sumo logic

SOLUTIONS BRIEF

Cloud SIEM

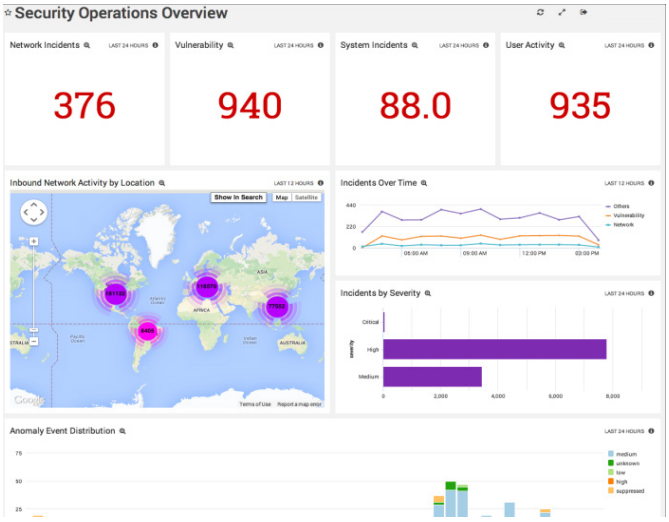
Cloud SIEM for the hybrid, multi-cloud, and microservices for the modern IT

Sumo Logic Cloud SIEM provides threat detection and incident response for modern IT environments such as hybrid, multi-cloud, and microservices. Whether you're looking for your first cloud SIEM, replacing your legacy SIEM, looking for an add-on solution to monitor cloud workloads, or seeking to consolidate your SIEM tools, Sumo Logic is the leading solution in the market.

Product Overview

Sumo Logic Cloud SIEM is built from the ground-up to detect and respond to threats in real-time for hybrid and multi-cloud environments. Customers love Sumo Logic for its rapid deployment, quick time-to-value, ease-of-use, and unified data model which consolidates many IT tools into Sumo Logic.
We have more than a thousand customers that rely on Sumo Logic Cloud SIEM for their day-to-day security operations. Unique multi-tenant architecture provides elastic scale and performance, as well as security insights across customers, delivering Cloud SIEM as a service. No hardware, software, facilities, capacity planning issues, long term contracts, or massive capital expenditure involved.

- Sumo Logic is built on a secure cloud platform with a robust portfolio of security and compliance certifications including SOC2.0, FedRAMP Ready, PCI DSS, HIPAA, masking, and encryption at rest and in motion.
- Our architecture supports security monitoring of cloud deployments, hybrid IT, modern application architecture, and DevSecOps environments.
- Sumo Logic leverages advanced machine learning algorithms to accelerate threat detection and investigation at cloud scale.



Cloud SIEM

Sumo Logic Cloud SIEM delivers a unified view of all security events for managing alerts, running analytics for rapid detection of threats, deep forensic investigation, and quick incident response. Our focus is on environments that are evolving towards the modern IT and cloud transformation.
Sumo Logic is perfectly suited to be a cloud-native security solution that can help you secure your cloud journey, whether you need to monitor old IT before transition, or modern IT during and after cloud transformation.

Rapid detection of threats based on the correlation

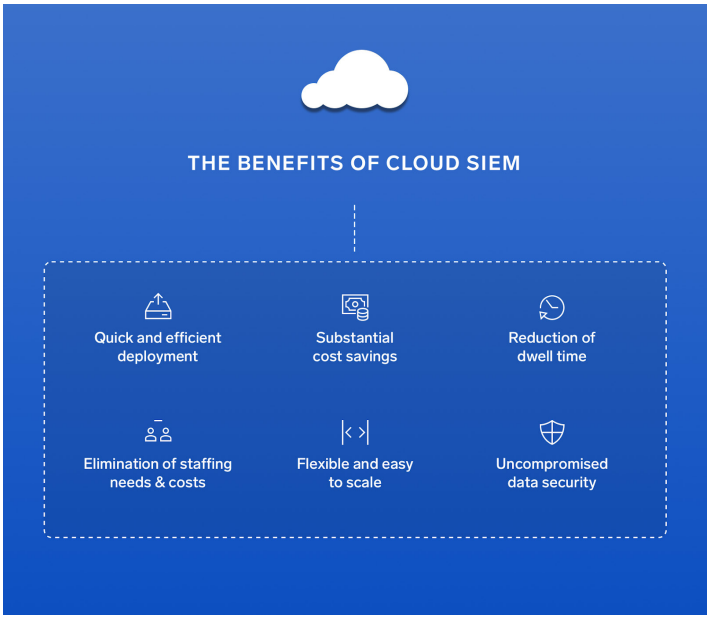
Cloud SIEM has built-in correlation based on our comprehensive query functionality that includes a rich family of operators, our search query language, ability to create templates, as well as a number of advanced machine learning algorithms such as LogReduce, LogCompare, Outlier detection, and many more. Subqueries let users create sophisticated correlation rules easily deploying custom security use cases with no domain expertise needed.

You can build your own library of saved searches which are analogous to correlation rules to implement security use cases such as user behavior analytics, incident management, IoT security orchestration, privileged access monitoring, etc. Saved searches can then be run regularly to detect threats in near-real time.

Built-in security content for quick time to value

The Sumo Logic marketplace has hundreds of apps that come with pre-built dashboards, queries, and alerts. For security use cases, we have over 40 apps, that are critical to our customers.
These apps when installed and connected with your infrastructure, Sumo Logic collects, analyzes, and shows visuals on your data. You can also configure alerts based on your priorities to send real-time emails that you can use to start incident response

immediately or send it to ticketing systems to trigger incident response workflow. Our customers create search queries for their custom apps/devices to create dashboards. You can also create alerts from these searches to trigger incident response workflows.



Build and run cloud-based SOC

Sumo Logic Cloud SIEM enables companies small or large, such as Genesys and Anheuser Busch, to build and maintain their SOC. In fact, Sumo Logic does a better job delivering SOC natively from the cloud. For instance, Anheuser Busch, the largest beer manufacturing company in the world, has built its SOC with Sumo Logic Cloud SIEM. The CISO of Anheuser says that we have established a culture of collaboration through our cloud security intelligence platform between their NOC and SOC. Genesys, one of the largest call center technology companies, uses Cloud SIEM as their SOC platform and they have built a new SOC-less operations that has no physical centralized place, but a virtual, distributed, security operations.

Elastic scalability when you need it the most

Legacy networking and security tools were not built to handle the abnormal increase in the volume of alerts and events to handle when there is an attack or a threat. Due to their finite resources, the efficacy of these devices and storage solutions is quickly broken down by the elastic, unpredictable, and highly dynamic nature of cloud environments. This makes the on-prem or single-tenant cloud solution not useful when you need it the most. Sumo Logic is born in the cloud to provide organizations with the same benefits they expect to achieve as they move to the cloud -- flexibility, scalability, and agility as the types, quantities, and sources of data continue to increase. We have seen customers go from 1TB/day to 70TB/day and back to 1TB/day in a matter of few hours without any capacity planning or breaking the infrastructure.

About Sumo Logic

Sumo Logic is a secure, cloud-native, Continuous Intelligence Platform for DevSecOps delivering real-time, continuous intelligence from structured, semi-structured and unstructured data across the entire application lifecycle and stack.
More than 2,000 customers around the globe rely on Sumo Logic for the intelligence to build, run and secure their modern applications and cloud infrastructures. Only Sumo Logic delivers its platform based on a true, multi-tenant, SaaS architecture, enabling digital businesses to thrive in the Intelligence Economy.

Founded in 2010, Sumo Logic is a privately held company based in Redwood City, Calif. and is backed by Accel Partners, Battery Ventures, DFJ Growth, Franklin Templeton, Greylock Partners, IVP, Sapphire Ventures, Sequoia Capital, Sutter Hill Ventures and Tiger Global Management. For more information, visit www.sumologic.com.

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

www.sumologic.com