rubrik

REDUCE IDENTITY SYSTEM RTO BY 86%

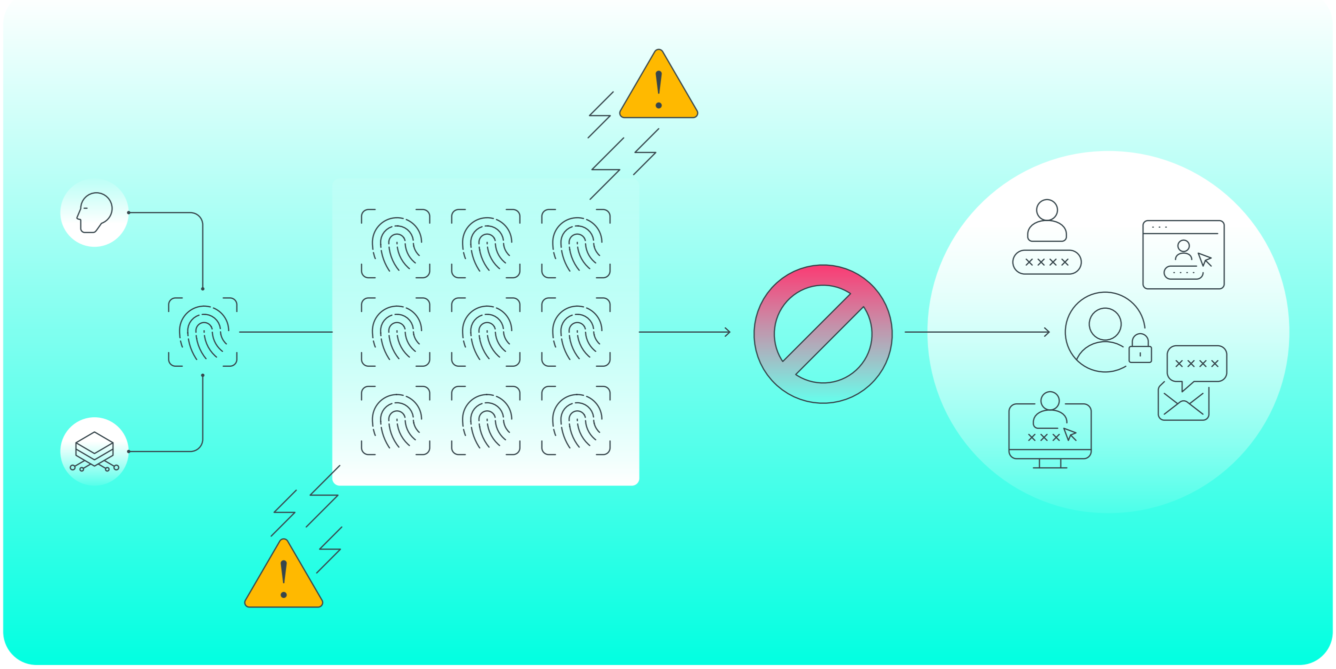
HOW TO GET BUSINESS BACK ON TRACK IN HOURS, NOT WEEKS

Contents

Your Attack Surface is Exposed: The Identity Protection Imperative

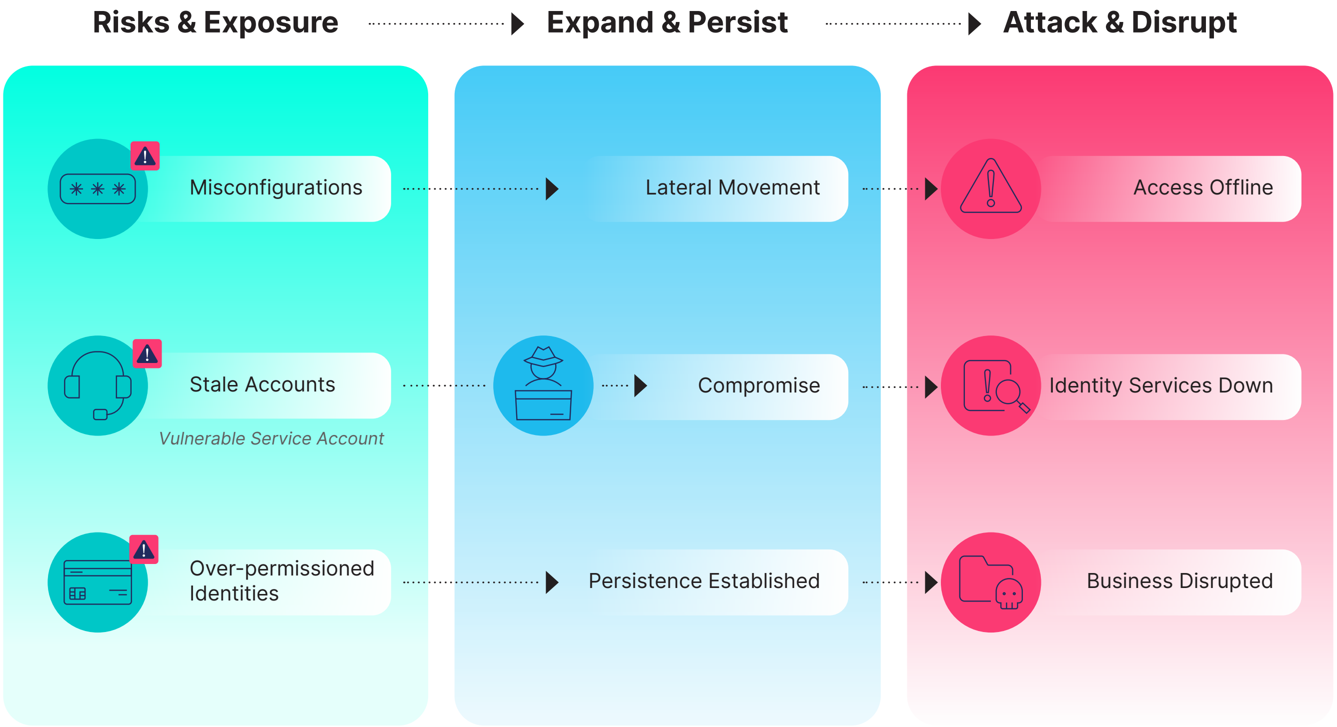
Identity is the security perimeter of the modern enterprise. However, fragmentation and manual recovery make identity your single greatest point of operational risk. After all, critical identity infrastructure, such as Active Directory (AD), Entra ID, and Okta, forms the backbone of access to your organization’s vital applications and data.

If you lose these systems, you may be locked out. Applications may be as good as dead. Data is locked. You have multiple exposed IAM systems, yet no unified control. You have multiple identities to manage, yet no single-pane-of-glass visibility. System access is compromised, but you don’t have a log of exactly what’s happening.



Worse still, attackers gain unfettered access. They steal data, create backdoors, and establish long-term persistence.

Anatomy of an Identity Attack



Risks & Exposure → Expand & Persist → Attack & Disrupt

Risks & Exposure:
- Misconfigurations
- Stale Accounts

  Vulnerable Service Account
- Over-permissioned Identities

Expand & Persist:
- Lateral Movement
- Compromise
- Persistence Established

Attack & Disrupt:
- Access Offline
- Identity Services Down
- Business Disrupted

Just like that, your entire business is at a standstill.

So what do you do in such a situation?

You already know that you need to start your recovery process, but do you know how? When did you last test your identity recovery process, and how long did recovery take? Many organizations struggle to back up and recover identity systems. Your teams might spend weeks manually sorting through screenshots of pre-attack identity systems, or documentation and change control logs. You likely take manual steps to restore IAM systems. This labor-intensive, error-prone process prolongs downtime and increases the risk of incomplete restores. Without automated solutions, extended downtime is guaranteed.

Teams waste weeks manually sorting through screenshots of pre-attack infrastructure. Manually logging every step. Painstakingly restoring access. This is how organizations guarantee failure.

In addition, your current native backup strategy guarantees weeks of downtime, not hours, when AD and Entra ID are compromised simultaneously. After all, in a hybrid identity infrastructure configuration, you must treat AD and Entra ID as a single entity. This is a large part of why separate point solutions for recovery won't work and mean weeks of downtime. The weeks-long downtime could cost your company over $3 million in *avoidable* post-breach costs, and will drastically increase your risk of a denied cyber insurance claim due to re-infection.

$4.67M

Average cost of breaches involving compromised credentials

$1.91M

Average cost of recovery

100 DAYS

How long it took to recover

But know that it's not all doom and gloom! In fact, firms that have a robust breach management plan can save more than $4 million in data breach costs.

In addition, automation is one of the most impactful investments to reduce the impact of breaches. The reality is that identity attacks are inevitable, but irreversible damage, business disruption, and revenue loss are not. With an automated solution like Rubrik Identity Recovery, you can significantly reduce your risk of incurring very avoidable losses after a compromise, and get back to business in hours, not weeks. In fact, companies that use automation save between $1.9 million to $2.2 million in costs.

We've talked about the current state of identity attacks and illustrated that you can recover in mere hours.

Now let's go deeper

What would happen if an organization that relies on a hybrid AD and Entra ID infrastructure faced a scorched earth scenario?

What are the hidden costs nobody told you about, and how would your organization handle them?

Scorched Earth: What Happens When Identity Infrastructure is Compromised and Everything Breaks?

A scorched earth (or worst-case) scenario involves total identity compromise. The attacker compromises on-premises AD and cloud Entra ID simultaneously.

The worst outcome? Destroyed IAM systems and a double extortion demand.

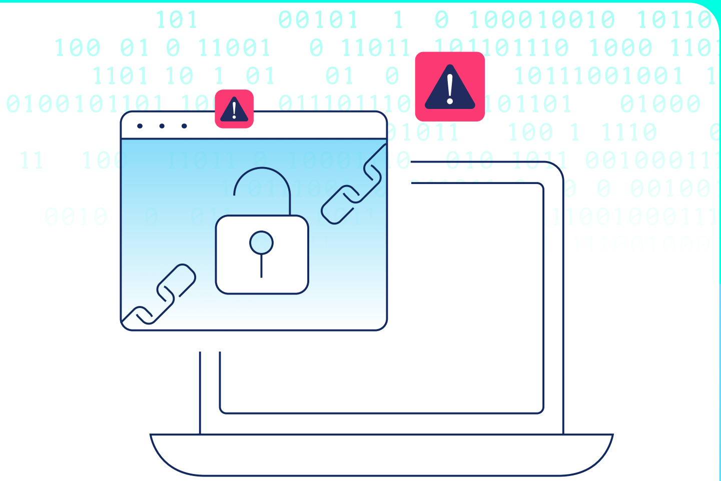
Imagine a Fintech firm running on a hybrid AD and Entra ID environment for all users and applications.

The attack begins: the attackers use spear phishing. They compromise an IT task worker and escalate privileges to Domain Admin, pivot from Domain Admin to Entra, create a Global Admin backdoor to establish persistence, and exfiltrate sensitive financial and healthcare data.

Next, the attackers delete Azure and M365 backups. This means that not only are you unable to recover your identity services, but your applications and data are lost too!

The final blow is ransomware.

Did you know that Microsoft reported that ransomware and extortion drive 52% of attacks?



All your systems can be obliterated, so you seriously consider paying the ransom.

The result is total paralysis and a double-extortion demand: one ransom for the encrypted on-premises systems, and a second, larger ransom to prevent the leak of the stolen cloud data.

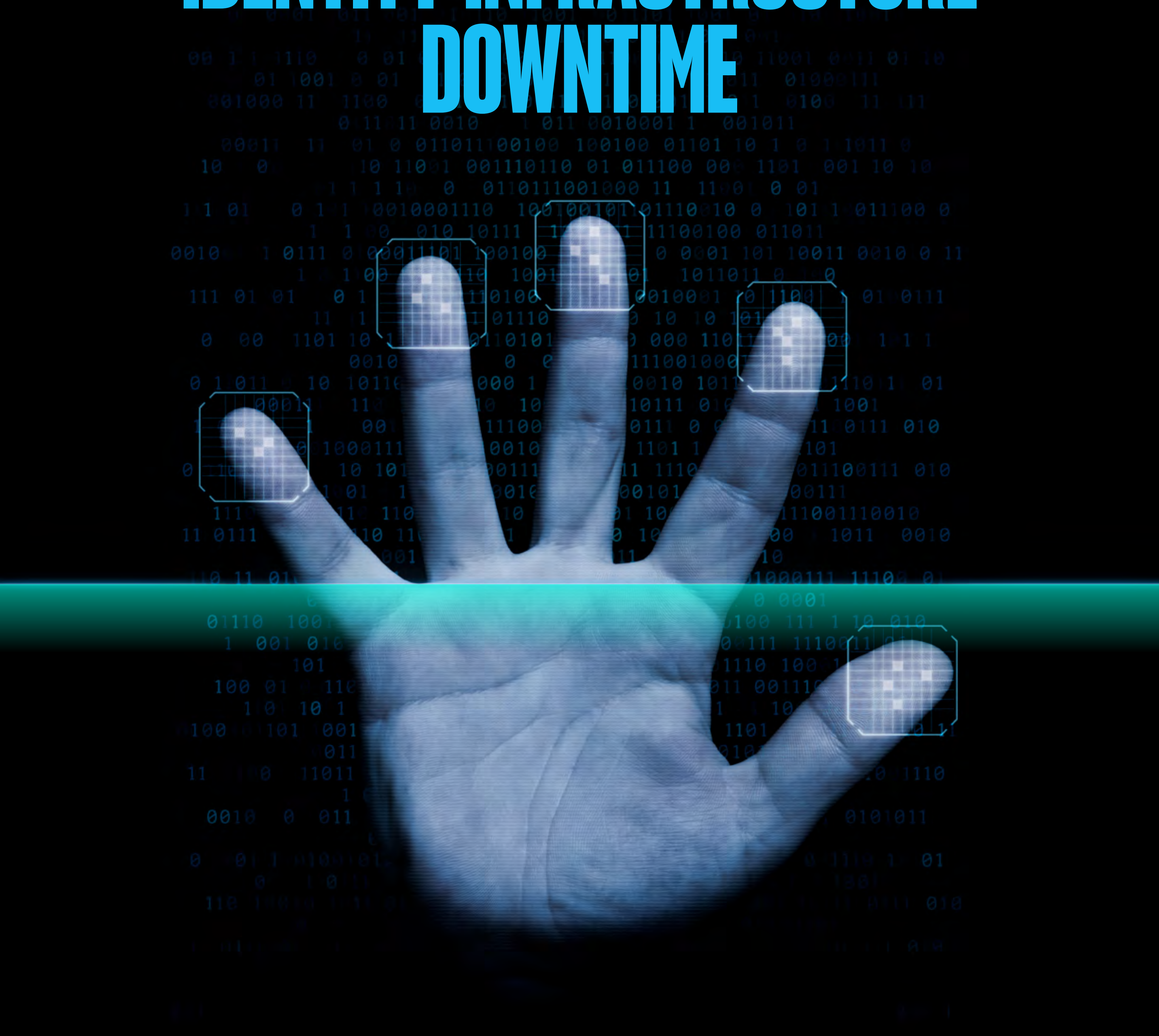
This is the catastrophe, and it is happening now.

You'll realize that the immediate business impacts of relying on a weeks-long, complex recovery are obvious: operational downtime leading to lost revenue and a potential ransom payment. You'll also face irreversible data loss and compliance consequences.

But these are just the tip of the iceberg!

Next, let's explore the hidden costs of identity infrastructure downtime.

The Top 5 Hidden Costs of IDENTITY INFRASTRUCTURE DOWNTIME



When dealing with a scorched earth scenario, the cumulative hidden costs do a lot of damage. Here are the top 5 costs you may never have thought about.

1

Revenue Loss > Ransom Demand

Imagine this: Your on-premises and cloud identity systems are down. All core business functions stop. This means immediate, sustained revenue loss. This loss dwarfs the ransom demand.

Worse, paying the ransom is not a guarantee; if the attackers go back on their word, recovery may never happen.

THE BOTTOM LINE FOR THE CISO

Automated identity recovery will go a long way in securing your identity infrastructure so that your identities and data won't be held hostage in the first place.

2

Complex, Error Prone Recovery Processes

Recovering identity systems is a long-winded, highly technical process in which a single misstep can send you back to the beginning. If you pair technical debt (think about all the undocumented configurations and deviations from default deployments!) with real-world complications, you have a perfect storm.

THE BOTTOM LINE FOR THE CISO

Eliminate this costly technical debt and the potential risk of re-compromise by using an automated recovery solution. The ability to restore clean, known-good environments ensures that you don't accidentally leave behind dangerous, temporary assets to haunt your infrastructure.

3

The Regulatory Fallout

Compromised PHI, PII, and financial data triggers severe non-compliance penalties. Think about the massive impact that HIPAA, GDPR, and PCI DSS can have for your business.

THE BOTTOM LINE FOR THE CISO

After a compromise occurs, you likely need to file a report with relevant authorities. To do this, you'll need to know exactly what happened during the breach, when, and the changes made. You can get this information with an immutable audit log. This helps to stay on top of SOC 2, GDPR, and other compliances.

4

The Increased Cyber Insurance Trap

Just like in the aftermath of a moderate car accident, a major breach triggers a premium spike in cyber insurance. Future coverage becomes prohibitively expensive.

Worse still, the insurer might investigate. If they find a failure to maintain basic security hygiene, the insurance company will deny the claim. In fact, 63% of claims are partially or fully denied.

THE BOTTOM LINE FOR THE CISO

If you don't want exposure to millions in recovery costs out-of-pocket, consider an identity recovery tool that will guard against this.

5

Loss of Business Continuity and Reputational Damage

Identity compromise is a public failure that shatters market confidence, leading to cratering stocks, customer migration, and a decline in market capitalization.

The business suffers service interruptions that trigger contractual penalties. Breach notification costs alone can hit $390,000. Lucrative client and partner relationships end, accelerating very avoidable financial and reputational damage.

THE BOTTOM LINE FOR THE CISO

Automated recovery is a strategic investment that protects your company's stock and reputation by minimizing the operational and financial fallout. Automation helps you retain critical security staff by relieving them of manual cleanup, allowing teams to focus on innovation instead. This investment allows your organization to thrive, not just survive!

It is possible to avoid these hidden and not-so-hidden costs altogether and recover in hours, not weeks, saving even as much as $50M in potential impact. Rubrik can help you do this.

Let's discuss a 5-step action plan that your teams can follow to rebuild your organization's hybrid identity infrastructure.

A 5-Step Action Plan for Your Teams

REBUILD A HYBRID AD + ENTRA ID ENVIRONMENT WITH RUBRIK

Faster, Easier Recovery with Rubrik

Native recovery tools are not designed to handle fast, automated recovery that guarantees your critical identities and data are restored.

Microsoft’s documentation: 150+ pages, 20+ manual steps per domain. Entra ID Recycle Bin? Only 30 days of soft-deleted objects. With native tools, you’re facing weeks of downtime and massive reinfection risk.

A third-party solution like Rubrik can collapse recovery from weeks to hours, shortening the data breach cycle. In fact, shorter yet still days-long data breach cycles were associated with cost savings of 29%.

Imagine how much you would save if you could cut recovery to hours!

Rubrik vs. Native Tooling: The Options between which to Choose

Features	Rubrik	Native Tooling (Recycle Bin)
Backup Immutability	**Yes** (Logically air-gapped, ransomware-proof)	**No** (Backups exist within the same production tenant)
Recovery Scope	**Comprehensive** AD Forests, Entra ID Users, Conditional Access Policies, App Registrations	**Limited** AD only via native Windows Server tools; Entra ID only soft-deleted objects (30-day limit)
Hybrid Recovery	**Orchestrated** Single workflow restores AD first, then automatically restores hybrid objects and their attributes to Entra ID.	**Manual & Complex** Requires multiple disjointed tools and painstaking manual steps to restore attributes.
Reinfection Risk	**Low** Utilizes clean room recovery to restore your environment to a known-good state.	**High** No built-in validation for malware or persistent threats in the backup.

YOUR 5-STEP HYBRID IDENTITY RECOVERY ACTION PLAN with Rubrik

Step 01

Isolate & Assess

Stop the attack. Find a clean recovery point.

Launch Rubrik's automated AD & Entra ID Recovery. Scan thousands of point-in-time snapshots in 60 seconds for IOCs. Swiftly identify your clean recovery snapshot.

Step 02

Recover AD

Restore the on-premises AD forest without reintroducing threats.

Execute Active Directory Forest Recovery (ADFR) using the clean snapshot you identified in Step 1. If you see malicious changes, use Rubrik's real-time monitoring, logging, & rollback features to surgically revert those items.

Step 03

Recover Entra Connect

Recover Entra Connect to re-establish the AD & Entra ID connection.

Use Rubrik to recover the Entra Connect server from a full, immutable, logically airgapped system backup.

Fully redeploying Entra Connect should be a last resort because of the manual reconfiguration required, and also since any state from the metaverse database will be lost. You'll need a full resync, which can take days in large, complex environments.

Step 04

Sync Changes to Entra ID

Link the recovered AD with Entra ID.

With connectivity between AD and Entra ID re-established, use Rubrik for Entra ID cross-tenant hybrid orchestration. This recovers critical Entra ID components like enterprise applications, application registrations, and conditional access policies, maintaining vital object interrelationships.

Entra Connect is a Tier-0 asset. If compromised, it's the attacker's bridge from AD to the cloud. You need a third-party solution to recover in hours, not weeks. Make it Rubrik.

Step 05

Verify and Test

Verify the restored environment to ensure it's clean and threat-free.

With Rubrik, deploy the recovered AD and orchestrated Entra ID into a clean room recovery environment. Validate that the identity infrastructure is malware-free before connecting to production. Verify that you can successfully authenticate via AD and synchronize to Entra ID.

Post-mortem

No Hiding from an Immutable Audit Log!

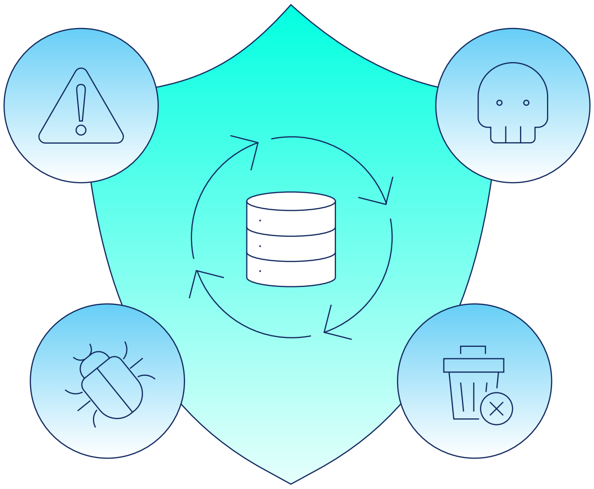
After you restore business continuity (congratulations!), don't forget to conduct a post-mortem.

As part of the post-mortem, a reliable audit trail must establish the attack path, pinpoint compromise times, and satisfy regulatory requirements. But traditional audit trails may be compromised or incomplete.

Rubrik's immutable audit logs will fix this problem. The logs will help you review every critical identity change across AD and Entra ID with actor attribution. This streamlines forensics and helps you prove a robust security posture to avoid increased cyber insurance premiums and denied claims.

Act Now to Secure your Identity Infrastructure

The time to secure your recovery is before the breach; don't wait for the attack that paralyzes your operations and destroys your data. If you are not certain you can quickly recover both on-premises AD and cloud Entra ID in the event of a cyberattack, your business is exposed. Challenge us: Schedule a live validation session to see how Rubrik can reduce your full hybrid identity recovery RTO from days to hours. As a bonus, discover how our immutable audit log will help you during your next regulatory audit.



Any unreleased services or features referenced in this document 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.

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

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

Reduce-Identity-System-RTO-by-86%_How-to-get-business-back-on-track-in-hours-not-weeks / 20251127