Intercept X

Intercept X Advanced, Intercept X Advanced with EDR, Intercept X Advanced with XDR, Intercept X Advanced with MTR

Sophos Intercept X es la mejor protección para endpoints del mundo. Detiene las ciberamenazas más recientes con una combinación de IA con Deep Learning, funciones antiransomware, prevención de exploits y otras técnicas.

Sophos Intercept X utiliza un completo enfoque de defensa exhaustiva para la protección de endpoints, en lugar de depender de una técnica de seguridad principal. Este enfoque por capas combina técnicas modernas y tradicionales para detener la más amplia gama de amenazas.

Detenga las amenazas desconocidas

La IA con Deep Learning de Intercept X destaca en la detección y el bloqueo de malware incluso si es desconocido. Lo consigue examinando detenidamente los atributos de los archivos de cientos de millones de muestras para identificar amenazas sin necesidad de firmas.

Bloquee el ransomware

Intercept X incluye funciones antiransomware avanzadas que detectan y bloquean los procesos de cifrado malicioso utilizados en los ataques de ransomware. Los archivos que se han cifrado se revierten a un estado seguro, lo que minimiza cualquier impacto en la productividad empresarial.

Impida los exploits

La tecnología antiexploits detiene las técnicas de explotación de las que se sirven los atacantes para infiltrarse en dispositivos, robar credenciales y distribuir malware. Al detener las técnicas usadas en toda la cadena de ataque, Intercept X mantiene protegida su empresa frente a los ataques sin archivos y los exploits de día cero.

Defensas por capas

Además de una moderna y potente funcionalidad, Intercept X también utiliza técnicas tradicionales probadas. Algunos ejemplos de estas funciones incluyen el bloqueo de aplicaciones, el control web, la prevención de pérdidas de datos y la detección de malware basada en firmas. Esta combinación de técnicas modernas y tradicionales reduce la superficie de ataque y ofrece una defensa en profundidad óptima.

Seguridad Sincronizada

Las soluciones de Sophos funcionan mejor de forma conjunta. Por ejemplo, Intercept X y Sophos Firewall comparten datos para aislar automáticamente los dispositivos comprometidos al tiempo que se realiza la limpieza, y luego restablecen el acceso a la red una vez neutralizada la amenaza. Todo ello sin necesidad de que intervenga ningún administrador.

Aspectos destacados

- Detiene las amenazas desconocidas mediante IA con Deep Learning
- Bloquea el ransomware y revierte los archivos afectados a un estado seguro
- Impide las técnicas de explotación usadas durante toda la cadena de ataque
- Responde preguntas críticas sobre la búsqueda de amenazas y las operaciones de TI con EDR
- Proporciona una seguridad 24/7/365 por medio de un servicio totalmente administrado
- Vea y sírvase del firewall, el correo electrónico y otras fuentes de datos* con XDR
- Fácil de desplegar, configurar y mantener incluso en entornos de teletrabajo

**Cloud Optix y Sophos Mobile disponibles en breve*

SOPHOS

Detección y respuesta para endpoints (EDR)

Sophos EDR, diseñado para administradores de TI y especialistas en ciberseguridad, responde preguntas críticas sobre la búsqueda de amenazas y las operaciones de TI. Por ejemplo, identifica dispositivos con problemas de rendimiento o procesos sospechosos que intentan conectarse en puertos no estándar y después accede de forma remota al dispositivo para tomar medidas correctivas.

Managed Threat Response (MTR)

Servicio de búsqueda, detección y respuesta a amenazas 24/7/365 prestado por un equipo de expertos de Sophos. Los analistas de Sophos responden a posibles amenazas, buscan indicadores de peligro y proporcionan análisis detallados sobre los eventos que incluyen lo que ha ocurrido, dónde, cuándo, cómo y por qué.

Detección y respuesta ampliadas (XDR)

Vaya más allá de los endpoints y servidores, y sírvase del firewall, el correo electrónico y otras fuentes de datos*. Obtenga una visión holística de la posición de ciberseguridad de su empresa con la capacidad de profundizar en detalles granulares. Por ejemplo, entienda los problemas de red de sus oficinas y qué aplicaciones los están provocando.

**Integración de XDR en Sophos Cloud Optix y Sophos Mobile disponible en breve*

Gestión sencilla

Intercept X se gestiona a través de Sophos Central, la plataforma de administración en la nube para todas las soluciones de Sophos. Es un único panel intuitivo para todos sus dispositivos y productos que facilita el despliegue, la configuración y la gestión de su entorno incluso en condiciones de teletrabajo.

Especificaciones técnicas

Intercept X admite despliegues Windows y macOS. Para obtener la información más reciente, lea los requisitos del sistema de Windows y la hoja de datos de Mac.

Resumen de licencias

Funciones	Intercept X Advanced	Intercept X Advanced with EDR	Intercept X Advanced with XDR	Intercept X Advanced with MTR Standard	Intercept X Advanced with MTR Advanced
Protección base (Control de apps, detección de comportamientos y más)	✓	✓	✓	✓	✓
Protección next-gen(Deep Learning, antiransomware, protección contra ataques sin archivos y más)	✓	✓	✓	✓	✓
EDR (Detección y respuesta para endpoints)		✓	✓	✓	✓
XDR (Detección y respuesta ampliadas)			✓		Véase la nota*
Managed Threat Response (MTR – Servicio 24/7/365 de búsqueda y respuesta a amenazas)				✓	✓
MTR Advanced (Búsqueda sin pistas, contacto dedicado y más)					✓

***Nota:** el equipo de MTR tendrá la capacidad de utilizar los datos y la funcionalidad XDR para los clientes de MTR Advanced. Sin embargo, los clientes de MTR quedarán limitados a la funcionalidad EDR en su consola de Sophos Central a menos que compren una licencia XDR.

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

05-04-21 DS-ES (PS)

SOPHOS

Sophos EDR y XDR

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

Intercept X consolida una potente detección y respuesta para endpoints (EDR) 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. Sophos XDR amplía 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 tanto de la funcionalidad XDR como de EDR, 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*

**Capacidades de XDR disponibles en macOS en breve*

SOPHOS

Casos de uso de EDR y XDR

EDR

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?

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

XDR

- 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
- 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

Los clientes de XDR tienen acceso a toda la funcionalidad y los casos de uso de EDR

¿Qué incluye?

	Detección y respuesta para endpoints (EDR)	Detección y respuesta ampliadas (XDR)
Consultas de productos de fuentes de datos entre productos		✓
Consultas entre productos		✓
Consultas de endpoint y servidor	✓	✓
Sophos Data Lake	✓	✓
Periodo de retención de Data Lake	7 días	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

22-03-21 DS-ES (MP)

SOPHOS

SOPHOS

Managed Threat Response (MTR)

Respuesta a amenazas a cargo de expertos

Sophos Managed Threat Response (MTR) es un servicio totalmente administrado prestado por un equipo de expertos que ofrece funciones de búsqueda, detección y respuesta a amenazas las 24 horas.

Aspectos destacados

- Funciones avanzadas de búsqueda, detección y respuesta ofrecidas como un servicio totalmente gestionado
- Colabore con un equipo de respuesta las 24 horas que toma medidas para contener y neutralizar las amenazas de forma remota
- Decida y controle qué acciones realiza el equipo de MTR y cómo se gestionan los incidentes
- Combina la prestigiosa tecnología del Machine Learning con un equipo de expertos altamente cualificados
- Dos niveles de servicio (Standard y Advanced) ofrecen un conjunto completo de funciones para empresas de todos los niveles de madurez

La notificación de amenazas no es la solución, sino el punto de partida

Pocas empresas cuentan con las herramientas, las personas y los procesos adecuados para gestionar eficazmente su programa de seguridad las 24 horas, a la vez que se protegen de forma proactiva contra las amenazas nuevas y emergentes. Más allá de la simple notificación de ataques o comportamientos sospechosos, el equipo de Sophos MTR emprende acciones específicas en su nombre para neutralizar incluso las amenazas más sofisticadas y complejas.

Con Sophos MTR, su empresa contará con el soporte de un equipo de cazadores de amenazas y expertos en respuesta, disponible las 24 horas, que se dedicarán a:

- Buscar y validar de forma proactiva posibles amenazas e incidentes.
- Utilizar toda la información disponible para determinar el alcance y la gravedad de las amenazas.
- Aplicar el contexto empresarial adecuado para las amenazas válidas.
- Iniciar acciones para interrumpir, contener y neutralizar amenazas de forma remota.
- Brindar asesoramiento práctico para abordar la causa raíz de los incidentes recurrentes.

Respuesta humana acelerada por máquinas

Sophos MTR, basado en nuestra tecnología de Intercept X Advanced with EDR, fusiona la tecnología del Machine Learning con el análisis de expertos para ofrecer una búsqueda y detección de amenazas mejoradas, una investigación más a fondo de las alertas y acciones específicas para eliminar las amenazas con rapidez y precisión. Esta fusión de la prestigiosa protección para endpoints y EDR inteligente de Sophos con un equipo de expertos en seguridad de primera categoría da lugar a lo que llamamos "respuesta humana acelerada por máquinas".

Control y transparencia totales

Sophos MTR le permite tomar las decisiones y controlar cómo y cuándo se derivan los incidentes potenciales, qué acciones de respuesta (si las hubiera) desea que tomemos y quién debe incluirse en las comunicaciones. Sophos MTR le ofrece tres modos de respuesta para que pueda elegir la forma de trabajo óptima para el equipo de MTR a la hora de colaborar con usted durante un incidente:

Notificar: Le notificamos la detección y le proporcionamos datos para ayudarle con la priorización y la respuesta.

Colaborar: Trabajamos con su equipo interno o puntos de contacto externos para responder a la detección.

Autorizar: Gestionamos las acciones de contención y neutralización y le informamos de las medidas tomadas.

Niveles de servicio de Sophos MTR

Sophos MTR ofrece dos niveles de servicio (Standard y Advanced) a fin de proporcionar un conjunto completo de funciones para empresas de todos los tamaños y niveles de madurez. Independientemente del nivel de servicio seleccionado, las empresas pueden beneficiarse de cualquiera de los tres modos de respuesta (Notificar, Colaborar o Autorizar) para adaptarse a sus necesidades específicas.

Sophos MTR: Standard

Búsqueda de amenazas a partir de pistas las 24 horas

Las actividades o artefactos maliciosos confirmados (indicios sólidos) se bloquean o detienen automáticamente, lo que libera la carga de trabajo de los analistas de amenazas para que puedan realizar búsquedas a partir de pistas. Este tipo de búsqueda de amenazas implica la agregación e investigación de eventos causales y adyacentes (indicios débiles) para descubrir nuevos indicadores de ataque y de peligro que antes no podían detectarse.

Comprobación del estado de seguridad

Mantenga el máximo rendimiento de sus productos de Sophos Central, empezando por Intercept X Advanced with EDR, con exámenes proactivos de sus condiciones operativas y mejoras de configuración recomendadas.

Informes de actividades

Los resúmenes de las actividades de los casos facilitan la priorización y comunicación para que su equipo sepa qué amenazas se han detectado y qué acciones de respuesta se han llevado a cabo dentro de cada periodo del informe.

Detección de adversarios

La mayoría de los ataques eficaces dependen de la ejecución de un proceso que puede parecer legítimo para las herramientas de supervisión. Mediante técnicas de investigación patentadas, nuestro equipo determina la diferencia entre un comportamiento legítimo y las tácticas, técnicas y procedimientos utilizados por los atacantes.

Sophos MTR: Advanced *Incluye todas las funciones de Standard, más lo siguiente:*

Búsqueda de amenazas sin pistas las 24 horas

Aplicando la ciencia de datos, la información sobre amenazas y la intuición de experimentados cazadores de amenazas, combinamos el perfil de su empresa, sus activos de alto valor y usuarios de alto riesgo para anticiparnos al comportamiento de los atacantes e identificar nuevos indicadores de ataque.

Telemetría optimizada

Las investigaciones sobre amenazas se complementan con la telemetría de otros productos de Sophos Central que van más allá del endpoint para ofrecer una imagen completa de las actividades del adversario.

Mejora proactiva de la posición de seguridad

Mejore de forma proactiva su posición de seguridad y refuerce sus defensas con una guía prescriptiva para solucionar las debilidades de configuración y arquitectura que merman sus funciones de seguridad general.

Responsable de respuesta a incidentes dedicado

Cuando se confirma un incidente, se le asigna un responsable de respuesta a amenazas dedicado para que colabore directamente con sus recursos locales (equipo interno o partner externo) hasta que se neutralice la amenaza activa.

Soporte telefónico directo

Su equipo tiene acceso telefónico directo a nuestro centro de operaciones de seguridad (SOC). Nuestro equipo de operaciones de MTR está disponible las 24 horas y cuenta con el apoyo de equipos de soporte en 26 emplazamientos en todo el mundo.

Detección de recursos

Desde datos sobre recursos que incluyen versiones de sistemas operativos, aplicaciones y vulnerabilidades hasta la identificación de activos gestionados y no gestionados, ofrecemos información valiosa durante las evaluaciones de impacto, la búsqueda de amenazas y como parte de las recomendaciones para mejorar la postura proactiva.

D512

SAVANT CONSULTORES
RNC: 131221173
Santo Domingo, R.D.

Ventas en España:
Tel.: (+34) 91 375 67 56
Email: comercialES@sophos.com

Ventas en América Latina:
Email: Latamsales@sophos.com

17-09-2018 DSES (GH)

SOPHOS