Joint Solution Brief

LogRhythm

Okta v3

Combining LogRhythm SIEM with Okta's Identity Cloud to deliver a robust identity monitoring solution

Benefits

- Engage defense tools to work with other network inspection technologies to detect and stop network threats and unauthorized network access
- Collect authentication data from across the enterprise to supply greater visibility on-prem, in the cloud, and across devices
- Effectively coordinate security and IT functions to remediate user accounts

Solution overview

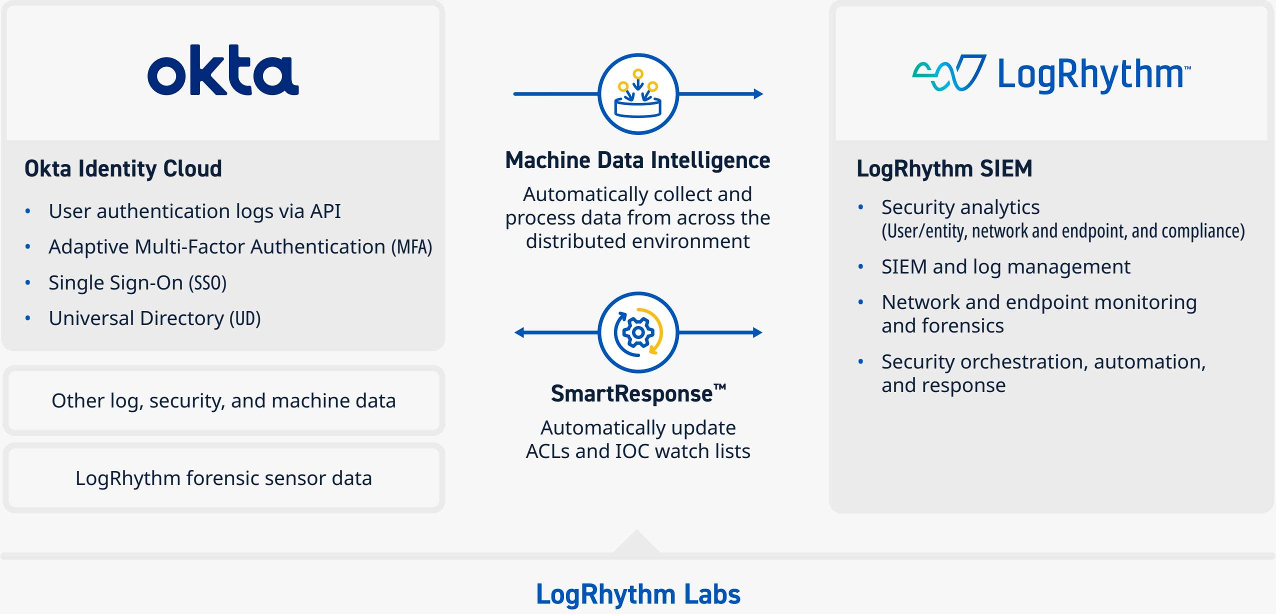
By integrating LogRhythm SIEM with Okta Identity Cloud, security teams can monitor and protect account activity to gain unified, real-time visibility across the organization and identify critical security threats. The solution generates exceptionally detailed forensic evidence, including tracking and reporting on all account access activity. Security analysts and audit teams correlate the information they need to identify and respond to the most critical incidents — those involving compromised credentials or unauthorized access — and meet demanding compliance requirements.

The partnership allows customers to link events triggered by suspicious or malicious credential activity and establish a foundational pillar for organizations seeking to build a Zero Trust architecture. LogRhythm and Okta are tightly integrated, combining the value of best-of-breed identity and access management solution with the threat management capabilities of the LogRhythm SIEM platform. The combined offering empowers customers to identify behavioral anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence.

okta

About LogRhythm and Okta

LogRhythm and Okta work together to help organizations around the globe increase visibility and protect against modern cyberattacks. LogRhythm offers extensive support for and integration across Okta's product portfolio. The combined solution empowers security teams to identify behavioral anomalies, internal, and external threats, and to prioritize their responses based on accurate enterprise security intelligence. LogRhythm and Okta empower security teams to navigate a changing threat landscape with confidence. Together, LogRhythm and Okta are ready to defend.



okta

Okta Identity Cloud

- User authentication logs via API
- Adaptive Multi-Factor Authentication (MFA)
- Single Sign-On (SSO)
- Universal Directory (UD)

Other log, security, and machine data

LogRhythm forensic sensor data

Machine Data Intelligence

Automatically collect and process data from across the distributed environment

SmartResponse™

Automatically update ACLs and IOC watch lists

LogRhythm™

LogRhythm SIEM

- Security analytics (User/entity, network and endpoint, and compliance)
- SIEM and log management
- Network and endpoint monitoring and forensics
- Security orchestration, automation, and response

LogRhythm Labs

Log Collection

LogRhythm SIEM ingests accurate authentication data collected by Okta so customers can use industry-leading enterprise security intelligence and threat management capabilities. The combination helps customers monitor and secure a range of systems and applications throughout IT environments, helping customers respond to security threats based on accurate, relevant, and up-to-date information. Okta leverages the integration with LogRhythm to provide identity and access management to secure workforces and customer identities in cloud, hybrid, and on-prem environments.

LogRhythm ingests real-time authentication data shared by Okta to alarm when suspicious or unauthorized authentication meets preset thresholds/conditions. By sharing normalized authentication data for a given environment, Okta integrates with LogRhythm SIEM to identify anomalies that that can be correlated among identity, network, and endpoint threat data. This allows customers to save time and resources by focusing security personnel on alerts that matter.

How it works

Customers can configure alerts specific to their needs, providing real-time alerting, which is then ingested by LogRhythm SIEM. Based on the customer's configurations and normalized authentication data, LogRhythm can incorporate data from Okta into automated advanced correlation rules to deliver highly focused alerts that identify authentication failures and/or suspicious activity occurring within the environment.

How automated workflows work

To streamline security response workflows, organizations can use LogRhythm SmartResponse™, which is part of LogRhythm's security orchestration, automation, and response (SOAR) solution.

A LogRhythm SmartResponse accelerates response to security threats to minimize damage, eliminating manual intervention by security analysts. This advanced capability is delivered to end users through the LogRhythm SmartResponse for Okta. While LogRhythm has a dedicated engineering team that builds plugins, this is, by nature, an open framework that enables Okta customers to modify or write their own custom integrations.

The LogRhythm SmartResponse for Okta v3 contains multiple actions, which are configured to execute automatically in response to an alarm, or manually through analyst workflow. For example, if a customer's employee is no longer employed, that specific user account can be automatically deactivated to reduce the risk of the credentials being used maliciously. The LogRhythm SmartResponse centralizes functionalities of manual and automated actions between LogRhythm SIEM and Okta.

LogRhythm SmartResponse for the Okta v3 integration

Action	Description	Use Case
Create Configuration File	Execute this action and rerun it before using the other available actions whenever you change the fixed-value parameter	Functionality must run first before other LogRhythm SmartResponse functions can execute
Add User to Group	Adds a user to a group using information such as group name, first name, last name, and email ID	Inserts a user to a group after if an alarm is triggered
Close Session	Closes session for a specified user based on information such as first name, last name, and email ID	Shuts down sessions for a specified user if an alarm triggers
Deactivate User	Deactivates a user based on information such as first name, last name, and user email ID	Disables/deactivates a user account suspected of being compromised until a final determination can be made
Get Group Information	Displays information for a specified group using information such as group name	Returns information about a Group affected by an alarm during investigations
Get User Information	Displays data for a user based on information such as first name, last name, and user email ID	Returns contextual information regarding an affected user account to assist with investigations
Reset Multifactor Authentication	Resets all enrollments for a specified user based on information such as first name, last name, and user email ID	Resets all enrollments for a specified user when an alarm is triggered
Reset Password	Resets a user's password based on information such as first name, last name, and email ID	Changes the password for a suspected compromised account
Search User	Searches for users based on parameters such as user first name, last name, title, status, department, and organization	Seeks out a specified user when an alarm is triggered
Suspend User	Suspends a specified user based on information such as first name, last name, and email ID	Suspends a user in the case of malicious activity; The group and app assignments are retained
Unlock User	Unlocks a specified user based on information such as first name, last name, and email ID	Releases a specified locked user account during an investigation
Unsuspend User	Unsuspends a specified user based on information such as first name, last name, and email ID	Unsuspends any suspended user

For more information, request a LogRhythm demo.
logrhythm.com/demo

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 330 // +65 6222 8110 // +61 2 8019 7185

www.logrhythm.com