

# Singularity™ EPP+EDR

Prevención, detección, investigación y respuesta unificadas

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.

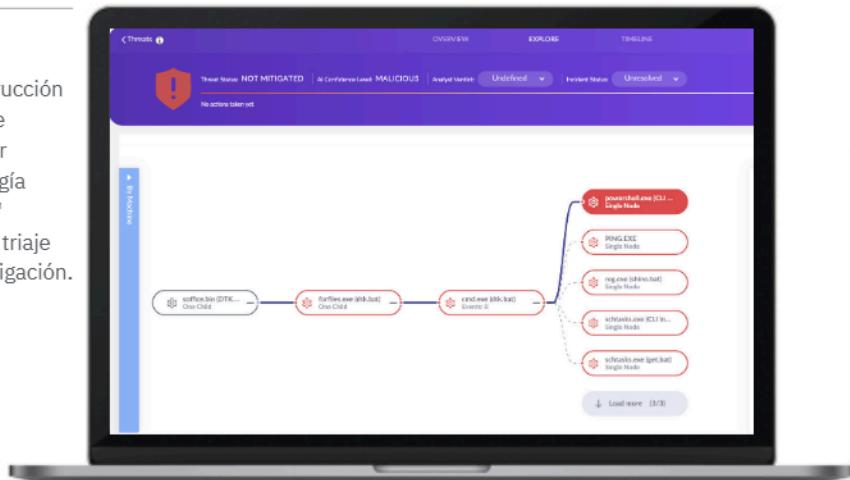
## Optimizada por Deep Visibility™ y ActiveEDR™

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.



## Gartner

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

### 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