SOLUTION OVERVIEW

LogRhythm and Amazon Web Services (AWS)

LogRhythm
The Security Intelligence Company

Safeguard and Monitor Your AWS Infrastructure

Organizations around the world use the Amazon Web Services (AWS) platform to host their sensitive corporate applications and data. It provides the elasticity needed to grow with your company and saves costs by reducing the need to purchase, maintain, and place physical hardware. However, to safeguard your AWS applications and data, you need to be able to monitor your AWS infrastructure as well as the rest of your distributed IT environment and cloud applications in an integrated manner. This allows you to rapidly detect and neutralize security threats stemming from any vector before they can result in a damaging cyber incident or data breach.

Gain Holistic Visibility into AWS with LogRhythm

The expansion of your organization's network into AWS adds more complexity and new sources of security risk, thus complicating and increasing the need for visibility and security monitoring. Together with AWS, LogRhythm simplifies your security operations and gives you end-to-end visibility into your services on AWS, in real time, from a single pane of glass. LogRhythm's Threat Lifecycle Management Platform continuously collects, normalizes, and analyzes rich forensic data collected from your AWS deployments, including:

- AWS Config: Configuration change, resource allocation
- AWS CloudTrail: Audit-level logging for AWS activity
- Amazon CloudWatch: Monitor AWS resources and applications (metrics and alarms)
- AWS S3 Server Access: File access, file removal, changes

AWS telemetry is combined with the petabytes of other machine data LogRhythm collects and analyzes from across your broader distributed IT environment.

Benefits of Integrating LogRhythm and AWS

- Real-time detection of threats across AWS applications and data
- Integrated visibility across both AWS and broader corporate network environments
- Reduced risk and accelerated threat response through automation
- End-to-end Threat Lifecycle Management and tight integration of cloud computing environments and security intelligence solutions

How it Works

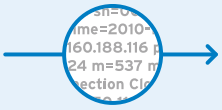
Setting up monitoring for AWS is simple. Each service needs its own AWS Identification and Access Management (IAM) user. The IAM user is assigned to a LogRhythm System Monitor Agent and the Agent can be quickly configured to collect logs from the service. The agents consolidate and collect log and machine data from your AWS services. LogRhythm System Monitor Agents can run on-premise or in the cloud and use AWS APIs.

Amazon Web Services

- Secure Cloud Services Platform
- On Demand Computing
- Simple Storage Service (S3)
- Monitoring Cloud Resources and Applications (CloudWatch)

Other Log, Security, and Machine Data

LogRhythm Forensic Sensor Data



Machine Data Intelligence

Automatically collect and process data from across the distributed environment

LogRhythm

Threat Lifecycle Management Platform

- Behavioral Security Analytics (User/Entity, Network & Endpoint)
- SIEM & Log Management
- Network Monitoring & Forensics
- Endpoint Monitoring & Forensics
- Security Automation & Orchestration

LogRhythm Labs

LogRhythm's machine analytics correlates and analyzes this data to detect and corroborate potential threats and to baseline normal behavior patterns. This analysis allows you to monitor your services on AWS and be alerted on suspicious activity, keeping your data and resources secure. This enables you to:

- Gain visibility into AWS authentication and access activity to detect compromised credentials
- Monitor and control access to AWS services to detect inappropriate use of resources
- Receive alerts based on suspicious AWS usage to detect data exfiltration or tampering with applications or data
- Report on access, usage, and modifications
- Ensure compliance requirements are met

LogRhythm and Amazon are tightly integrated, bridging the value of Amazon Web Service's suite of cloud computing services with the advanced security analytics and incident response capabilities of LogRhythm's Threat Lifecycle Management Platform. The combined offering empowers you to accurately capture and monitor real-time data from AWS deployments to detect suspicious activity, prioritize attacks, and automate adaptive threat response.

Use Case: Compliance

Challenge: You store, process, or transmit cardholder data through AWS; therefore, you are required to be compliant with PCI-DSS.

Solution: Although many AWS services are PCI-DSS certified, LogRhythm provides out-of-the-box functionality to simplify your investigations with alarms and reports that are automatically associated with the correct PCI-DSS asset categories. For example, you can schedule reports or generate them on demand. Investigations and alarms provide your team with immediate notification of activities, such as configuration changes that impact your AWS-hosted cardholder data so you can identify areas of non-compliance in real time.

Use Case: Cloud Visibility

Challenge: As resources and services move offsite, the lack of visibility and control often makes detecting insider threats very difficult.

Solution: Combining Amazon's CloudTrail API history with LogRhythm's advanced statistical and behavioral analytics enables your security team to detect and respond to advanced internal and pivoting external threats. By baselining user and service activity and then alerting on highly corroborated anomalies, LogRhythm lowers the time to detect and respond to data exfiltration, compromised accounts, or administrative users inappropriately using company cloud resources.

Additional Reading:

- LogRhythm Device Configuration Guides > Amazon Web Services (AWS) Log Collection
- LogRhythm Cloud Monitoring Datasheet
- LogRhythm on the Amazon Marketplace

About LogRhythm

LogRhythm, a leader in Threat Lifecycle Management, empowers organizations to rapidly detect, respond to, and neutralize damaging cyber threats early in the threat lifecycle to prevent damaging data breaches and cyber incidents. Our patented award-winning platform uniquely unifies next-generation SIEM, log management, network and endpoint monitoring, user entity and behavior analytics (UEBA), security automation and orchestration and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides unparalleled compliance automation and assurance, and enhanced IT intelligence.

About Amazon Web Services

For 10 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 90 fully featured services for compute, storage, networking, database, analytics, application services, deployment, management, developer, mobile, Internet of Things (IoT), Artificial Intelligence (AI), security, hybrid and enterprise applications, from 42 Availability Zones (AZs) across 16 geographic regions. AWS services are trusted by millions of active customers around the world monthly—including the fastest growing startups, largest enterprises, and leading government agencies—to power their infrastructure, make them more agile, and lower costs. To learn more about AWS, visit https://aws.amazon.com.