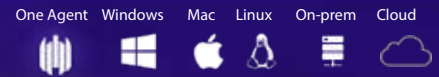


SentinelOne EPP Datasheet

► Protección Autónoma que le Ahorra Tiempo

SentinelOne Endpoint Protection Platform (EPP) unifica la prevención, detección y respuesta en un Agente de propósito único, basado en el aprendizaje automático y la automatización. Proporciona prevención, detección y corrección de ataques en todos los vectores principales, eliminación rápida de amenazas de forma completamente automática, capacidades de respuesta impulsadas por políticas y visibilidad completa en el ambiente del Endpoint, con un contexto completo y análisis forense en tiempo real.

La suite de siguiente generación del futuro, nacida del Endpoint y orquestada por Inteligencia Artificial.



EPP	EDR	Manageability	Services	Cloud Intel.
<ul style="list-style-type: none"> Static AI Behavior AI Anti-Exploitation Lateral Movement Credential Theft Prevention 	<ul style="list-style-type: none"> Threat Hunting IOC Search Remediation Encrypted Traffic Visibility Containment and Rollback 	<ul style="list-style-type: none"> Device Control API and SDK Application Inventory File Integrity Monitoring Vulnerability & Patch Management 	<ul style="list-style-type: none"> Vigilance MDR 	<ul style="list-style-type: none"> Threat Feeds IP Reputation Automated Analysis Shared Intelligence

Usuarios Endpoint

Windows XP, 7, 8, 8.1, 10
 Mac OSX 10.9.x, 10.10.x, 10.11x, macOS 10.12x macOS 10.13 (High Sierra)
 CentOS 6.5, 7.0, 7.2
 Red Hat Enterprise Linux 6.5, 7.0, 7.2
 Ubuntu 12.04, 14.04, 16.04, 16.10
 openSUSE 42.2

Servidores Endpoint

Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016
 CentOS 6.5, 7.0, 7.2
 Red Hat Enterprise Linux 6.5, 7.0, 7.2
 Ubuntu 12.04, 14.04, 16.04, 16.10
 SUSE Linux Enterprise Server 12SP1
 Oracle Linux 6.5 - 6.9, 7.0+
 Amazon Linux (AMI) 2016.09+, 2017.03+

Ambientes Virtuales

Citrix XenApp, XenDesktop
 Microsoft Hyper-V
 Oracle VirtualBox
 VMware vSphere
 VMware Workstation
 VMware Fusion
 VMware Horizon



SentinelOne EPP Datasheet

► Protección

Prevención autónoma de varias capas que cubre todos los vectores de ataque, incluso cuando no está en línea

Tecnología de aprendizaje automático que no se basa en firmas y no requiere actualizaciones o escaneos recurrentes.
Mitigación del contexto completo de la actividad maliciosa, lo que reduce el tiempo y el costo de arreglar los dispositivos infectados.
Proporciona los forenses correctos. El bloqueo no es suficiente, los clientes quieren saber de dónde vienen las amenazas y lo que intentaron hacer.

► Visibilidad

Visibilidad Multiplataforma en los Endpoint: vamos más allá de los límites de EPP y EDR con valor agregado, capacidades tales como datos de higiene de TI.

Visibilidad en el tráfico cifrado, ya que todos los usuarios están expuestos al phishing y el 70% del tráfico web es encriptado.
Visibilidad en todas las aplicaciones y procesos en ejecución.
Visibilidad profunda para Caza de Amenazas (Threat Hunting).

► Simplicidad

Un Agente ligero que proporciona la siguiente funcionalidad:

EPP
EDR
HIPS
Monitoreo de Integridad de Archivos
Vulnerabilidad / Gestión de riesgos

Consola administrada alojada en la nube, en las instalaciones o en un modelo híbrido.
Mayor eficacia, menor impacto en el sistema y una experiencia óptima para el usuario final.

► Automatización

La plataforma SentinelOne está construida con un enfoque de API primero y tiene integraciones con SonicWall, Fortinet, Splunk, QRadar, LogRhythm, Demisto, Phantom e incluso Alexa, por nombrar algunos.

Aisla automáticamente el dispositivo infectado e Inmuniza el resto de los Endpoints.
Recuperar archivos en el improbable caso de ransomware.

El 44% de las empresas enfrentó infecciones de Ransomware en los últimos 12 meses.

A
T
A
Q
U
E
S

ANTES

Inteligencia Artificial Estática
Previene Ataques
Realiza Pre-ejecución

DURANTE

Analisis por Comportamiento IA.
Constantemente monitorea y mapea cada proceso en ejecución para detectar comportamientos incongruentes.

DESPUÉS

EDR automatizado.
Automatiza la remediación y la respuesta ... incluso la Reversión/ Roll-Back.

Historia de éxito:

Administrador de Red y Seguridad
Ramo: Aseguradora



"SentinelOne nos dio todo lo que necesitábamos y más de lo que esperábamos. La inteligencia artificial y las capacidades de automatización hacen que nuestro trabajo sea mucho más fácil sin exigir más infraestructura, tiempo del personal o complejidad. No podemos pedir más que eso"



https://www.sentinelone.com/wp-content/uploads/2017/06/SentinelOne_ANA_Seguros_Case_Study-1.pdf