

3 Whys for Okta Recovery



Why do anything?

- ? Responsibility to Back up & Recover Okta Resources**
While Okta promises service availability and reliability of its platform, the customer is responsible for recovering tenant-level configurations, policies, users, groups, and integrations. Native recovery of the customer's Okta tenant could take days.
- ? Risk of Operational Failure**
Okta environments are a complex web of interconnected objects (users, groups, policies, applications), with no native dependency mapping. Restoring objects in the wrong order can cause operational failures or incomplete recoveries due to broken links.
- ? Vulnerability to Tampering & Business Disruption**
Native backups are stored on-platform with no air gap and can be deleted or corrupted. Attackers or malicious insiders can alter configurations, disable MFA, or delete integrations. Okta can't easily reverse these unwanted changes, disrupting business operations for hours or days.
- ? Limited Retention**
Okta does not have a retention standard, which is insufficient for meeting long-term disaster recovery, forensics, or compliance goals.

24 hours¹

Time taken to fail over to a disaster recovery region with Okta

\$6000/min²

Approximate cost of downtime

Why now?

Attackers are increasingly targeting identity systems such as Okta because locking users out of IdPs is an efficient way to disrupt a business.



52%³

Vulnerabilities related to credentials



\$4.67M⁴

Cost per breach when attackers use compromised credentials



90%⁵

Proportion of IT & security leaders believing that identity-driven attacks were the top threats to their organizations

Why Rubrik?



Protect Critical Identity Data with Immutable Backups

Rubrik stores backups in a Rubrik-hosted, airgapped cloud vault and offers unlimited data retention. This keeps your critical identity data protected and tamper-resistant against threats.



Recover in Minutes with Granular Restore

Rubrik's solution delivers granular rollback to quickly undo misconfigurations or deletions of critical Okta objects (users, groups, policies, apps, etc.). This reduces business disruption and downtime.



Boost Operational Resilience with Dependency-Aware Restore

Rubrik automatically sequences objects and their dependencies to restore your Okta environment in the right order. This helps services come back online correctly the first time.



Reduce Tool Sprawl with Unified, Multi-IdP Recovery

Rubrik is the only vendor with a unified, streamlined platform for identity recovery across Okta, Active Directory (AD), and Entra ID. This means you can avoid wasting resources coordinating multiple complex recovery workflows.

Extending Okta's Value with Rubrik

Together, Rubrik and Okta keep identity systems secure and enterprises resilient. While Okta provides service availability and access, Rubrik bridges the tenant-level recovery gap, providing immutable backups and the ability to swiftly restore identity systems to a trusted state. This extends your organization's cyber resilience and recovery across the hybrid identity estate spanning AD, Entra ID, and Okta. With Rubrik, you can help your business remain operational, no matter the threat.

Learn more about
Okta recovery

1: https://support.okta.com/help/s/article/frequently-asked-questions-on-enhanced-disaster-recovery?language=en_US

2: <https://www.isaca.org/resources/news-and-trends/industry-news/2024/centralized-services-and-their-impact-on-business-continuity>

3: <https://www.crowdstrike.com/en-us/resources/reports/global-threat-report-executive-summary-2025/>

4: <https://www.ibm.com/reports/data-breach>

5: <https://zerolabs.rubrik.com/reports/the-identity-crisis>