SOPHOS NDR

Vea y detenga las amenazas en toda la red de la era de la IA.

Una solución para detectar y defenderse contra amenazas conocidas y desconocidas.

Sophos NDR combina análisis de comportamiento impulsado por IA y ML, análisis de tráfico cifrado, análisis de red y búsqueda de amenazas con inspección profunda de paquetes y capacidades de IDS/IPS. Las opciones de despliegue flexibles, la respuesta activa en línea y la defensa conectada a través de Sophos Fusion ayudan a las organizaciones a ampliar la visibilidad en las redes híbridas y monitorizar los recursos no administrados y sin agente para detener las amenazas con mayor rapidez y reforzar la defensa coordinada.

77%

de los equipos de TI carecen de visibilidad completa en entornos híbridos[1]

3,4 horas

tiempo medio que tardan los atacantes en atacar Active Directory tras obtener acceso[2]

3 días

tiempo medio antes de que un atacante sea detectado dentro de un entorno[2]

LO QUE OFRECE SOPHOS NDR

Cuatro resultados para una defensa de red más sólida.

Vea más en toda la red.

Obtenga visibilidad a nivel de red de las comunicaciones que involucran recursos administrados, no administrados y sin agente. Identifique comportamientos sospechosos y actividades de ataque que podrían no ser visibles para los controles individuales.

- Análisis de comportamiento para identificar comportamiento sospechoso en toda la red
- Visibilidad de los recursos no administrados, de IoT y OT, y sin agente
- Detección del movimiento lateral y de las comunicaciones de mando y control

Detenga las amenazas más rápido.

Reduzca el tiempo entre la detección y la respuesta. En un dispositivo Sophos NDR con el complemento IDS/IPS, el modo activo en línea puede bloquear automáticamente paquetes maliciosos conocidos en la ruta de la red.

- Bloquear paquetes maliciosos conocidos en tiempo real
- Pasar de la monitorización pasiva a la prevención activa en línea
- Aplicar inspección profunda de paquetes y IDS/IPS directamente en la ruta de tráfico

Despliegue la solución a su manera.

Despliegue la solución como dispositivo virtual, en hardware dedicado de Sophos NDR o en hardware compatible de terceros. Adapte la monitorización y la aplicación de medidas a su arquitectura, sus requisitos y su tolerancia al riesgo.

- Despliegues virtuales ilimitados
- Opciones de hardware adaptadas a su entorno
- Modos de despliegue SPAN/TAP y en línea para satisfacer los requisitos operativos

Simplifique las operaciones mediante Sophos Fusion.

Integre la telemetría de red, las detecciones y el contexto de red en Sophos Fusion, junto con información de estaciones de trabajo, cortafuegos, identidad, correo electrónico y nube, para la investigación y la respuesta coordinada.

- Unificar el contexto de red con información de todo Sophos Fusion
- Enriquezca las investigaciones de Sophos MDR y XDR con telemetría NDR
- Coordinar la detección y la respuesta en todo el sistema de defensa Sophos Fusion

SOPHOS NDR DE UN VISTAZO

- Los análisis de comportamiento basados en IA y aprendizaje automático descubren amenazas desconocidas y esquivas
- Capacidades probadas de inspección profunda de paquetes y IDS/IPS identifican amenazas conocidas
- Bloqueo en línea activo de tráfico malicioso conocido
- Opciones de despliegue como dispositivo virtual, en hardware dedicado de Sophos o en hardware compatible de terceros

A QUIÉN VA DIRIGIDO SOPHOS NDR

- Organizaciones que buscan cerrar brechas de visibilidad de red
- Equipos de seguridad que buscan visibilidad en recursos no administrados y sin agente
- Organizaciones que requieren un despliegue NDR flexible en redes diversas y distribuidas
- MSP y MSSP que amplían la monitorización de redes, la búsqueda de amenazas y los servicios de seguridad gestionados

SU VENTAJA FRENTE A LAS AMENAZAS DE RED

Detección de comportamientos y prevención activa en una sola solución.

Mayor cobertura de detección

Los atacantes pueden explotar las brechas de visibilidad en redes híbridas, dispositivos no administrados y recursos sin agente. Sophos NDR combina análisis de comportamiento, análisis de tráfico cifrado, búsqueda de amenazas, inspección profunda de paquetes e IDS/IPS para detectar amenazas conocidas y desconocidas.

Bloquear amenazas directamente en la ruta de la red

La detección por sí sola puede hacer que los equipos de seguridad respondan después de que el tráfico malicioso ya haya alcanzado su destino. En un dispositivo Sophos NDR con el complemento IDS/IPS, el modo activo en línea inspecciona el tráfico en tiempo real y bloquea automáticamente paquetes maliciosos conocidos en la ruta de la red.

Defensa conectada a través de Sophos Fusion

Las amenazas de red rara vez existen de forma aislada. Sophos NDR aporta telemetría de red, detecciones y contexto de red a Sophos Fusion, lo que ayuda a los equipos a acelerar las investigaciones y coordinar la respuesta en todo el sistema de defensa.

OPINIONES DE LOS CLIENTES

"En general, mi experiencia con Sophos NDR ha sido bastante buena. Ayuda mucho a obtener visibilidad sobre el comportamiento anómalo de la red y a detectar patrones que normalmente pasarían desapercibidos en la monitorización tradicional. Algo que realmente aprecio es que las alertas son claras y fáciles de interpretar, lo que acelera el análisis y la toma de decisiones."[3]

Seguridad de TI y gestión de riesgos, sector bancario — Gartner® Peer Insights™

SOPHOS FUSION

Un único sistema. Todos los puntos de control. Una defensa coordinada.

Sophos NDR forma parte de Sophos Fusion, el sistema de ciberdefensa más completo del mundo. Protege a las organizaciones de las amenazas basadas en IA cuya velocidad de propagación supera la capacidad de reacción de los responsables de seguridad.

sophos.com/NDR →

[1] SolarWinds, Informe sobre el estado de la monitorización y la observabilidad de 2026

[2] Sophos, Informe de Sophos sobre adversarios activos de 2026

[3] https://www.gartner.com/reviews/market/network-detection-and-response/vendor/sophos/product/sophos-ndr/review/view/6513218

El contenido de Gartner Peer Insights consiste en las opiniones de usuarios finales individuales basadas en sus propias experiencias; no deben considerarse declaraciones de hecho, ni representan las opiniones de Gartner ni de sus afiliados. Gartner no apoya a ningún proveedor, producto o servicio descrito en este contenido ni ofrece ninguna garantía, expresa o implícita, con respecto a este contenido, sobre su exactitud o integridad, incluida cualquier garantía de comercialización o conveniencia para fines particulares.

Gartner® y Peer Insights™ son marcas comerciales de Gartner, Inc. y/o asociados. Reservados todos los derechos.

© Copyright 2026. Sophos Ltd. Todos los derechos reservados. 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.

2026-10-23 SB-ES (TA)

SOPHOS