SentinelOne

Singularity™ AI SIEM

The Industry's Fastest AI-Powered Open SIEM for All Your Data and Workflows

Over the past decade, rising cyber threats and exploding data volumes have made security more complex, yet our tools have barely evolved.

Singularity™ AI SIEM offers a ground-breaking alternative to legacy SIEMs with enterprise visibility, real-time detection, and enhanced productivity. Leveraging advanced AI and automation capabilities, you can enable your SOC analysts to detect and respond to threats faster allowing you to then allocate resources more effectively to improve your overall security posture, boost cyber resilience, increase SOC efficiency, and maintain compliance.

Secure your organization with SentinelOne in whichever way works best for you. This solution possesses the functionality to replace expensive, cumbersome, and slow legacy SIEM systems with an automated, scalable, and high-speed AI SIEM or uplevel your security through a phased approach.

Overhaul Your SIEM From Top to Bottom

- Gain real-time AI powered protection for the entire enterprise
- Move into a cloud-native AI SIEM
- Take advantage of limitless scalability and endless data retention
- Accelerate your workflows with Hyperautomation
- See significant cost savings with even more product functionality

Bring Your SIEM Into the Future at Your Own Pace

- Augment and integrate SentinelOne into your SOC
- Ingest all excess data and keep your current workflows
- Filter, enrich, and optimize the data in your legacy SIEM
- Introduce AI-based, real-time protection
- Lower your security costs while gaining more robust protection

100x
Faster Than Legacy SIEM

50%
Lower Operational Costs

246%
Return on Investment

99%
Reduction in Risk Exposure

80%
Faster Threat Hunting

Lower Costs. Greater Value.

+ Exabyte scale that can handle any data load
+ No indexing, just speed
+ Store data for as long as you need
+ Make analysts more efficient and effective
+ Never be locked-in to any vendor

Different From The Bottom Up

We take a holistic approach to securing your organization, starting with how your data is ingested and managed. AI SIEM is a cloud-native SaaS built for infinite scalability and includes a robust columnar database. While it's possible to pair a basic columnar database with a low-cost SIEM, this approach often results in limited functionality, inflexible SQL-like queries, and minimal support for effective data investigation or insight generation. AI SIEM excels in hunting and investigations, allowing users to seamlessly navigate logs and uncover actionable insights.

Our solution also features a multi-tenant architecture with a massively parallel query engine. Unlike next-gen SIEMs that fragment data across repositories and rely on custom views to access disparate data, we centralize all information into a single, unified repository for instant querying.

With hot storage and AI SIEM, we eliminate cold storage delays and ensure data is always accessible for fast and efficient investigations. AI SIEM also enables the massive ingestion of structured and unstructured data, with OCSF natively supported, to accelerate threat hunting while reducing long-term storage costs. With an open ecosystem, you'll never be locked-in to any vendor.

This architecture enables AI SIEM to run many complicated computations simultaneously, significantly outpacing legacy SIEM systems. This level of performance not only speeds up interactive queries that an analyst might make during an investigation but also powers real-time dashboards, threat hunting, and unlocks the power of Purple AI.

Shifting the Security Analyst Role From Monotonous Tasks and Laborious Hands-on Investigations to System Supervision and Optimization

AI SIEM utilizes Hyperautomation to instantly create and manage powerful automated workflows. For example, creating workflows to autonomously mitigate threats frees your analysts to focus on strategic initiatives and high-priority investigations. In contrast to SOAR solutions, Hyperautomation aims to simplify automation, making it more accessible to security analysts without the need to code. It reduces complexity by having a no-code drag-and-drop canvas to create custom workflows.

When routine tasks are offloaded through automation, high-impact work requiring human input is seamlessly enhanced with PurpleAI. It provides tools like hunting quickstarts, auto-summaries, and suggested queries, reducing threat-hunting times from hours to minutes. With natural language processing, analysts can input queries conversationally, which AI translates into structured PowerQueries. Additionally, AI generates detailed investigation notebooks, simplifying knowledge sharing across teams. This accelerates insights, improves investigation efficiency, and fosters seamless collaboration.

Why Choose AI SIEM?

Modern Architecture

Cybersecurity starts with your data. You can't detect what you can't see. Because AI SIEM is built on a cloud-native modern architecture, it delivers rich, unfiltered data for complete visibility, enhancing your overall security posture.

Operational Autonomy

Autonomous operations thrive on broad, enriched security-specific data. AI SIEM delivers comprehensive insights and can automatically mitigate critical threats before they disrupt your business.

Intelligent Tools

Analysts are augmented with AI to supercharge their productivity. To stay ahead of attacks, conduct deeper investigations with streamlined workflows, contextual follow-up queries, and natural language support. Even less experienced analysts can now confidently threat hunt.

Singularity™ AI SIEM Key Features

Incident Response

Accelerate your incident response with automated playbooks. Our SIEM solution provides step-by-step guidance for handling threat scenarios, ensuring consistent and effective responses.

GenAI

Leverage a solution designed for data protection and privacy. Purple AI is never trained with customer data and is architected with the highest level of safeguards.

AI-Enhanced Detection

Leverage the power of AI to detect even the most sophisticated threats. Our advanced algorithms analyze vast amounts of data, identifying patterns and anomalies that traditional SIEM solutions might miss.

Real-Time Visibility

Achieve real-time visibility into your security environment. Our intuitive dashboard provides a comprehensive overview of all security events, enabling swift and informed decision-making.

Automated Workflows

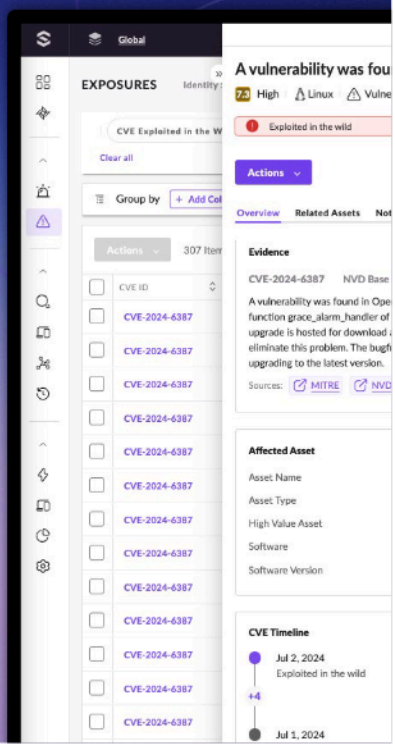
Automate and accelerate repetitive tasks and streamline security workflows. SentinelOne AI SIEM reduces manual intervention, allowing your team to focus on more strategic initiatives.

OCSF Supported Ingestion

Easily integrate your security stack with supported partner connectors. Ingest both structured and unstructured data, with OCSF natively supported. And detect threats on ingestion.

Threat Intelligence Integration

Enhance your security operations with integrated threat intelligence. Stay informed about the latest threats and vulnerabilities and proactively defend against potential attacks.



Innovative. Trusted. Recognized.

Gartner

A Leader in the 2024 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Industry-leading ATT&CK Evaluation

+ 100% Detections. 88% Less Noise
+ 100% Real-time with Zero Delays
+ Outstanding Analytic Coverage, 5 Years in a Row

Gartner Peer Insights

95% recommend SentinelOne

Endpoint Protection Platforms reviews for SentinelOne Singularity Platform

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · VB 100 VIRUS · 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