Okta Identity Threat Protection and Rubrik

Leverage Rubrik's user-centric visibility into sensitive data access and Okta to automate response to changes

CHALLENGE

Data breaches are inevitable. Traditional cybersecurity has focused largely on preventing threats and safeguarding the perimeter and network infrastructure. However, prevention alone cannot stop 100% of attacks nor data breaches. Defenders need threat context from their security tools combined with *data context*—information on what is being targeted. They cannot understand the true risk without understanding if an attack is targeting high value data and whether it was an isolated or targeted event. Without context, they cannot prioritize and take action against potential threats to that data.

SOLUTION

Rubrik Security Cloud provides visibility into user access to data, and it can automatically monitor for changes to access permissions to sensitive data. Rubrik is the first data security platform vendor of its kind to integrate with Identity Threat Protection with Okta AI, to help customers proactively detect changes to users' sensitive data access levels and automate remediation.

PROACTIVELY KNOW WHEN USER DATA ACCESS RISK LEVELS CHANGE

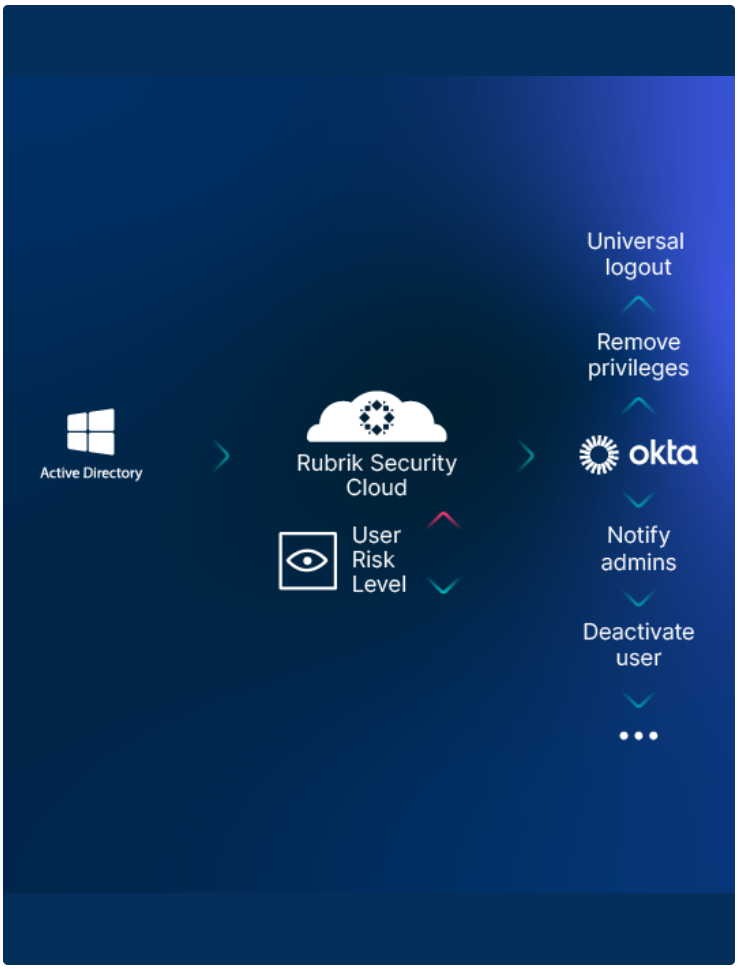
Rubrik automatically monitors for changes to users' access permissions to sensitive data.

UNDERSTAND OVERALL RISK USING DATA AND THREAT CONTEXT FROM MULTIPLE SOURCES

Okta combines data context and user risk change information from Rubrik with its own (1st party) and 3rd party user, device, network and data risk events, to create a risk level.

ENABLE FASTER THREAT RESPONSE AND REMEDIATION

Based on the overall risk level, Okta Identity Threat Protection can take a remediation action on the impacted user.



HOW THE INTEGRATED SOLUTION WORKS

1. Rubrik Security Cloud offers a capability called User Intelligence where we assign risk levels (high, medium, low, none) based on the sensitivity of data. We understand user access to sensitive data and track user risk over time (e.g. permission changes, AD group level changes, and access to certain data that elevates their risk level).

2. User Intelligence automatically tracks changes to a specific user's risk level. If a user's risk level changes, the Rubrik Security Cloud (transmitter) sends this information to Okta (receiver) using the Shared Signals Framework. Some examples are below, but it would be any change in the risk level.

    a. None to something higher (Low, Medium or High)

    b. High to something lower (Medium, Low, None)

    c. Low to None

3. Okta uses the Shared Signals Framework to receive security-related events and other data-subject signals from third-party security vendors. Okta combines the incoming Rubrik user risk level (high, medium, low, none) with signals from other products in the security ecosystem. Okta Identity Threat Protection orchestrates tailored responses based on policy configuration and the assessed user risk levels. For example, a medium risk level may prompt Identity Threat Protection to send notifications to the SIEM or incident response team, while a high risk level may trigger user re-authentication, kill a user session, or even log users out of supported applications with the capability enabled.

HOW WE ARE DIFFERENT

1. Rubrik is the first data security platform vendor of its kind that integrates with Identity Threat Protection, to help customers proactively detect changes to users' sensitive data access risk levels and automate remediation.

2. Rubrik provides ongoing incremental scanning of data and AD changes, and can provide complete visibility across user access to data (for Windows VMs and AD principals).

3. Rubrik's data context combined with threat context from other security tools allows organizations to get a clearer understanding of the risk associated with attacks. This combined context enables defenders to prioritize threats and take appropriate actions to protect high-value data.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

brf-okta-identity-threat-protection-and-rubrik / 20241003