macOS Sentinel Agent
Runtime Security and EDR at the Endpoint

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

Your Mac user endpoints deserve and expect the same quality of protection your Windows users enjoy. The SentinelOne macOS Sentinel combines EPP and EDR in a single agent that does not pull any punches on would-be attackers. Premium static and behavioral AI-driven prevention, detection, and response operate autonomously at the endpoint, in real-time, with or without a network connection.

And now, our macOS Sentinel agent has gone kextless, foregoing kernel extensions in favor of efficient user-space APIs to deliver the security capabilities SentinelOne customers have come to expect. Whether Windows, mac, or Linux, user endpoint or cloud workload, SentinelOne provides one intuitive management console to rule them all.
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.

BENEFITS
- Distributed intelligence at the endpoint
- Real-time detection and response vs. novel attacks
- Accelerated investigation with Storyline
- 1-Click Remediation, no scripts needed
- Reduced MTTR

Automatic Storyline™ accelerates triage and investigation.

ATT&CK®
2020 MITRE ATT&CK
- Fewest Misses
- Most 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.

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?