SentinelOne

SILICON

Singularity™ EPP+EDR

Unified Prevention, Detection, Investigation, Response

The speed, sophistication, and scale of threats has evolved, leaving first generation prevention and EDR solutions behind

When attackers pierce prevention measures, endpoint detection and response needs to happen autonomously, in real-time at the endpoint, with or without a network connection. SentinelOne Singularity EPP+EDR combines next-gen prevention and EDR capabilities in a single Sentinel agent to achieve autonomous EPP at machine speed.

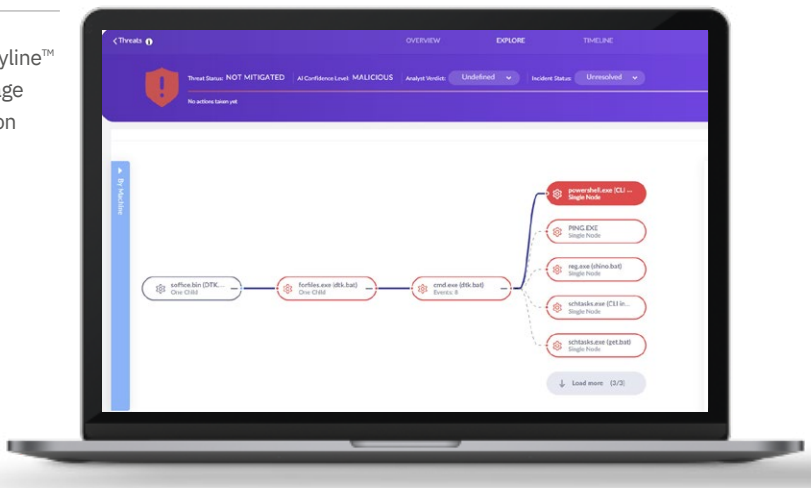
Powered by Deep Visibility™ & ActiveEDR™

ActiveEDR uses behavioral AI to identify malicious processes as they occur, tagging correlated events and automatically building an attack Storyline™ to visualize and accelerate the investigation. In Protect Mode, the Sentinel not only identifies the attack but automatically thwarts the contagion. Then, with patented 1-Click Remediation, an analyst can reverse all unauthorized changes that may have occured. No scripts required.

Robust Forensics, Intuitive Simplicity

EDR can no longer be the exclusive domain of the few. To slash MTTR (Mean Time to Repair) and maximize productivity, EDR 2.0 must simplify detection and response. AI continuously monitors every event, across every OS and every environment, whether data center, cloud service provider, office, or remote work location. Deep Visibility powers hunting and investigation with zero learning curve, bringing IR and hunting to a wider pool of security talent.

Automatic Storyline™ accelerates triage and investigation



SINGULARITY EPP+EDR

Autonomous, AI-driven Prevention and EDR at machine speed

KEY FEATURES

+ Consolidated, autonomous EPP/EDR
+ EPP-only, EDR-only. Combined modes. Same product.
+ Linux, macOS, Windows, Kubernetes, and Docker
+ Online/offline protection, detection & response
+ Automated event correlation into Storylines
+ Patented 1-Click Remediation & Rollback
+ Full alignment with MITRE ATT&CK® framework
+ Flexible EDR data retention, 14-365+ days options
+ Remote forensics for every OS

Gartner peerinsights™

“

Great customer service, even better product.

★★★★★

SENIOR DIRECTOR, IT
Healthcare

Key Capabilities

- **Autonomous, real-time** detection and remediation of complex threats with no need for human intervention.
- **Uncompromising protection** across Windows, Linux, and macOS - physical, virtual, container, cloud, data center, anywhere.
- **Accelerated triage and root cause analysis** with incident insights and the best MITRE ATT&CK® alignment on the market, with or without MDR. Investigate in seconds with automated correlations and Storylines.
- **1-Click Remediation & Rollback** simplifies response and slashes MTTR (Mean Time to Repair).
- **Intuitive user experience** of Deep Visibility, S1QL, and STAR™ (Storyline Active Response) reduces the skills required to add threat hunting to your security operations.
- **Data retention options** to suit every need, from 14 to 365+ days.
- **Rapid deployment** interoperability features ensure a fast, smooth rollout.
- **Integrated threat intelligence** for detection and enrichment from leading 3rd party feeds as well as our own proprietary sources.

KEY BENEFITS

+ Less dwell time
+ Accelerated IR
+ Reduced MTTR
+ Less alert fatigue
+ Higher analyst productivity
+ A Singularity Platform component

MANAGED DETECTION & RESPONSE

Vigilance MDR empowers customers to focus only on the incidents that matter making it the perfect endpoint add-on solution for overstretched IT/SOC Teams.

Visit **https://s1.ai/s1mdr** for more info

READY FOR A DEMO?

Visit the SentinelOne website for more details

Awards & Recognition

ATT&CK®

2020 MITRE ATT&CK

- Fewest Misses
- Highest Techniques + Tactics Correlations
- Best Data Enrichment Coverage

FORRESTER®

2020 FORRESTER WAVE™ EDR

Strong Performer

kuppingercole ANALYSTS

2020 KUPPINGERCOLE MARKET COMPASS

Featured EPDR Innovator

SentinelOne is a Customer First Company

Continual measurement and improvement drives us to exceed customer expectations.

96%

96% of Gartner Peer Insights™ 'Voice of the Customer' Reviewers recommend SentinelOne

97%

Customer Satisfaction (CSAT) is ~97%

Net Promoter Score in the "great" to "excellent" range

About SentinelOne

SentinelOne founded in 2013 and headquartered in Mountain View, California, is a cybersecurity software company. SentinelOne Singularity is one platform to prevent, detect, respond, and hunt in the context of all enterprise assets.

SILICON™

silicon.co.nz
Level 1, 90 Abel Smith Street
Te Aro
Wellington