rubrik

Identity Resilience for Hybrid Environments

Identity is the single point of failure. Make it resilient.

Rubrik Identity Resilience is the industry's only unified platform that recovers identity, removes persistence, and prevents reinfection at machine speed without sacrificing legitimate business change spanning workforce and customer identities, delivering visibility, response, and clean recovery all from one platform.

The challenge

AI-powered attacks are targeting identities across every layer of the environment, and breach is inevitable. Assume breach. Attackers don't hack in anymore; they log in, then move laterally through identity to reach the crown jewels. 83% of privilege escalation incidents involve no software vulnerability at all. Identity compromise is also a leading indicator of what's coming next, with 73% of ransomware victims having had a credential leak or infostealer infection in the year before the attack. Legacy recovery tools take weeks through manual processes, and restoring from backup leaves attacker persistence in place. That risk compounds across a hybrid identity estate, where every IdP recovers differently, and none of them recover fast. Active Directory recovery still means manual runbooks and 20+ error-prone steps, miss one and the process restarts. Entra ID's Recycle Bin only recovers specific soft-deleted objects for 30 days, with no way to reverse policy changes or rebuild broken relationships. Okta has no native backup or recovery at all. Each directory recovers on its own island, on its own timeline, while the business stays down.

The solution

Rubrik Identity Resilience protects hybrid identity environments (Active Directory, Entra ID, Okta) with immutable, air-gapped backups and orchestrated recovery. It delivers unified visibility, detects risky changes, and enables rapid rollback of malicious modifications. It also proactively remediates misconfigurations and overprovisioned privileges through built-in workflows (e.g., removing stale delegations, disabling dormant accounts). With Identity Roll Forward, it surgically reconstructs AD preserving legitimate changes like onboarding/offboarding while reversing unauthorized attacker modifications, cutting recovery to hours.

> **"Clean recovery isn't just about restoring data—it's about restoring trust. Unverified identities hand the keys back to the adversary."**
>
> **Cory West, CTO, Piper Sandler**

Key benefits

- Recover any IdP, AD, Entra ID, or Okta, from one platform, spanning workforce and customer identities
- Cut cyber recovery time from days to hours
- Erase attacker footholds, not your work
- Always know your last clean, recoverable state
- Revert at the speed of AI-driven attacks, automatically
- Lower total cost than stitching together point solutions per identity provider
- Stay audit-ready with built-in compliance reporting



The Rubrik Security Cloud console: unified policy violations, identity insights, and protection status across AD, Entra ID, and Okta.

Key capabilities

Persistence removal

Leverage third party risk signals and Rubrik intelligence to identify what's clean. Recover and rebuild to clean and current, safely roll forward legitimate changes and eliminate persistence.

- **Zero Trust, Natively Immutable Backup:** Physically isolated backups protected by quorum authorization, MFA, and TOTP, with unlimited retention.
- **Entra Clean Roll Back and Cross-Tenant Recovery:** Roll back unauthorized Entra ID changes without a disruptive full-tenant restore, or instantly fail over into a standby, uncompromised tenant when the primary environment is locked out.
- **Entra Governance Recovery:** Restore Identity Governance configurations, Enterprise Apps, App Registrations, service principals, and Conditional Access policies, not just the directory itself to a known-good state.
- **User-Defined Auto-Rollback with Roll Forward:** Auto-revert unauthorized AD and Group Policy changes, then triage change by risk - safe, suspicious, harmful reapplying only what's authorized to remove persistence.
- **Entra Intune Recovery:** Protect Microsoft Intune policies alongside Entra ID because conditional access relies on Intune's device state. A restored Entra tenant stays broken if Intune is wiped or corrupted.
- **SLA-Driven Backup Governance:** Define and enforce backup frequency, retention, replication, and archival policies at the forest level, with per-domain-controller overrides.
- **AD Forest Recovery, Vetted and Identity-First Recovery:** AppFlows-enabled auto-provisioning of clean infrastructure in an Isolated Recovery Environment, prioritizing identity so dependent systems come back in order, with every recovery candidate checked against threat intelligence including the Google Threat Intelligence Feed.

Preemptive recovery

Continuously monitor identity health, expose vulnerabilities and contextualize every failure or misconfig. Always know your clean state, revert rapidly with automated workflows to match the speed of AI-driven attacks.

- **Activity Classification for HRIS and IGA Tools:** Auto-classify changes from trusted sources like Workday and IGA platforms, filtering legitimate activity out of the alert queue.
- **Microsoft Defender and CrowdStrike Integrations:** Closed-loop response from detection to clean recovery. Defender and CrowdStrike identify and contain, Rubrik correlates and recovers.
- **Clean Point of Recovery Detection & Proactive Vulnerability Scanning:** Auto-pinpoint the last known-good state by comparing snapshots at the attribute level, while continuously scanning for risks like weak-password global admins or dormant super-admins, with forensic rewind on any compromised identity's actions.
- **User-Defined Alerts and Policies with IdP Access Analysis and Impact:** Configure custom detection policies across every IdP and quantify the blast radius of privileged identities before they're exploited.
- **Sign-in Logs Tracking with Compliance-Ready Reporting:** Sign-in activity auto-ingests into the immutable Rubrik Security Cloud, backed by audit-ready activity and inventory reports.

Unify identity resilience

Protect and recover workforce and customer identities in one platform powered by Rubrik AI, and eliminate manual operations.

- **One SaaS-Based Console for Every IdP:** Consolidate your entire hybrid identity estate - AD, Entra ID, and Okta into a single console, eliminating the blind spots and tool sprawl of legacy AD tools and siloed SaaS point solutions.
- **Full-Fidelity Inventory:** Get a complete inventory of Okta users, groups, and relationships, unified with AD and Entra in one view.

Try Now >

SAFE HARBOR

Any unreleased services or features referenced on this page are not currently available and may not be made generally available on time or at all, as may be determined in our sole discretion. Any such referenced services or features do not represent promises to deliver, commitments, or obligations of Rubrik, Inc. and may not be incorporated into any contract. Customers should make their purchase decisions based upon services and features that are currently generally available.

NOTE

Please speak to Rubrik representatives to confirm the availability and functionality of Rubrik's products and services before making any purchase or renewal decisions.

rubrik

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

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

Rubrik (RBRK), the Security and AI company, operates at the intersection of data protection, cyber resilience and enterprise AI acceleration. The Rubrik Security Cloud platform is designed to deliver robust cyber resilience and recovery including identity resilience to ensure continuous business operations, all on top of secure metadata and data lake. Rubrik's offerings also include Predibase to help further secure and deploy GenAI while delivering exceptional accuracy and efficiency for agentic applications.

For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.

Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.

Identity-Resilience-Hybrid_Solution-Brief_v1.1 / 20260917