SOPHOS

Intercept X

La mejor protección para endpoints del mundo

Sophos Intercept X detiene la más amplia gama de ataques con una combinación única de detección de malware con Deep Learning, prevención de exploits, protección antiransomware y mucho más.

Aspectos destacados

- El motor n.º 1 en detección de malware, con tecnología Deep Learning
- Prevención de exploits para detener las técnicas que utilizan los atacantes para controlar software vulnerable
- Mitigación de adversarios activos para evitar la persistencia en el equipo
- Análisis de causa raíz para ver qué ha hecho el malware y de dónde procedía
- Tecnología de prevención específica para el ransomware
- Detección y respuesta para endpoints (EDR) que ofrece una potente higiene para las operaciones de seguridad TI y búsqueda de amenazas tanto para administradores de TI como para analistas de seguridad

Sophos Intercept X 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.

Entre las técnicas modernas se incluyen la detección de malware con Deep Learning, la prevención de exploits y funciones específicas antiransomware. Entre las técnicas base se incluyen la detección de malware basada en firmas, el análisis de comportamientos, la detección de tráfico malicioso, el control de dispositivos, el control de aplicaciones, el filtrado web y la prevención de pérdidas de datos, entre otras.

Detección de malware con Deep Learning

La inteligencia artificial integrada en Intercept X es una red neuronal de Deep Learning, una forma avanzada de Machine Learning que detecta el malware tanto conocido como desconocido sin necesidad de firmas. Con la tecnología Deep Learning, Intercept X tiene el mejor motor de detección de malware de la industria, tal y como han demostrado consultoras independientes. Esto permite que Intercept X detecte el malware que se cuela con otras herramientas de seguridad para endpoints.

Detener el exploit es detener el ataque

El ritmo de detección de nuevas vulnerabilidades en el software, que los proveedores deben corregir constantemente con parches, es alarmante. En contraposición, la aparición de nuevas técnicas de explotación es mucho más escasa y, además, son reutilizadas una y otra vez por los atacantes con cada vulnerabilidad descubierta. La prevención de exploits repele a los atacantes bloqueando las herramientas y técnicas de explotación que utilizan para distribuir malware, robar credenciales y eludir la detección. Esto permite a Sophos proteger su red de hackers esquivos y ataques de día cero.

Protección probada contra el ransomware

Intercept X utiliza el análisis de comportamientos para detener el ransomware desconocido y los ataques de arranque maestro, lo que lo convierte en la tecnología antiransomware más avanzada disponible. Aunque se exploten o secuestren archivos o procesos de confianza, CryptoGuard los detendrá y restituirá sin ninguna interacción por parte del usuario o del personal de soporte informático. CryptoGuard trabaja de forma silenciosa a nivel del sistema de archivos, haciendo un seguimiento de los equipos remotos y procesos locales que intentan modificar los documentos y otros archivos.

Detección y respuesta para endpoints (EDR)

Sophos Intercept X Advanced es la primera solución EDR diseñada para administradores de TI y analistas de seguridad para resolver casos de uso de operaciones de TI y búsqueda de amenazas. 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, responda de forma remota con precisión.

Implementación y gestión simplificadas

Administrar su seguridad desde Sophos Central significa que ya no tendrá que instalar o desplegar servidores para proteger sus estaciones de trabajo. Sophos Central ofrece políticas predeterminadas y configuraciones recomendadas para garantizar que obtiene la protección más eficaz desde el primer día.

Managed Threat Response (MTR)

Se trata de un servicio totalmente administrado de búsqueda, detección y respuesta a amenazas las 24 horas prestado por un equipo de expertos de Sophos. Gracias a la detección y respuesta inteligentes para endpoints de Intercept X Advanced with EDR, los analistas de Sophos responden a posibles amenazas, buscan indicadores de peligro y ofrecen un análisis detallado de los eventos, que incluye lo que ha ocurrido, dónde, cuándo, cómo y por qué.

Especificaciones técnicas

Sophos Intercept X admite Windows 7 y posterior, de 32 y 64 bits. También puede ejecutarse en paralelo a soluciones antivirus y para endpoints de terceros a fin de añadir detección de malware con Deep Learning, protección contra exploits y ransomware, análisis de causa raíz y Sophos Clean.

	Funciones	
EXPLOIT PREVENTION	Aplicación de la prevención de ejecución de datos	✓
	Selección aleatoria del diseño del espacio de direcciones obligatoria	✓
	ASLR de abajo a arriba	✓
	Página NULL (Protección de desreferencia NULL)	✓
	Asignación de pulverización del montón	✓
	Pulverización dinámica del montón	✓
	Eje de la pila	✓
	Ejecución de la pila (MemProt)	✓
	Mitigaciones de ROP basadas en pilas (Autor de llamada)	✓
	Mitigaciones de ROP basadas en ramas (Asistidas por hardware)	✓
	Sobrescritura del controlador de excepciones estructurado (SEHOP)	✓
	Filtrado de tabla de direcciones de importación (IAF)	✓
	Carga de bibliotecas	✓
	Inyección de DLL reflectiva	✓
	Shellcode	✓
	Modo Dios de VBScript	✓
	Wow64	✓
	Syscall	✓
	Vaciado de procesos	✓
	Secuestro de DLL	✓
	Omisión de AppLocker Squiblydoo	✓
	Protección de APC (Double Pulsar / AtomBombing)	✓
	Aumento de privilegios de procesos	✓
MITIGACIONES DE ACTIVE ADVERSARY	Protección contra robos de credenciales	✓
	Mitigación de cuevas de código	✓
	Protección contra Man-in-the-Browser (Navegación segura)	✓
	Detección de tráfico malicioso	✓
	Detección de shell Meterpreter	✓

	Funciones	
ANTI-RANSOMWARE	Protección contra archivos de ransomware (CryptoGuard)	✓
	Recuperación automática de archivos (CryptoGuard)	✓
	Protección del registro de arranque y disco (WipeGuard)	✓
BLOQUEO DE APLICACIONES	Navegadores web (incluido HTA)	✓
	Complementos de navegadores web	✓
	Java	✓
	Aplicaciones multimedia	✓
	Aplicaciones de Office	✓
DEEP LEARNING	Detección de malware con Deep Learning	✓
	Bloqueo de aplicaciones no deseadas (PUA) con Deep Learning	✓
	Supresión de falsos positivos	✓
	Live Protection	✓
RESPONDER INVESTIGAR ELIMINAR	Análisis de causa raíz	✓
	Sophos Clean	✓
	Seguridad sincronizada con Security Heartbeat	✓
IMPLEMENTACIÓN	Puede ejecutarse como agente independiente	✓
	Puede ejecutarse junto a un antivirus existente	✓
	Puede ejecutarse como componente de un agente Sophos Endpoint existente	✓
	Windows 7	✓
	Windows 8	✓
	Windows 8.1	✓
	Windows 10	✓
	macOS*	✓

* Admite las funciones CryptoGuard, Detección de tráfico malicioso, Seguridad Sincronizada con Heartbeat, Análisis de causa raíz

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

11-05-2020 DS (PS)

SOPHOS