Sophos Network Detection and Response

Supervise el tráfico de red para identificar actividad maliciosa más rápido

Cada segundo cuenta cuando hay un adversario en su entorno. Pero, con demasiada frecuencia, los responsables de la defensa se ven ralentizados por las limitaciones de visibilidad y datos. Y esto se vuelve aún más complicado cuando las herramientas de seguridad no funcionan bien de forma conjunta.

Unos datos más completos permiten una estrategia de detección más precisa

Las organizaciones pueden beneficiarse de un enfoque holístico a la detección y respuesta a amenazas y de formas más rápidas de correlacionar un volumen y una variedad de datos cada vez mayores. Cuanto más exhaustiva es la visibilidad y el contexto, más precisa es la investigación de la actividad de las amenazas. Esto significa que, al integrarse la telemetría de seguridad, se obtiene una visión más precisa de toda la ruta del ataque.

Como complemento de Sophos MDR, el dispositivo virtual Sophos Network Detection and Response (NDR) supervisa el tráfico de red para identificar flujos de red sospechosos. Las detecciones se envían a Sophos Data Lake, se evalúan y se les asigna la puntuación de riesgo que corresponda, y así se generan los casos que investiga y valida el equipo de respuesta a amenazas de Sophos. Las detecciones de NDR pueden desencadenar una investigación de las conexiones internas del host con los servidores de la red, y también se pueden utilizar para optimizar las búsquedas de actividad de amenazas en los endpoints a fin de determinar qué dispositivos se están comunicando.

Su protección requiere herramientas que funcionen bien en conjunto

Sophos NDR es una integración nativa de Sophos MDR. Se conecta fácilmente, no produce demasiado ruido ni puntuaciones de riesgo no coincidentes, y no requiere tiempo para establecer una base de referencia como otras soluciones. En la tabla de abajo se describe la funcionalidad de los motores de detección de Sophos NDR.

Sophos NDR se ofrece como dispositivo virtual. Una vez desplegado, se autentica con la consola de administración de Sophos Central y empieza a enviar datos. El estado y las detecciones de NDR pueden visualizarse en Sophos Central.

Aspectos destacados

- Añada detecciones de red a Sophos MDR para supervisar flujos de red sospechosos a los que no puede acceder el software para endpoints
- Permita investigaciones y búsquedas de amenazas en conexiones internas del host con los servidores de la red y otras conexiones de red
- Detecte malware en el tráfico cifrado que con frecuencia permanece oculto
- Visualice fácilmente el estado y las detecciones del sensor de NDR en Sophos Central

Motores de detección y casos de uso de Sophos NDR

Motores de detección	Descripción
Análisis de cargas cifradas (EPA)	Detecta servidores de comando y control (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.

SOPHOS

Identifique comportamientos sospechosos más allá de sus endpoints

Sophos NDR utiliza motores independientes de detección de amenazas para detectar comportamientos anormales y sospechosos del tráfico como:

- Conexiones desde un dispositivo desconocido
- Datos cargados durante una sesión remota
- Incremento en el uso de archivos de datos de propiedad
- Sesiones de red generadas por familias de malware

Sophos NDR tiene la capacidad de detectar posibles comportamientos maliciosos e identifica:

- **Dispositivos desprotegidos**: Sophos NDR identifica dispositivos legítimos que no se han protegido y que podrían utilizarse como puntos de entrada de los ciberataques.
- **Recursos no autorizados**: además de supervisar el tráfico a los dispositivos desprotegidos, Sophos NDR identifica los dispositivos no autorizados que se comunican a través de la red.
- **Sensores de IoT y TO**: los dispositivos del Internet de las cosas (IoT) y la tecnología operativa (TO) presentan desafíos para la supervisión de amenazas porque muchos de estos dispositivos no son compatibles con los agentes de protección de endpoints. Sophos NDR supervisa los datos de los dispositivos IoT y TO para detectar la actividad de los atacantes.
- **Ataques de día cero**: Sophos NDR cuenta con un proceso patentado para detectar los servidores C2 de día cero usados por los atacantes que se basa en patrones observados de tamaño de los paquetes de las sesiones, dirección y tiempos entre llegadas.
- **Amenazas internas**: Sophos NDR proporciona visibilidad sobre los flujos de tráfico de red y la exfiltración de datos que inicialmente podrían parecer "normales" procedentes de usuarios internos.

Los precios de Sophos NDR dependen del número total de usuarios y servidores de la organización. El software del dispositivo virtual está incluido con la licencia. En la tabla de abajo se describen los requisitos del sistema de Sophos NDR.

Requisitos del sistema para Sophos NDR

Velocidad de red	1 Gbps	5 Gbps	10 Gbps
CPU	4	8	16
RAM	16 GB	32 GB	64 GB
Almacenamiento	160 GB	320 GB	640 GB
N.º estimado de usuarios	Hasta 2000	Hasta 10 000	Hasta 30 000

*Variará en función de la organización.

Más información sobre Sophos NDR

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

22-11-15 DS-EN (DD)

SOPHOS