Sophos XDR

Intercept X Advanced with XDR, Intercept X Advanced for Server with XDR

Intercept X consolida una potente detección y respuesta ampliadas (XDR) con una protección para endpoints inigualable. Busque amenazas para detectar adversarios activos o aplíquelo a sus operaciones de TI a fin de mantener la higiene de su seguridad informática. Cuando se encuentre un problema de forma remota, responda con precisión. Amplíe la visibilidad más allá del endpoint con exhaustivas fuentes de datos que incluyen el endpoint, el servidor, el firewall y el correo electrónico.

Responda a preguntas sobre la búsqueda de amenazas y las operaciones de TI

Consiga respuestas rápidamente a preguntas críticas para el negocio. Tanto administradores de TI como profesionales de la ciberseguridad verán un valor añadido real cuando estén realizando operaciones de TI y tareas de búsqueda de amenazas en su día a día.

Empiece con la mejor protección

Intercept X detiene las filtraciones antes de que puedan iniciarse. Esto significa que obtiene una mejor protección y dedica menos tiempo a investigar incidentes que deberían haberse detenido automáticamente. También tiene acceso a información sobre amenazas detallada que le brinda los conocimientos necesarios para tomar medidas rápidas e informadas.

Profundice en los detalles y responda con rapidez

Cuando identifique algo que requiera más investigación, puede partir de Sophos Data Lake y profundizar para obtener datos detallados en tiempo real, directamente desde el dispositivo, además de hasta 90 días de datos históricos. Cuando se confirme un problema, acceda de forma remota al dispositivo y tome las medidas necesarias, como desinstalar una aplicación y reiniciarlo.

Visibilidad entre productos

Sophos XDR va más allá del endpoint y el servidor, al permitir que Sophos Firewall, Sophos Email y otras fuentes de datos* envíen datos clave a Sophos Data Lake, lo que le proporciona una visión increíblemente amplia del entorno de su empresa.

Obtenga información incluso cuando un dispositivo está sin conexión

Sophos Data Lake, un componente clave de la funcionalidad XDR, es un repositorio de datos en la nube. Hace posible la capacidad de almacenar y acceder a información crítica de sus endpoints, servidores, firewall y correo electrónico, además de utilizar información sobre dispositivos incluso cuando se encuentran sin conexión.

Póngase en marcha en segundos

Elija de una biblioteca de consultas SQL ya escritas para formular una amplia variedad de preguntas de TI y seguridad. Si lo prefiere, puede personalizarlas o escribir sus propias consultas. También puede consultar la comunidad de Sophos, donde se comparten consultas regularmente.

Aspectos destacados

- Responda a preguntas críticas para el negocio sobre la búsqueda de amenazas y las operaciones de TI
- Diseñado para administradores de TI y analistas de seguridad
- Tome medidas correctivas de forma remota en los dispositivos de interés
- Obtenga una visión holística del entorno de TI de su empresa y profundice en detalles granulares cuando sea necesario
- Sírvase de endpoints, servidores, firewall, correo electrónico y otras fuentes de datos*
- Consultas SQL predefinidas totalmente personalizables
- Disponible para Windows, macOS y Linux

**Cloud Optix y Sophos Mobile disponibles en breve*

SOPHOS

Casos de uso

Operaciones de TI

- ¿Por qué funciona lento un equipo?
- ¿Qué dispositivos tienen vulnerabilidades conocidas, servicios desconocidos o extensiones de navegador no autorizadas?
- ¿Hay programas ejecutándose que deberían eliminarse?
- Identifique dispositivos no administrados, invitados o IoT
- ¿Por qué va lenta la conexión de red de la oficina? ¿Qué aplicación lo está provocando?
- Revise los últimos 30 días para identificar actividad inusual en un dispositivo extraviado o destruido

Búsqueda de amenazas

- ¿Qué procesos están intentando establecer una conexión de red en puertos no estándar?
- Muestre procesos que tienen archivos o claves de registro modificados recientemente
- Enumere los indicadores de peligro detectados con asignaciones a la plataforma MITRE ATT&CK
- Amplíe investigaciones hasta 30 días sin tener que volver a conectar el dispositivo
- Utilice detecciones ATP e IPS desde el firewall para investigar hosts sospechosos
- Compare información de encabezado del correo electrónico, SHA y otros indicadores de peligro para identificar tráfico a un dominio malicioso

¿Qué incluye?

	Detección y respuesta ampliadas (XDR)
Fuentes de datos entre productos	✓
Consultas entre productos	✓
Consultas de endpoint y servidor	✓
Sophos Data Lake	✓
Periodo de retención de Data Lake	30 días
Periodo de retención de datos en disco	✓
Biblioteca de consultas SQL	✓
Capacidades de protección en Intercept X	✓

Para obtener más información sobre las licencias, consulte las guías de licencias de Intercept X e Intercept X for Server.

Pruébelo gratis hoy mismo

Regístrese para una evaluación gratuita de 30 días en es.sophos.com/intercept-x

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

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

08-07-21 DS-ES (PS)

SOPHOS