Bits: Protección Avanzada para tus Puntos Finales

Paquetes de productos de la plataforma Singularity de SentinelOne

La plataforma SentinelOne Singularity brinda a los equipos de operaciones de TI y SOC una manera más eficaz de salvaguardar los activos de información contra las sofisticadas amenazas actuales, mejorando la protección y la eficiencia en el proceso.

Singularity brinda capacidades distintivas en la protección, detección y respuesta de endpoints, seguridad de IoT, seguridad en la nube y operaciones de TI, unificando múltiples tecnologías existentes en una única solución.
Los agentes "Sentinel" autónomos y eficientes en recursos están disponibles para Windows, Mac, Linux y Kubernetes, y soportan una variedad de factores de forma que incluyen entornos físicos, virtuales, VDI, centros de datos de clientes, centros de datos híbridos y proveedores de servicios en la nube.

Los Sentinels son gestionados a través de la plataforma SaaS de múltiples inquilinos, disponible a nivel mundial, diseñada para ofrecer una administración flexible y fácil de usar que se adapta a tus requisitos. Además, la suscripción a los servicios de Vigilance Managed Detection & Response (MDR) está disponible para respaldar a tu organización de seguridad las 24 horas del día, los 7 días de la semana.

Esta ficha técnica describe las ofertas de productos en diferentes niveles conocidos como SentinelOne Core, Control y Complete. Cada paquete de productos se basa en lo siguiente:

Singularity Complete Operaciones de seguridad		Incorpora o sustituye EDR para potenciar las capacidades de observación, exploración e investigación y respuesta.
	Singularity Control Higiene de operaciones de TI	Reduce el número de agentes de punto final necesarios mediante la consolidación.
	Singularity Core Protección de punto final	Sustituye los productos de antivirus y NGAV poco eficientes por opciones más efectivas.
Singularity Platform		Plataforma global de SaaS

¿POR QUÉ TE RECOMENDAMOS SENTINELONE?

- SentinelOne ofrece soluciones de seguridad de punto final de alta calidad y eficacia. La empresa logra una verdadera integración de EPP+EDR, lo que permite eliminar los agentes de terminales redundantes y disminuir los costos operativos de manera significativa.
- La atención al cliente de SentinelOne ha logrado un índice de satisfacción del 97%, lo cual demuestra la satisfacción de la gran mayoría de los clientes con el servicio recibido.
- Asimismo, el 96% de los clientes recomiendan de manera positiva a SentinelOne, respaldando la calidad y eficacia de sus soluciones.
- La plataforma de SentinelOne cuenta con una interfaz adaptable que ofrece flujos de trabajo personalizables para ahorrar tiempo. Además, gracias a la inteligencia artificial avanzada en detección de comportamientos, se ha logrado una efectiva resolución de ransomware.
- La protección autónoma de SentinelOne permite una respuesta inmediata ante cualquier incidente.
- El diseño de ActiveEDRTM de SentinelOne en Storyline™ está pensado para responder de manera eficiente a incidentes y detectar amenazas, lo que se traduce en un importante ahorro de tiempo y reducción de la fatiga para los profesionales encargados de ello.
- La retención de datos de EDR es una solución asequible que garantiza la conservación de la información relevante.
- Además, SentinelOne ofrece integraciones sencillas de XDR con otros proveedores para una mayor interoperabilidad.

¿Preparado para una demostración?

Visita nuestro sitio web para obtener más detalles.

Atributos y propuestas de la plataforma Singularity

Cada uno de los usuarios de SentinelOne cuenta con disponibilidad a estas características de la consola de administración de SaaS.

- Despliegue mundial de SaaS. Muy accesible. Opción de ubicación geográfica (Estados Unidos, Unión Europea, APAC).
- Autenticación y autorización administrativa adaptable: SSO, autenticación multifactor (MFA), control de acceso basado en roles (RBAC).
- Gestión adaptable para que se ajuste a la estructura organizativa de tu empresa.
- Registro de incidentes de amenazas con un historial de 365 días.
- SentinelOne integra inteligencia de amenazas y tácticas MITRE ATT&CK, junto con indicadores de compromiso (IOC).
- Análisis de seguridad basado en datos para el panel de control
- Notificaciones personalizables mediante correo electrónico y registro de sistema (syslog).
- Integraciones XDR habilitadas por API de Singularity (SIEM, entorno de pruebas de seguridad, Slack, proveedores de inteligencia de amenazas externos, entre otros).
- API exclusiva con más de 340 características disponibles.

Singularity Core

Core es la base de todas las ofertas de seguridad para puntos finales de SentinelOne. Es el producto de seguridad de nivel de entrada para organizaciones que buscan reemplazar los sistemas antivirus o NGAV heredados por un EPP más efectivo y fácil de administrar. Core también ofrece funciones básicas de detección y respuesta de puntos finales (EDR) que demuestran la verdadera integración de capacidades EPP+EDR. La Inteligencia de Amenazas forma parte de la oferta estándar e se integra a través de las funciones de inteligencia artificial y Cloud Sentinel.

Las características principales de SentinelOne incluyen:

- **El análisis integrado de IA estática y IA conductual** impide y detecta una amplia variedad de ataques en tiempo real antes de que generen perjuicios. Core defiende contra malware identificado y desconocido, troyanos, instrumentos de pirateo, programas de secuestro de datos, vulnerabilidades de almacenamiento, empleo inadecuado de secuencias de comandos, macros erróneas y otros riesgos.
- **Los Sentinel son autosuficientes**, lo que implica que emplean tecnología de prevención y detección sin necesidad de estar conectados a la nube, y desencadenarán respuestas de protección en tiempo real.
- **La restauración es ágil** y permite que los usuarios retomen sus actividades en cuestión de minutos sin necesidad de generar nuevas imágenes o desarrollar scripts. Cualquier modificación no autorizada que ocurra durante un ataque puede revertirse mediante la Remediación con 1 clic y la Reversión con 1 clic para Windows.
- **Acceso confiable a la administración de SaaS.** Selecciona entre las ubicaciones de Estados Unidos, Unión Europea y APAC. Paneles fundamentados en datos, gestión de políticas por sitio y grupo, análisis de incidentes con integración de MITRE ATT&CK, y muchas más opciones.

Singularity Control

Control está diseñado para empresas que buscan una seguridad de primer nivel que se encuentra en SentinelOne Core, con la incorporación de características adicionales de "paquete de seguridad" para la gestión de puntos finales.

Las funcionalidades de SentinelOne Control incluyen:

- **Todas las funciones de SentinelOne Core**
- **Firewall de Control** para la gestión de la conectividad de red hacia y desde los dispositivos, incluyendo el reconocimiento de la ubicación.
- **Control de Dispositivos** para la gestión de dispositivos USB y periféricos Bluetooth/BLE.
- **Visibilidad no autorizada** para identificar dispositivos en la red que requieren la protección del agente Sentinel.
- **Administración de vulnerabilidades**, además del registro de aplicaciones, para obtener detalles acerca de las aplicaciones de terceros que presentan vulnerabilidades conocidas listadas en la base de datos MITRE CVE.

SENTINELONE PREVIENE EL RANSOMWARE Y OTROS ATAQUES SIN ARCHIVOS MEDIANTE EL USO DE INTELIGENCIA ARTIFICIAL DE COMPORTAMIENTO Y POTENTES CAPACIDADES DE REMEDIACIÓN AUTOMÁTICA.

Singularity Complete

Complete se ha diseñado para empresas que requieren una protección y control modernos de los puntos finales, junto con funciones avanzadas de EDR que se conocen como ActiveEDR™. Asimismo, Complete cuenta con la tecnología innovadora de Storyline™, que de manera automática contextualiza todas las interacciones de los procesos del sistema operativo, incluso entre reinicios, a cada segundo del día, y las almacena para futuras investigaciones. Storyline™ evita que los analistas tengan que realizar tareas tediosas de correlación de eventos y los guía rápidamente hacia el origen del problema. SentinelOne Complete ha sido diseñado para aliviar la carga de los administradores de seguridad, los analistas de SOC, los cazadores de amenazas y los respondedores de incidentes, ya que automáticamente correlaciona la telemetría y la asigna al marco MITRE ATT&CK®. Las empresas globales más exigentes confían en SentinelOne Complete para satisfacer sus intransigentes demandas de ciberseguridad.

Algunas de sus características incluyen:

- **Todas las características de SentinelOne Core + SentinelOne Control**
- **Tecnología innovadora Storyline™** para un análisis rápido y una resolución sencilla
- **Integración de la visibilidad ActiveEDR™** para datos benignos y maliciosos
- **Retención histórica de datos de EDR de 14 a 365+ días** con capacidad de consulta a gran escala
- **Método de búsqueda según el marco de trabajo de MITRE ATT&CK®**
- **Etiquetar las actividades benignas como amenazas** para su aplicación en las funciones de EPP
- **Automatización de las funciones de seguimiento y respuesta activa** de StorylineTM (STAR)
- Funciones como líneas de tiempo, acceso remoto a la terminal, recuperación de archivos, integraciones con entornos seguros y más

> Funcionalidades de administración altamente adaptables además de características robustas de EPP/EDR

> ¡Adiós al ransomware... SentinelOne supera a la competencia!

> La configuración y la implementación resultaron sumamente sencillas. El panel de administración en la nube se muestra intuitivo y accesible.

Servicios de Monitoreo de Detección y Respuesta (MDR) Suscripción

SentinelOne Vigilancia Detección y Respuesta Gestionada (MDR) es una suscripción de servicio diseñada para incrementar la seguridad de las organizaciones de los clientes. Vigilancia MDR añade valor al asegurarse de que cada amenaza se revise, tome acción, documente y escale según sea necesario. En la mayoría de los casos, se analizan y resuelven las amenazas en aproximadamente 20 minutos y solo se contacta en situaciones urgentes. Vigilancia MDR permite a los clientes enfocarse únicamente en los incidentes relevantes, lo cual la convierte en la solución complementaria ideal para equipos de TI/SOC abrumados.

Servicios de Preparación de SentinelOne Suscripción

SentinelOne Readiness es un servicio de suscripción de asesoramiento diseñado para guiar al equipo de la organización antes, durante y después de la instalación del producto con una metodología estructurada que lo pone en funcionamiento rápidamente y mantiene su instalación en óptimas condiciones a lo largo del tiempo. Los clientes de Readiness son guiados a través de las mejores prácticas de implementación, se les brinda asistencia regular para la actualización de agentes y reciben evaluaciones de salud trimestrales con ONEscoreTM para asegurar que su estado de SentinelOne esté optimizado.

Funciones incluidas

	Singularity Complete	Singularity Control	Singularity Core
Plataforma global de software como servicio (SaaS). Acceso seguro, alta disponibilidad, gestión de políticas EPP, respuesta a incidentes de EDR y búsqueda de amenazas, análisis, Control de IoT (con opción Ranger)	✓	✓	✓
Características de operaciones de seguridad de EDR			
Visibilidad profunda ActiveEDRTM	✓		
Giro profundo de pivote StorylineTM	✓		
Cacería de visibilidad profunda mediante la técnica MITRE ATT&CK ®	✓		
Lista de seguimiento automatizada de respuesta activa de StorylineTM (STAR)	✓		
Obtención manual/automática de archivos (Windows, Mac, Linux)	✓		
Visibilidad profunda Marcar hallazgo benigno como amenaza para respuesta de ejecución	✓		
Almacenamiento ampliado de datos históricos de EDR (disponible de 14 a 365 días)	✓		
Acceso remoto seguro (Windows Powershell, Mac y Linux bash)*	✓	✓	
Funciones de IT OPS / Higiene y Suite de seguridad			
Control de Firewall del sistema operativo con reconocimiento de ubicación (Windows, Mac, Linux)	✓	✓	
Control de dispositivos USB (Windows, Mac)	✓	✓	
Control de Bluetooth® / Bluetooth de Baja Energía® (Windows, Mac)	✓	✓	
Detección de dispositivos no autorizados	✓	✓	
Vulnerabilidad de la aplicación (Windows, Mac)	✓	✓	
Funciones básicas de protección de endpoints			
Motor StorylineTM del agente Sentinel autónomo	✓	✓	✓
Prevención de ataques basados en archivos mediante IA estática y Sentinel Cloud	✓	✓	✓
Detección de ataques sin archivos mediante IA de comportamiento	✓	✓	✓
Respuesta autónoma a amenazas/eliminación, cuarentena (Windows, Mac, Linux)	✓	✓	✓
Respuesta autónoma de remediación / 1 clic, sin necesidad de secuencias de comandos (Windows, Mac)	✓	✓	✓
Respuesta autónoma de reversión / 1 clic, sin necesidad de secuencias de comandos (Windows)	✓	✓	✓
Dispositivo en cuarentena en la red	✓	✓	✓
Análisis de incidentes (MITRE ATT&CK®, línea de tiempo, explorador, anotaciones de equipo)	✓	✓	✓
Agente anti-manipulación	✓	✓	✓
Inventario de aplicaciones	✓	✓	✓

***Incluido con Singularity Control por tiempo limitado**

Servicios y Soporte Global de Vanguardia

Asistencia técnica por vía telefónica, en línea y mediante correo electrónico	Incluido
Centro de recursos del producto / Acceso al portal de asistencia	Incluido
Asistencia estándar de 9x5	Incluido
Asistencia empresarial de 24x7x365, Sigue al Sol para Sev 1 y 2	Disponible
Gestor de cuenta técnico asignado + asistencia empresarial	Disponible
Suscripción de Vigilancia de Detección y Respuesta Administrada (MDR)	Disponible
Implementación de preparación de SentinelOne y suscripción de mantenimiento continua	Disponible

SOPORTE DE SO

SentinelOne respalda una amplia gama de distribuciones de Windows, Mac y Linux, así como sistemas operativos de virtualización.
Las exclusiones típicas de software están registradas en su portal de asistencia.

Agente Sentinel de Windows

Todas las estaciones de trabajo de Windows que comienzan con 7 SP1 a través de Windows 10
Todos los servidores de Windows a partir de 2008 R2 SP1 hasta Server/Core 2019

Agente Sentinel de Mac

macOS Catalina, Mojave, High Sierra

Agente Sentinel de Linux

Ubuntu, Redhat (RHEL), CentOS, Oracle, Amazon AMI, SUSE Linux Enterprise Server, Fedora, Debian, Virtuozzo, Scientific linux

Agente heredado de Windows

XP, servidor 2003 y 2008, POS2009

Plataformas de contenedores compatibles

Kubernetes autoadministrado v1.13+ (autoadministrado, AWS Kubernetes (EKS), Azure AKS)

Virtualización y VDI

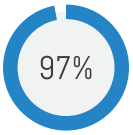
Citrix XenApp, Citrix XenDesktop, Oracle VirtualBox, VMware vSphere, VMware Estación de trabajo, VMware Fusion, VMware Horizonte, Microsoft Hyper-V

SentinelOne es una empresa que prioriza al cliente

La medición y la mejora continuas los impulsan a superar las expectativas de los clientes.

96%

96% de Gartner Peer Insights™
Los revisores de 'La voz del cliente' recomiendan SentinelOne



La satisfacción del cliente
(CSAT) también ~97%

Acerca de Bits

BITS Ingeniería y Desarrollo. Innovation 2 Be Great. Empresa de Tecnología en redes informáticas, Conoce nuestro curriculum corporativo para conocer nuestra experiencia con más de 15 años con casos de éxito en la industria tecnológica.

https://www.bits.com.mx/

ventas@bits.com.mx
(+52) 614 433 3867