes de correo electrónico de spam o correo electrónico de phishing está configurado con un estado de seguridad Rojo. Sophos Endpoint luego busca usuarios o aplicaciones maliciosas previamente no identificadas, y Sophos Email bloquea los mensajes antes de que lleguen a una bandeja de entrada.

Una estación de trabajo o servidor puede permanecer en el estado de seguridad Rojo durante segundos o incluso días, dependiendo de la remediación requerida. Una vez limpio, el estado de seguridad del dispositivo vuelve a Verde y el acceso se restaura automáticamente en todo el sistema.

El valor se muestra más claramente cuando nadie está mirando. Un servidor comprometido tarde un viernes por la noche se desconecta en segundos, en lugar de darle al adversario todo el fin de semana para moverse por la red.

**ESCENARIO**

Sophos Endpoint encuentra una amenaza y establece el estado de seguridad de Security Heartbeat en rojo. El nuevo estado se comparte automáticamente con cada punto de control Sophos conectado. Cuando se elimina la amenaza de la estación de trabajo, se sigue el mismo ciclo para restaurar el acceso.

## SIGNAL

## RESPUESTA COORDINADA

SOPHOS FUSION
AI-Native Cybersecurity Defense System




**SOPHOS ENDPOINT**

Detecta una amenaza

**SOPHOS FIREWALL**

Elimina la conectividad de red y restringe el acceso a la red.

**SOPHOS WIRELESS**

**SOPHOS SWITCH**

**SOPHOS WORKSPACE PROTECTION**

Restringir el acceso del dispositivo a los recursos de red.

**SOPHOS ENDPOINT**

Las estaciones de trabajo sanas rechazan la comunicación de red.

## Sophos Endpoint y un firewall de terceros

La coordinación no se limita a los puntos de control de Sophos. Un cliente que ejecuta Sophos Endpoint junto con un firewall Fortinet puede tener un dispositivo comprometido que active una respuesta en el firewall Fortinet. El cliente define cuál es esa respuesta y hasta dónde llega, lo que mantiene la automatización dentro de sus propios límites de control de cambios. Las capacidades de automatización y manuales de estrategias (SOAR) de Sophos XDR hacen esto posible, trabajando con la integración de Fortinet en Sophos Fusion.



## Tecnología y telemetría de Microsoft

Casi todas las organizaciones ejecutan tecnología de Microsoft, y la identidad es el vector principal para los ataques de ransomware. Un token de sesión robado o una cuenta comprometida le da a un adversario una forma legítima de entrar, y ninguna contención de estaciones de trabajo ayuda si la cuenta en sí permanece comprometida. La respuesta debe acceder al entorno de Microsoft para completar la remediación.

Bloquear la cuenta es el ejemplo más claro: Sophos Fusion puede bloquear una cuenta de Microsoft comprometida para excluir al adversario y luego desbloquearla una vez que la cuenta esté segura para volver a usarse. La cuenta se trata como un punto de control como cualquier otro, algo que el sistema puede ver y sobre lo que puede actuar, no algo que un administrador maneje por separado después.

La integración es bidireccional. La telemetría de una variedad de fuentes de Microsoft alimenta el mismo lago de contexto unificado que los puntos de control de Sophos, Microsoft Entra ID y Microsoft Graph Security, entre otros. Así que una señal de Microsoft puede provocar una respuesta en un punto de control de Sophos tan fácilmente como al revés. Un inicio de sesión sospechoso detectado por Microsoft puede aislar una estación de trabajo protegida por Sophos, sin que ninguna de las partes esté configurada para vigilar a la otra.

## El borde de la red, cableado e inalámbrico

Los switches y los puntos de acceso rara vez se consideran parte de una defensa. Son infraestructura, comprados para mover tráfico y mantener a la gente conectada, y la mayoría de las organizaciones los tratan en consecuencia. Sin embargo, se encuentran en el punto donde cada dispositivo se conecta con la red, lo que los convierte en uno de los primeros lugares donde se puede detener un dispositivo comprometido o no autorizado.

En Sophos Fusion, Sophos Switches y los puntos de acceso Sophos Wireless funcionan como puntos de control: contribuyen con lo que ven sobre los dispositivos conectados y pueden actuar sobre lo que encuentra el sistema en general. Los administradores pueden identificar dispositivos nuevos o no autorizados, clientes en un SSID inesperado o un dispositivo conectado al puerto incorrecto de un switch.

Respuesta a Amenazas Activas, una capacidad de Seguridad Sincronizada en Sophos Firewall, convierte ese contexto en acción. Usando la telemetría en el lago de contexto unificado, un dispositivo puede ser bloqueado en la capa de acceso cableada o inalámbrica antes de que avance más en la red. Los clientes eligen si activar la respuesta a amenazas activas, manteniendo la decisión de permitir el bloqueo automatizado en la capa de acceso en sus manos.

Los dispositivos de red de terceros siguen el mismo patrón que el ejemplo de Firewall de terceros anterior.



## Sophos AI Defense descubre el uso de IA en la sombra.

La coordinación no se trata solo de malware e intrusiones. Sophos AI Defense es un punto de control en Sophos Fusion que rige cómo se utiliza la IA en una organización. Interpreta la telemetría de actividad de IA de una variedad de productos Sophos en el lago de contexto unificado, junto con cada otra señal, visible para Sophos EDR, Sophos XDR y Sophos MDR. Sophos AI Defense está diseñado para mostrar los detalles granulares del uso de IA, y una vez que esa información está en el lago de contexto unificado, pasa por la misma funcionalidad de Seguridad Sincronizada que todo lo demás.

Shadow AI muestra por qué esto es necesario. Un empleado comienza a usar una herramienta de IA de la que nadie sabe, pegando código fuente y registros de clientes en ella. El navegador ve los datos pegados, la estación de trabajo ve la aplicación y el Firewall ve tráfico a un servicio de IA desde un dispositivo que puede no estar gestionado en absoluto. Ningún punto de control ve el panorama completo, por lo que la herramienta queda sin descubrir.

Sophos AI Defense ensambla esas señales y las evalúa en contexto, proporcionando a un analista de seguridad la evidencia que necesita para entender lo que sucedió. Combina telemetría, tales como identidad, permisos, comportamiento, exposición de datos y la ubicación tanto del usuario como del modelo de IA, lo que diferencia el uso aceptable de la actividad no administrada, con privilegios excesivos o que infringe la política.

La aplicación luego se ejecuta en los puntos de control:

- Sophos Workspace Protection controla el navegador, incluyendo copiar y pegar, subir, descargar y capturas de pantalla.
- Sophos Endpoint restringe el acceso a aplicaciones y sitios web de IA en todos los grupos de usuarios y tipos de dispositivo.
- Sophos Firewall controla el tráfico de servicios de IA en la capa de red, incluidos dispositivos no administrados y actividad no basada en navegador.
- Los productos Sophos pueden inspeccionar indicaciones, cargas y interacciones con IA en tiempo real, manteniendo el código fuente, los registros de clientes y los datos financieros dentro del negocio.
- Un administrador puede bloquear una herramienta de IA específica en todo el entorno desde Sophos Fusion.

La política no es el final. Un comportamiento de agente no autorizado o una violación se refleja en los mismos flujos de trabajo de Sophos EDR, Sophos XDR y Sophos MDR que cualquier otra detección, gestionados mediante la automatización y los libros de procedimientos ya utilizados para amenazas de identidad, endpoint y red. Hasta qué punto llega la coordinación depende de qué puntos de control están conectados a Sophos Fusion.

**82 %**

de organizaciones han descubierto herramientas o flujos de trabajo de IA desconocidos en su entorno.[2]

2 Cloud Security Alliance, El problema del agente de IA en la sombra en entornos empresariales, 2025

## Coordinación más allá de la respuesta a amenazas

Entre los puntos de control de Sophos, la coordinación va más allá de compartir un veredicto de amenaza. Un punto de control puede hacerle una pregunta directa a otro y actuar en función de la respuesta. Una estación o servidor protegido por Sophos Endpoint ya sabe la mayor parte de lo que un Sophos Firewall no puede decirte sobre el tráfico de red. Tres intercambios muestran lo que eso hace posible: identificar la aplicación detrás del tráfico en un puerto, identificar al usuario detrás de una sesión y decidir si un dispositivo es apto para recibir acceso en absoluto.

### Control de aplicaciones sincronizado

Toma una conexión no clasificada en un puerto inusual. Un Firewall que lo inspecciona en aislamiento ve un flujo de paquetes y poco más. El Sophos Firewall puede preguntar a Sophos Endpoint qué aplicación está enviando y recibiendo en ese puerto y obtener una respuesta sobre qué aplicación es la responsable. Los clientes pueden entonces permitir o bloquear la aplicación sobre esa base. Con el tiempo, esto también construye una imagen precisa de lo que se está ejecutando en la red, lo cual suele ser más variado de lo que nadie espera.

### Identidades, no direcciones IP

La identidad del usuario funciona de la misma manera. Sophos Endpoint pasa la información del usuario autenticado a Sophos Firewall, por lo que la política se puede escribir en torno a las personas y su identidad en lugar de en torno a usuarios o direcciones IP que cambian. Elimina un ejercicio de mapeo que los administradores mantendrían manualmente y que tiende a quedar desactualizado.

### Solo los dispositivos sanos se conectan

Las decisiones de acceso también se benefician; una VPN tradicional no tiene forma de saber si un dispositivo goza de un buen estado de seguridad o no, y autoriza el acceso basándose únicamente en sus credenciales. Sin embargo, Sophos Workspace Protection comprueba el estado de seguridad del dispositivo con Sophos Endpoint antes de conceder nada, por lo que una estación comprometida nunca llega a las aplicaciones o datos de la red.

Intercambios como estos no son un conjunto fijo. Cada uno existe porque Sophos lo construyó, y Sophos ha seguido expandiendo las capacidades con el tiempo. Lo que se comparte entre los puntos de control de Sophos hoy es considerablemente más rico que lo que se compartía entre ellos hace una década.

Ninguno de esto comienza como respuesta a amenazas, pero rara vez se mantiene separado de ella. Una aplicación que nadie puede explicar, o un usuario conectado donde no tiene por qué estar, es un detalle operativo ordinario hasta el momento en que no lo es. La visibilidad que facilita la gestión de una red facilita la detección de una amenaza emergente.

## Una respuesta coordinada en un entorno híbrido

Este ejemplo del mundo real de Sophos MDR muestra la Seguridad Sincronizada en acción. La organización afectada era un cliente de Sophos MDR que utilizaba Sophos Endpoint y Sophos Email, junto con Microsoft Entra ID, Microsoft Graph Security y un firewall de Fortinet. También ejecutaron un Sophos Firewall en una red separada. Cada uno de esos puntos de control alimentaba el mismo lago de contexto unificado.

- El atacante comenzó con un señuelo asistido por IA, utilizando una página de phishing alojada en un sitio legítimo. El usuario hizo clic e introdujo su contraseña.
- El kit robó el token de sesión en vivo en lugar de la credencial. Al hacerlo, el atacante logró eludir la autenticación multifactor, dejando ineficaz el restablecimiento de contraseña.
- El adversario inició sesión desde infraestructura de atacante conocida y creó una regla de bandeja de entrada silenciosa que ocultaba cualquier correo electrónico de un proveedor específico, lo que es la configuración para fraude bancario.
- Cuatro puntos de control registraron algo sospechoso: Sophos Endpoint, dos soluciones de Microsoft y el firewall de Fortinet. Ninguna señal individual fue lo suficientemente fuerte como para provocar una respuesta.
- Una detección de Sophos diseñada para ese propósito se activó y las señales individuales se consolidaron en una cadena de ataque.
- El inicio de sesión fue bloqueado, las sesiones fueron revocadas y la estación de trabajo fue aislada con éxito. Las direcciones IP maliciosas fueron bloqueadas en el Sophos Firewall, utilizando la telemetría proporcionada por el firewall de Fortinet.

Un humano cerró entonces el caso. Un analista confirmó que la regla de la bandeja de entrada nombraba a un proveedor específico, lo que fue lo que lo identificó como preparación para fraude bancario.



# Cómo los clientes habilitan la Seguridad Sincronizada

Seguridad Sincronizada no es un producto, un código de artículo (SKU) ni un complemento, y no hay nada extra que licenciar. Los clientes lo obtienen automáticamente cuando dos o más puntos de control funcionan juntos dentro de Sophos Fusion, independientemente de si los puntos de control son Sophos o no Sophos.

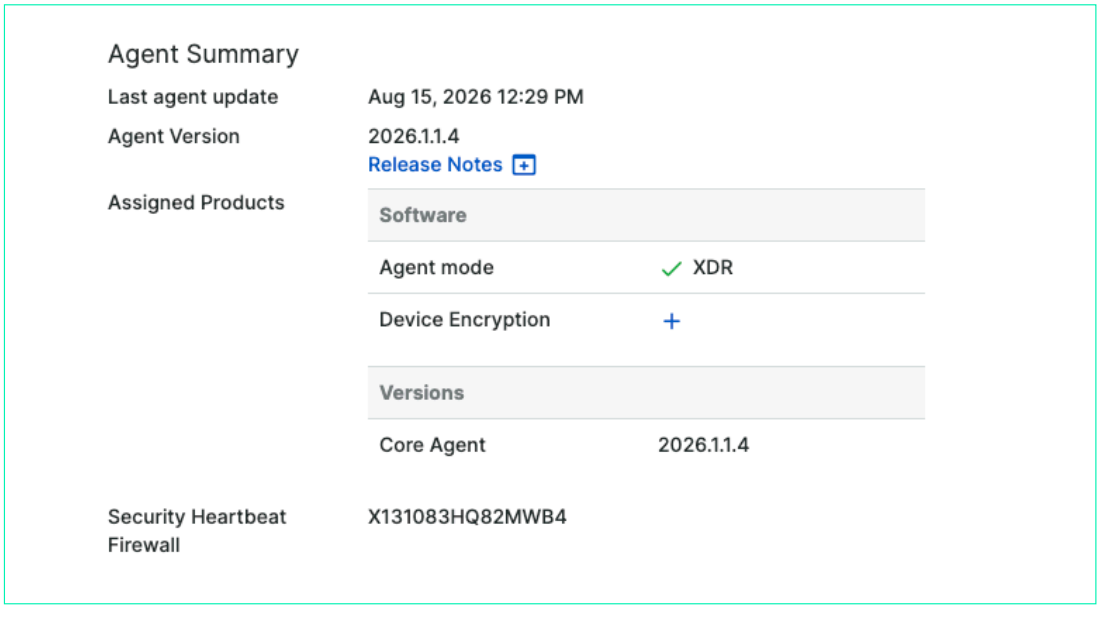
Sophos Endpoint y Sophos Firewall gestionados a través de la misma cuenta de Sophos Fusion es un punto de partida común. La coordinación entre ellos es activa tan pronto como ambos están conectados a esa cuenta, sin nada adicional que configurar. Los casos de uso que se basan en el estado de seguridad, como usar el estado de seguridad como parte de las reglas del Firewall o las políticas de Workspace Protection de Sophos, son configurados por el cliente.

La coordinación con puntos de control de terceros comienza integrando el punto de control en Sophos Fusion, que admite integraciones nativas de Sophos y más de 500 de terceros. Sin embargo, el nivel de respuestas automatizadas disponibles varía de un punto de control a otro. La respuesta a amenazas activas en los puntos de control de Sophos es un ejemplo, habilitado por el cliente, no por defecto.

Sophos proporciona automatizaciones y libros de procedimientos que se ejecutan automáticamente a través de Seguridad Sincronizada, cubriendo una amplia gama de casos de uso. Los clientes pueden añadir los suyos cuando una automatización predeterminada no se adapta a su entorno, como se describe anteriormente.

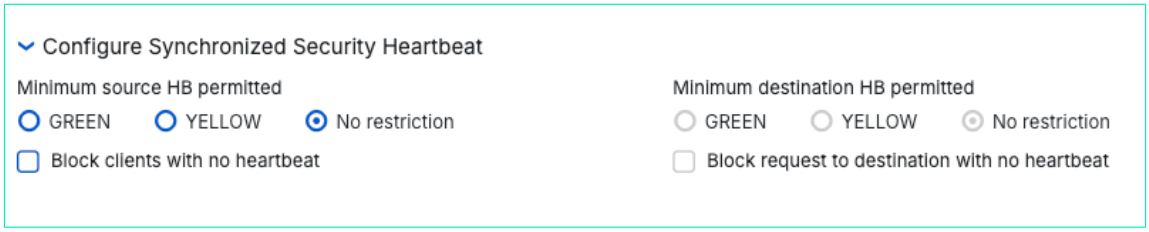
## Sophos Endpoint coordinándose con Sophos Firewall

Para confirmar que Sophos Endpoint está coordinándose con Sophos Firewall, abra el resumen del equipo en Sophos Fusion. En él se muestra el número de serie de Sophos Firewall que recibe el Security Heartbeat de ese endpoint.



## Políticas de Sophos Firewall con Seguridad Sincronizada

Una regla de Firewall puede requerir opcionalmente un estado de seguridad Verde antes de que se permita que un dispositivo acceda a internet. Los dispositivos no protegidos (es decir, aquellos que no ejecutan Sophos Endpoint) no podrían conectarse, al igual que cualquier dispositivo con un estado de seguridad cuestionable.




# Juntándolo todo

El problema nunca fue la escasez de herramientas de seguridad. Era que las herramientas que una organización ya posee tienden a funcionar en aislamiento, y los atacantes han construido sus métodos para explotar las lagunas entre ellas. Seguridad Sincronizada permite que sus herramientas de seguridad funcionen como una defensa unificada y coordinada.

Si ejecuta dos o más puntos de control dentro de Sophos Fusion, la Seguridad Sincronizada ya trabaja en su nombre. Conecta más puntos de control y llega más lejos. Las herramientas que no son de Sophos en las que ya has invertido se integran en la respuesta en lugar de quedarse al margen.

Cuánto se ejecute automáticamente queda a tu criterio. La coordinación que ignore tus procesos de control de cambios no tendría sentido, por lo que estableces la profundidad de la automatización, punto de control por punto de control.

Ese es el valor práctico del Sophos Cyber Defense System. No se trata de una lista más larga de productos, sino de aquellos que ya utilizas para responder en conjunto a velocidad de máquina, más rápido de lo que un ataque acelerado por IA puede moverse entre ellos.

# Para saber más, visite www.sophos.com/synchronizedsecurity

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

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

© Copyright 2026. Sophos Ltd. Reservados todos los derechos.
Constituida en Inglaterra y Gales N.º 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido.
Sophos es una marca registrada de Sophos Ltd. Otros productos y empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.