Sophos Network Detection and Response

Un potente complemento para Sophos XDR y Sophos MDR

Sophos NDR funciona junto con sus endpoints y firewalls gestionados para supervisar la actividad de red en busca de patrones sospechosos y maliciosos que las soluciones no pueden ver. Sophos NDR detecta flujos de tráfico anormales de sistemas no gestionados, dispositivos IoT, recursos no autorizados, amenazas internas, ataques de día cero desconocidos y patrones inusuales en lo más profundo de la red.

Sophos NDR ofrece una visibilidad crucial de la actividad de red que otros productos no incluyen

Los atacantes son expertos en eludir la detección, pero todo ataque necesita moverse por la red. Sophos NDR detecta patrones de tráfico de red sospechosos que pasan desapercibidos a sus endpoints y firewalls gestionados, por ejemplo:

- **Dispositivos de red desconocidos o desprotegidos**: incluyen dispositivos IoT u OT legítimos que los sensores de endpoints no pueden gestionar totalmente, así como sistemas desconocidos o no identificados de la red. Estos dispositivos pueden verse afectados durante un ataque. Sophos NDR identifica y supervisa estos dispositivos en busca de comportamientos sospechosos o maliciosos que puedan indicar un ataque.
- **Recursos no autorizados**: Sophos NDR puede identificar y supervisar fácilmente aquellos recursos no autorizados que puedan incorporarse a la red ya comprometidos o utilizarse para iniciar un ataque.
- **Actividad de comando y control (C2) nueva y desconocida**: muchos ataques y filtraciones se orquestan a distancia mediante comunicaciones que parecen legítimas entre el atacante y sus procesos remotos dentro de la red. Sophos NDR puede detectar nueva actividad de comando y control de día cero para identificar un ataque dirigido individualizado que puede estar iniciándose.
- **Patrones y flujos de tráfico de red sospechosos o maliciosos**: pueden ser señales importantes en la identificación temprana de un ciberataque. Los indicios pueden incluir actividad de red o accesos remotos fuera de horas de trabajo, cargas de datos sospechosas o exfiltraciones, patrones de tráfico anormales y tráfico malicioso generado por malware conocido.

NDR funciona junto con su firewall

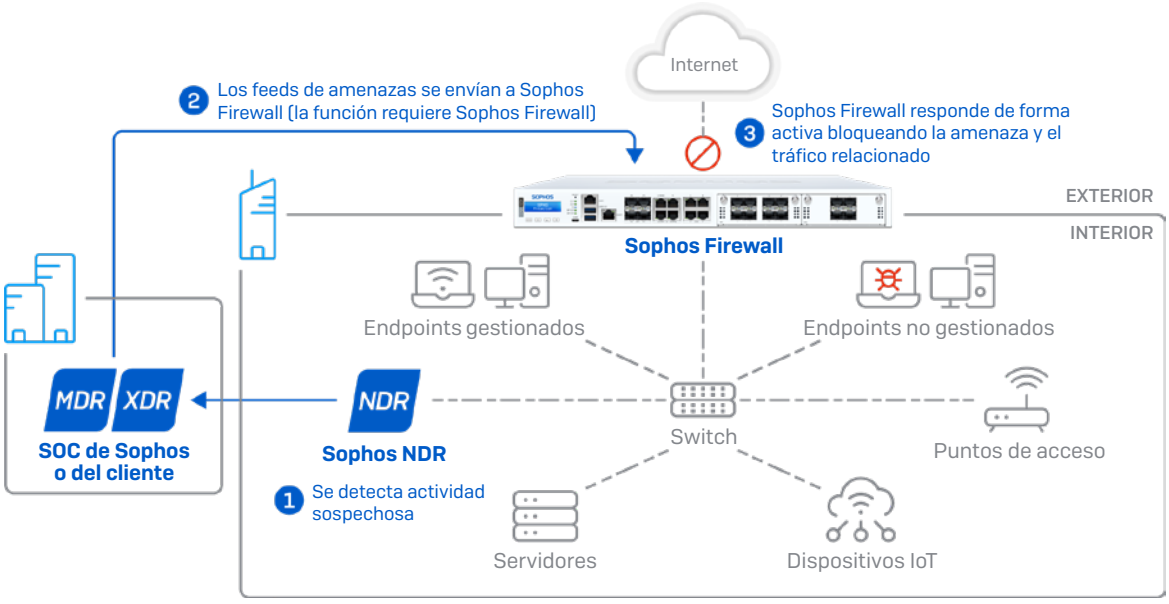
Los firewalls tienen un papel fundamental en la protección del perímetro de red y el control de lo que entra y sale. Sophos NDR es el complemento perfecto para su solución de firewall, ya que funcionan de manera conjunta para ofrecer información clave y protección en la parte más profunda de la red, donde el firewall no tiene visibilidad. También incluye tecnologías que identifican de forma única la actividad sospechosa y maliciosa que transita por su red interna y que ninguna protección para firewalls o endpoints puede detectar.

Aspectos destacados

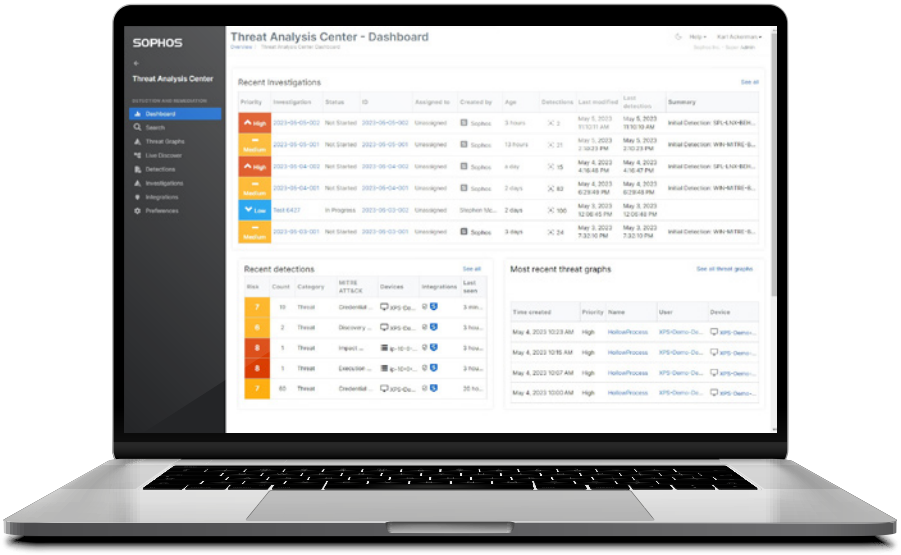
- El complemento perfecto para Sophos XDR y MDR que ofrece detecciones en lo más profundo de una red.
- Funciona junto con su firewall para detectar actividad y amenazas en la red.
- Detecta actividad de red sospechosa procedente de dispositivos desconocidos o no gestionados, recursos no autorizados y servidores C2 de día cero.
- Inspecciona flujos de tráfico cifrado sin comprometer la PII.
- Despliegue, configuración y gestión desde Sophos Central.
- Utilice la consola de investigación para obtener información clave sobre la actividad de red sospechosa y analizar o investigar patrones anómalos.

SOPHOS

Sophos NDR opera en lo más profundo de la red para detectar ataques

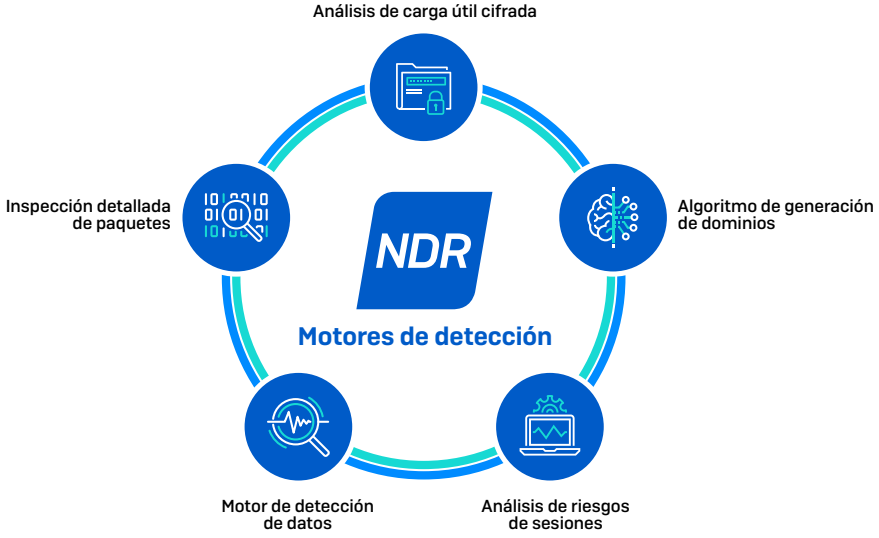


- Supervisa el tráfico en la parte más profunda de una red usando cinco motores en tiempo real.
- Detecta la actividad de todos los recursos de la red, incluidos los sistemas no gestionados, los dispositivos IoT y los recursos no autorizados, e identifica el fabricante y el sistema operativo, así como cualquier patrón de tráfico sospechoso procedente de estos dispositivos.
- Envía datos y alertas a Sophos Central Data Lake y al equipo SOC de Sophos MDR o a su equipo XDR.
- Obtenga visibilidad e información clave sobre la actividad de la red y las aplicaciones, los flujos de riesgo y el tráfico sospechoso con una consola de investigación fácil de utilizar.
- Si tiene Sophos Firewall, dispondrá de respuesta automatizada a las amenazas para bloquearlas inmediatamente y evitar la propagación lateral.
- Se ejecuta como un dispositivo virtual en plataformas de hipervisor populares como VMware y Hyper-V.
- Se conecta directamente a su switch mediante el reflejo de puertos SPAN para supervisar todo el tráfico.
- Inspecciona los datos de paquetes cifrados sin comprometer los datos PII.



Motores de detección de Sophos NDR

Sophos NDR incluye cinco motores de detección que, de forma continua, analizan los flujos de tráfico de red y aplican análisis de Machine Learning con IA para identificar actividad sospechosa y maliciosa en lo más profundo de la red.



Motores de detección	Descripción
Análisis de cargas cifradas (EPA)	Detecta servidores C2 de día cero y nuevas variantes de familias de malware basándose en patrones observados de tamaño de sesión, dirección y tiempos entre llegadas.
Algoritmos de generación de dominios (DGA)	Identifica la presencia de tecnología de generación dinámica de dominios utilizada por el malware para evitar la detección.
Inspección detallada de paquetes (DPI)	Supervisa el tráfico tanto cifrado como no cifrado utilizando indicadores de peligro (IOC) conocidos para identificar rápidamente a los atacantes y las tácticas, técnicas y procedimientos (TTP) de las amenazas.
Análisis de riesgos de sesiones (SRA)	Potente motor lógico que se sirve de reglas que avisan sobre una multitud de factores de riesgo basados en las sesiones.
Motor de detección de dispositivos (DDE)	Motor de consulta extensible que utiliza un modelo de predicción con Deep Learning para analizar el tráfico cifrado en busca de patrones en flujos de red no relacionados y detectar actividad de escaneado de puertos y de ataques por fuerza bruta SSH.

Licencias de Sophos NDR

Sophos NDR es el complemento perfecto para Sophos XDR y Sophos MDR y está disponible como paquete de integración. Los precios de Sophos NDR dependen del número total de usuarios y servidores de la organización. El software del dispositivo virtual se incluye con la licencia, y puede desplegar tantos sensores de NDR como necesite. Esta opción es más asequible y flexible que las ofertas de la competencia que cobran por instancia.

Especificaciones técnicas de Sophos NDR

Plataformas compatibles

- VMware ESXi6.7 y posterior
- Microsoft Hyper-V 6.0.600118016 (Windows Server 2016) o posterior
- Amazon AWS c5n.2xlarge
- Hardware certificado

Hardware	Rendimiento máx.	Conexiones/seg. máx.	N.º de CPU	Memoria
Dell R660 (2 sockets)	40Gbps	120 K	64	128GB
Dell R660 (1 socket)	40Gbps	80 K	32	64GB
Dell R650	20Gbps	40 K	24	64GB
Dell R450	10Gbps	20 K	16	32GB
Dell R350	4Gbps	8000	8	32GB
Intel Nuc 13.ª gen.	2.5Gbps	4 K	12	32GB

Requisitos del sistema para VM

Las VM de Sophos NDR admiten hasta 1 Gbps por sensor:

- Utilice los valores de VM predeterminados para volúmenes de tráfico medios:
  - Hasta 500 Mbps
  - Hasta 70 000 paquetes/s
  - Hasta 1200 flujos/s
- Redimensione la VM para 8 vCPU para volúmenes de tráfico altos:
  - Hasta 1 Gbps
  - Hasta 300 000 paquetes/s
  - Hasta 4500 flujos/s

Recursos adicionales:

- Recursos de NDR en Sophos Community
- Mejore las operaciones de seguridad con Sophos Network Detection and Response (NDR)
- Especificaciones del hardware certificado

Para obtener más información, visite

es.sophos.com/ndr

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

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

24-12-19 DS-ES (MP)