SOPHOS
Cybersecurity evolved.

Intercept X Advanced with EDR

Detección y respuesta para endpoints creada para la búsqueda de amenazas y las operaciones de TI

Sophos Intercept X Advanced with EDR combina 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.

Aspectos destacados

- La EDR se combina con la mejor protección de endpoints
- Diseñado para analistas de seguridad y administradores de TI
- Mantenga la higiene de TI y busque amenazas de forma proactiva antes de que se produzcan daños
- Haga cualquier pregunta sobre lo que ha ocurrido en el pasado y lo que ocurre ahora
- Consultas SQL predefinidas totalmente personalizables
- Hasta 90 días de acceso rápido a datos en disco históricos y actuales
- Responda de forma remota con precisión usando una herramienta de línea de comandos
- Detecte, investigue y priorice incidentes con la ayuda del Machine Learning
- Acelere las investigaciones y reduzca el tiempo de permanencia del atacante
- Disponible para Windows, MacOS* y Linux

**Próximamente*

La EDR parte de la base de la mejor protección

Para detener las filtraciones antes de que comiencen, la prevención es crucial. Intercept X consolida la mejor protección para endpoints del mundo y la EDR en una única solución. Esto significa que la mayoría de amenazas se detienen incluso antes de que puedan causar daños. Intercept X Advanced with EDR proporciona una garantía adicional de ciberseguridad al ofrecer la capacidad de detectar, investigar y responder a posibles amenazas de seguridad.

Incluir la EDR en una suite de protección de endpoints de máxima calidad permite a Intercept X reducir significativamente la carga de trabajo de EDR. Al impedirse más amenazas, se genera menos ruido, lo que evita que los analistas pierdan el tiempo investigando falsos positivos y un abrumador volumen de alertas.

Añada experiencia, no personal

Detecte automáticamente, priorice e investigue amenazas usando inteligencia artificial: Intercept X Advanced with EDR se sirve del Machine Learning para detectar y priorizar automáticamente posibles amenazas. Si se descubre un archivo potencialmente malicioso, los usuarios pueden emplear el análisis de malware con Deep Learning para analizar automáticamente el malware con sumo detalle, descomponiendo los atributos y el código de los archivos y comparándolos con millones de archivos.

Consultas predefinidas diseñadas por profesionales para profesionales: los analistas de seguridad y administradores de TI pueden empezar a utilizar Sophos EDR desde el primer momento gracias a las consultas SQL listas para usar clasificadas por caso de uso. Las consultas se pueden editar fácilmente para búsquedas personalizadas, crearse de cero u obtenerse de nuestra comunidad.

Responda a las preguntas difíciles reproduciendo las funciones de analistas difíciles de encontrar: Intercept X Advanced with EDR reproduce las tareas que normalmente realizan los analistas expertos, de modo que las empresas pueden añadir experiencia sin tener que añadir personal.

Creado para la búsqueda de amenazas y las operaciones de TI

Sophos Intercept X Advanced es la primera solución EDR diseñada para administradores de TI y analistas de seguridad. Le permite hacer cualquier pregunta sobre lo que ha ocurrido en el pasado y lo que está ocurriendo ahora en sus endpoints. Busque amenazas para detectar adversarios activos o aplíquelo a sus operaciones de TI a fin de mantener la higiene de su seguridad TI. Cuando se encuentre un problema de forma remota, responda con precisión. Esto se consigue a través de dos funciones clave: Live Discover y Live Response.

Live Discover: haga cualquier pregunta para anticiparse Live Discover concede a los analistas de seguridad y administradores de TI la capacidad de formular cualquier pregunta que se les ocurra en relación con sus endpoints y servidores, así como responder a ella. Descubra rápidamente los problemas de sus operaciones de TI para mantener la higiene informática y haga preguntas detalladas para detectar actividad sospechosa. Live Discover utiliza consultas SQL predefinidas totalmente personalizables que pueden buscar rápidamente en hasta 90 días de datos en disco históricos y actuales. Algunos ejemplos de casos de uso son:

Operaciones de TI

- ¿Por qué funciona lento un equipo? ¿Tiene un reinicio pendiente?
- ¿Qué dispositivos tienen vulnerabilidades conocidas, servicios desconocidos o extensiones de navegador no autorizadas?
- ¿Hay programas ejecutándose que deberían eliminarse?
- ¿Está activado el uso compartido remoto? ¿Hay claves SSH no cifradas en el dispositivo? ¿Hay cuentas de invitado activadas?
- ¿Tiene el dispositivo una copia de un archivo específico?

Búsqueda de amenazas

- ¿Qué procesos están intentando establecer una conexión de red en puertos no estándar?
- Enumerar los indicadores de peligro (IOC) detectados con asignaciones a la plataforma MITRE ATT&CK
- Mostrar procesos que tienen archivos o claves de registro modificados recientemente
- Buscar detalles sobre ejecuciones de PowerShell
- Identificar procesos camuflados como services.exe

Live Response: responda de forma remota con precisión Cuando se descubren problemas, Live Response proporciona a los usuarios acceso de línea de comandos a los endpoints y servidores de toda la infraestructura de su empresa. Acceda de forma remota a los dispositivos para realizar más investigaciones o corregir cualquier problema. Los administradores pueden reiniciar dispositivos, finalizar procesos activos, ejecutar scripts, editar archivos de configuración, instalar y desinstalar software, y ejecutar herramientas forenses, entre otras acciones.

Detección y respuesta gestionadas

Sophos Managed Threat Response (MTR) es un servicio totalmente administrado prestado por un equipo de expertos de Sophos que ofrece búsqueda, detección y respuesta a amenazas las 24 horas. Mientras que otros servicios de detección y respuesta gestionadas (MDR) simplemente le avisan de los ataques y eventos sospechosos, con Sophos MTR su empresa cuenta con el respaldo de un equipo de élite de cazadores de amenazas y expertos en respuesta que toman medidas concretas en su nombre para neutralizar incluso las amenazas más sofisticadas. Los clientes que optan por utilizar Sophos MTR también reciben Intercept X Advanced with EDR.

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Endpoint Protection
Técnicas base	✓	✓	✓
Deep Learning	✓	✓	
Antiexploits	✓	✓	
Antiransomware de CryptoGuard	✓	✓	
Detección y respuesta para endpoints (EDR)	✓		

Pruébelo gratis hoy mismo

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

Ventas en España:
Tel.: (+34) 913 756 756
Email: comercialES@sophos.com

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

12-05-20 DS-ES (MP)

SOPHOS