SentinelOne

DATA SHEET

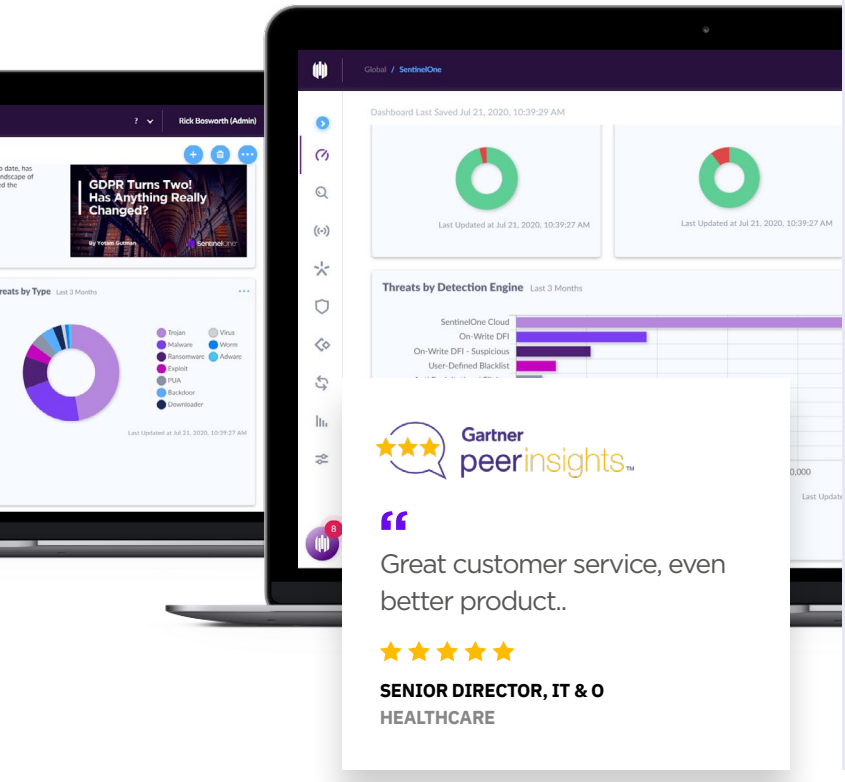
macOS Sentinel Agent

Runtime Security and EDR/XDR at the Endpoint

macOS devices are an increasingly popular choice among enterprise users. Endpoints using macOS demand the same high-quality protection, detection, and response as Windows endpoints.

SentinelOne combines robust protection and EDR in an autonomous agent that works with or without cloud connectivity. Built-in Static and Behavioral AI Engines deliver machine-speed prevention, detection, and response against even the most advanced threats, to keep users secure and productive.

SentinelOne supports the latest macOS versions, often within days of release, and Apple processors, for optimum performance that does not compromise on security. Whether you have endpoints on Windows or macOS, or cloud workloads on Linux and Kubernetes, SentinelOne provides a single security console to manage them all.



KEY FEATURES

Operations

- Native support for Apple processors
- Easy deployment via common MDM
- ONE multi-tenant console
- Auto agent update via console
- macOS application inventory
- Catalina, Big Sur, Monterey, and Ventura

Security

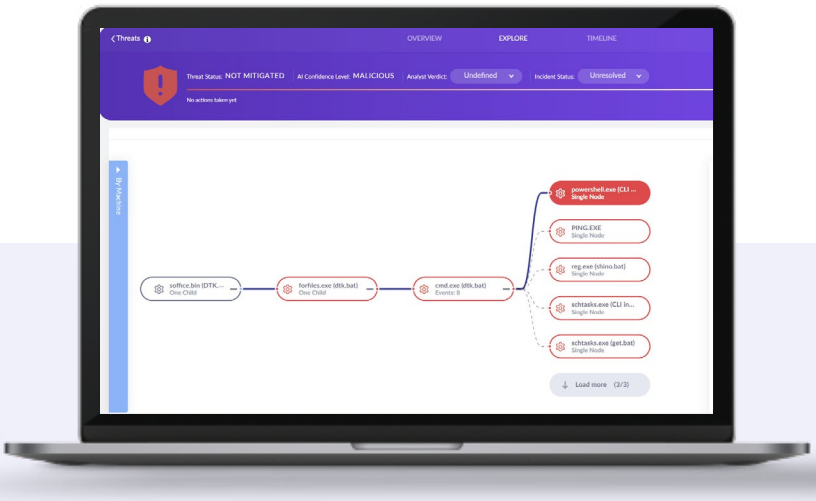
- On-agent Static and Behavioral AI Engines block malware, fileless, and advanced threats
- Remote Shell and Remote Scripts Orchestration (RSO)
- Robust anti-tamper
- Device and Firewall Control
- Auto-correlate events into Storyline™ and map to MITRE ATT&CK TTPs
- Storyline Active Response (STAR™) custom rules
- Automatic quarantine
- Network isolation
- Application Vulnerability Management

Storyline™ Makes SentinelOne a Better Choice

SentinelOne pioneered Storyline technology to reduce threat dwell time and simplify EDR searching and hunting operations. Storyline automatically correlates all software operations in real time at the endpoint and builds actionable context on the fly for every linked process across all process trees, every millisecond of every day. Automated responses are triggered on-agent in real time, via Storyline Active Response (STAR™), our XDR cloud engine, or manually by analysts.

For endpoint protection (EPP), static and behavioral AI engines continually examine thousands of concurrent OS stories and seek out-of-bounds files and processes warranting immediate protective responses. For endpoint detection & response (EDR), Sentinels do the correlation heavy lifting to save the analyst time and headache. Storyline context of both malicious and benign data is maintained during long term storage (14 to 365+ days) within the Singularity Platform so that it is available instantly when the analyst needs it.

Never build another PID tree again. We do it for you.



Automatic Storyline™ accelerates triage and investigation

BENEFITS

- **On-agent AI eliminates cloud latency impact on protection**
- **Rapid support for new macOS releases**
- **Accelerated investigation with Storyline**
- **Optimized for DEV and heavy file operation use cases**
- **Extensive data retention options**
- **Reduced MTTR**

Gartner peerinsights™

"Complete endpoint protection... spot on."

★★★★★

CTO
Retail, 1B - 3B USD

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2021 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY™

Record Breaking ATT&CK Evaluation
- 100% Protection. 100% Detection.
- Top Analytic Coverage 3 Years Running
- 100% Real-time with Zero Delays

Gartner peerinsights™ 4.9 ★★★★★

99% of Gartner Peer Insights™
EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · AICPA SOC · TEVORA PCI DSS Attestation HIPAA Attestation · VB 100 VIRUS virusbtn.com · AAA · SE Labs BEST Innovator WINNER 2021

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733