



Rubrik Identity Resilience

Roll Forward: Clean *and* Current Recovery for Your Identity Estate

Erase Persistence. Not Progress.

Today, [82%](#) of breaches use stolen credentials rather than malware, meaning attackers log in, not break in. They blend into normal authentication traffic and plant persistence mechanisms that traditional backups, unable to separate malicious changes from legitimate modifications, unwittingly restore. Security teams are stuck in a paradox: wipe months of valid work or stay compromised. A full rebuild implies:

- **Massive Data Loss:** Rolling back wipes legitimate changes made since the snapshot: new hires, offboarding, password resets, group membership changes, and application syncs are erased.
- **Post-Restore Debt:** Even a successful restore leaves admins with weeks or months of manual re-entry to reintroduce everything the rollback erased.

Roll Forward with a Better Way: Remove Attacker Persistence. Keep Business Progress.

Rubrik's Identity Roll Forward restores your IdP to a known clean state, then re-applies legitimate changes—such as new hires, password resets, group updates, DNS changes—automatically. That way, your systems are returned to clean *and* current in hours, not months. You lose nothing and remove attacker persistence.

The Roll Forward Difference

Detect and remove the changes that constitute attacker persistence, so a clean recovery is actually clean, persistence-free, and constitutes a current directory state.

Roll Forward in 3 Steps

STEP 01

Restore to a Trusted Baseline

Rubrik's Threat Hunting and Threat Monitoring scan backups for known IoCs. This helps you pinpoint a clean snapshot to recover. Rubrik restores your IdP to this clean baseline.

STEP 02

Analyze Identity Drift

After a full restore, Rubrik generates a comprehensive Diff Table that compares the current state against the clean state to identify changes made during compromise. Using signals from the Identity Intelligence Fabric [ITDR (CrowdStrike and Microsoft Defender for Identity), HRIS (Workday), and IGA (Sailpoint)], Rubrik automatically labels each change as safe, harmful, or unclassified.

STEP 03

Interactive Merge

The admin reviews the triaged changes and selects wanted changes to reapply. Rubrik pushes these changes into the live environment.

