DATA SHEET

# CLOUD MONITORING

LogRhythm
The Security Intelligence Company

Moving your business information to the cloud may help your organization realize substantial benefits such as lower costs, freed up capital, and increased flexibility.

However, when you use cloud services, your corporate data may be accessible to the entire internet. With critical intellectual property (IP) such as customer lists and competitive analysis, as well as sensitive data like employee records and customer credit card information stored in the cloud, security is a substantial concern.

## Who is Monitoring and Protecting Your Cloud Services?

The expansion of your organization's network perimeter into the cloud makes centralized monitoring and control difficult. Cloud infrastructure and applications often do not have the same level of authentication and access audit controls in place as an on-premises solution. In addition, cloud services may have inadequate or inaccessible internal facilities for monitoring and reporting on user activity. Suddenly you have a huge blind spot.

Cloud monitoring can provide critical visibility across many security use cases, including:

- Detecting compromised account or privilege misuse within cloud infrastructure that could otherwise go unnoticed
- Providing visibility into contractors and other third parties that access your cloud services but do not interact with your corporate network
- Ensuring employees are in compliance with your cloud services terms of use policies

## Get Control Over Your Cloud Security

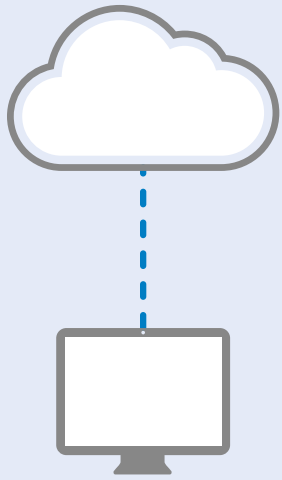
You need to have at least the same level of centralized security analytics for cloud infrastructure and applications as you do for your on-premises solutions—if not more. Monitor your cloud-based infrastructure with the LogRhythm Security Intelligence and Analytics Platform to:

- Gain visibility into cloud authentication and access activity
- Monitor and control access to cloud services
- Receive alerts based on suspicious cloud usage
- Report out on access, usage, and modifications

LogRhythm offers several ways to set up monitoring depending on your infrastructure architecture and needs:

### Benefits of using LogRhythm for Cloud Monitoring

- Gain a global view into user behavior—both on-premises and in the cloud—with centralized security analytics
- Incorporation of cloud services/ apps into prepackaged security analytics modules, including extensive User and Entity Behavior Analytics (UEBA), makes it quick and easy to get up and running
- Lower your total cost of ownership (TCO) for cloud monitoring through the LogRhythm platform's ease of configuration, operation, and management
- Quickly and easily meet your organization's compliance requirements



| Virtual Data Collectors in the Cloud | System Monitors Running on VMs | Cloud-Based API Support |
|---|---|---|
| Provides remote, high-performance collection of all machine data including log messages, application data, security events, and network flows. A single Virtual Data Collector is capable of collecting and transmitting up to 10,000 messages per second from thousands of devices and cloud services. | Can be deployed on individual virtual machines capturing local log data (e.g., flat files) and providing endpoint forensic monitoring. System Monitors can be deployed on Windows, Linux and UNIX VMs running in the cloud. | LogRhythm offers remote collection of audit logs from cloud services provided via API. |

## Cloud-Based API Support

Currently supported cloud services that provide API feeds to send audit logs directly to the LogRhythm Security Intelligence and Analytics Platform:

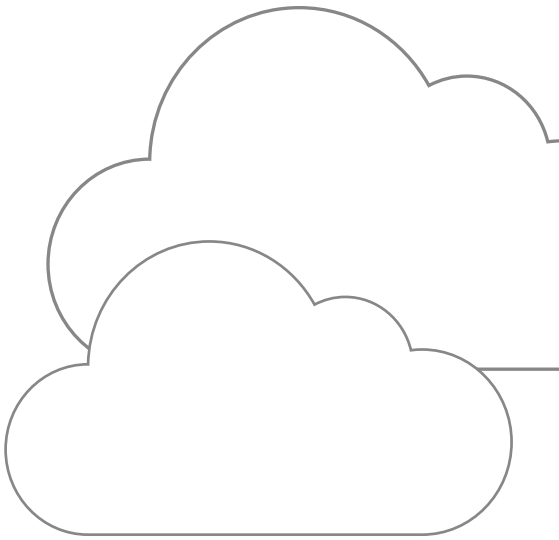
| Cloud Service | What LogRhythm Monitors |
|---|---|
| **AWS** | |
| Config | Configuration changes, resource allocation |
| CloudTrail | Audit log for AWS API calls |
| S3 Server Access | Audit accesses to S3 buckets/files, File Integrity Monitoring |
| CloudWatch | Monitor AWS resources and applications (metrics and alarms) |
| **Box** | Audit logins and File Integrity Monitoring |
| **Cradlepoint ECM** | Cloud router audit event |
| **Office 365** | |
| Azure AD | Active Directory audit events (logon, logoff, access) |
| Exchange | Email events |
| Sharepoint | File Integrity Monitoring |
| **Okta** | System log, authentication audit events |
| **Salesforce** | App management and usage, security audit events |

In addition, LogRhythm offers support for many leading Cloud Access Security Broker (CASB) products, including Netskope, Skyhigh, and Cloudlock.

## Cloud Monitoring Use Cases

**Usage of Cloud Services**

Your organization uses Box to store and share company files, including confidential data. You need to know who's logging into Box, what's getting uploaded, what's being downloaded, and by whom. Using LogRhythm, you can easily track user logins and any access or changes to cloud-based files. In addition, you can correlate this data with other data sources using AI Engine to quickly detect and respond to insider threats and compliance violations.



**File Monitoring in the Cloud**

Your organization would like to monitor the integrity and access of key assets stored in the cloud. With LogRhythm, you can monitor these sensitive files for accesses and changes just like files stored in your data center.

**Abnormal Authentication Activity**

Your organization uses a cluster of Amazon Web Services (AWS) hosted virtual machines and you need to receive alerts when compromised or rogue users access these VMs to potentially exfiltrate data. Using machine learning techniques, the LogRhythm Security Intelligence and Analytics Platform can detect abnormal activity such as logins to new cloud services, unusual logins to services, and logins at unusual times of day or locations.

**Additional Reading:** Device Configuration Guides at https://onlinehelp72.logrhythm.com/Content/5DeviceGuides/AWSCloudConfigServerEvents.htm