SentinelOne

DATA SHEET

Singularity™ Endpoint Protection (EPP+EDR)

Autonomous, AI-driven Prevention and EDR at Machine Speed

The speed, sophistication, and scale of threats have evolved, and legacy AV solutions have failed to keep pace. Organizations lack the global visibility and context needed to combat these threats, creating blind spots that attackers can exploit. Security teams are already overwhelmed with the number of false positives and low detection efficacy of first-generation EDR solutions, which often require manual triage, response, and remediation.

When attackers pierce prevention measures, endpoint detection and response needs to happen autonomously and in real-time. SentinelOne Singularity Endpoint Protection (EPP+EDR) combines next-gen prevention and EDR capabilities in a single platform with a single agent.

Scalable Security Platform

Singularity is architected as a highly available SaaS solution with true multi-tenancy and multi-site hierarchy. Best-in-industry coverage across all major operating systems and a rich integration ecosystem extends the platform to your existing security investments.

Robust Prevention & Control

Replace legacy AV solutions with Static AI models trained to detect threats by looking at various static attributes extracted from executables, eliminating dependencies on signatures, and offering superior detection of file-based threats. Limit your attack surface with native firewall control and granular device control for USB & Bluetooth, Bluetooth Low Energy.

Threat Detection with Storyline™

Behavioral AI evaluates threats — like fileless attacks, lateral movement, and actively executing rootkits — in real-time, delivering high-fidelity detections without human intervention. Individual events are automatically correlated into a context-rich Storyline to reconstruct the attack from start to finish. Threat intelligence is infused from proprietary and 3rd party sources to increase detection efficacy.

Patented 1-Click Remediation

Remediate all affected endpoints with a single click, without the need to write any new scripts, simplifying and reducing mean time to respond. With STAR™ (Storyline Active Response), create automated hunting rules specific to your environment that trigger alerts and responses when rules detect a match.

Deep Visibility™ Threat Hunting

Deep Visibility powers hunting and investigation with zero learning curve, bringing IR and hunting to a broader pool of security talent. Uplevel SOC resources to enable proactive threat hunting with automated hunting rules, intel-driven hunting packs, and support for MITRE ATT&CK techniques. Easy to use search and pivoting lightens analyst load when hunting across large volumes (up to 365 days) of EDR telemetry.

SINGULARITY EPP+EDR

Autonomous, AI-driven Prevention, and EDR at machine speed

KEY FEATURES

+ EPP-only, EDR-only. Combined modes. Same product.
+ AI-based malware & ransomware protection. No signatures.
+ Autonomous operation. Works on and off-network.
+ Linux, macOS, Windows, Kubernetes, and Docker
+ Automated event correlation with Storyline
+ Patented 1-click remediation & rollback
+ Hunt by MITRE ATT&CK® Technique
+ STAR™ proactive, custom hunting and response rules
+ Flexible EDR data retention up to 365 days
+ Frictionless Singularity Marketplace integration

Gartner peerinsights™

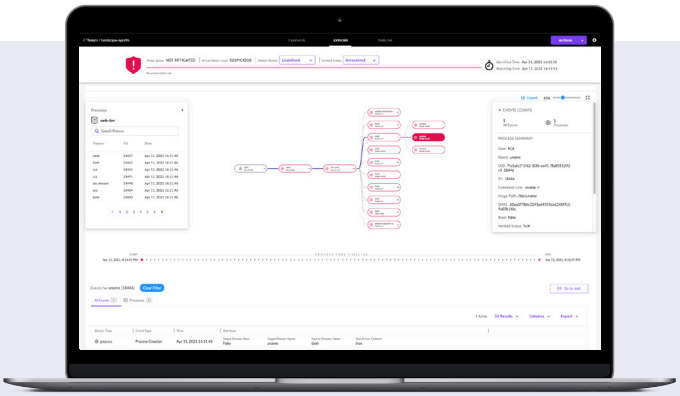
“

Great customer service, even better product.

★★★★★

SENIOR DIRECTOR, IT

Healthcare



Automatic Storyline™ accelerates triage and investigation

Key Capabilities

- **Single cloud-delivered platform** with true multi-tenant capabilities to address the needs of global enterprises and MSSPs
- **Autonomous, real-time** detection and remediation of complex threats with no need for human intervention.
- **Industry-leading coverage** across Windows, Linux, and macOS - physical, virtual, container, cloud, data center, anywhere.
- **1-Click remediation & rollback** simplifies response and slashes MTTR (Mean Time to Remediate).
- **Accelerated triage and root cause analysis** with incident insights and the best MITRE ATT&CK® alignment on the market, with or without Vigilance MDR. Investigate in seconds with automated correlations and Storyline.
- **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 proprietary sources.

KEY BENEFITS

+ Shorter dwell time
+ Accelerated Incident Response
+ Reduced MTTR
+ Less alert fatigue
+ Global visibility
+ Higher analyst productivity
+ Minimal management & maintenance overhead

READY FOR A DEMO?

Visit the SentinelOne website for more details

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

Highest Ranked in all Critical Capabilities Report Use Cases

MITRE ENGENUITY™

Record Breaking ATT&CK Evaluation

- No missed detections. 100% visibility
- Most Analytic Detections 2 years running
- Zero Delays. Zero Config Changes

Gartner peerinsights™ 4.9 ★★★★★

98% of Gartner Peer Insights™

Voice of the Customer Reviewers recommend SentinelOne

FedRAMP · ISO 27001 CERTIFIED by schellman · VB 100 VIRUS virusbtn.com · TEVORA PCI DSS Attestation HIPAA Attestation

About SentinelOne

More Capability. Less Complexity. SentinelOne is pioneering the future of cybersecurity with autonomous, distributed endpoint intelligence aimed at simplifying the security stack without forgoing enterprise capabilities. Our technology is designed to scale people with automation and frictionless threat resolution. Are you ready?

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733