Data Sheet

Cloud Security

LogRhythm
The Security Intelligence Company

Digital transformation is driving organizations to move business information to the cloud. While substantial benefits (e.g., lower costs, freed-up capital, increased productivity) are often realized, there are risks. Centralized monitoring and control becomes more difficult as you expand your organization's network perimeter to include the cloud. Additionally, cloud infrastructure and applications are often implemented without the same level of authentication and access control as internal IT systems. Cloud services may also have inadequate or inaccessible internal facilities for auditing and reporting on user activity.

The drawbacks of moving to the cloud often result in a lack of visibility into the environments where your data resides, leaving your organization vulnerable to cyber threats. That is why it is crucial to have a platform that provides centralized visibility across on-premise and cloud infrastructure and applications to identify threats regardless of their point of entry.

Gain Control Over Your Cloud Security

Real-time monitoring capabilities are critical to rapidly detecting and neutralizing security threats across your cloud infrastructure, distributed IT environment, and cloud applications. LogRhythm's NextGen SIEM Platform offers comprehensive, single pane of glass visibility into your cloud-based solutions. From infrastructure to applications, both in the cloud and on-premise, LogRhythm provides the ideal detection and response solution for monitoring and securing your cloud services.

With LogRhythm, you'll be able to:

- Detect compromised accounts or privilege misuse within cloud infrastructure that could otherwise go unnoticed
- Get visibility into contractors and other third parties that access your cloud services but do not interact with your corporate network
- Ensure employees comply with your internal policies on the use of cloud services
- Leverage a single solution for threat qualification, investigation, and response regardless of the threat's entry point

If your organization is impacted by compliance regulations, you may think you are restricted from leveraging many cloud-based solutions due to monitoring requirements. LogRhythm enables you to enjoy the benefits of the cloud while adhering to your compliance mandates. The LogRhythm NextGen SIEM Platform monitors your cloud services for alignment to compliance requirements, enabling you to:

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

With LogRhythm, you can be confident in your ability to quickly detect and respond to threats to keep your sensitive data safe, no matter where it resides.

Benefits of using LogRhythm for Cloud Security

- Gain a global view into user behavior – both on premise and in the cloud – with centralized security analytics
- Rapidly spot suspicious cloud-based activities through incorporation of cloud services/apps into prepackaged threat detection modules, including User and Entity Behavior Analytics (UEBA)
- 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

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

- **Support for cloud APIs:** Offers remote collection of audit logs via the LogRhythm SysMon agent leveraging cloud service APIs.
- **Virtual data collectors in the cloud:** Provides remote, high-performance collection of machine data, including log messages, application data, security events, and network flows, from thousands of devices and cloud services.
- **Endpoint monitoring on cloud-based systems:** LogRhythm SysMon captures local log data (e.g., flat files) and provides endpoint forensic monitoring. LogRhythm SysMon supports Windows, Linux, and UNIX VMs running in your cloud environments.

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 shared, what's being downloaded, and by whom. Using the LogRhythm NextGen SIEM Platform, you can easily track user logins and any access, shares, or changes to cloud-based files. In addition, AI Engine correlates this data with other data sources to quickly detect and respond to compromised user accounts, insider threats, and compliance violations.

Abnormal Authentication Activity

Your organization uses a cluster of AWS-hosted virtual machines (VMs). You need to receive alerts when compromised or rogue users access these VMs to potentially exfiltrate data. Using machine learning techniques, LogRhythm detects abnormal activity, such as logins to new cloud services, unusual logins to services, and logins at unusual times of day or locations.

File Monitoring in the Cloud

Your organization needs to monitor the integrity and access of key assets stored on SharePoint, OneDrive, and other cloud applications. With LogRhythm, you can easily monitor these sensitive files for accesses and changes.

Vulnerable Asset Protection

Your organization needs to tie current vulnerability data to potential threats and ongoing attacks, so you can respond quickly and appropriately. LogRhythm incorporates results from cloud-based vulnerability management solutions, like Tenable.io. When attacks designed to exploit known vulnerabilities are seen impacting a vulnerable device, LogRhythm SmartResponse™ plugins can actively defend your organization by initiating actions to neutralize specific cyberthreats (e.g., adding attacking IPs to firewall ACLs, disabling accounts that may have been compromised, killing suspicious processes and services).

Support for Cloud Services

LogRhythm offers industry-leading support for over 800 different data sources. Below is a sample of common cloud services the LogRhythm NextGen SIEM Platform supports. LogRhythm continuously adds to the number of supported cloud-based products. Check the LogRhythm Community for the latest list.

IaaS/PaaS

- AWS
  - Config
  - CloudTrail
  - CloudWatch
  - S3 Server Access
- Azure

SaaS

- Box
- Office 365
  - Azure AD
  - Data Loss Prevention (DLP)
  - Exchange
  - Message Tracking
  - SharePoint
  - Teams
- Salesforce

Cloud Security Solutions

- Carbon Black Defense
- Cisco Cloudlock
- Cisco Email Security & Web Security
- Cisco Umbrella
- Cradlepoint ECM
- Crowdstrike Falconhost
- CyberArk
- Cylance
- Netskope
- Okta
- Palo Alto Open Application Framework
- Qualys
- Sailpoint
- SentinelOne
- Skyhigh
- Tenable.io
- Zscaler