sumo logic | Continuous Intelligence Platform™

SOLUTIONS BRIEF

Cloud Security Monitoring & Analytics

Stay ahead of your changing attack surface by surfacing deep security insights

Built in the cloud for the cloud, Sumo Logic alleviates the challenges of security monitoring for your cloud and multi-cloud infrastructure.

Product overview

Sumo Logic's security analytics solution provides cloud security monitoring and analytics that is built from the ground-up to detect and respond to threats in real-time. With Sumo Logic, organizations gain quick time-to-value, ease-of-use, and a low total cost of ownership. Built in the cloud, our elastic scaling platform makes it fast and easy to gain deep security insights and increase security posture with pre-built applications and full coverage of your cloud infrastructure. Our automated cloud security monitoring and analytics platform provides the flexibility to manage all your data analysis use cases from a single, unified view.

Capabilities

Full cloud coverage

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.

Rapid threat detection

Sumo Logic applies advanced machine learning algorithms to accelerate threat detection and investigation at cloud scale. Our solution quickly uncovers activity that can indicate an early-stage attack by identifying spikes or anomalies based on the organization's baseline of historical data. You can also build a library of saved correlation rules to implement security use cases, such as incident management, IoT security orchestration, and privileged access monitoring.

Extensive log data retention

Sumo Logic provides a cost effective, efficient solution for collecting and analyzing log and event data, including insights into network traffic, user activity, suspicious access, configuration changes, and more.

Benefits

Full cloud coverage
Provides complete cloud coverage to unify your security analytics and investigations across AWS, Azure, and GCP.

Deep security insights
Provides deep security insights with integrated threat intelligence correlation and deep search-based investigation along with the solution's rich data visualization.

Ease of use and low total cost of ownership
Our cloud-native, elastic scaling solution and cloud licensing model provide unparalleled ease of use and low total cost of ownership.

Flexible and easy to extend
Our platform provides extensibility of your existing security investments and the option to automate your SecOps workflows with Sumo Logic Cloud SIEM.

Built with security-first principle

Our strong commitment to data security is validated by the 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, and CSA STAR Level 2 Certification.

Granular visibility

Sumo Logic offers a unified view of all security events for managing your security posture, including running analytics for rapid detection of threats, deep forensic investigation, and quick incident response.

Scalable SaaS delivery model

Sumo Logic is built in the cloud to provide a low total cost of ownership and scalability as the types, quantities, and sources of your organization's data continues to grow. Sumo Logic's elastic scaling can ingest petabytes of data a day giving you end-to-end visibility of your security and compliance posture at all times.

Controlled, secure data access with unlimited seats

Sumo Logic provides unlimited seats making it easy to provide your security and compliance users with real-time access, without worrying about licensing limits. Sumo Logic's role-based access control enables your organization to set per-user permissions based on filters that your organization defines. This allows you to enforce access based on the different duties within your organization.

Extensibility that supports your needs

Whether your primary goal is to gain security insights or demonstrate compliance, our platform easily tailors to your needs. And Sumo Logic makes it easy to automate your security operations workflows with the option to adopt Sumo Logic Cloud SIEM when ready.

Quick start AWS security monitoring

Automatically implement best practice configurations for your AWS security monitoring—in minutes. Our AWS Security Quick Start app helps you get started, instantly, with best practice configurations for the security monitoring of your AWS services, as well as Sumo Logic apps designed for AWS Security.

Cost effective licensing that fits your budget

Our data tiers licensing model provides economic flexibility for your cloud security monitoring needs by aligning your log monitoring and analytics needs 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.

About Sumo Logic

Sumo Logic Inc., (NSDQ: SUMO) is the pioneer in continuous intelligence, a new category of software, which enables organizations of all sizes to address the data challenges and opportunities presented by digital transformation, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform™ automates the collection, ingestion, and analysis of application, infrastructure, security, and IoT data to derive actionable insights within seconds. More than 2,100 customers around the world rely on Sumo Logic to build, run, and secure their modern applications and cloud infrastructures. Only Sumo Logic delivers its platform as a true, multi-tenant SaaS architecture, across multiple use-cases, enabling businesses to thrive in the Intelligence Economy. 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