

Security analytics for AWS

Deep security, compliance and performance insights for your AWS environment

Legacy security monitoring and analytics solutions are not natively designed to understand the AWS Cloud environment well, and legacy approaches are complex, costly, and don't scale to handle cloud data volumes. Sumo Logic alleviates these challenges.

Product overview

Sumo Logic's security analytics solution for AWS provides security monitoring and continuous compliance that is built from the ground-up to detect and respond to threats in real-time. Our solution provides deep insights into your AWS infrastructure, workloads, and full stack monitoring of your environment, delivering quick time-to-value, ease-of-use, and a low total cost of ownership.

Whether your main focus is security, compliance, or operational insights, our automated cloud security analysis, retention, and reporting provides the flexibility to manage all your data analysis use cases from a single, central solution.

Capabilities

Deep security insights

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 user behavior analytics, incident management, IoT security orchestration, and privileged access monitoring.

Accelerate compliance readiness, without the complexity

Sumo Logic simplifies your compliance efforts and shortens audit cycles with pre-built searches, dashboards, and reports to demonstrate continuous compliance. Sumo Logic makes it easy to log and monitor user access and platform configuration changes across all AWS workloads, and the compliance dashboards and applications are routinely updated making it easy to adapt to changing requirements with minimal effort.

Operational intelligence for secure DevOps

As your organization adopts a cloud strategy to increase business agility, it is important that your investments enable you to achieve this in a secure and efficient manner. Sumo Logic provides the

analytics and insights that help you drive your digital cloud initiatives forward with confidence and clarity. Sumo Logic delivers continuous security and operational intelligence with pre-built dashboards, searches, queries and reports for all your AWS workloads.

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 our machine learning-driven detection, integrated threat intelligence correlation, and deep search-based investigation along with the solution's rich data visualization.

Rapid compliance readiness

Broad integration support and pre-built reports that provide granular visibility help accelerate your compliance readiness.

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.

Multi-cloud visibility

As a cloud-native solution, Sumo Logic provides complete coverage for your public, hybrid, and multi-cloud environments with monitoring that unifies your security analytics and investigations across AWS, Azure, and GCP. With a comprehensive set of

applications and integrations for AWS services and off-the-shelf applications, Sumo Logic delivers instant visibility through pre-built dashboards, searches, queries, and reports.

Deep security insights

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 user behavior analytics, incident management, IoT security orchestration, and privileged access monitoring.

Scalable SaaS delivery model

Sumo Logic is built in the cloud to provide flexibility, scalability, and agility 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.

Native integrations and AWS visibility

Delivering the industry's most comprehensive set of solutions that monitor the service delivery and performance of an organization's AWS infrastructure, Sumo Logic's native integrations ensure services are available and performing at expected levels. With Sumo Logic, you can easily collect AWS metadata and CloudWatch metrics to visualize your entire AWS infrastructure and platform elements, making it simple to quickly identify trends, potential threats, and optimize performance.

Built with security-first principle

Sumo Logic is the industry's benchmark in delivering secure SaaS. Built on top of the secure AWS infrastructure, our cloud-native solution has additional third-party security validations, including:

- PCI DSS 3.2.1 Service Provider Level 1 attestation of compliance
- ISO 27001 Certification
- CSA STAR Level 2 Certification
- SOC 2 Type 2 Audit Report
- HIPAA Security Rule Attestation of Compliance

AWS Security monitoring use cases

Quick start AWS security monitoring

Automatically implement best practice configurations for your AWS security monitoring—in minutes. Our AWS Security Quick Start helps you get started, instantly, with best practice configurations for 12 built-in Sumo Logic apps designed for AWS security monitoring.

AWS GuardDuty

Convert GuardDuty data into user-friendly dashboard views to graphically depict and quickly visualize threats, trends, anomalies and outliers

AWS Security Hub

- Detect, investigate, and respond to AWS security events
- Ensure continuous compliance with PCI, HIPAA, GDPR, and other regulations
- Correlate your AWS security events with other cloud and hybrid security events to gain holistic security visibility
- Enable and accelerate your cloud migration
- Secure your workloads before, during, and after your cloud migration

App for AWS CloudTrail

- Investigate user behavior patterns
- Monitor platform configuration changes
- View account settings, usage and billing status
- Perform visitor analytics, improve quality of service, and reduce errors and downtime
- Correlate Amazon CloudFront data with internal data
- Measure the business impact of CDN performance and quality of service

App for Elastic Load Balancing

- Analyze status codes based on the ELB and backend instances
- Integrate IP address with number and size of requests
- Get a comprehensive overview of the environment
- App for Amazon Simple Storage Service (S3)
- Monitor all data that resides within Amazon S3 buckets
- Index, search, and analyze performance and audit/access logs
- Generate reports and determine AWS billing and usage patterns

App for AWS Configuration

- Monitor the modification of AWS resources
- Analyze configuration trends
- View relationships between AWS resources

App for Amazon VPC Flow Logs

- Understand network latency and failures
- Monitor trending behaviors and traffic patterns
- Generate network traffic alarms for observed anomalies and outliers

Sumo Logic Amazon Kinesis Connector

- Uses a Java connector between Kinesis Streams and Sumo Logic
- Provides a scalable integration with Amazon CloudWatch Logs

