



Intelligent Roll Forward Rubrik Identity Resilience

REMOVE PERSISTENCE. RECLAIM CONTROL. BRIDGE TO AI.

Today, the “SOS” from leadership has shifted from ransomware to Identity and AI. Attackers are no longer just deploying malware; 82% of detections are now malware-free because threat actors are stealing credentials and logging in. When your Identity Provider (IdP) is compromised, you face a recovery paradox: roll back to a “clean” state from weeks or months ago and lose all business progress, or stay in a “dirty” state where the attacker still has a backdoor.

Rubrik Identity Resilience introduces a third way: Intelligent Roll Forward.

THE PROBLEM: THE “SLEDGEHAMMER” REBUILD

Standard identity incident response has reached a breaking point. When an IdP like Active Directory or Entra ID is breached, organizations are often forced into a “Sledgehammer” rebuild—recovering the entire environment to a pre-compromise version to ensure the attacker is gone.

Massive Data Loss

Rolling back wipes out legitimate business progress, including offboarding, new hires, password resets, and critical application syncs.

Operational Paralysis

Full rebuilds are so destructive and time consuming that many organizations avoid them, leaving persistence mechanisms (backdoors) in place.

Post-Restore Debt

Admins face weeks of manual “re-entry” to fix everything the restore broke.

THE SOLUTION: INTELLIGENT ROLL FORWARD

Rubrik’s Intelligent Roll Forward capability (currently in Research Preview) allows you to recover at the speed of business by keeping the “good” changes while killing the “bad.”

Remove Persistence:

Eliminate the “Identity Gap” by purging attacker backdoors without a manual, weeks-long forest rebuild.

Merge Engine:

The industry’s only solution that re-applies authorized business changes to a clean base, preventing “Identity Amnesia.”

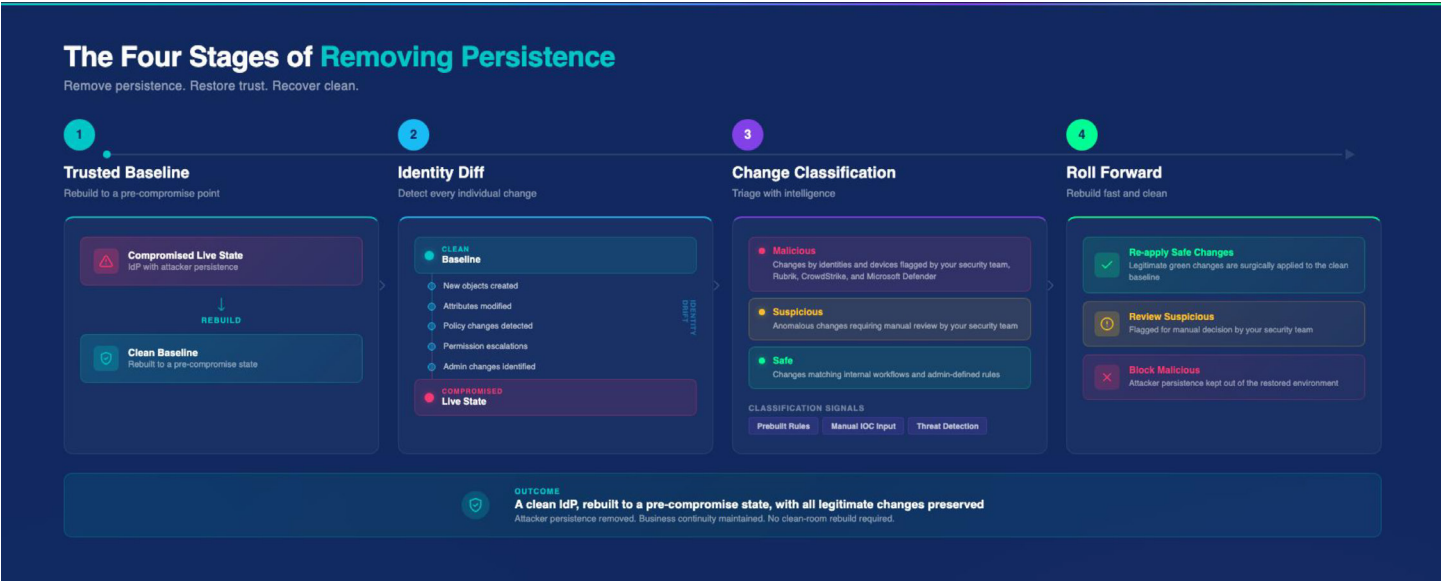
XDR & ITSM Integration:

Automatically label changes as Red if the author has an active alert in CrowdStrike or Microsoft Defender, or Green if they match an approved ServiceNow or Jira ticket.

Behavioral Clean-Point Recommendation:
Leverage behavioral analytics to identify the exact moment identity behavior deviated from the baseline, suggesting a trusted snapshot based on evidence rather than guesswork.

Downstream Re-Synchronization:
Ensure the restored IdP remains the “Source of Truth” for your entire SaaS stack (Salesforce, AWS, etc.), preventing a cascade of authentication failures.

HOW IT WORKS



RUBRIK IDENTITY RESILIENCE VS. LEGACY APPROACHES

FEATURE	RUBRIK IDENTITY RESILIENCE	LEGACY APPROACHES
RECOVERY STRATEGY	✔ Active: Intelligent Roll Forward	✘ Passive: Manual, blind rollback
DATA INTEGRITY	✔ Keeps “Good” while killing “Bad”	✘ All-or-nothing (lose weeks of data)
CLEAN POINT	✔ Evidence-based recommendation	✘ “Safe guess” or detection-only
BUSINESS IMPACT	✔ >80% RTO Reduction	✘ Weeks of manual forensic audit



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

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

Rubrik (NYSE: 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.