

# Operations & security for AWS apps

Continuous Intelligence for modern apps and infrastructure

As organizations transition their mission-critical applications to the AWS cloud, it is critical that they monitor the performance and security of these apps to deliver excellent customer experience to their end customers. To address these challenges, organizations need continuous intelligence - real-time business, operational and security insights about their apps and cloud infrastructure.

Sumo Logic's machine data analytics service centralizes and unifies log data and time-series metrics and leverages advanced analytics to uncover real-time insights into application operations and security. More than 1,600 customers around the globe rely on Sumo Logic for the analytics and insights to build, run and secure their AWS modern apps and infrastructures.

## Improve visibility to lower risk of moving to AWS cloud

As organizations transition from on-premise or other cloud infrastructures to AWS, they struggle to get visibility into their digital assets and infrastructures. Sumo Logic enhances customers' abilities to simplify and accelerate movement to the cloud. Because of the logging and monitoring capabilities of Sumo Logic, users can easily get visibility into the new workloads as they are moved from an on-premises environment to the AWS cloud. Sumo Logic scales on-demand and streamlines everything from small to massive cloud deployments by providing real-time visibility into operational status, KPIs, usage metrics and compliance violations.

---

**“Sumo Logic has allowed McGraw Hill Education to move to AWS with confidence, enable real-time visibility across the entire stack, all at reduced TCO.”**

### McGraw Hill

Shane Shelton, Sr. Director, Application Performance & Development Operations

## Deliver excellent app performance and customer experience

Sumo Logic provides operational 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. Teams immediately visualize and monitor their workloads, use machine learning algorithms to detect app and infrastructure performance and availability issues, and leverage advanced analytics to expedite root-cause analysis. Ultimately, by monitoring and resolving performance issues quickly, DevOps teams can accelerate release cycles and improve customer experience.

## Strengthen cloud security and compliance

Sumo Logic simplifies compliance and security monitoring – often the biggest barriers to cloud adoption. InfoSec teams can leverage Sumo Logic's machine data analytics to strengthen their security postures. Unlike traditional SIEMs, there is no need to write rules or alerts based on events. With Sumo Logic, security professionals can monitor user behavior and visualize or alert on anomalies to quickly drill down on an unusual spike in user activities. Sumo Logic also captures and reports on 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, outliers, and anomalies in real-time.

## The cloud-native analytics service

**A modern solution for your modern app** - Sumo Logic is a cloud-native, microservices-based platform that is purpose-built to meet the needs of today's most demanding modern application teams - with out of the box support for cloud platforms like AWS, plus native integrations with Docker and Kubernetes  
**True SaaS with infinite scale**— 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** – Sumo Logic delivers the industry's most comprehensive set of integrations with native AWS services to ensure that your apps and infrastructure are available and performing at expected levels.

**Machine learning-driven 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, Sumo Logic's 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 II Attestation
- HIPAA-HITECH Attestation
- FIPS 140-2 level 2 Compliant
- E.U.- U.S Privacy Shield
- E.U. Cookie Compliance
- AES 256-bit encryption at rest / TLS encryption in transit / KEK to encrypt our encryption keys

## Sumo Logic for AWS app and infrastructure management

Sumo Logic was born in the cloud and was purpose-built to support AWS workloads and to help your organization stay current and relevant. By integrating with a host of AWS services, Sumo Logic can provide your organization with a highly elastic and scalable machine data analytics platform that grants you full visibility across your entire stack. Additionally, Sumo Logic provides pre-built applications and integrations with your AWS environment so you can easily visualize and detect anomalies. Sumo Logic has already pre-built the following applications:

- **AWS CloudTrail** - Feeding CloudTrail data into Sumo Logic allows you to track and monitor your AWS infrastructure for operational and security insights.
- **Amazon CloudFront** - Analyzing and correlating Amazon

CloudFront data with the origin data and/or other data sets allows you to improve availability and end-user experiences while enforcing rigorous security controls.

- **AWS Elastic Load Balancing (ELB)** - Analyzing raw AWS ELB data helps you determine latency issues and optimize your system configuration based on information from across all Availability Zones about source IPs and traffic to EC2 backend instances.
- **Amazon Simple Storage Service (S3)** - Sumo Logic can examine critical elements of your S3 service including access logs and reveal information such as request type, resource name, and the time the request was processed.
- **Amazon VPC Flow** - Ingesting your VPC Flow Logs directly into Sumo Logic continuous intelligence service allows you to monitor and visualize your IP traffic within your VPC for operational and security insights.
- **AWS Config** - The Sumo Logic app for AWS Config delivers real-time interactive visualizations to track configuration changes made to critical resources in your AWS infrastructure.
- **Amazon Kinesis Connector** - The Sumo Logic AWS Kinesis Connector enables real-time AWS Kinesis data streams to be ingested by the Sumo Logic cloud-native platform.
- **Amazon Lambda** - The Sumo Logic AWS Lambda App enables monitoring and tracking of key operational indicators such as duration, memory utilization and number of requests across all your Lambda Functions
- **Amazon Lambda Function** - Sumo Logic visualizes operational and performance trends about all the Lambda functions in your account, providing insight into executions such as memory and duration usage.
- **Amazon GuardDuty** - Integrating Sumo Logic with AWS GuardDuty provides preconfigured dashboards and insights (such as severity, VPC, IP, account ID, region, and resource type) into unexpected and potentially malicious activities.
- **AWS Inspector**: Ingest your Amazon Inspector scan results directly into Sumo Logic service to monitor and visualize your security findings over time for vulnerabilities or deviations from best practices.
- **AWS Security Hub**: Sumo Logic completes the security response process by providing holistic security visibility across AWS security events. Users can correlate, investigate, then take actions to respond, and extend compliance checks to a number of other key regulatory frameworks such as PCI, GDPR, HIPAA, and others.

## 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](http://www.sumologic.com).

