# Sophos XDR


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

Intercept X es la única solución XDR del sector que sincroniza la protección nativa de endpoints, servidores, firewalls, correo electrónico, la nube y O365. Obtenga una visión holística del entorno de su organización con conjuntos de datos exhaustivos y un análisis profundo para la detección, investigación y respuesta a las amenazas, tanto para los equipos SOC dedicados como para los administradores de TI.

## 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.

## Sepa en qué centrarse

Céntrese en las cuestiones importantes con una lista priorizada de detecciones sospechosas y configuraciones vulnerables que incluya información clave para una investigación más a fondo. Elija de una biblioteca de plantillas ya escritas para formular una amplia variedad de preguntas de operaciones de TI y búsqueda de amenazas o cree sus propias plantillas.

## Minimice la investigación y el tiempo de respuesta

Las investigaciones guiadas por IA le permiten comprender rápidamente el alcance y la causa de un incidente y minimizar el tiempo de respuesta. Acceda a los dispositivos para conocer su estado en tiempo real y obtener hasta 90 días de datos históricos o 30 días de datos históricos en Data Lake.

## Visibilidad entre productos

Consiga una visibilidad máxima de su organización con la integración nativa de datos de Intercept X, Intercept X for Server, Sophos Firewall, Sophos Email, Sophos Mobile, Cloud Optix y Microsoft Office 365.

## Soporte para múltiples plataformas y sistemas operativos

Inspeccione su entorno ya sea en la nube, local o virtual en despliegues de infraestructura de Windows, macOS, Linux, Amazon Web Services, Microsoft Azure, Google Cloud Platform y Oracle Cloud.

## Aspectos destacados

- Responda a preguntas críticas para el negocio sobre la búsqueda de amenazas y las operaciones de TI
- Sírvase de una lista priorizada de detecciones e investigaciones guiadas por IA
- 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
- Integraciones nativas con endpoints, servidores, firewalls, correo electrónico, la nube, dispositivos móviles y O365
- Acceda a una biblioteca de casos de uso de plantillas personalizables ya escritas

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
- Localice dispositivos móviles sin parches aplicados o con software no actualizado

## 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
- Identifique a usuarios con múltiples intentos de autenticación fallidos

# ¿Qué incluye?

| | Detección y respuesta ampliadas (XDR) |
|---|---|
| Fuentes de datos entre productos | ✓ |
| Detección, investigación y respuesta entre productos | ✓ |
| Lista de detecciones priorizada e investigaciones guiadas por IA | ✓ |
| Sophos Data Lake | ✓ |
| Periodo de retención de Data Lake | 30 días |
| Información del estado en tiempo real | ✓ |
| Periodo de retención de datos en disco | Hasta 90 días |
| Biblioteca de plantillas de operaciones de TI y búsqueda de amenazas | ✓ |
| 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



06-01-22 DS-ES (MP)

SOPHOS