SentinelOne

Singularity™ XDR

Extend Protection, Detection, and Remediation to Endpoint and Beyond

The cybersecurity threat landscape is evolving exponentially in both speed and scope. Meanwhile, most security teams struggle to keep pace with emerging threats with the resources they have at hand. These organizations often lack global visibility and context across their technology stacks, creating gaps in what they can see and detect. Simultaneously, analysts juggle point tools for each vector, forcing them to analyze data in isolation and manually investigate. Today's security teams need a more proactive solution to identify, contain, and remediate emerging threats.

SentinelOne Singularity XDR unifies and extends detection and response capabilities across multiple security layers, including endpoint, cloud, identity, network, and mobile, providing security teams with centralized end-to-end enterprise visibility, powerful analytics, and automated response across a large cross-section of the technology stack.

Comprehensive Coverage Across Your Enterprise Stack With Operational Simplicity

Deliver native protection across multiple solutions, including endpoint, cloud, identity, mobile, and devices. It enables frictionless third-party integrations, including threat intelligence, SIEM, SOAR, email, SASE, sandbox, and more, enabling you to leverage your existing investments.

Increased Security Team Efficiency

Auto-correlate individual events into an attack sequence, to streamline investigation and response. Analysts can automatically resolve threats with one click, without scripting across the estate. Execute orchestrated remediation actions in a single step, including network quarantine, auto-deploy agents on unprotected workstations, or automate policy enforcement across cloud environments.

Streamline Security Workflows Powered by a Unified Data Store

Unify and correlate the enterprise security data in one convenient, context-rich, cost-effective platform. Ingest native and third-party data in real-time, to break down silos and eliminate blind spots. Visualize data from disparate security solutions spanning endpoints, cloud workloads, network-connected (IoT) devices, and networks. Surface insights and inform action from your security solutions.

Key Features And Benefits

See
Maximize visibility across every corner of the enterprise

Protect
Protection coverage with unrivaled speed, efficiency, and simplicity

Resolve
Automate response across the entire connected security ecosystem with a single click

+ Streamline operations and security workflows
+ Streamline operations and security workflows
+ Reduce mean time to respond with simple, fast, and relevant automation
+ Up-level analyst productivity
+ Accelerate time to value for security analysts
+ Combine native and open XDR to offer customers the flexibility they need without limiting them to one solution multi-tenant capabilities to address the needs of global enterprises and MSSPs

Auto-Enrich Threats With Integrated Threat Intelligence

Singularity XDR integrates threat intelligence for detection and enrichment from leading third-party feeds and proprietary sources, to auto-enrich incidents with real-time threat intelligence. This empowers security teams with additional contextual risk scores on indicators of compromise (IOCs) such as IPs, hashes, vulnerabilities, and domains. Singularity XDR maps events to the MITRE ATT&CK framework to make analysis and investigation easy for security teams. Customers can also leverage a query library of hunts curated by our researchers and threat hunters who continually evaluate new methodologies and uncover new IOCs and Tactics, Techniques, and Procedures (TTPs).

Scale Your Team with One Intuitive Solution

Singularity XDR provides a single solution for extended threat detection, investigation, response, and hunting.

A single source of prioritized alerts that ingests and standardizes data across multiple sources	A single consolidated view to quickly understand the progression of attacks across security layers	A single solution to rapidly respond to and proactively hunt for threats

Frictionless Integration with Leading Security Ecosystem Vendors

Singularity Marketplace enables customers to extend Singularity XDR with bite-sized, one-click applications to help enterprises unify prevention, detection, and response.

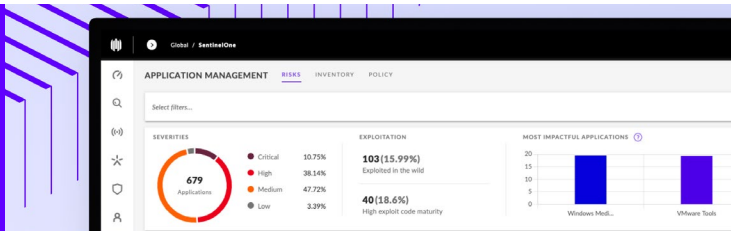
Gartner Peer Insights™

"All in all, the solution is the easiest solution I have ever had for fighting threats and one of the easiest software deployments I have done. Their service is exceptional.

Security And Risk Manager
CONSTRUCTION

Ready for a Demo?

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733



Innovative. Trusted. Recognized.

Gartner

A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

+ 100% Protection. 100% Detection
+ Outstanding Analytic Coverage, 4 Years Running
+ 100% Real-time with Zero Delays

Gartner Peer Insights™

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR Level One · Virus 100 · SE Labs Best Innovator Winner 2021 · Trusted Cloud Provider CSA

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

sentinelone.com

sales@sentinelone.com
+1 855 868 3733