SOPHOS
Security made simple.

Intercept X

Deep Learning Malware Detection , Exploit Prevention, Anti-Ransomware, análisis de causa raíz y Sophos Clean

Sophos Intercept X utiliza la técnica adecuada en el momento adecuado para detener amenazas desconocidas y repeler al atacante. Añádalo como capa adicional a su antivirus o ejecútelo con Sophos Endpoint Protection para una protección de última generación completa.

Aspectos destacados

- Modelos de deep learning entrenados para detectar malware nunca antes visto
- Exploit Prevention detiene las técnicas que utilizan los atacantes para controlar software vulnerable
- Active Adversary Mitigation para evitar la persistencia en el equipo
- Análisis de causa raíz para ver qué ha hecho el malware y de dónde procedía
- Sophos Clean elimina el malware y los restos que deja atrás
- Aumenta su inversión antivirus existente

Construya su seguridad para endpoints de última generación

Los días del simple escaneado de archivos han pasado a la historia. Hoy en día, nuestro objetivo es impedir que las amenazas lleguen a los dispositivos, detenerlas antes de que se ejecuten, detectarlas si han eludido los métodos de prevención y no solo limpiar los programas maliciosos, sino también analizar y deshacer todos los cambios que hayan realizado. Sophos Intercept X utiliza múltiples capas de tecnología que coexisten con su antivirus para proporcionar una protección de última generación completa.

Detección de malware de aprendizaje profundo

Intercept X, probado por SophosLabs utilizando redes neuronales de deep learning, detecta los archivos de malware nuevos y nunca antes vistos con precisión y sin firmas. Los métodos de machine learning alternativos suelen necesitar científicos de datos que identifiquen los atributos que deben buscar. El modelo resultante queda limitadopor la efectividad de la selección de atributos y los datos de entrenamiento. El deep learning utilizado en Intercept X identifica los atributos importantes para poder distinguir entre el malware y los archivos benignos por sí mismo. Esto, junto con un extenso conjunto de datos de entrenamiento suministrado por SophosLabs, garantiza que se cree un límite de decisión efectivo entre los archivos benignos y los maliciosos. Este modelo entrenado tiene un tamaño inferior a 20 MB y solo necesita actualizaciones ocasionalmente. En la nube, SophosLabs está continuamente testando el modelo y supervisando la eficacia del límite de decisión utilizando muestras de malware nuevo y nunca visto anteriormente.

Proteja el software vulnerable

Se descubren nuevas vulnerabilidades a un ritmo alarmante. Esto respresenta defectos en el software que deben ser corregidos con parches por los proveedores. En cambio, de promedio solo aparecen nuevas técnicas de explotación dos veces al año y son reutilizadas una y otra vez por los atacantes con cada vulnerabilidad descubierta. Exploit Prevention detiene las técnicas, lo que evita a su vez que el atacante explote la vulnerabilidad antes de que pueda corregirse.

Detección eficaz de ransomware

La tecnología CryptoGuard detecta el cifrado espontáneo de datos maliciosos para detener en seco el avance de ransomware. 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.

Análisis de causa raíz

Identificar los programas maliciosos y aislarlos y eliminarlos resuelve el problema inmediato. Pero, ¿sabe realmente lo que ha hecho el malware antes de eliminarlo, o cómo se introdujo en primer lugar? El análisis de causa raíz le muestra todos los eventos que llevan a una detección. Podrá comprender qué archivos, procesos y claves de registro ha tocado el malware y activar la limpieza del sistema en profundidad para retroceder en el tiempo.

Implementación y gestión simplificadas

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

	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)	✓
	Heap Spray Allocation	✓
	Dynamic Heap Spray	✓
	Stack Pivot	✓
	Stack Exec (MemProt)	✓
	Stack-based ROP Mitigations (Autor de llamada)	✓
	Branch-based ROP Mitigations (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	✓
	Hollow Process	✓
	Secuestro de DLL	✓
	Omisión de AppLocker Squiblydoo	✓
	Protección de APC (Double Pulsar / AtomBombing)	✓
	Aumento de privilegios de procesos	✓
MITIGACIONES DE ADVERSARIOS ACTIVOS	Protección contra robos de credenciales	✓
	Mitigación de Code Cave	✓
	Protección contra Man-in-the-Browser (Navegación segura)	✓
	Detección de tráfico malicioso	✓
	Detección de shell Meterpreter	✓

Cuatro pasos para lograr la protección

1. Visite sophos.com/intercept-x para comenzar su evaluación.
2. Cree una cuenta de administrador de Sophos Central.
3. Descargue e instale el agente de Intercept X.
4. Administre su protección a través de Sophos Central.

Especificaciones técnicas

Sophos Intercept X admite Windows 7 y posterior, de 32 y 64 bits. Puede ejecutarse junto a Sophos Endpoint Protection Standard o Advanced si se administra con Sophos Central. También puede ejecutarse en paralelo a soluciones antivirus y para endpoints de terceros a fin de añadir detección de malware de deep learning, anti-exploit, protección contra ransomware, análisis de causa raíz y Sophos Clean.

	Funciones	
ANTIRANSOMWARE	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 Deep Learning	✓
	Bloqueo de aplicaciones no deseadas (PUA) de aprendizaje profundo	✓
	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

¿Ya utiliza Sophos Endpoint Protection y administra la solución con Enterprise Console? Puede gestionar sus endpoints mediante Sophos Central y habilitar Intercept X para el despliegue automático.

Pruébelo gratis hoy mismo

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

Ventas en España:
Tel.: (+34) 913 756 756
Correo electrónico: seusales@sophos.com

Ventas en Latin America:
Correo electrónico: Latamsales@sophos.com

2017-09-10-DS-ES (MP)

SOPHOS