sumo logic

Cloud Infrastructure Security for AWS

Securing your AWS cloud infrastructure with AWS-native services and Sumo Logic security analytics

Sumo Logic Cloud Infrastructure Security delivers immediate visibility across your entire AWS infrastructure, enabling DevSecOps teams to seamlessly manage your cloud attack surface — in minutes.

Product overview

Modern fast-moving cloud environments need ongoing audits of configurations, vulnerability assessment, versioning, access and change analysis, and other activity monitoring to ensure they are well maintained and not subject to risks created by aging or drifting configuration, access rights, or software. Sumo Logic Cloud Infrastructure Security for AWS helps teams gain ongoing security visibility into the diverse aspects of their environment and provides customizable alerting, evaluation, and remediation of issues. Sumo Logic's rapid onboarding process makes setup easy, allowing AWS users to add the crucial single-pane-of-glass necessary for efficient risk and threat monitoring, detection, and response in under 15 minutes.

Cloud Infrastructure Security for AWS capabilities

Find cloud security gaps
Understand and address security control gaps in your AWS environment, pinpointing vulnerabilities and misconfigurations leveraging AWS Security Hub. Security practitioners can validate that security controls are working properly and navigate through findings by resource, resource type and category with pre-packaged automated resolution workflows to aid in a speedy recovery.

Visualize the threat landscape
Keep track of active threats in your AWS cloud environment with data visualizations that make prioritizing and responding to threats easy. Quickly manage your changing cloud attack surface, leveraging GuardDuty data and CloudTrail analytics coupled with Sumo Logic alerts. Stay ahead of would-be cybercriminals and ensure your organization's critical data is safe.

Monitor cloud access and activity
Mitigate identity-based attacks and maintain a strong cloud security posture with views into changes in config and IAM activities and suspicious network, user, and web activities. Knowing precisely who can access what at any point in time, in addition to monitoring changes in access privileges, can be instrumental in remediating identity-based attacks in the cloud.

Sumo Logic AWS Built-in Security Quick Start
Automatically configure essential AWS security services, such as GuardDuty, Security Hub and CloudWatch, in minutes using our AWS Built-in certified Security Quick Start. The AWS team rigorously tests Built-in solutions to provide customers with peace of mind and ease of use for selecting solutions. These work seamlessly with Cloud Infrastructure Security for AWS for full-stack security visibility.

Built with security-first principles
Our firm commitment to data security is validated by the platform's third-party compliance attestations and certifications, including PCI DSS, SOC 2 Type II, HIPAA, ISO 27001 and CSA STAR Level 2.

Scalable SaaS delivery model
Sumo Logic is built in the cloud to provide a low total cost of ownership and scalability as your organization's data types, quantities and sources continue 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 for your security team, ensuring users have real-time access without worrying about licensing limits. Sumo Logic's role-based access control enables your organization to set permissions for individuals and groups depending on the scope of their role, allowing 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. Sumo Logic makes it easy to automate your security operations workflows with the option to upgrade to Sumo Logic Cloud SIEM when ready.

Benefits

Combat complexity
Empower teams to collaborate through data-driven, actionable insights via a unified, full-stack security view of your AWS infrastructure and insight into threat activity across the environment.

Full-stack security visibility
Leverage native AWS tools and telemetry to accelerate security and reliability management workflows, maintain security visibility into your AWS environment and manage risk and attack surface.

Maximize efficiency
Share dashboards and work together to manage your cloud attack surface easily with curated security content and customizable alerting, evaluation and remediation flows.

Optimize costs
Cloud Infrastructure Security for AWS simplifies costs without sacrificing effective cloud security, letting you ingest and centrally store all your data securely without the need for "hot and cold storage."

Cost-effective licensing that fits your budget

With no per-user fees and no surprise overages, Sumo Logic offers an industry-leading flexible data tiering and credits licensing model, providing economic flexibility for monitoring 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 you need to monitor, alert and analyze in real time.

- **Frequent analytics** is optimized for high usage, ad-hoc data analysis, allowing you to focus on data searches and visualization.

- **Infrequent analytics** is reserved for low-usage data sets retained over a long period but seldom pulled in for analysis.

Book a demo

About Sumo Logic

Sumo Logic, Inc. empowers the people who power modern, digital business. Sumo Logic enables customers to deliver reliable and secure cloud-native applications through its Sumo Logic SaaS Analytics Log Platform, which helps practitioners and developers ensure application reliability, secure and protect against modern security threats, and gain insights into their cloud infrastructures. Customers worldwide rely on Sumo Logic to get powerful real-time analytics and insights across observability and security solutions for their cloud-native applications. For more information, visit **www.sumologic.com.**