

E-BOOK

8 reasons why you need Sumo Logic for your SIEM

Before you choose a SIEM, see how Sumo Logic can help you secure your cloud journey, match the changing attack surface, and bring innovation back to your SOC.



Undoubtedly, security information and event management (SIEM) solutions are an essential part of an organization's security operations strategy. In fact, visibility into applications and data assets, as well as effective use of analytics rank at the top as factors that improve enterprise cyber resilience.¹

Getting the most out of your SIEM means adopting a solution that has the right balance of capabilities that deliver the scalability and threat analytics power to provide you with actionable security insights, without the complexity and resource constraints that are inherent in legacy SIEM solutions.

With a modern approach to security operations, Sumo Logic strikes that balance. Here are 8 reasons to consider Sumo Logic in your SIEM evaluation short list:

#1: Cloud-native architecture

There is so much that a SIEM must do to be effective, so, as a starting point, it's important to make a firm decision on the solution's architecture to ensure it can scale to meet the demands that will be put on it. That decision should be laser-focused on selecting a cloud-native solution.

Built in the cloud, our platform provides a low total cost of ownership and endless scalability as the types, quantities, and sources of your organization's data grows. Sumo Logic's platform provides the dynamic scaling and elasticity you need; it can ingest petabytes of data a day giving you end-to-end visibility of your security and compliance posture at all times. With its cloud-native scalability, Sumo Logic enables you to ingest data from any and all of your sources and to query however much data you want, at any time you need.

#2: Quickly identify IOCs and gain automated insights

Attackers can gain access to your data and environment from any unsuspecting avenue. Sumo Logic provides a comprehensive approach to quickly uncover activity that can indicate an early stage attack by identifying spikes and anomalies based on your organization's baseline of historical data.

Unrestricted by the processing power of on-premises hardware, the cloud-native solution automates your alert triage process and efficiently analyzes all records in order to surface Insights for your analysts to immediately investigate. Insights dramatically decrease validation and investigation times by presenting an automatically generated storyline of potential security incidents containing all of the relevant information your analysts need to make rapid response decisions.

#3: Serves as a single platform that unifies teams and consolidates tools

Sumo Logic helps you mitigate the overload of tools by allowing you to use a single platform that analyzes and correlates data across your on-premises, cloud, and multi-cloud environments. Serving your many security requirements, the platform provides comprehensive capabilities to meet your needs for log management, metrics, SIEM, endpoint detection and response (EDR), network detection and response (NDR), threat intelligence, and alert triage.

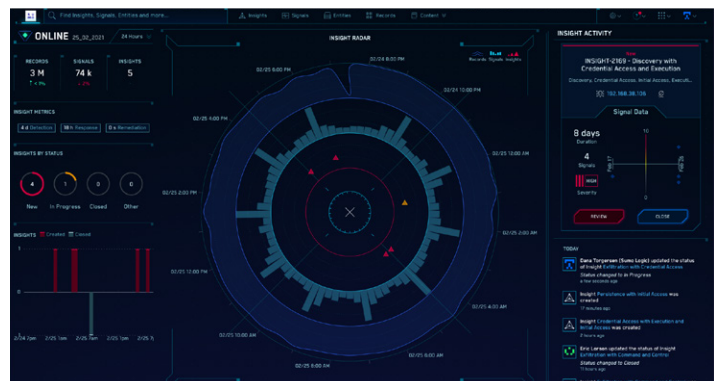


In addition, Sumo Logic enables you to unify your development and security staff with a solution that makes it easy for users to work together from the same consistent and trusted data set, without incurring additional per user licensing fees.

#4: Powerful and simple user interfaces that streamlines your workflows

Legacy SIEM solutions have often had a reputation as being significantly complex and only usable by security staff with advanced training. With our unparalleled ease of use, Sumo Logic alleviates this challenge.

Everything in the solution's user interface and workflow is designed for simplicity and ease of use by your security analysts. Sumo Logic makes it fast and easy to gain deep security insights and achieve continuous compliance with pre-built applications, pre-built dashboards and queries, native integrations, and focused SecOps workflows. Sumo Logic helps streamline your investigation, threat hunting, response, and remediation processes, requiring less time and resources. Sumo Logic's LogReduce™ and LogCompare machine learning algorithms also help incident investigators to rapidly distill context while querying across large data volumes. Insight management enables collaboration across your entire SOC team.





#5: Native coverage for multi-cloud and on-premises environments

Sumo Logic provides full coverage for your infrastructure, offering the flexibility to support any future infrastructure changes you make as you continue your digital transformation initiatives.

Our cloud-native platform provides a convergence of data sources, collecting millions of logs and security-relevant data from cloud, on-premises, and hybrid architectures. And, as a cloud-native solution, Sumo Logic provides complete coverage for your public, hybrid, and multi-cloud environments with security monitoring that unifies your security analytics and investigations across AWS, Azure, and GCP.

Simplifies the data collection process with turnkey integrations that can be activated by an API key and readily supports creating custom correlations across your data sources.

#6: Easy-to-use with fast time-to-value

Digital transformation has made corporate infrastructures incredibly dynamic and continuously evolving. As a result, content development for your SIEM use cases must be simple and effective.

As a cloud-native solution, Sumo Logic provides fast startup and simple, intuitive management that allows your SOC team to experience value in days. The solution easily integrates across your systems and features hundreds of apps that provide pre-built dashboards, queries, and alerts, such as content for your cloud and on-premises security, PCI and other compliance requirements.

Sumo Logic easily supports custom rule creation to help you develop new use cases, over time, that address your organization's specific needs. In addition, the platform makes it easy to train and onboard users by providing online and onsite certification courses, high-quality product documentation, and an intuitive user interface with built-in help tips.

#7: Architected using security best practices

Entrusting your data to a third-party service provider requires rigorous security measures, so taking your SIEM to the cloud means it must apply airtight security best practices.

Sumo Logic's strong commitment to data security is validated by our platform's third-party compliance attestations and certifications, including PCI DSS 3.2.1 Service Provider Level 1 attestation of compliance, SOC 2 Type 2 Audit Report, HIPAA Security Rule Attestation of Compliance, ISO 27001 Certification, FedRAMP Authorization (moderate impact level), and CSA STAR Level 2 Certification.

#8: High ROI with cloud-friendly licensing model

Your SIEM solution should be a long-term investment, so it's important to consider the upfront and on-going costs as part of your selection decision. Sumo Logic provides a cost effective licensing model that fits your budget.

Our credits and data tiers-based licensing model provides economic flexibility for your cloud security needs by aligning your log monitoring and analytics requirements to the value of your data. You can segment your data with multiple tiers:

- Continuous analytics analyzes mission-critical data that you need to monitor, dashboard, and alert.
- Frequent analytics is optimized for high usage, ad-hoc data analysis, allowing you to focus on data searches and visualization.
- Infrequent analytics is optimized for your low usage, ad-hoc analysis of data sets—perfect for audit and compliance use cases.

Summary

Security analysts have a critical role in securing the organization. Selecting a modern SIEM solution that combines powerful analytics with cloud scalability, automation, and ease of use throughout will provide your organization with a good fit today and into the future.

Sumo Logic is focused on delivering analysts with the insights they need to secure their cloud journey, match the changing attack surface, and bring innovation back to their SOC. Our cloud-native SIEM is the perfect solution for the modern SOC.

Learn more

To learn how Sumo Logic's SIEM solution can modernize your SOC, visit: www.sumologic.com/solutions/cloud-siem-enterprise/

1 Ponemon. Cyber Resilient Organization Report. 2020.

SIEM requirements	Sumo Logic	Other SIEM solutions
Real-time visibility across an organization's cloud, multi-cloud, and on-premises environment.	✓	✗ Lack visibility that supports an organization's complete infrastructure investments (cloud, multi-cloud, and on-premises environment).
Cloud-native architecture that provides an API-driven approach that simplifies integrations from all data sources.	✓	✗ Don't support breadth of native integrations and require extensive time to set up and administer.
Clear, purpose-built user interfaces and workflows designed for simplicity and ease of use by your entire security team to solve a wide range of use cases.	✓	✗ Significantly complex and only usable by security staff with advanced training.
Analytics and automation that reduce alert funnel from millions of security records down to a handful of manageable insights to accelerate & streamline investigations to find the "needle in a haystack"	✓	✗ Inundated with too many security alerts that create fatigue and limit ability to uncover critical IOCs.

s

u

Continuous Intelligence Platform™

m

o



sumo logic

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
855 Main Street, Redwood City, CA 94603

www.sumologic.com