SentinelOne

SentinelOne ActiveEDR

Powerful visibility, autonomous detection, automated response, and proactive hunting — Simplified

SentinelOne ActiveEDR is an advanced EDR and threat hunting solution that delivers real-time visibility with contextualized, correlated insights accelerating triaging and root cause analysis. The solution lightens the SOC burden with automated threat resolution, dramatically reducing the mean time to remediate the incident. ActiveEDR enables more proactive hunting capabilities to uncover stealthy, sophisticated threats lurking in the environment.

Key capabilities

Detect high-velocity threats with patented Storyline

Storyline automatically correlates atomic events into unified context rich stories that provide campaign level insights.

Accelerate investigations with seamless MITRE techniques

Sentinel-One ActiveEDR maps attacks in real-time, providing analysts immediate in-product indicators and attack context.

Remediate entire attacks with 1-click rollback

Remediate entire attack storylines with a single click, speeding up threat resolution.

Customize EDR to your environment with STAR

Create custom alerts specific to your environment with automated hunting rules.

Proactively hunt to uncover advanced adversaries

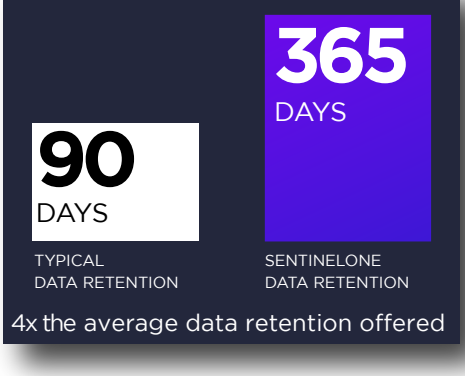
Empower hunting teams to easily uncover and stop advanced hidden attacks with an intuitive user interface.

Investigate historical data with extended data retention

EDR data retention of 365 days and beyond for full historical analysis of any attack.

SOLUTIONS BENEFITS

+ Get high efficacy, actionable threat detection without the noise
+ Rapidly uncover and contain advanced threats to reduce incident dwell time and time to resolution
+ Get a complete understanding of the root cause to close existing gaps
+ Empower and uplevel the security team with an easy-to-use, intuitive product
+ Reduce SOC burden by automating manual tasks with automated correlation and one-click remediation
+ Single cloud-delivered platform with true multi-tenant capabilities to address the needs of global enterprises and MSSPs
+ Best-in-industry coverage across Linux, MacOS, Windows
+ Affordable EDR data retention of 365 days+ for full historical analysis



Stream telemetry locally to automate SOAR workflows with Cloud Funnel

SentinelOne Cloud Funnel enables secure, near-real-time streaming of EDR telemetry from SentinelOne Deep Visibility to your data lake via a Kafka subscription. SentinelOne Deep Visibility aggregates endpoint telemetry data in the cloud from your fleet of autonomous Sentinels, where AI reveals hidden threats, correlates activity, and delivers actionable insights. A Kafka subscription securely sends your telemetry to your own data lake. Your connection to Deep Visibility is secured via TLS 1.2+, and access is governed by SCRAM (Salted Challenge Response Authentication Mechanism) supported by Kafka. When new data is available, Kafka streams to your data lake. Once there, Security teams may take any number of actions on their EDR data, such as correlation with non-SentinelOne data sources, integration with SIEM tooling, and orchestration and enrichment of security incident workflows.

Gartner peerinsights.

"SentinelOne smokes the competition."

★★★★★

Sr. Director, Cybersecurity
Retail, 1B - 3B USD

Gartner peerinsights.

"Easy and effective EPP and EDR."

★★★★★

Security Analyst
Manufacturing, 3B - 10B USD

Gartner peerinsights.

"One of the greatest EDRs I have used to date!"

★★★★★

Security and Risk Management
Healthcare, 3B - 10B USD

SOLUTION HIGHLIGHTS

+ Real-time detection and remediation of complex threats with no need for human intervention
+ Accelerated triage and root cause analysis with incident insights and the best MITRE ATT&CK alignment on the market, with or without MDR
+ Integrated threat intelligence for detection and enrichment from leading 3rd party feeds as well as our proprietary sources
+ Patented 1-Click Remediation & Rollback
+ Intuitive user experience reduces the skills required to add threat hunting to your security operations
+ Data retention options to suit every need, from 14 to 365+ days. Hunt by MITRE ATT&CK Technique
+ Uncompromising protection across Windows, Linux, and macOS endpoints - physical, virtual, container - cloud or data center
+ Rapid deployment interoperability features ensure a fast, smooth rollout
+ RESTful APIs and pre-built integrations to various Enterprise applications and services

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 · AAA Certified · ISO 27001 CERTIFIED by schellman · VB 100 VIRUS virusbtn.com · AAA Certified · 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?

Data Magic Computer Services

datamagic@datamagicinc.com
469-635-5500

DATA MAGIC COMPUTER SERVICES