

Singularity™ EPP+EDR

Prevención, detección, investigación
y respuesta unificadas

Gartner®

Gartner incluye a SentinelOne
entre los líderes del Gartner
Magic Quadrant para plataformas
de protección de endpoints

La velocidad, sofisticación y escala de las amenazas han evolucionado, dejando atrás a las soluciones EDR y de prevención de primera generación

Cuando los ciberdelincuentes consiguen eludir las medidas de prevención, las funciones de detección y respuesta para endpoints (EDR) deben activarse en tiempo real y de manera autónoma en el endpoint, esté o no conectado a la red. SentinelOne Singularity EPP+EDR combina las funciones EDR y de prevención de próxima generación en un solo agente para ofrecer protección autónoma ultrarrápida.

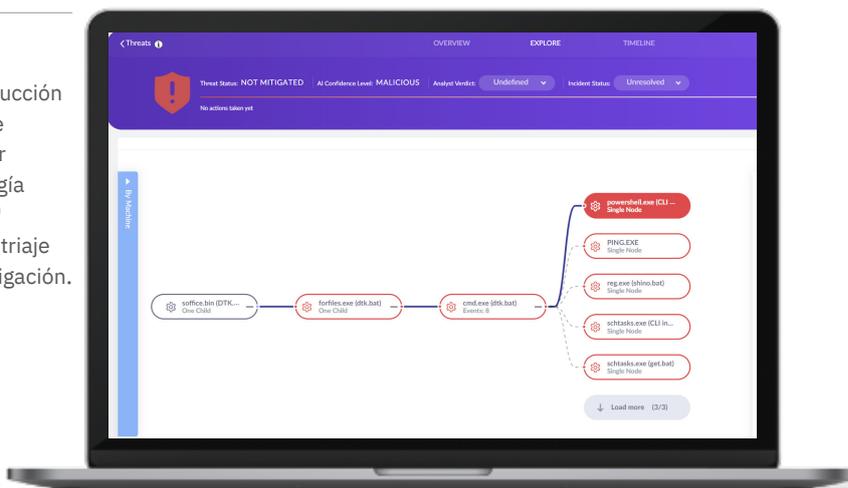
Optimizada por Deep Visibility™ y ActiveEDR™

La funcionalidad ActiveEDR utiliza inteligencia artificial basada en el comportamiento para identificar los procesos maliciosos a medida que se producen. Etiqueta los eventos correlacionados y crea automáticamente un relato Storyline™ para visualizar y acelerar la investigación. En modo de protección, el agente Sentinel no solo identifica el ataque, sino que lo neutraliza automáticamente. A continuación, un analista puede anular todos los cambios no autorizados que se hayan realizado con la funcionalidad de corrección con un clic patentada. Y todo ello sin necesidad de recurrir a scripts.

Investigación forense robusta e intuitiva

Las funciones EDR no pueden ser privilegio exclusivo de una minoría. Para reducir el tiempo medio de reparación (MTTR) y maximizar la productividad, las soluciones EDR de nueva generación deben simplificar la detección y la respuesta. La inteligencia artificial supervisa de forma permanente todos los eventos, en todos los sistemas operativos y en todos los entornos, ya sea un centro de datos, un proveedor de servicios en la nube, una oficina o un lugar de trabajo remoto. Deep Visibility permite la caza e investigación sin formación previa, poniendo la respuesta a incidentes y la caza de amenazas a disposición de un mayor número de miembros del equipo de seguridad.

El relato
o reconstrucción
del ataque
creado por
la tecnología
Storyline™
acelera el triaje
y la investigación.



SINGULARITY EPP+EDR

Prevención y EDR autónomas
y ultrarrápidas basadas en
inteligencia artificial

CARACTERÍSTICAS PRINCIPALES

- + EPP/EDR autónomas y consolidadas
- + Solamente EPP o EDR, o bien modos combinados con el mismo producto
- + Linux, macOS, Windows, Kubernetes y Docker
- + Protección, detección e intervención online y offline
- + Correlación automatizada de eventos en forma de relatos Storyline
- + Funciones patentadas de corrección y reversión con un clic
- + Conformidad con el marco MITRE ATT&CK®
- + Retención de datos EDR flexible, con opción de 14 a más de 365 días
- + Investigación forense remota para todos los sistemas operativos



Un servicio de atención
al cliente excelente, un
producto excepcional.



DIRECTOR DE TI
Atención sanitaria

Funciones principales

- ✓ **Detección y corrección autónomas en tiempo real** de amenazas complejas, sin intervención humana.
- ✓ **Protección implacable** en Windows, Linux y macOS, independientemente del entorno (físico, virtual, contenedor, nube o centro de datos).
- ✓ **Triage y análisis de causa raíz acelerados** gracias a información oportuna sobre incidentes y el respeto del marco MITRE ATT&CK® más riguroso del mercado, con o sin servicio MDR. Investigación en segundos gracias a correlaciones automáticas y relatos Storyline.
- ✓ **Corrección y reversión con un clic** para una respuesta simplificada y un tiempo medio de reparación (MTTR) reducido.
- ✓ **Experiencia de usuario intuitiva** de DeepVisibility, S1QL y STAR™ (Storyline Active Response) que reduce las competencias necesarias para que más miembros de su equipo de seguridad puedan llevar a cabo la caza de amenazas.
- ✓ **Opciones de retención de datos** adaptadas a todas las necesidades, de 14 a más de 365 días.
- ✓ **Despliegue acelerado** gracias a funciones de interoperabilidad que garantizan un despliegue rápido y fluido.
- ✓ **Inteligencia sobre amenazas integrada** para la detección y enriquecimiento de los principales flujos de inteligencia de terceros, así como de nuestras propias fuentes propietarias.

¿PREPARADO PARA UNA DEMOSTRACIÓN?

Para obtener más información, visite el sitio web de SentinelOne

VENTAJAS PRINCIPALES

- + Tiempo de permanencia reducido
- + Respuesta a incidentes más rápida
- + Tiempo medio de reparación reducido
- + Disminución de la fatiga de alertas
- + Aumento de la productividad de los analistas
- + Componente de la plataforma Singularity

DETECCIÓN Y RESPUESTA GESTIONADAS

Vigilance MDR permite a los clientes centrarse únicamente en los incidentes importantes, lo que la convierte en el complemento perfecto para los equipos de TI/SOC sobrecargados.

Visite <https://s1.ai/s1mdr> para obtener más información

ATT&CK®

MITRE ATT&CK 2020

- Tasa más baja de errores de detección
- Mayor número de detecciones
- Mejor cobertura de enriquecimiento de datos

Gartner

GARTNER MAGIC QUADRANT 2020 PARA LA PROTECCIÓN DE ENDPOINTS

- Cuadrante de líderes
- Las funciones críticas obtienen la mejor puntuación en los tres tipos de perfiles definidos por Gartner

FORRESTER®

INFORME FORRESTER WAVE™ 2020 PARA SOLUCIONES EDR

"Strong Performer"

kuppingercoie
ANALYSTS

MARKET COMPASS 2020 DE KUPPINGERCOIE

Innovador en el mercado de EPDR

SentinelOne sitúa a sus clientes en centro de sus prioridades

Nuestras evaluaciones y mejoras continuas superan las expectativas de nuestros clientes.



97%

de los evaluadores del informe Gartner Peer Insights™ "Voice of the Customer" 2020 recomiendan SentinelOne.

97%

Satisfacción de los clientes (CSAT)



TEVORA™
Certificación PCI DSS
Certificación HIPAA



Gartner peer insights™
4.9 ★★★★★

Acerca de SentinelOne

Más capacidad. Menos complejidad. SentinelOne desarrolla soluciones de ciberseguridad para el futuro que se basan en inteligencia autónoma y distribuida en los endpoints, con el fin de simplificar la pila de seguridad sin dejar de ofrecer a las empresas las funciones que necesitan. Nuestra tecnología está diseñada para reforzar los equipos de seguridad gracias a la automatización y a una resolución de las amenazas de gran eficacia. ¿Está preparado?

sentinelone.com

sales@sentinelone.com

+ 1 855 868 3733