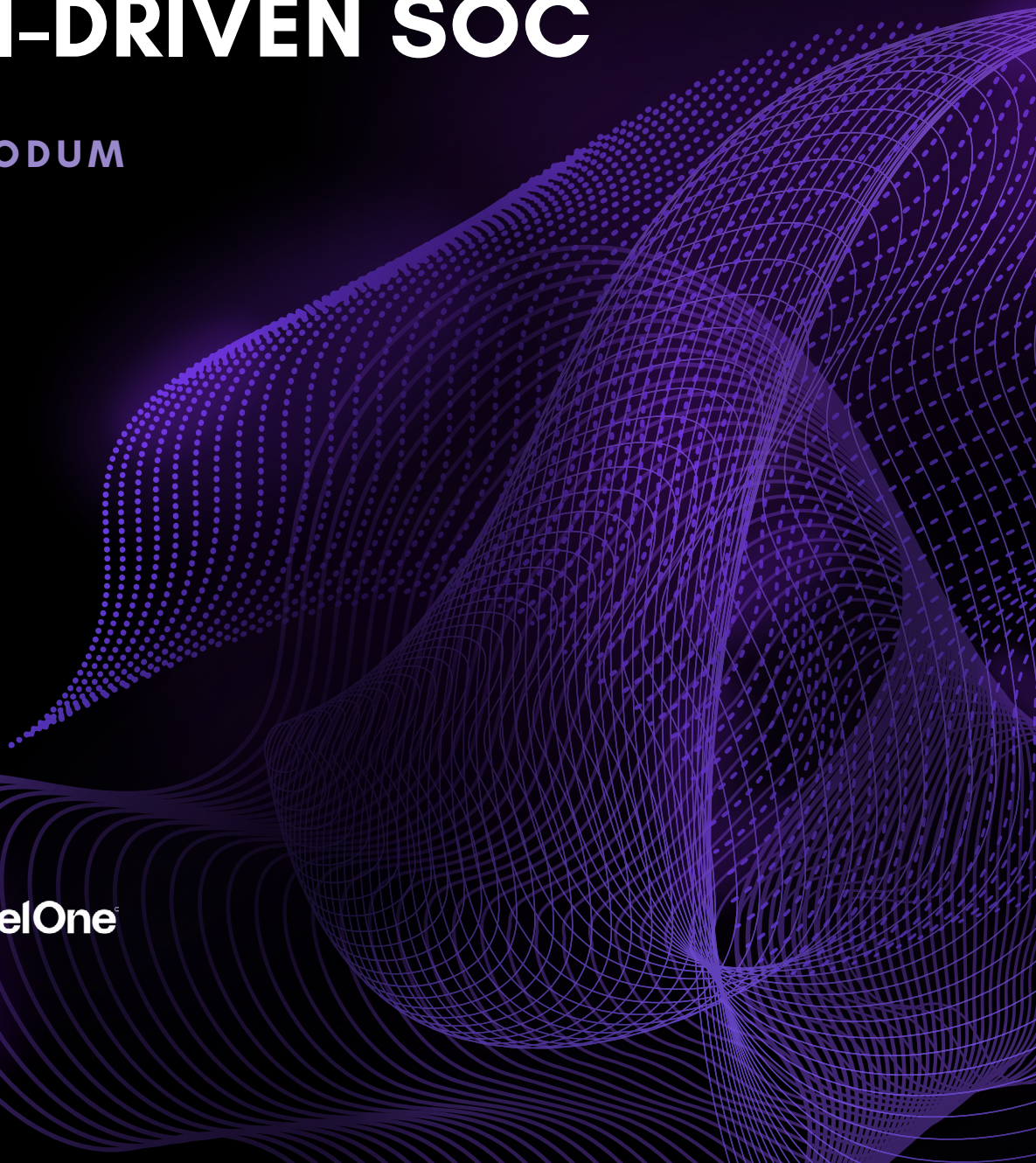
Software Analyst®
Cyber Research

SEPTEMBER
2025

SENTINELONE AI SIEM: THE EDR ADVANTAGE IN SIEM AND THE ROAD TO AN AI-DRIVEN SOC

FRANCIS ODUM



SentinelOne®

About Software Analyst Cybersecurity Research

SACR is a modern research and advisory firm built for today's cybersecurity leaders. We deliver in-depth, timely analysis across SOC operations, Identity, Network, Cloud, Application Security, Data, and AI Security; equipping CISOs, security teams, founders, investors, and practitioners with the insight they need to navigate high-stakes decisions.

With an engaged community of over **80,000** readers and followers, SACR connects with a global network of cybersecurity decision-makers and innovators. Our access to leaders across categories and industries gives us a direct line to the conversations shaping the market. By pairing these insights with rigorous technical analysis and continuous market tracking, we produce research that is both data-driven and grounded in the realities of modern security operations.

Whether you're seeking clarity on emerging technologies, evaluating vendors, or tracking market shifts, SACR delivers trusted, independent research designed to help you see clearly and decide with confidence.

We explore the newest frontiers of cybersecurity.

Whether you're looking at emerging vendors, evolving threats, or shifting architectures, or timely, opinionated insights help modern security leaders make smarter, faster decisions.

Table of Contents

The EDR Advantage in the SIEM Pivot

Practitioners,

Today, we're doing a deep dive into how EDR vendors are pivoting into the SIEM market. This has become an unexpected, but potentially highly successful wedge for these players to rip out legacy SIEMs. It's something I never expected.

Here is how I see it. EDR vendors are moving into SIEM because they already sit where the signal starts, on the endpoint and increasingly on cloud workloads. That vantage point gives them richer telemetry with process lineage, identity context, and device posture. When you start with higher fidelity data, correlation tends to improve, investigations move faster, and you spend less time chasing noise. This time-ordered telemetry is more complex for attackers to evade. Starting with higher-fidelity data means better correlation, faster investigations, and less noise for analysts on a SIEM.

The second advantage is architectural. An EDR-first platform can use a single agent and a shared data model to collect protection events and operational logs, then stream everything into one analytic fabric. That removes extra forwarders and one-off collectors, simplifies deployment, and shortens time to value.

The third advantage is the response loop. EDR vendors already control precise response actions on the host. When you layer SIEM analytics and workflow on top, you can close cases inside one console, from detection to containment to ticketing.

Lastly, GTM advantage matters. EDR vendors already have massive customer footprints and proven detection content, so pivoting into SIEM is a natural land-and-expand strategy. The challenge will be matching the breadth of integrations, compliance content, and migration tooling of established players. But the right to win is clear: stronger signal, unified workflow, and a platform that takes teams from detection to response without leaving the console.

Today, we have a commissioned study report by SentinelOne that delves into the expansion of their platform with their new AI SIEM as an EDR vendor.

Key Executive Summary

- If you read our last report, The Convergence of SIEMs and Data Lakes: Market Evolution, Key Players and What's Next. We elaborately discussed everything happening within the existing SIEM market. The evolution of Security Information and Event Management (SIEM) has reached a critical inflection point as security operations centers (SOCs) grapple with unprecedented data volumes, alert fatigue, and the complexity of modern cloud-native environments. SentinelOne, known for its leading-edge endpoint detection and response (EDR), has entered the SIEM market with an ambitious vision: to deliver a unified, AI-powered platform capable of transforming detection, investigation, and response through agentic reasoning, hyperautomation, and a cloud-native data lake.

- This report provides an in-depth analysis of SentinelOne' Singularity AI SIEM, contextualized by industry challenges, competitive positioning, and the platform's roadmap for the autonomous SOC. It also aims to educate the market about the current state of SIEM technology and emerging trends.

- SentinelOne's Singularity AI SIEM is not merely an extension of its EDR heritage; it represents a re-architecture of the SOC around automation, usability, and scale. For organizations struggling with SIEM cost pressures, operational inefficiencies, and compliance gaps, this platform offers a compelling alternative to traditional players. SentinelOne's AI SIEM is positioned to unify detection, investigation, and response. Its vision is to transition from human-in-the-loop to an autonomous SOC where AI agents handle most processes while analysts focus on strategic oversight.

- SentinelOne enters the SIEM market against entrenched incumbents such as Splunk, Microsoft Sentinel, Elastic, and Palo Alto Cortex XSIAM. Where Splunk dominates with broad ecosystem integrations but struggles with high ingest costs and operational complexity, SentinelOne positions itself as a cost-predictable, AI-native alternative built on an always-hot data lake. Against Microsoft Sentinel, which benefits from deep cloud integration but often locks customers into the Azure stack, SentinelOne emphasizes openness through OCSF standards, multi-cloud support, and ingestion of competitor EDR data. Versus Palo Alto Networks' Cortex XSIAM, which markets automation at scale, SentinelOne differentiates by embedding Purple AI's natural-language analytics and native hyperautomation directly into the SIEM—avoiding bolt-on SOAR modules or separate licenses. Elastic remains strong among developer-led adopters, but SentinelOne appeals to CISOs by unifying endpoint, identity, and cloud telemetry into a single agent-driven platform with out-of-the-box automation. In short, SentinelOne competes by reframing SIEM as an AI-first, unified, and cost-predictable platform, targeting enterprises that are frustrated with legacy cost structures and operational drag yet unwilling to be locked into a single vendor's ecosystem.

Industry Themes:
The State of the SOC & SIEM in 2025

The Biggest Challenges Facing SOCs Today. Across the industry, SOCs are struggling with several converging pressures:

- **Alert Overload and Context Deficiency:** According to SACR's CISO survey, 53% of respondents cite a lack of contextualized alerts as their primary challenge, closely followed by overwhelming false positives (47%) and integration issues with existing security tools (45%). Alert fatigue, fragmented visibility, and coordination challenges are rampant, with most organizations handling over 4,000 cloud security alerts per month but requiring nearly 7,000 alerts to identify a single true incident.

- **Slow Detection and Response:** The average time to detect a cloud breach is 4–12 days, with 71% of organizations taking at least 1–7 days to even identify an incident. Limited visibility into runtime environments and evolving threats further compound these delays, based on State of AI in Security Operations 2025, report from Prophet AI.

- **Siloed Teams and Fragmented Tooling:** Organizational silos hinder collaboration, especially between SOC, cloud security, and platform teams. This fragmentation leads to blind spots and inefficiencies, with 44% of organizations citing fragmented visibility due to too many separate tools as a major challenge.

- **Resource Constraints and Complexity:** Concerns about performance degradation (28%), resource consumption (23%), and agent sprawl (21%) are significant barriers to implementing effective detection and response solutions in the cloud.

- **Compliance Complexity:** Companies are also facing federal mandates like M2131 that impose strict data retention and visibility demands.

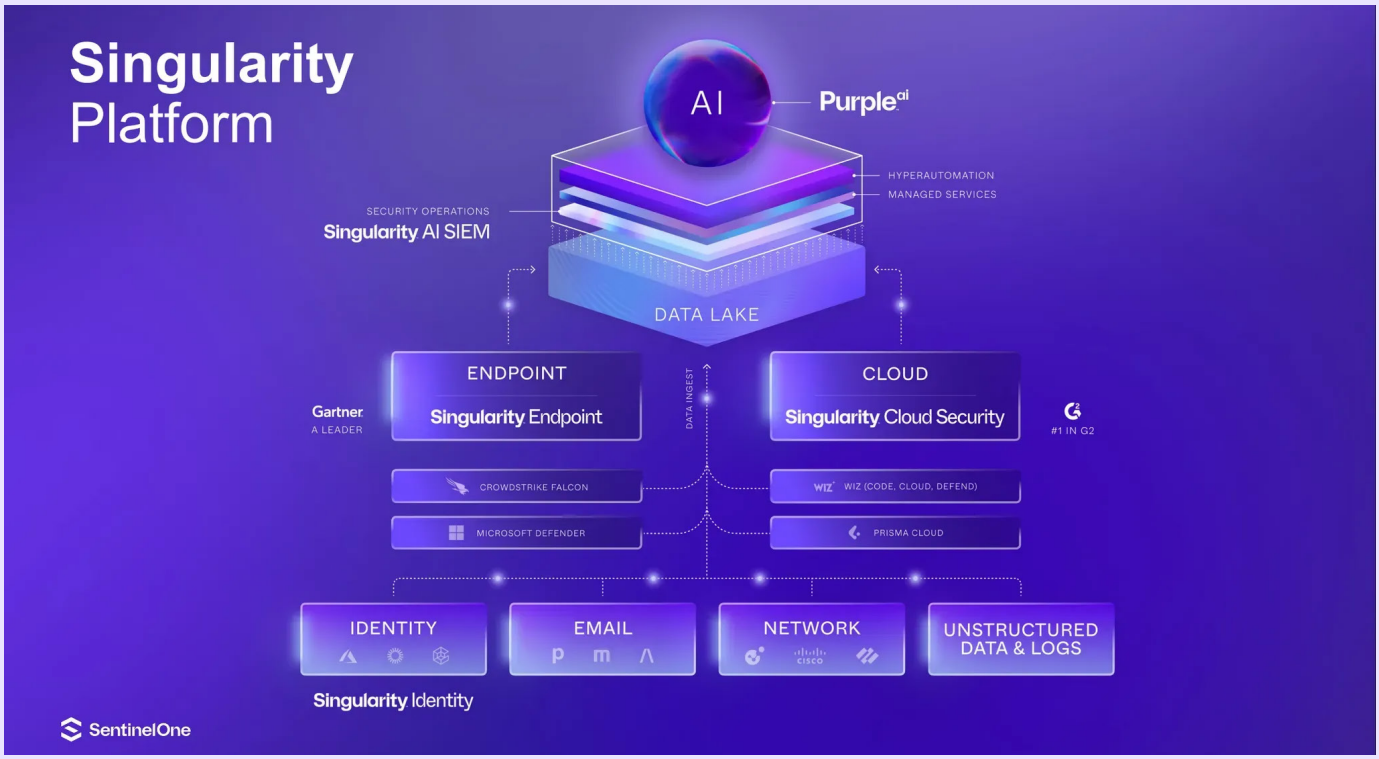
- **The Urgency Around Reinventing the SOC:** Based on research and discussions with top leaders, the traditional SOC model dependent on rule-based detection, manual investigations, and fragmented toolchains is no longer sustainable. As attackers leverage AI to scale their operations, defenders must do the same or risk being outpaced. The gap between what defenders must see and what legacy SIEMs can surface is widening, fueling both alert fatigue and missed threats. The transition to a data-first, AI-driven, and highly automated SOC is now an urgent imperative, not a distant aspiration.

The need for contextual intelligence and integrated automation is now considered essential for effective operations, as traditional systems struggle to keep pace with rising telemetry volumes, complex alerts, and the demand for faster incident response.

SentinelOne's Core Capabilities: The Foundation

History & Context

To better understand SentinelOne's vision for its AI SIEM, it helps to begin where they started.



EDR/XDR Platform Evolution

SentinelOne's reputation was built on its strong EDR capabilities, which remains one of the most mature and widely deployed in the market. SentinelOne was recently named a Gartner® Magic QuadrantTM Leader; this is the fifth-time running where they have been named a Leader by Gartner for their EDR capabilities.

They have earned consistent recognition for their performance in third-party evaluations such as the MITRE ATT&CK Evaluations. The company has demonstrated high detection fidelity, minimal delays in response times, and strong coverage across a wide array of MITRE TTPs (Tactics, Techniques, and Procedures). Their autonomous EDR solution has consistently ranked highly for its ability to detect sophisticated threats without needing continuous tuning, and it performs exceptionally well in visibility, telemetry fidelity, and automated correlation. SentinelOne's proprietary behavioral AI engine allows it to detect novel threats in real time, even in the absence of known signatures, and respond with autonomous containment and rollback capabilities.

SentinelOne's EDR strengths gives them a good opportunity to go after the SIEM opportunity. This level of precision and automation in endpoint telemetry is foundational to the strength of their AI SIEM. Many legacy SIEMs rely on fragmented or noisy data sources, SentinelOne's AI SIEM is directly fueled by high-fidelity data from its EDR sensors. This direct integration means the SIEM ingests more contextual and structured endpoint data from the outset, resulting in better signal-to-noise ratios and faster detection cycles.

Moreover, it enables immediate enrichment for incident investigations without having to rely on third-party enrichment tools. They have deep visibility and AI detection across all MITRE attack mappings. SentinelOne's static AI engine provides robust malware detection and behavioral analytics across endpoints, leveraging agent-based solutions.

The trust SentinelOne has earned through its EDR performance gives it a credible 'right to win' in the SIEM space. By starting from the endpoint—the most critical telemetry source in any security architecture—and extending upwards into log aggregation, natural language investigations (via Purple AI), and autonomous workflows, SentinelOne is not bolting SIEM onto its platform; it's building a SIEM from the ground up with its EDR as the intelligent sensor layer. At the same time, the platform is built to ingest third-party telemetry, including data from other EDR providers, ensuring that adoption is not limited to existing SentinelOne customers. This architectural alignment positions SentinelOne to reframe what SIEM can be in a post-EDR-first, AI-native security era.

SentinelOne Security Data Capabilities

In 2021, they acquired a company called Scalyr which added and brought high-speed log analytics and observability capabilities to ingest more data logs. This acquisition would later become foundational to their ability to build a scalable backend for security data, not just for EDR, but for future SIEM workloads.

At the time, SentinelOne had already built a strong reputation in endpoint detection and response (EDR) but lacked the telemetry ingestion, storage, and query capabilities needed to compete with established SIEM vendors. Scalyr, a high-performance log management and analytics platform, offered exactly a cloud-native, index-free, columnar architecture designed to process massive volumes of structured and unstructured data with sub-second query speeds. This architecture stood in contrast to traditional SIEMs that relied on tiered storage, which introduced latency and limited real-time visibility. We will talk more about this business in later sections of the report.

Cloud Security

SentinelOne expanded their capabilities to protect cloud infrastructure and workloads. Singularity Cloud Workload Security (CWS), delivers real-time threat detection and autonomous response for cloud servers, VMs, containers, and serverless providing runtime protection and EDR-like capabilities for cloud workloads. This meant, for example, that SentinelOne's agent could now be deployed on Linux servers in AWS or pods in a Kubernetes cluster and feed telemetry back to the same central platform as endpoint data. By securing cloud workloads and even some containerized environments, SentinelOne started collecting a broader set of security data. In 2022, SentinelOne launched Singularity Cloud native Security (CNS) that provided customers with agentless cloud posture management, shift-left capabilities and evidenced-backed risk prioritization, adding data on cloud configurations and vulnerabilities as well as developer artifacts to its existing real-time cloud workload telemetry. This growing telemetry footprint across endpoints and cloud workloads laid the groundwork for SentinelOne's Singularity Data Lake and correlation engine.

Identity Protection

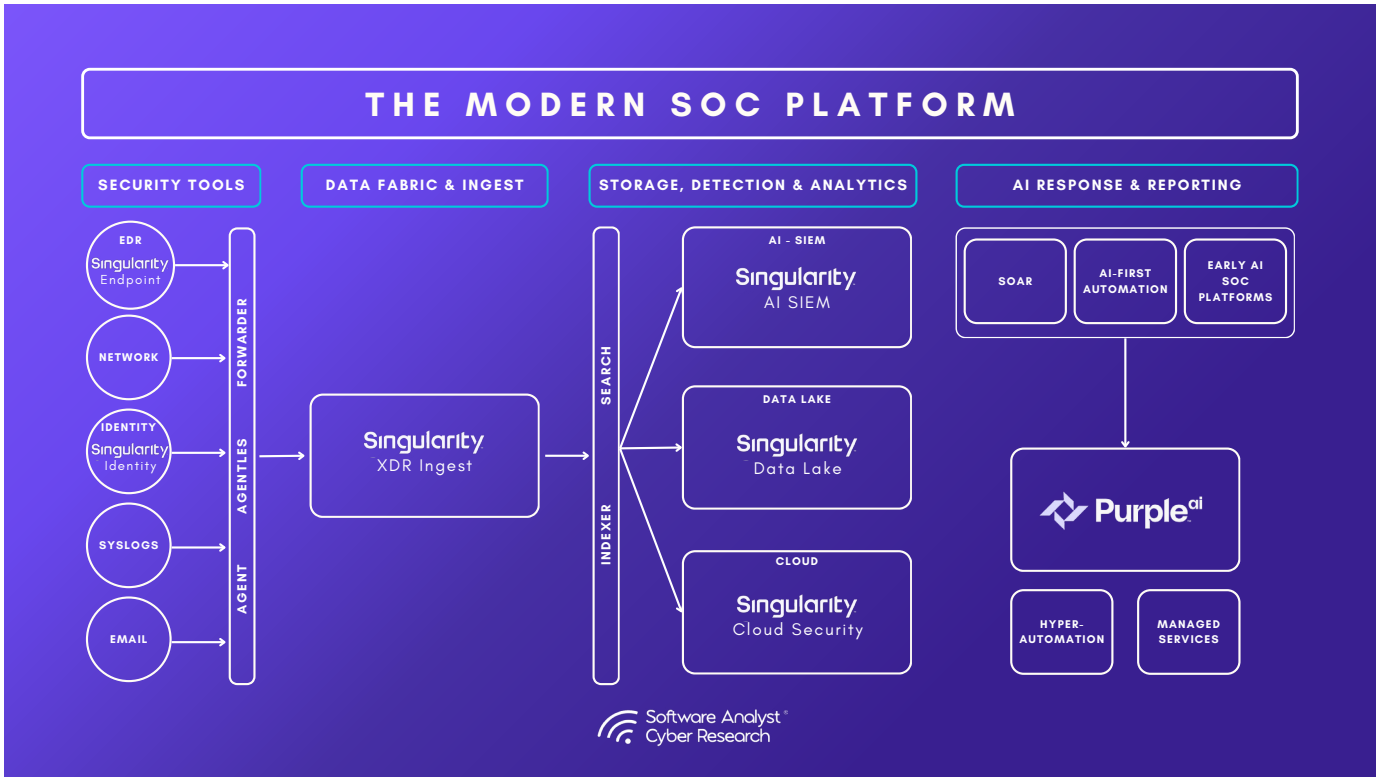
In March 2022, SentinelOne announced a major acquisition of Attivo Networks, an identity security and deception technology company, for over $600M. Attivo specialized in detecting credential theft, Active Directory attacks, and lateral movement by using decoys and analyzing suspicious identity activity. With the acquisition, SentinelOne gained capabilities to monitor and defend the identity layer, an increasingly critical battleground where attackers exploit users, credentials, and misconfigurations to move undetected. (These capabilities were woven into the Singularity Platform, extending protection beyond Active Directory to include cloud identity providers including Entra ID, Okta, Ping, and more. Singularity Identity, which is a part of SentinelOne's unified agent experience, can now continuously monitor identity infrastructures for misconfigurations and risky exposures, detect credential theft and impersonation attempts through deception techniques, and surface compromised credentials found on the dark web. Features also enabled adaptive access controls like MFA re-authentication or session blocking to stop attackers in their tracks. With Attivo's technology integrated, SentinelOne's Singularity Platform could now cover "identity-based threats across endpoint, cloud workloads, IoT, mobile, and data wherever it resides," extending zero-trust principles across the enterprise and unifying on premises and cloud identity protection. This solidified SentinelOne's approach to cover all core surfaces: endpoint, cloud, and identity. That expanded surface area, combined with investments in log analytics and cloud-scale infrastructure, would become the foundation for the SIEM strategy that followed.

SentinelOne Singularity AI SIEM: Present Capabilities and Vision

SentinelOne's Singularity AI SIEM is positioned as a modern, autonomous platform designed to unify data ingestion, detection, investigation, and response. Its vision is to move from human-in-the-loop to an autonomous SOC where AI agents handle most processes and analysts focus on strategic oversight.

The capabilities that follow are not stitched-on modules. They build on the company's existing footprint in endpoint, identity, and cloud telemetry and reflect a cohesive effort to re-architect security operations around scale, usability, and automation.

Core Capabilities of SentinelOne's AI-SIEM



There are a number of capabilities that we believe that are noteworthy for practitioners.

1. Unified Data Ingestion
2. Data Lake Architecture
3. Out-of-the-box unified search and correlation, threat hunting, detections, natural language queries (with Purple AI), Dashboards, and MDR support
4. Built-in AI and Automation capabilities

Impact of the Observo AI acquisition

Recently, SentinelOne announced its intent to acquire Observo AI in one of the company's recent major acquisitions. This acquisition of Observo AI could reshape how SOCs approach data management. The Software Analyst has extensively written about the rise of security data pipelines and how this is evolving the SIEM market. Our report highlighted how many SIEMs vendors have long faced challenges with the massive volume of security data and the rising costs tied to ingestion, enrichment, and storage. By embedding Observo AI's pipeline technology, SentinelOne is moving data processing closer to the source, enabling inline filtering, enrichment, and even detection before logs are routed to a SIEM or data lake. This reduces noise, improves security data quality, eases the burden on analysts, and optimizes infrastructure by ensuring only meaningful data consumes compute and storage resources. At the same time, Observo AI's cold storage model offers a more economical way to retain data for compliance or historical analysis without overloading high-cost systems.

Why ObservoAI?

SentinelOne explained that this acquisition reflected months of rigorous evaluation, extensive customer input, and the same disciplined approach that defines SentinelOne's thorough M&A decisions. ObservoAI outperformed alternatives in months-long technical evaluation, scoring significantly higher than similar platforms.

The evaluation on Observo focused on several key criteria:

- Scalability: ObservoAI was able to demonstrate superior scalability during the evaluation (up to 600MB per query) allowing searches across millions of logs.
- On-premises deployment capabilities: On-premises deployment capabilities are important for SentinelOne's customer base, many of whom operate in regulated industries
- OCSF parsing capabilities: Observo supports OCSF format, which eliminates vendor lock-in by providing an open schema that normalizes event data at the source. An important necessity for enabling interoperability between SIEM, XDR, and data pipeline platforms.

Overall, we see this acquisition as a significant step forward for SentinelOne because it extends the company's platform beyond its AI SIEM boundaries, into a modern security operations platform that addresses the long standing needs of enterprises looking for scalable data handling, seamless integrations, and faster time-to-detection. It positions SentinelOne to compete not only on SIEM capabilities but also on a strong foundational data architecture.

This acquisition is a big win for customers as it addresses the concerns of customers related to:

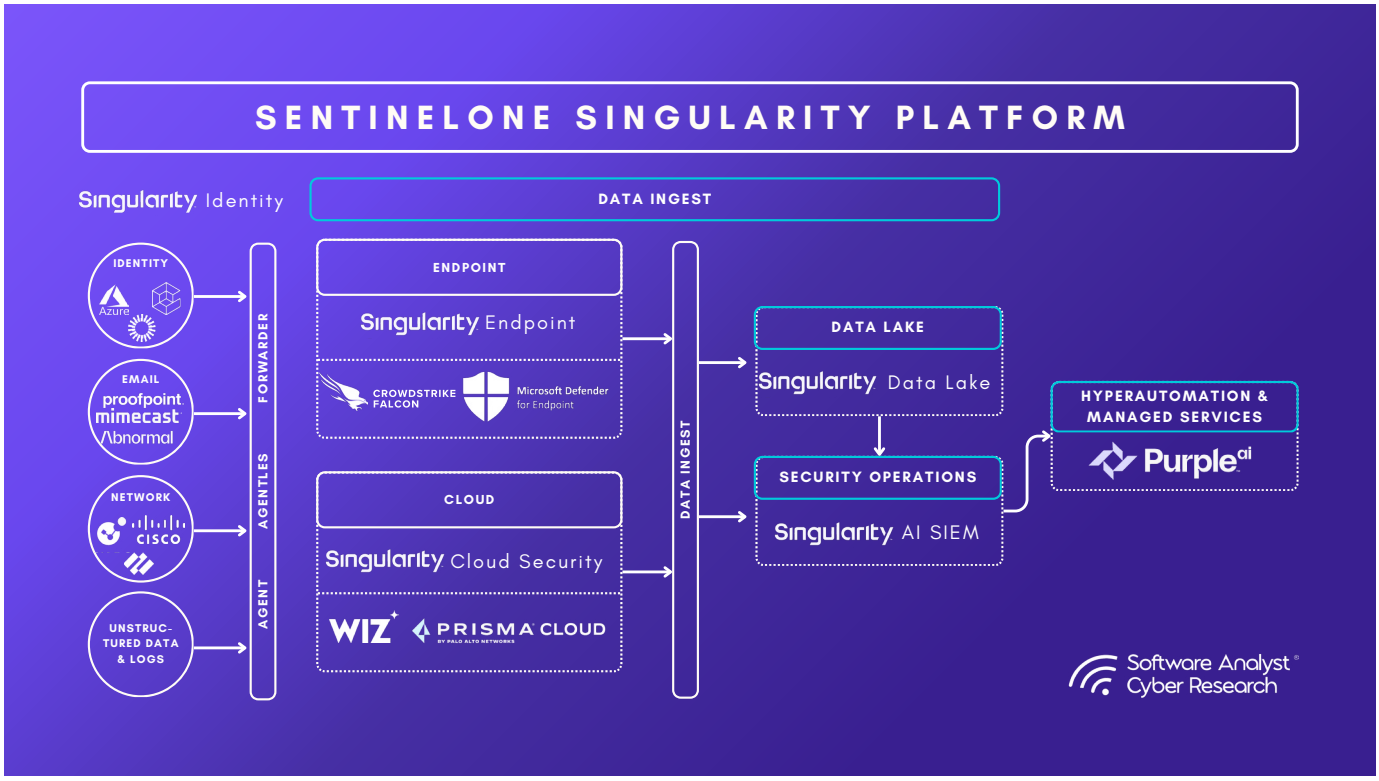
- Better data ingestion and faster data onboarding: AI-powered parser discussed earlier and strong OCSF support simplify normalization and reduce the lift to ingest diverse logs into SentinelOne's data lake.
- Smooth migrations from legacy SIEMs: Smooth migrations from legacy SIEMs: Observo can extract data out of platforms like Splunk and push it into SentinelOne, easing hybrid and migration scenarios.
- Data quality with less noise, lower cost: Better filtering removes duplicative or low-value logs, reducing storage and query noise. Pricing will also reward customers for filtering, based on both initial ingest and post-filter storage.
- Better performance at scale: Customers keep "all data hot" and can run large, fast searches across millions of logs, supported by high query scalability and speed. There is significantly better time to detect threats and cost-efficient storage.

By unifying AI-native parsing, cost-saving log filtering, and seamless legacy SIEM offload into a high-performance, all-hot data lake, Observo AI makes SentinelOne faster to adopt, cheaper to operate, and more effective at scale.

Unified Data Ingestion (Structured/Unstructured, Agent/Agentless)

A foundational feature of any SIEM is the ability to ingest data from diverse sources. Singularity AI SIEM is designed with an "open data fabric" philosophy: it can pull in practically any log or event stream in the environment. There are two primary modes for data ingestion:

- Agent-Based Ingestion: The same SentinelOne agent deployed on endpoints (Windows, Mac, Linux) or cloud workloads can now perform log collection duties in addition to its EDR functions. This is a single unified agent that can tap into OS event logs, application logs, command-line audit data, etc., and forward them to the Singularity Data Lake. The benefit here is deployment simplicity i.e. organizations don't need to install separate log forwarders or collectors on each system (unlike, say, deploying Splunk forwarders or Beats agents in addition to an EDR agent). For example, the SentinelOne agent on a Linux server could collect syslogs or authentication logs and send them up, while simultaneously acting as the endpoint security sensor. This unified agent approach reduces agent bloat and streamlines data collection.
- Agentless / API Ingestion: Singularity AI SIEM also supports agentless ingestion via APIs, cloud-to-cloud connectors, and standard protocols. This is a viable solution for many modern sources (cloud services, SaaS applications, network appliances) where installing an agent is not feasible. This includes logs from sources like Office 365, G Suite, AWS CloudTrail, Microsoft Entra ID, Salesforce, firewall appliances, EDR solutions (even competitors), and more.
- OCSF Support: SentinelOne supports Open Cybersecurity Schema Framework (OCSF), an emerging industry standard schema for security logs. This means as it ingests events, it can normalize them into a common format. For instance, whether the login failure event came from Windows or Okta or a VPN, OCSF helps map it to a unified schema (with fields like actor, action, outcome, etc.). Using OCSF, SentinelOne is easing data integration and correlation across sources; analysts don't have to constantly translate between different log formats.Third-Party Security Tool Ingestion: SentinelOne ingests data from third-party security tools,



even other EDRs to avoid vendor lock-in. This is important since not all endpoints are on SentinelOne, by feeding in data from other EDRs. In practice, setting up these integrations is typically done through provided connectors or by sending logs via syslog/CEF to the platform.

- Security Data Pipeline Partners: Partnerships with data pipeline companies like Cribl, Abstract, and Databahn enhances threat detection, reduces alert noise, and streamlines operations using AI-driven analytics, while offering no-code integration and scalable migration for organizations looking to modernize their security stack. By enabling data filtering before ingestion, the joint solution cuts storage and processing costs while improving detection accuracy. These companies provide standardized feeds ensuring high-quality data inputs for SentinelOne's AI models, positioning the company more competitively in the SIEM market.

Data Lake Architecture

At the heart of the storage and analytics engine for the SIEM is the Singularity Data Lake. This is SentinelOne's schema-free, cloud-native data lake capable of ingesting logs at exabyte scale.

Unlike traditional SIEMs, SentinelOne's data lake eliminates the distinction between "hot" and "cold" storage. All ingested data remains instantly searchable for up to seven years, without requiring rehydration or complex indexing. That means analysts can query months or even years of data, including high-volume sources like endpoint telemetry or DNS logs, with no lag, no tiering, and no tuning.

This is a significant advance over legacy platforms, where predefined indexes and storage tiers often slow down investigations and inflate costs. Buyers value the always-hot architecture because it enables rapid, comprehensive threat hunting without storage delays or budget shocks.

Under the hood, SentinelOne uses a columnar, massively parallel query engine. Queries are distributed across containers, broken into manageable tasks, and aggregated swiftly, enabling real-time investigations without performance tradeoffs. It's this architecture that allows the system to scale to exabyte levels while maintaining fast search response even under load.

The Singularity Data Lake also supports flexible deployment models. Delivered as a cloud-native SaaS, it supports multi-tenant hierarchies (useful for large enterprises or MSPs) and offers compliance-oriented options such as local VPC hosting in regulated regions.

And when paired with Purple AI, SentinelOne's natural language and reasoning engine, the data lake becomes not just fast, but accessible to analysts at every level.

Unified Search, Correlation & Threat-Hunting Powered by Purple AI

SentinelOne's AI SIEM platform brings together structured query support, contextual correlation, and natural language interaction into a unified experience for detection engineering and threat hunting. The system supports standard query languages including KQL and SPL, which helps organizations migrating from legacy platforms such as Splunk or Microsoft Sentinel preserve their existing detection content and workflows. In addition, SentinelOne includes its own high-performance query language, PowerQuery, and overlays these capabilities with Purple AI, a natural language interface that allows analysts to perform searches and investigations without needing to write queries manually. Analysts can pose plain-English questions such as "Show me all PowerShell executions launching MSHTA in the last 24 hours," and Purple AI will automatically translate that into a structured query and execute in an auto-saving investigation notebook. This significantly reduces friction for junior analysts and accelerates response for more experienced users.

SentinelOne also addresses practitioner concerns about delayed threat detection by bringing detection closer to the source - at ingestion. Instead of waiting for detections to occur after index storage, as in traditional SIEM platforms, this faster detection capability sets SentinelOne's AI SIEM apart.

A core differentiator of SentinelOne's approach is its integration of endpoint telemetry through Storyline with traditional log data. Storyline is SentinelOne's process-tracking model that maps the full execution chain of endpoint activity. When this is combined with logs from sources like Windows events, IAM systems, or cloud services, the platform is able to correlate and link related activities into a single, coherent incident. For example, a suspicious process detected on an endpoint may be automatically correlated with a user creation event in Active Directory, with both surfaced as one unified alert. This reduces noise, improves detection accuracy, and lowers the manual effort required for triage.

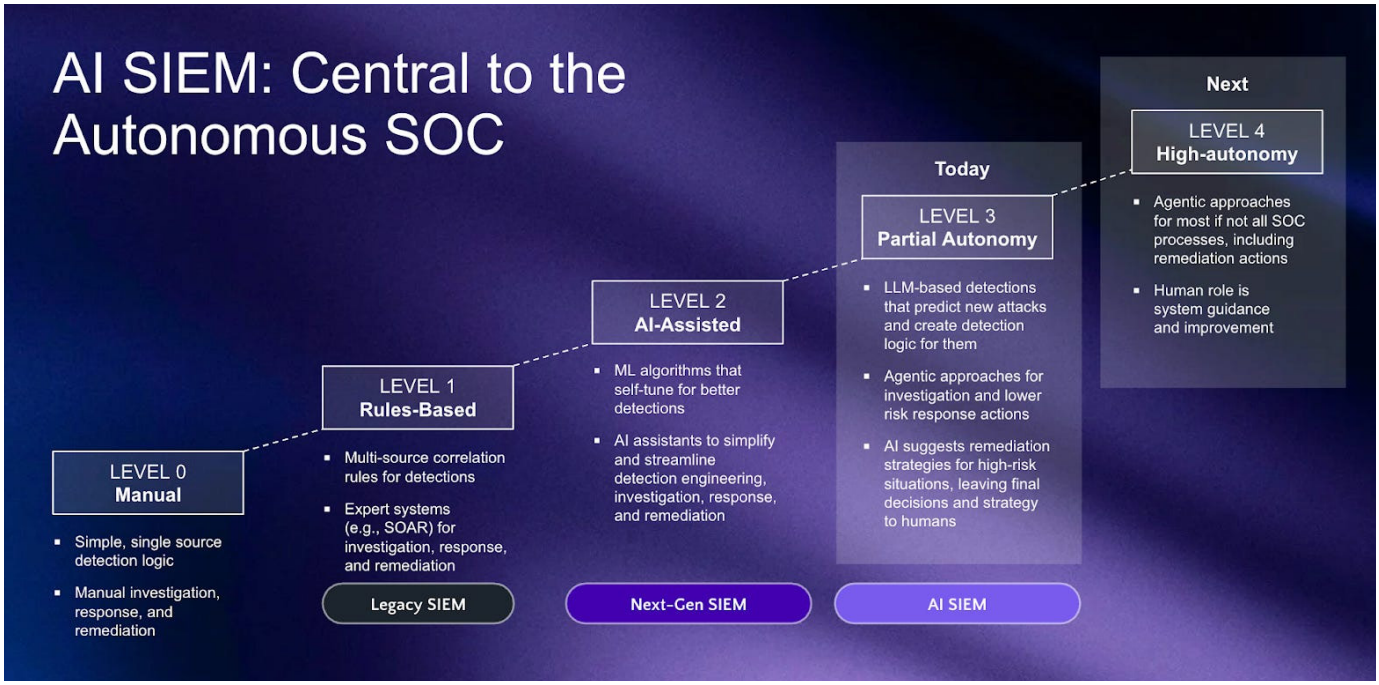
Purple AI plays a central role in investigative workflows. It allows analysts to pivot from one data point to the next through natural language, without requiring them to leave the interface or switch tools. For instance, an analyst investigating a suspicious IP address can ask, "Where else did this IP appear?" or "Retrieve packet capture for this traffic," and Purple AI will execute the necessary queries across both logs and endpoint telemetry. This improves the speed and depth of investigations while keeping the workflow centralized.

The platform also supports flexible rule creation. Analysts can build detection logic through traditional query editors or visual builders, and SentinelOne is developing AI-generated detection capabilities that suggest correlation logic based on observed patterns. These rules follow traditional SIEM constructs such as conditional logic and temporal constraints, but the interface is designed to reduce the technical barrier while still supporting sophisticated detection requirements. These AI-generated rules aim to help teams discover new threats that may not have been covered by static logic.

Overall, SentinelOne's integration of search, correlation, and threat hunting provides a balanced approach that supports both experienced detection engineers and newer SOC analysts. The combination of Storyline telemetry, natural language interaction through Purple AI, and flexible rule creation results in faster investigation cycles and greater detection coverage. The emphasis on accessibility without sacrificing depth reflects a broader trend in the SIEM market toward simplifying operations while enhancing analytic power.

Agentic-AI Capabilities

This is the vision SentinelOne envisions for their SIEM.



Purple AI: Agentic Reasoning and Natural Language Analytics

Purple AI sits at the heart of SentinelOne's AI SIEM, acting as a reasoning engine that can interrogate the platform's always-hot columnar data lake at speed. Analysts type a plain-English question—"Show me every host that fetched recipe.exe in the last 24 hours"—and Purple AI fans the query across every onboarded source (EDR, cloud, identity, firewall, even non-SentinelOne tools) before returning a contextual narrative complete with MITRE mappings and next-step suggestions. The SIEM's massively parallel query architecture keeps these searches interactive, so even complex hunts finish in seconds, unlocking true natural-language threat-hunting, self-documenting notebooks and guided investigations for less-experienced staff.

Every alert that lands in the console is triaged automatically. Purple AI compares each signal against "trillions" of historical datapoints, assigns a confidence score, and labels likely false-positives versus genuine threats; Tier-1 analysts see the verdict immediately, while low-confidence noise can be auto-closed, slashing alert fatigue and mean-time-to-respond. Because the same AI also enriches alerts with threat-intel, vulnerability context and root-cause traces, junior analysts can resolve issues that once required a senior SME.

When action is required, Purple AI hands off to Singularity Hyper-automation: a no-code canvas where the SOC can chain its decisions to any API, blocking traffic in Palo Alto, disabling an Okta user, or opening a ServiceNow ticket, without writing Python. These low-code playbooks are included natively, avoiding the SOAR bolt-ons and extra licensing seen in rival stacks.

Finally, the upcoming agentic innovation will push Purple AI from "assistant" to "agent." It will reach into multiple SIEMs, assemble full cases, decide on containment, execute the response and close the ticket, moving SentinelOne up the autonomy curve from AI-assisted Level 2 to partial autonomy Level 3 for many SOC workflows. In short, Purple AI turns SentinelOne's SIEM into an analyst that can assist, recommend and act, freeing human talent to focus on strategy instead of sifting through noise.

Singularity Hyperautomation

SentinelOne bakes Singularity Hyperautomation directly into its AI SIEM, so response automation sits one click away from every alert rather than in a separate SOAR console. A drag-and-drop canvas lets analysts, no scripting required, chain together playbooks that isolate hosts, disable users, open ServiceNow tickets, or call any REST endpoint. Each block is added visually and the engine can talk to "any API" for truly bespoke actions. During live demos this low-code builder was used to block malicious traffic in Palo Alto firewalls and push a confirmation to Slack the moment Purple AI scored an alert as high-risk. Unlike bolt-on SOARs, Hyperautomation shares the SIEM's data model and licensing: responses are metered in a simple bucket, avoiding per-workflow or seat fees. Customers call the feature critical because it turns investigation outcomes into repeatable, policy-driven actions that slash MTTR and free analysts from repetitive tasks. In short, Hyperautomation closes the loop inside SentinelOne's platform: detect, decide, and remediate, all from the same screen, at the speed of API calls.

SentinelOne AI SIEM is built for openness: it ingests data from any source, including other EDRs, and is OCSF-compatible for normalization and integration. The platform's hierarchical multi-tenancy enables organizations to consolidate disparate SIEMs, while still providing segregated access and reporting as needed. Buyers in complex or federated environments value this flexibility, as it addresses both vendor lock-in concerns and the need to unify fragmented security operations.

Core Differentiators That Matter to Buyers

Based on our discussions, there are core capabilities that really matter to security leaders. SentinelOne positions its AI SIEM around a handful of buyer-centric differentiators that all show up in day-to-day SOC workflows.

Strong Data Ingestion & Parsing Capabilities

The acquisition of Observo AI now embeds strong AI-powered parsing capabilities for SentinelOne's SIEM. Observo used AI-native approach with superior AI-powered parsing capabilities to ensure that only quality security data reaches the SIEM platform, while eliminating noise. Secondly, they now have the ability to perform faster deployment of data sources. ObservoAI also demonstrated that they could quickly onboard data sources, reducing integration friction and accelerating time-to-value for SOC teams relative to other competitors. This will significantly enhance SentinelOne's core offerings to all SIEM customers.

Compliance, On-Prem and Hybrid Support

Security leaders often ask: can the SIEM support our compliance needs and unique deployment constraints (especially in regulated industries or government)?

- **Compliance Reporting and Data Sovereignty:** Singularity AI SIEM includes features for compliance use-cases, such as maintaining required log retention (as per PCI DSS, HIPAA, SOX, GDPR, etc.), ensuring logs are immutable and tamper-evident, and providing pre-built reporting for controls. SentinelOne's materials reference federal mandates like M-21-31 (which is a US government memo mandating certain logging levels and retention for federal agencies). Dashboards are available to demonstrate compliance with such mandates out of the box. Additionally, SentinelOne is certified for FedRAMP for government cloud, ISO 27001, SOC 2 for the service itself) to satisfy auditors that using their cloud SIEM meets regulatory standards. For multinational customers, SentinelOne offers hosting in various regions (e.g., AWS regions worldwide) to meet data residency laws. The hierarchical multi-tenancy feature allows data to be segregated by entities, which can support scenarios like restricting EU data to EU-based personnel under GDPR.
- **On-Premises and Air-Gapped Environments:** Officially, Singularity AI SIEM is delivered as a cloud service. However, some organizations (e.g., defense, critical infrastructure) have environments that are air-gapped or cannot send logs offsite. SentinelOne has not broadly advertised a fully on-prem version of AI SIEM (unlike Splunk which can be entirely on-prem). That said, there are a few possibilities: Enterprise Data Gateway offers a solution for sensitive networks to selectively route data one-way, without introducing ingress concerns. SentinelOne also offers a Virtual Private Cloud deployment (a dedicated instance in a cloud that's logically isolated), or in the future, a customer-managed version of DataSet (since DataSet, the underlying tech, does have an option for on-prem or VPC deployment as it was pitched for observability). For now, most of SentinelOne's SIEM deployments are likely cloud/SaaS. In hybrid scenarios, the agent-based collection can help with connectivity – agents can buffer and send data securely to the cloud SIEM, even if sources are on-prem. For extremely sensitive pockets, one approach some SentinelOne customers can use is forwarding only metadata or alerts to the cloud while keeping raw logs on-prem. SentinelOne's open integration (like support for syslog output or its own APIs) means an organization could forward alerts from the AI SIEM to an on-prem system if needed for record-keeping. Also, the mention of multi-SIEM unified alerts indicates SentinelOne anticipates some customers will run it alongside other SIEMs, possibly keeping legacy systems for local requirements but using SentinelOne to aggregate and enhance with AI.

Pricing Model

SentinelOne addresses a recurring pain point with legacy SIEMs by implementing a usage-based pricing model that charges based on average monthly ingest and query load rather than peak data volumes. This approach eliminates unpredictable consumption-based pricing that traditionally penalizes peak ingestion and leads to cost overruns. By removing “cost surprises,” organizations can ingest more data without forcing log filtering to stay under license caps. The unified agent model, which handles both EDR and log collection through a single deployment, further simplifies licensing. Combined with always-hot storage, this delivers both cost predictability and operational simplicity, factors repeatedly cited by buyers as decisive considerations in SIEM selection and migration decisions.

Cost surprises are tackled next: pricing is consumption-based, calculated on average monthly utilisation and query volume rather than peak ingest, so budgets track reality and not worst-case spikes. Even Hyperautomation actions draw from a simple “response bucket,” avoiding the seat- or playbook-based charges that plague stand-alone SOAR tools.

Deployment

They deliver the platform as a multi-tenant SaaS (hosted in public cloud with regional options). They support hierarchical multi-tenancy for large orgs or MSPs. They have an open ecosystem: integrations via REST APIs and support for industry schemas with out-of-the-box compliance dashboards and reporting (e.g. for regulatory frameworks).

Retention Capabilities:

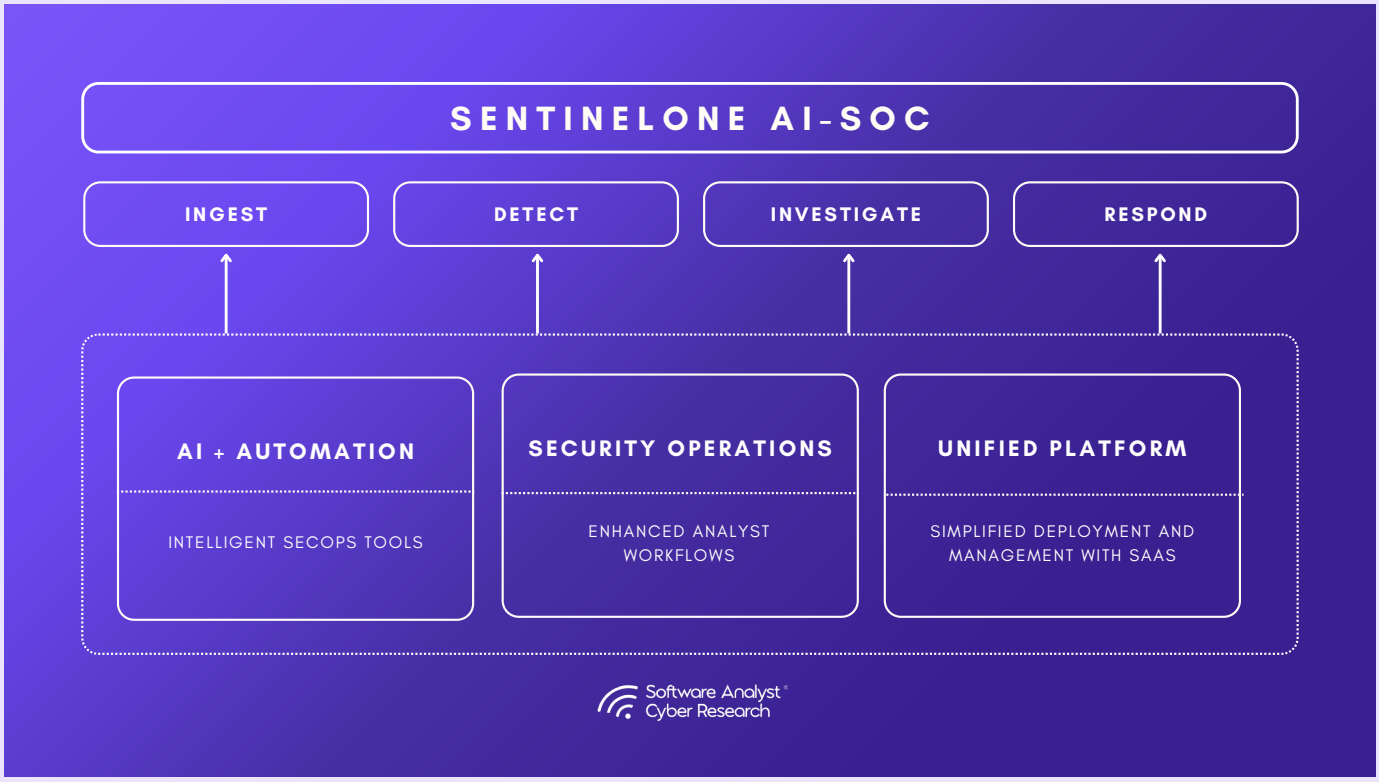
SentinelOne retains logs in an always-hot state for up to seven years. This eliminates rehydration delays and enables instant search across full-fidelity data, even for long-term investigations. Buyers value this because it allows real-time visibility without the traditional tiering or performance tradeoffs seen in legacy tools.

Open Ecosystem

An open ecosystem underpins the data strategy. OCSF-compatible pipelines let teams ingest and normalize telemetry from virtually any vendor, including rival EDRs, while partnerships with Cribl and others add routing flexibility. Collection can be agent-based or agentless. Yet where an agent is required, the single SentinelOne agent handles both protection and log capture across Windows, macOS, Linux, and cloud workloads, eliminating the "fleet-within-a-fleet" problem of running parallel collectors.

Response Mechanism

Response is native, too. Singularity Hyperautomation's drag-and-drop canvas turns any alert or Purple AI verdict into a playbook that can isolate a host, disable a user, or call out to any REST API without writing code. Live demos routinely show a Purple-scored high-risk alert triggering a Palo Alto block and Slack notification in seconds.



Summary

Finally, all of this sits in a single console that unifies EDR, XDR, and SIEM views, so analysts never context-switch while moving from endpoint telemetry to log analytics or automated response. Customers highlight the zero-training ramp and faster investigations that come from keeping everything in one place, a fit that resonates most with mid- to large-size enterprises looking to modernize away from legacy SIEMs or consolidate multiple security tools into a unified, AI-driven platform.

The Road Ahead: SentinelOne AI-SIEM Roadmap

Autonomous SOC and Agentic AI

- Agentic Innovations in Purple AI: SentinelOne's multi-phase landmark release will transform Purple AI from assistant to an autonomous agent, capable of conducting end-to-end investigations without human intervention. This advancement will enable cross-SIEM case resolution, automated threat hunting, and complete incident response workflows, pushing security operations from AI-assisted (Level 2) to partial autonomy (Level 3) for routine SOC tasks.
- Hyperautomation Evolution: Building on its current no-code canvas, Singularity Hyperautomation will expand to support seamless integration with any REST API and enable sophisticated custom action chains without coding requirements. This evolution will transform the platform's response capabilities from guided to fully autonomous, drastically reducing MTTR while maintaining human oversight for critical decisions.
- Content and Intelligence Expansion: SentinelOne will continuously enhance its detection library, compliance dashboards, and integration ecosystem to achieve feature parity with legacy vendors while maintaining its architectural advantages. The roadmap includes AI-native threat intelligence correlation and cross-domain behavioral detection spanning cloud, identity, and endpoint security.
- This strategic roadmap positions SentinelOne's AI SIEM as not merely a modernized SIEM but as the foundation for tomorrow's autonomous security operations center, where human analysts focus on strategy and oversight while AI handles the detection, investigation, and response lifecycle.

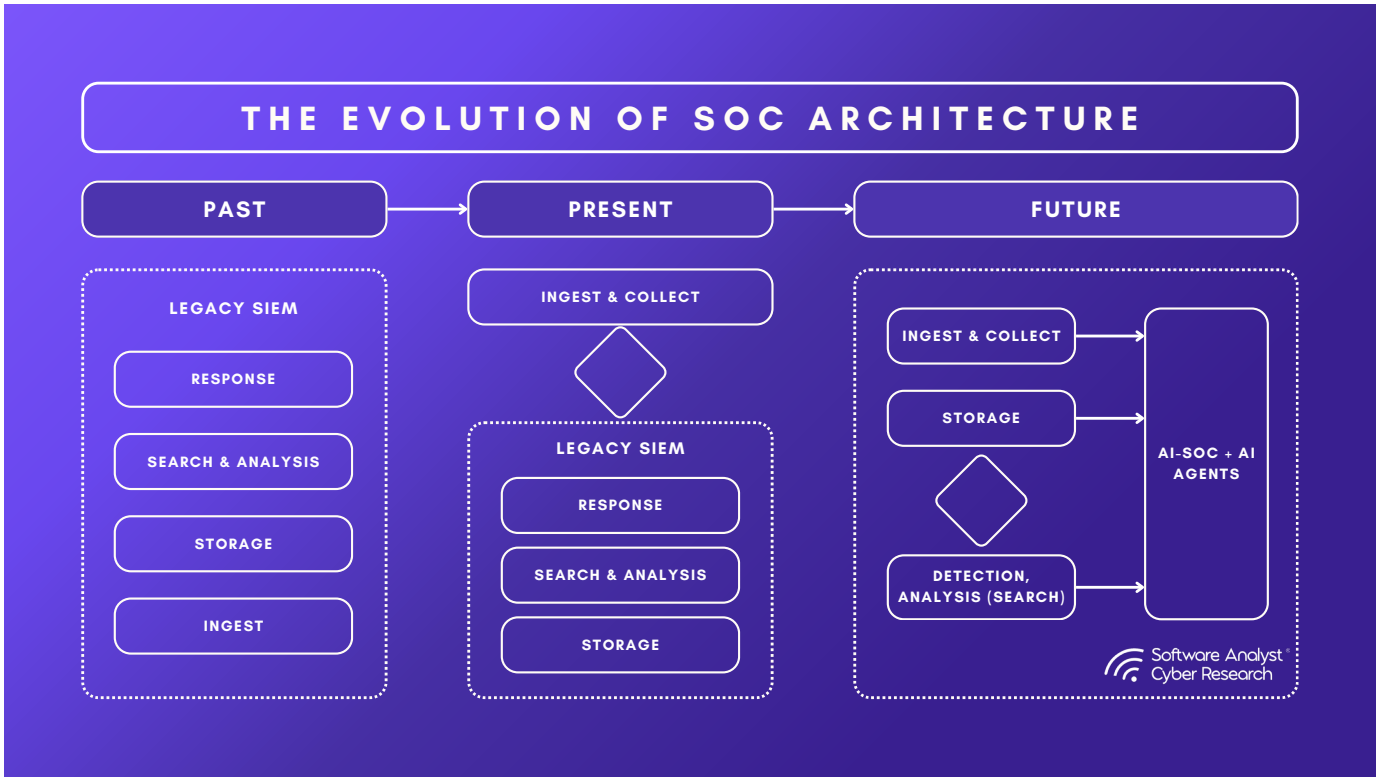
The Future SIEM: Federated AI SOC

In the past, organizations were locked into monolithic SIEMs like Splunk, whose byte-based ingest model became an Achilles' heel as cloud telemetry volumes soared, every gigabyte hitting Splunk's indexers drove license costs into the hundreds of thousands or even millions per year, forcing engineers to aggressively prune or discard data just to stay solvent.

Today, many SOCs have inserted a neutral ingestion tier with solutions like Observo's data pipeline to decouple collection from analysis: verbose logs are compressed, duplicates and low-value fields are dropped, high-value alerts still flow into Splunk, and bulk telemetry lands in cheaper lakes or warehouses, often cutting overall ingest by over 50 percent without rewriting dashboards or pipelines.

The SIEM of the past is now transforming into a Federated AI-SOC model. The future vision pushes this decoupling further, treating ingest, storage and detection as discrete, optimizable layers feeding an AI SOC control plane and autonomous AI agents capable of proactive investigations and remediation. Customers now want "Federated AI-SOC" capabilities, as customers won't always be able to ingest all the data into their SIEM, but will want to have security value such as hyper automation and AI on top of data which reside in other places.

Overall, SentinelOne's Singularity platform embodies this next-generation architecture by streaming its endpoint-derived telemetry into an always-hot, columnar data lake, applying Purple AI for natural-language threat hunting and correlation, and then using hyperautomation and agentic AI to close the loop on response; all within a single unified console that scales to massive data volumes and shifts repetitive triage from humans to intelligent co-pilots.



Final Conclusions & Key Summary

As the SIEM market undergoes one of its most significant shifts since its inception, three signals stand out:

- **Open Architecture and Ecosystem Integration:** SentinelOne's strategic commitment to open standards (OCSF) and API-first design aligns with the broader industry movement away from closed ecosystems. In an environment where 76% of enterprises operate across multiple cloud platforms, security teams are demanding more flexibility and less lock-in. SentinelOne's ability to ingest and normalize telemetry from virtually any vendor reflects that demand and helps unify a tooling landscape that has long been fragmented.

- **AI-Human Augmentation:** The evolution toward AI-augmented security operations represents the most significant market shift since cloud migration. SentinelOne's Purple AI and agentic reasoning capabilities position it at the forefront of this transition, addressing the 34% year-over-year increase in alert volumes that has overwhelmed traditional SOCs. By enabling analysts to interact with security data through natural language, SentinelOne is democratizing threat hunting capabilities previously limited to specialized teams.

- **Unified Data Platform Strategy:** Industry analysts project that by 2027, organizations with unified security data platforms will detect threats 70% faster than those with siloed tools. SentinelOne's data-first approach, consolidating EDR, XDR, and SIEM functions around a single high-performance data lake, directly addresses this trend while reducing the operational complexity that drives 82% of security breaches resulting from human error.

Software Analyst®
Cyber Research

business

personal

softwareanalyst.io

SACR®

Trusted research. Sharp insights. Real conversation.

CISO	VENDOR
SECURITY TEAMS	INVESTORS