sumo logic | Continuous Intelligence Platform™

WHITE PAPER

5 Best Practices for AWS Security Monitoring

Secure your cloud journey to AWS

Continuous innovation and speed to market are mandating dynamic paradigm shifts in how companies conceive, develop and implement IT operations and security strategies. The escalating demand for agility is driving cloud-based digital initiatives to the forefront of today's enterprise economy. Software-centric companies keenly focused on delivering differentiated customer experiences are reshaping markets and the way we do business.

One example is Amazon's revolutionary cloud computing business, Amazon Web Services (AWS), earning more than $30 billion in annual revenue. AWS, launched in 2006 and now the most widely adopted cloud IaaS provider, redefines computing and is the greatest disruptive force in today's enterprise technology market. Digital enterprises are migrating mission-critical workloads to the cloud and leveraging advanced AWS infrastructure to reap the benefits of agile development and competitive advantage. Business executives must have real-time visibility to ensure robust and consistent cloud security.

Security remains the number one pain point for cloud deployments

Cloud Computing Outlook (451 Research)

The number one cloud security issue is lack of visibility

Dave Shackleford, SANS Project

All workloads are not created equal. The complexity and pace of change that characterize many cloud deployments make them impossible to protect with traditional on-premises security systems. Likewise, simply moving existing workloads from enterprise datacenters to the cloud without rethinking security implications will jeopardize sensitive information assets. On the other hand, AWS workloads that feature purposefully baked-in cloud-centric security for modern applications will protect critical data… and allow security professionals to get a good night's sleep.

Five AWS Security Best Practices

A baseline level of security is built into AWS offerings, but companies that deploy these services are responsible for securing the apps running in their AWS environments.

> **"The cloud abstracts the complexity of the physical security from you and gives you the control through tools and features so that you can secure your application."**
>
> AWS security best practices

As your organization continues to migrate workloads to the cloud, here are some fundamental approaches you will want to adopt in order to better protect every layer of your AWS architecture:

1. Understand service provider and customer responsibilities in the AWS shared security model.

Amazon provides physical infrastructure security, but other service providers and enterprise customers are responsible for network and application security. In other words, AWS is responsible for the security of the cloud; customers are responsible for security in the cloud. All participants must invest in and share ownership of protecting the AWS ecosystem.

Tips:

- Protect your AWS credentials with access keys and/or certificates.
- Encrypt credentials before sending them over the wire, and incorporate a key rotation mechanism to counter compromise.
- Use certificates to authenticate access to specific AWS services.

> **"Through 2020, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities"**
>
> **Gartner**

2. Align AWS security strategy with enterprise control objectives.

Is your organization primarily concerned about data availability, integrity, confidentiality or sovereignty? Your core control objectives should drive your AWS cloud security strategy, framework and policies.

Tips:

- Protect sensitive data exchanged between browsers and servers by configuring SSL and creating a Virtual Private Cloud (VPC).
- Leverage Amazon GuardDuty to protect your AWS accounts and workloads from malicious activity and unauthorized behavior.
- Use Amazon VPC Flow Logs to capture information about web application traffic to and from network interfaces in your VPC.

- Maximize the security of your apps by regularly deploying and testing updated AMIs (Amazon Machine Images).

3. Adopt a holistic approach to security that encompasses people, process and technology.

Enterprise IT is expected to deliver capabilities to the business faster than ever before. The security focus is often on process and technology, but people are a critical part of the equation in combating data breaches. Embrace the DevSecOps approach, which tears down traditional barriers and enables these functional areas of the enterprise to collaborate as a dynamic force to create solutions.

> **"80% of companies report that end-user carelessness constitutes the greatest security threat to the enterprise, surpassing malware and hacker attacks."**
>
> AWS security best practices

Tips:
- Ensure sensitive data is protected regardless of where it is stored. Continuously monitor user application access, usage and modifications (AWS Config), including actions of privileged users.
- Rely on advanced machine learning to uncover dangerous user activity. Trigger real-time alerts when suspicious access occurs.

4. Rigorously manage AWS accounts, granting users permission to access only the resources they require.

Manage the permissions for users within your AWS environment with AWS Identity and Access Management (IAM). This service eliminates the need to share passwords or access keys, and eases the process of changing user access as necessary. IAM lets you give users unique credentials and grant role- and rule-based permissions to access only the AWS resources required for them to perform their jobs.

Tips:
- Encrypt all network traffic so that only authenticated users see data in clear text.
- Take and store periodic snapshots of your data to protect it from disaster.
- Rely more on IAM user credentials and less on enterprise AWS account credentials for access to AWS resources.

5. Monitor enterprise AWS usage to identify suspicious behavior.

Start with continuously monitoring all user actions related to AWS workloads by activating AWS CloudTrail and Amazon CloudWatch. Then inject the resulting log data and monitoring metrics into security analytics systems for enhanced search, alerting, visualization and correlation capabilities. Apply pattern clustering to log data to surface outliers and improve threat detection (internal and external).

Tips:
- Amazon CloudWatch tracks OS and application logs; AWS CloudTrail logs all API actions within IAM and most other AWS services.
- Run Amazon Inspector to learn how your workload apps are performing. This host-based agent runs scans to determine if changes in workloads will result in noncompliance.
- Create an immutable audit trail of your log data to meet regulatory compliance requirements and respond to auditors' ad-hoc requests for additional information.

Armed with the tools and capabilities provided by AWS, most customers can easily implement many of these best practices. However, robust AWS security does require an investment in new proactive application monitoring methodologies that can scale to manage and analyze massive volumes of machine data, including log event streams as well as infrastructure and application metrics. In order to attain end-to-end visibility of your AWS environment, you will need to deploy security analytics to continuously track and investigate user activity patterns and suspicious behavior.

Sumo Logic Analytics for Best-Practice Cloud Security

Sumo Logic's analytics platform is designed and delivered to mirror Amazon Web Services. Sumo helps organizations gain the instant visibility they require to confidently pursue and enable dynamic modern cloud applications. Data must be mastered, integrated and analyzed to gain the situational awareness that drives a proactive security posture.

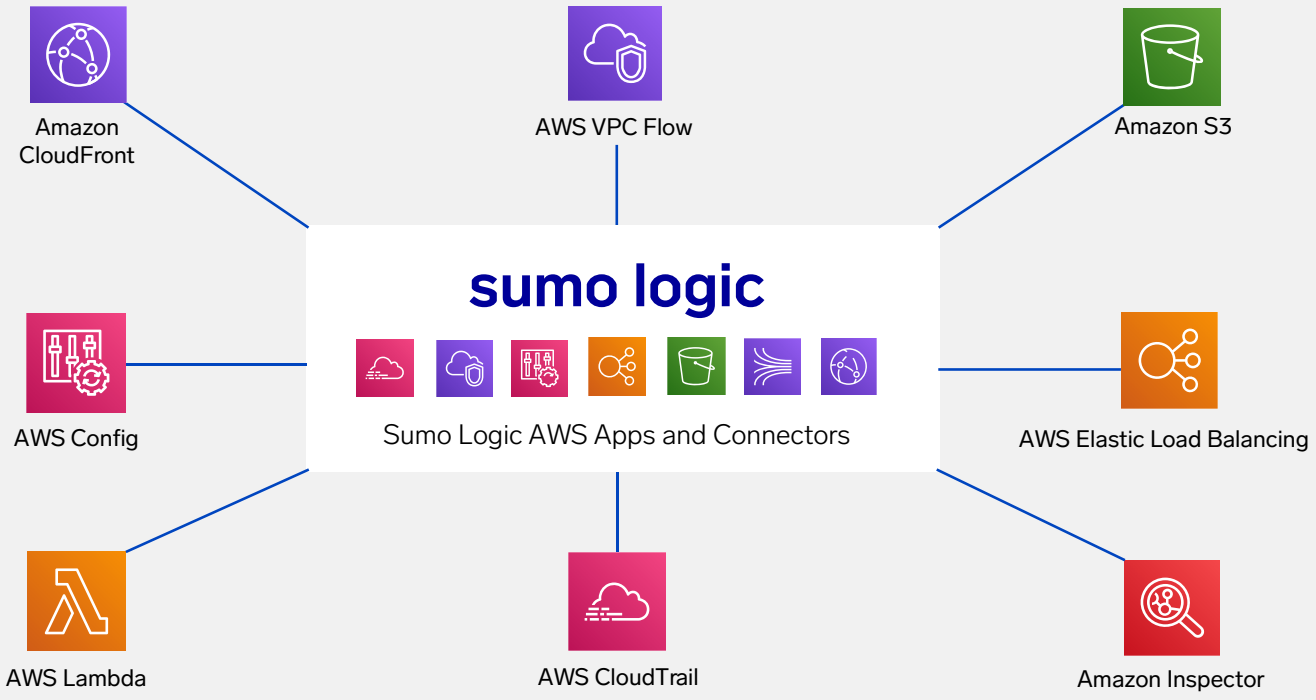
> **"You can't protect what you can't see. Enterprise IT may not be aware of cloud workloads… making protection impossible."**
>
> **Gartner**
>
> Best Practices for Securing Workloads in Amazon Web Services

Visibility Is Everything

A modern cloud environment generates a near insurmountable amount of logs. The shear volume makes it a daunting task to digest or derive valuable insights without a solution capable of intelligent analysis and correlation. By combining threat intelligence and the out-of-the-box solutions from AWS, Sumo Logic can help solve this. Sumo Logic's app for VPC Flow Logs consumes streams of complex AWS data and outputs vivid visualizations that reveal strengths and weaknesses. Every Amazon service is safeguarded by one or more security groups—rules that control network traffic and provide basic firewall like protection. Every one of dozens of tabular VPC Flow Logs (sampled above) associated with your apps must map directly to one of these Amazon CloudWatch groups. So, for every VPC, you must create a logging group in Amazon CloudWatch, and within each group, you must select the network interfaces you care most about, based on your data security priorities. It is also a good idea to set up workloadbased firewalls to fill gaps left by AWS security groups. Controlling and protecting applications and the services that support them should be the focus of your cloud security strategy, not signature-based antivirus or anti-malware scanning.

Cloud Security Analytics - Native AWS Integrations

Real-time insights about the Security & Operational Health of AWS Infrastructure



Operate and Innovate with Confidence and Security

Ingesting AWS logging data into Sumo Logic's analytics engine provides continuous visibility, a holistic view across VPCs, synchronization capability and actionable intelligence. Machine learning reduces millions of siloed data streams into digestible and meaningful patterns. Algorithms monitor transient enterprise workloads in real time, reveal normal behavioral patterns, and point you to anomalies and deviations that may be cause for concern. You gain the real-time visualization you need to quickly identify problems, detect root causes, and resolve cloud-based security threats. Sumo Logic transforms AWS data into opportunistic security, operational and business insights. Facilitating deep visibility across the AWS environment and integrating services for a comprehensive unified view allow you to see who is accessing AWS and when they are making changes (AWS CloudTrail), what they are changing (AWS Config), where this impacts network traffic and latency (AWS VPC Flow), and how this is affecting your security and compliance posture (Amazon Inspector). Continuously monitoring workloads, user access, and configuration changes in real time improves visibility across AWS services.

"Sumo Logic's ability to support VPC Flow Logs is critical for our security team to have full stack visibility. It allows us to capture and analyze traffic flow for all network interfaces, increasing our security posture over time, and do this in a seamless and consistent manner across our entire AWS infrastructure."

Interactive Intelligence

Jerrod Sexton
Security Engineer

The Industry's Most Secure Cloud-Native Analytics Platform

Sumo Logic was conceived and launched in the cloud; it's part of the company's DNA. Cloud audit, user monitoring and behavioral analysis are core capabilities. Sumo helps customers simplify and accelerate migrations to AWS by continuously monitoring and securing cloud apps.

- Instant Value. With Sumo Logic's cloud-native SaaS offering, you can get started in minutes and have access to all the latest capabilities without the need for time-consuming, expensive upgrades. Start small and expand as your business grows.
- Elastic Scalability. Our multi-tenant architecture scales on demand to support rapid application growth and cloud migration. The service overcomes the inherent limitations of traditional architectures by allowing organizations to burst as needed without any manual intervention.
- Proactive Analytics. Sumo Logic is known for powerful machine learning and analytics. We leverage machine learning to help make sense of expected and unexpected behavior across environments with pattern and outlier detection.
- Secure by Design. Sumo Logic maintains the highest level of security certification to protect your data, including: CSA STAR, PCI DSS 3.1 Service Provider Level 1, ISO 27001, SOC 2, Type II Attestation, FIPS 140 Level 2 and HIPAA.
- Reliability. SLAs on availability and performance ensure Sumo Logic services are always on and performing per expectations. Sumo Logic publishes live service status for greater transparency.

Gain the continuous visibility required to confidently and securely migrate mission-critical workloads to the cloud. Enhance baseline AWS infrastructure protection with Sumo Logic analytics for best practice cloud security.

About Sumo Logic

Sumo Logic is a leader in continuous intelligence, a new category of software, which enables organizations of all sizes 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 2,000 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.

Founded in 2010, Sumo Logic is a privately held company based in Redwood City, California, and is backed by Accel Partners, Battery Ventures, DFJ Growth, Franklin Templeton, Greylock Partners, IVP, Sapphire Ventures, Sequoia Capital, Sutter Hill Ventures, and Tiger Global Management. For more information, visit www.sumologic.com.

s u

See business differently

m o

sumo logic

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

www.sumologic.com