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 MDR

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 bien integrando estas capacidades en sus herramientas existentes de respuesta a amenazas con distintas opciones de despliegue.

Administración de Sophos Central: este agente ligero de Linux proporciona a los equipos de seguridad la información crítica que necesitan para investigar y responder a las amenazas de comportamiento, exploits y malware en un solo sitio. Al supervisar el host de Linux, esta opción de despliegue permite a los equipos administrar todas sus soluciones de Sophos desde un único panel intuitivo y así moverse ágilmente entre la búsqueda, la remediación y la administración de amenazas.

Integración de API: Sophos Linux Sensor es una opción de implementación muy flexible configurada de forma precisa para ofrecer el mejor rendimiento. El sensor de Linux utiliza API para integrar exhaustivas detecciones de amenazas en tiempo de ejecución, en entornos de host o contenedor, con sus herramientas de respuesta a amenazas existentes. Proporciona un mayor rango de detecciones, controles para crear conjuntos de reglas personalizadas y opciones de configuración para ajustar el uso de los recursos del host.

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

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 Detection and 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 MDR Complete
Agente de protección para Linux (Incluidos el escaneado de malware, la prevención de vulnerabilidades, el escaneado de archivos, etc.)	✔	✔	✔
Sensor Linux (Integración de detecciones en tiempo de ejecución en Linux y contenedores con sus herramientas de respuesta a amenazas existentes vía API)		✔	✔
Seguridad para la infraestructura en la nube (Supervisión de la posición de seguridad en la nube para prevenir riesgos de seguridad y cumplimiento)	✔	✔	✔
XDR (Detección y respuesta ampliadas)		✔	✔
MDR (Managed Detection and 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:
Tel.: (+34) 91 375 67 56
Email: comercialES@sophos.com

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

22-10-21 DS-ES (PC)

SOPHOS