sumologic®

SOLUTIONS BRIEF

Security Intelligence for AWS

Critical Insights for Security, Performance and Compliance in AWS

Many are quickly discovering that their legacy security monitoring and management tools are not adequate to provide them with the visibility and insights they need to manage their security, performance and compliance mandates in the AWS Cloud. Sumo Logic's AWS Cloud-native solution delivers organizations with holistic and real-time visibility and insights into infrastructures and the full stack of their modern applications in this new environment.

Simplify and Accelerate Migrations to AWS

As organizations transition to AWS from on-premise or other cloud providers, and migrate core infrastructure components, services and applications, the monitoring of the new infrastructure is a challenge. Sumo Logic easily scales ondemand, across any infrastructure to meet the challenges of cloud migration, and provides IT and Security teams with realtime visibility into the operational status, KPIs, and usage metrics of each infrastructure tier that is being migrated.

Visibility Across Hybrid Infrastructures

Sumo Logic provides operational and security visibility with a unified view across AWS, other cloud, and on-premise infrastructures. 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. IT and InfoSec teams immediately visualize and monitor their workloads easily, identify issues, and expedite root-cause analysis.

Augment Security and Compliance Monitoring

Sumo Logic simplifies and drives efficiencies around compliance and security monitoring – often the biggest barriers to cloud adoption. IT Security can monitor user access, platform configuration changes across all AWS and on-premise workloads, and generate audit trails to demonstrate compliance with internal security standards and industry regulations such as PCI and HIPAA. Pre-built apps and powerful machine learning algorithms automate cloud audits and quickly uncover compliance violations, threats, and anomalies in real-time.

The Cloud-Native Analytics Service

True SaaS — Sumo Logic's cloud-native architecture scales on demand to streamline massive workload migrations, expanding deployments, and seasonal spikes. As a cloud service, Sumo Logic easily overcomes the inherent limitations of traditional or managed service architectures that deliver rigid capacity and require overprovisioning.

Native AWS Integrations – Delivering the industry's most comprehensive set of solutions that monitor the service delivery and performance of an AWS infrastructure, native integrations ensure services are available and performing at expected levels.

Full-Stack Visibility – Sumo Logic delivers seamless cloud-to-cloud and cloud to on-premise integrations that deliver instant operational insights across microservices, traditional applications, edge services, and cloud services.

AWS Infrastructure Visibility – Sumo Logic enables organizations to easily collect AWS metadata and CloudWatch metrics to visualize the entire AWS infrastructure and platform elements to quickly identify trends, potential threats and optimize performance.

Machine Learning Analytics —With built-in pattern detection, anomaly detection, transaction analytics, outlier detection, and predictive analytics, Sumo Logic provides real-time visibility across thousands of data streams and seamlessly detects and predicts conditions that indicate potential performance, reliability or security issues.

Security Confidence — Sumo Logic is the industry's benchmark in delivering secure SaaS. Built on top of the secure AWS infrastructure, the cloud-native service delivers the following additional security measures to protect customer data:

- PCI/DSS 3.2 Service Provider Level 1 Certified
- ISO 27001 Certification
- CSA STAR Certification
- SOC 2 Type 2 & HIPAA Compliance Attestation
- 256 AES Encryption at Rest; TLS Encryption in Transit
- FIPS-140
- U.S. EU Safe Harbor framework
- GDPR compliant
- FedRamp (Pending)

Operational Visibility for Secure DevOps

As organizations begin to leverage a DevOps philosophy to increase business agility and capitalize on new market opportunities, it is important that the tools and technologies used will support this drive towards speed, flexibility and continuous innovation in a secure and efficient manner. Sumo Logic delivers continuous security and operational intelligence with pre-built dashboards, searches, queries and reports for all your AWS workloads. Sumo Logic helps drive your digital cloud initiatives forward with confidence and clarity.

App for AWS CloudTrail

- Investigate user behavior patterns
- Monitor platform configuration changes
- View account settings, usage and billing status

App for Amazon CloudFront

- 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
- 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 Config

- Monitor the modification of AWS resources
- Analyze configuration trend
- 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

- A Java connector between Kinesis Streams and Sumo Logic
- Allows for scalable integration with Amazon
- CloudWatch Logs

AWS GuardDuty

- AWS Lambda to ingest and securely send data (via HTTPS) to the Sumo Logic environment
- Converts GuardDuty data into user-friendly dashboard views to graphically depict and quickly visualize threats, trends, anomalies and outliers.

About Sumo Logic

Sumo Logic is the leading cloud-native, machine data analytics platform, that delivers real-time, continuous intelligence across the application lifecycle and stack. www.sumologic.com.

sumologic®

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

www.sumologic.com