SOPHOS
Cybersecurity made simple.

Intercept X Advanced with EDR

Detección y respuesta inteligentes para endpoints

Sophos Intercept X Advanced with EDR integra la detección y respuesta inteligentes para endpoints (EDR, endpoint detection and response) con la protección contra malware y exploits mejor valorada del mercado y otras funciones de protección de endpoints sin igual.

Aspectos destacados

- La EDR se combina con la mejor protección de endpoints
- Análisis de malware con Deep Learning
- Información sobre amenazas bajo demanda a cargo de SophosLabs
- Detección mediante Machine Learning y priorización de eventos sospechosos*
- Gracias a la investigación guiada, la EDR es accesible a la vez que potente
- Se responde a los incidentes con un solo clic

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 protección incomparable y la detección y respuesta para endpoints (EDR) en una sola solución. Esto significa que la mayoría de amenazas se detienen antes de que puedan causar daños e 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. Cuantas más amenazas se eviten, los equipos de seguridad tienen menos interferencias que investigar. Esto significa que los equipos pueden optimizar los recursos clave, lo que les permite centrarse en las actividades de TI en lugar de perseguir falsos positivos y un volumen abrumador de alertas.

Añada experiencia, no personal

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. A diferencia de otras soluciones de EDR que se basan en analistas humanos altamente cualificados para formular preguntas e interpretar datos, Intercept X Advanced with EDR se basa en el Machine Learning y se mejora gracias a la información sobre amenazas que mantiene SophosLabs.

Experiencia en seguridad*: Intercept X Advanced with EDR pone la experiencia en seguridad en manos del departamento informático al detectar y priorizar automáticamente las amenazas potenciales. Mediante el Machine Learning, los eventos sospechosos se identifican y se priorizan de acuerdo a su importancia. Los analistas pueden ver rápidamente dónde centrar su atención y entender qué máquinas pueden haberse visto afectadas.

Experiencia en malware: La mayoría de las empresas confían en expertos en malware especializados en ingeniería inversa para analizar archivos sospechosos. Este enfoque no solo lleva mucho tiempo y es difícil de lograr, sino que supone un nivel de sofisticación de ciberseguridad que no tienen la mayoría de las empresas. Intercept X Advanced with EDR ofrece un mejor enfoque al servirse del análisis de malware con Deep Learning, que analiza automáticamente el malware con sumo detalle, descomponiendo los atributos y el código de los archivos y comparándolos con millones de archivos. Los analistas pueden ver fácilmente qué atributos y segmentos de código son similares a los archivos "buenos conocidos" y "malos conocidos" para determinar si un archivo debe bloquearse o permitirse.

Experiencia en información sobre amenazas: Cuando Intercept X Advanced with EDR eleva la prioridad de un archivo potencialmente sospechoso, los administradores de TI pueden recopilar más información accediendo a la información sobre amenazas que necesiten a cargo de SophosLabs, que recibe y procesa aproximadamente 400 000 muestras de malware nuevas al día. Esta y otras informaciones sobre amenazas se recopilan, agregan y resumen para facilitar el análisis. Esto significa que los equipos que no cuentan con analistas de información de amenazas especializados ni acceso a servicios de información de amenazas costosos y difíciles de entender pueden beneficiarse de uno de los mejores equipos de investigación de ciberseguridad y ciencia de datos del mundo.

Respuesta guiada a incidentes

Intercept X Advanced with EDR permite a los administradores dar respuesta a las cuestiones difíciles sobre incidentes de seguridad al proporcionar visibilidad sobre el alcance de un ataque, cómo ha empezado, qué se ha visto afectado y cómo responder.
Los equipos de seguridad de todos los niveles de cualificación pueden comprender rápidamente su posición en materia de seguridad gracias a las investigaciones guiadas, que ofrecen sugerencias de los pasos que se deben dar, representaciones visuales claras de los ataques y experiencia integrada.

Cuando se concluye una investigación, los analistas pueden responder con solo pulsar un botón. Las opciones de respuesta rápida incluyen la capacidad de aislar endpoints para realizar una reparación inmediata, limpiar y bloquear archivos y crear resúmenes forenses.

Casos de uso de la EDR

La detección y respuesta inteligentes para endpoints significa que los equipos de seguridad tienen la visibilidad y la experiencia que necesitan para responder a las preguntas difíciles que se plantean como parte de un esfuerzo de respuesta a incidentes.

Conteste las preguntas complejas sobre un incidente:

- Comprenda el alcance y el impacto de los incidentes de seguridad
- Detecte ataques que pueden haber pasado desapercibidos
- Busque indicadores de peligro en toda la red
- Priorice los eventos para una investigación más a fondo
- Analice archivos para determinar si son una amenaza o no deseados
- Informe con seguridad sobre la posición de seguridad de su empresa en cualquier momento

Más allá de la EDR

Para detener la más amplia variedad de amenazas, Intercept X Advanced with EDR utiliza un completo enfoque de defensa exhaustiva para la protección de endpoints, en lugar de simplemente depender de una técnica de seguridad principal. Este es "el poder del más", una combinación de técnicas base y modernas líderes. Intercept X Advanced with EDR integra la detección y respuesta inteligentes para endpoints (EDR) con la protección contra malware y exploits mejor valorada del mercado.

Entre las técnicas modernas se incluyen la detección de malware con Deep Learning, la prevención de exploits y funciones específicas antiransomware. Las técnicas base incluyen antivirus, análisis de comportamiento, detección de tráfico malicioso, prevención de fugas de datos y mucho más.

Intercept X Advanced with EDR combina las capacidades de detección y respuesta para endpoints con las funciones modernas de Intercept X y las técnicas base de Sophos Central Endpoint Protection. Se ofrece como una solución única, en un solo agente.

	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Intercept X	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 es.sophos.com/intercept-x

* Disponible a principios de 2019

Ventas en España:
Teléfono: (+34) 91 375 67 56
Correo electrónico: comercialES@sophos.com

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

02/10/18 DS-ES (3098-DD)

SOPHOS