Protección de cargas de trabajo en servidores

Protección para Linux

Intercept X Advanced for Server, Intercept X Advanced for Server with XDR e Intercept X Advanced for Server with MTR

Nube o centro de datos, host y contenedor. Proteja su infraestructura ahora y a medida que evoluciona con la protección de cargas de trabajo de alto impacto de Sophos pero de bajo impacto en el rendimiento.

Minimice los tiempos de detección y respuesta

Obtenga una visibilidad completa de sus hosts y cargas de trabajo en los contenedores, identificando malware, exploits y comportamientos anómalos antes de que puedan ser aprovechados por los atacantes. La detección y respuesta ampliadas (XDR) proporciona una visibilidad detallada de los hosts, los contenedores, los endpoints, el tráfico de red y los servicios de seguridad nativos en la nube de los proveedores.

Las detecciones de comportamientos y exploits nativos en la nube en tiempo de ejecución permiten identificar amenazas como escapes de contenedores, exploits del kernel e intentos de aumento de privilegios. Unos flujos de trabajo para la investigación de amenazas optimizados priorizan las detecciones de incidentes de alto riesgo y consolidan eventos relacionados para aumentar la eficiencia y ahorrar tiempo.

Mejore las operaciones de seguridad

Combata las amenazas con una visibilidad de hosts y contenedores en tiempo de ejecución y detecciones de amenazas procesables proporcionadas a través de nuestra consola de administración centralizada o integradas en sus herramientas existentes de automatización, orquestación, gestión de registros y respuesta ante incidentes.

Escoja entre dos opciones de despliegue para ajustarse de forma óptima a sus necesidades. La administración de Sophos Central proporciona a los equipos de seguridad la información crítica para investigar y responder a las amenazas de comportamiento, exploits y malware en un solo sitio. La integración de API a través del sensor Linux* está configurada de forma precisa para un rendimiento máximo, canalizando información útil a la plataforma de administración de datos de su elección.

Obtenga rendimiento sin fricciones

La protección de Intercept X for Server está optimizada para flujos de trabajo de DevSecOps, identificando ataques sofisticados a medida que se producen sin requerir un módulo kernel, orquestación, líneas de base ni escaneados de sistema. La limitación optimizada de recursos, incluyendo limitaciones de CPU, memoria y recopilación de datos, contribuyen a evitar costosos periodos de inactividad debido a la sobrecarga de hosts o problemas de estabilidad, garantizando así la optimización del rendimiento de las aplicaciones y el tiempo de actividad.

Aspectos destacados

- Protección de cargas de trabajo y contenedores de Linux en la nube, locales y virtuales
- Minimiza el tiempo para detectar y responder a amenazas
- Optimizado para cargas de trabajo de importancia máxima en las que el rendimiento es crucial
- Aproveche las fuentes de datos de endpoints, la red, el correo electrónico, la nube, M365 y dispositivos móviles con la detección y respuesta ampliadas (XDR)
- Comprenda y proteja la totalidad de su entorno en la nube con la gestión de la posición de seguridad en la nube incluida
- Proporciona una seguridad 24/7/365 por medio de un servicio totalmente administrado

* Disponible en breve

SOPHOS

Automatice su lista de comprobación de seguridad en la nube

Diseñe su entorno en la nube para cumplir los estándares recomendados con la visibilidad y las herramientas para que con la gestión integrada de la posición de seguridad en la nube incluyan la totalidad de su entorno en la nube pública:

- Identifique de forma proactiva cualquier actividad no autorizada, vulnerabilidades de imagen de hosts y contenedores y errores de configuración en Amazon AWS, Microsoft Azure y Google Cloud Platform (GCP)
- Detecte en todo momento recursos en la nube con los inventarios detallados y la visibilidad de la protección de hosts de Sophos y despliegues de Sophos Firewall
- Superponga automáticamente estándares de seguridad recomendados para detectar brechas en la posición de seguridad, identificar mejoras inmediatas y problemas críticos
- Detecte anomalías de alto riesgo en el comportamiento de roles de IAM de usuarios, señalando con rapidez patrones de acceso y ubicaciones inusuales y comportamientos maliciosos para prevenir una brecha

Colaboración que se suma a su equipo

Los analistas expertos del SOC de Sophos Managed Threat Response colaboran de forma estrecha con su equipo, supervisando su entorno 24/7 y buscando y remediando proactivamente amenazas en su nombre con la experiencia necesaria en Linux para aumentar la eficiencia. 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.

Especificaciones técnicas

Remítase a los requisitos de sistema en Linux para obtener información actualizada. Para obtener más información sobre las funciones en Windows, consulte la hoja de datos de Windows.

Características	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Intercept X Advanced for Server with MTR Advanced
Protección (incluyendo detección de malware con Deep Learning, escaneado de archivos y más)	✓	✓	✓
CSPM (gestión de la posición de seguridad en la nube: vea y proteja la totalidad de su entorno en la nube)	✓	✓	✓
XDR (Detección y respuesta ampliadas)		✓	✓
MTR (Managed Threat Response: servicio de búsqueda y respuesta a amenazas 24/7)			✓

Pruébelo gratis hoy mismo

Regístrese para una evaluación gratuita de 30 días en es.sophos.com/server

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

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

22-04-11 DS-ES (PC)