SentinelOne

FICHA TÉCNICA

Agente Sentinel para Linux

Un componente de SentinelOne Cloud Workload Security

Garantice la seguridad en tiempo de ejecución y disfrute de funciones EDR para los servidores Linux sin sacrificar la estabilidad.

Los equipos de seguridad deben poder garantizar la protección, detección, respuesta, visibilidad y caza de amenazas en todos los sistemas operativos. Linux no es una excepción. A diferencia de los antivirus y de las soluciones EDR de primera generación, SentinelOne ofrece las funciones de seguridad avanzadas que necesita el centro SOC para proteger los endpoints Linux en múltiples nubes, a través de una solución SaaS sencilla diseñada para ofrecer un rendimiento y automatización óptimas.

Los agentes Sentinel para Linux están diseñados para ejecutarse en máquinas físicas o virtuales en su centro de datos o en AWS, Azure o Google Cloud. Sirven de punto de aplicación de las directivas de seguridad y se administran en una consola multiinquilino única, junto con otros agentes Sentinel para Windows, macOS y Kubernetes.

La administración es flexible, distribuida y gestionada a través de controles basados en roles que se corresponden con la estructura de su empresa. El agente Sentinel para Linux es compatible con muchas familias de distribuciones Linux populares sin el riesgo de inestabilidad de los módulos de kernel.

DIFERENCIADORES DEL AGENTE SENTINEL PARA LINUX

- Compatibilidad con una gran variedad de familias de distribuciones de Linux
- Estabilidad operativa. Sin módulos de kernel.
- Prevención en tiempo real de ataques basados en archivos y ataques sin archivos
- Visibilidad EDR total + horizonte prolongado de retención de datos
- Funciones de respuesta profunda

¿EJECUTA EN LA NUBE CARGAS DE TRABAJO EN CONTENEDOR?

Sí, también ofrecemos un agente Sentinel para Kubernetes, que se distingue por la protección en tiempo de ejecución, las funciones EDR y soluciones únicas centradas en los contenedores.

CARACTERÍSTICAS DEL AGENTE SENTINEL PARA LINUX

Operaciones

+ Compatibilidad con las principales distribuciones de Linux
+ Estabilidad. Sin necesidad de módulos de kernel
+ Instalación sencilla en endpoints físicos, virtuales y alojados por un proveedor de servicios en la nube
+ Consola única para la administración multiinquilino y el control de acceso basado en roles
+ Inventario de aplicaciones

Prevención

+ Inteligencia en el agente para una protección sin retrasos asociados a la nube
+ Bloqueo y puesta en cuarentena en tiempo real de malware oculto en archivos binarios ELF, Windows y Mach-O gracias a la función StaticAI del agente
+ Bloqueo en tiempo real de las amenazas desconocidas previamente sin archivos, gracias a la inteligencia artificial basada en el comportamiento, integrada en el agente
+ Análisis del disco bajo demanda
+ Control de aplicaciones para las cargas de trabajo en contenedor
+ Control de aplicaciones para las máquinas virtuales de nube (próximamente)

Funciones ActiveEDR™ de nivel empresarial

+ Creación automática de contexto de árbol de PID (identificador de procesos) y creación de nuevos enlaces gracias a la función Storyline™
+ Automatización de Storyline Active Response
+ Retención de datos EDR de 14 a más de 365 días
+ Integración con el marco MITRE ATT&CK

Funciones de respuesta

+ Shell remoto seguro
+ Control mediante firewall
+ Aislamiento de red
+ Recuperación de archivos