Rubrik Identity Recovery

Keep Identity Services Resilient Against Cyber Attacks

Microsoft Active Directory (AD) is the backbone of identity for organizations worldwide, providing authentication for various workloads as well as DNS, DHCP, public key infrastructure, and more. However, its ubiquity makes it a primary target for attackers, as shown in recent stats: 71% YoY increase in cyberattacks targeting identity services between 2022 and 2023[2] and 80% of cyber attack exposures linked to AD in 2023.[1] Increasingly, cybercriminals have shifted from exploiting software vulnerabilities to leveraging compromised identities to access business applications and data.

If AD is destroyed, recovery is often complex and time-consuming—especially in large environments requiring the restoration of multiple domains. The distributed nature of Active Directory, while designed for redundancy to provide high availability, complicates attack remediation. Changes made to a single object replicate globally, making clean recovery difficult. Whether due to misconfigurations, corruption, or cyberattacks, traditional recovery methods are slow, complex, and risk reintroducing malware or vulnerabilities. Point solutions lack native immutability and assume a functioning production environment exists. However, in many cases, organizations need to recover to a clean environment and restore their identity systems to a trusted point in time.

Today, identity is no longer confined to on-prem environments. More and more organizations now operate in hybrid identity infrastructures, leveraging both AD and Entra ID for authentication. As Entra ID adoption grows, securing and recovering both on-prem and cloud-based identity systems is critical to operational resilience.

Hybrid Identity Recovery for Active Directory and Entra ID

A Zero Trust approach underpins Rubrik's protection model, with immutable backups, logical air gaps, encryption, and access controls ensuring that backups remain secure from ransomware and insider threats. With this, Rubrik ensures identity systems remain protected, available, and recoverable at all times. Rubrik Security Cloud automatically discovers and protects Active Directory and Entra ID, supporting recovery at enterprise scale. Organizations can restore entire AD forests, specific domains or domain controllers. Object-level search and recovery streamline the restoration of users, systems, groups, and Group Policy Objects, ensuring minimal downtime and disruption. Rubrik covers hybrid identity infrastructures with the restoration of Entra ID enterprise apps, app registrations and conditional access policies.

AUTOMATED IDENTITY PROTECTION

Continuously discover and protect domain controllers, Entra ID objects and their associated roles and services.

COMPREHENSIVE RECOVERY

Rapidly restore entire forests, trees, domain controllers and Entra ID enterprise apps and app registrations.
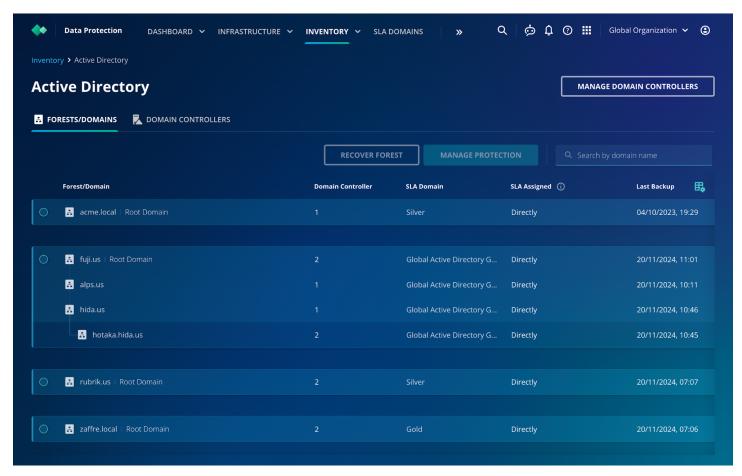
RESILIENT IDENTITY SERVICES

Withstand cyberattacks, malicious insiders and downtime with air-gapped, immutable, access-controlled backups.

1   XM Cyber The State of Exposure Management in 2024
2   IBM 2024 X-Force Threat Intelligence Index

HOW IDENTITY RECOVERY WORKS

Automated Discovery and Protection

Rubrik Security Cloud inventories domains, domain controllers, and automatically links to forest hierarchies, identifying Flexible Single Master Operation (FSMO) roles and critical services like DHCP and DNS. This ensures organizations can quickly assess their environment and prioritize recovery efforts by determining which domain controllers are providing which services. Rubrik Identity Recovery enables organizations to safeguard Active Directory Forests and protect domain controllers locally while leveraging the simplicity of a centralized orchestration engine. With global SLA domain policies, organizations can define and enforce backup frequency, retention, replication, and archival requirements. By default, all participating domain controllers inherit SLAs set at the forest level, but organizations can assign SLAs directly to specific controllers to override global settings as needed.

Rubrik Active Directory Forest Recovery (ADFR)

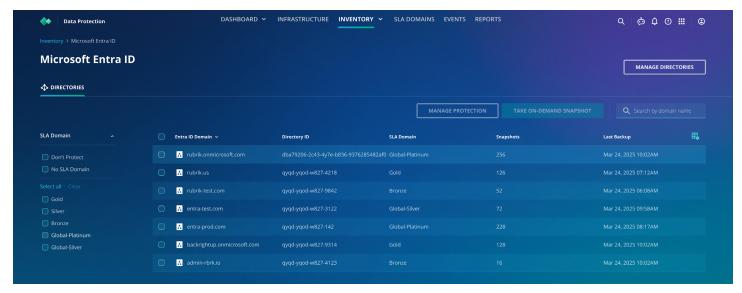## Flexible Recovery Options for Active Directory

Recovering Active Directory in complex environments—especially those with forest root, tree, and child domains—can be an overwhelming challenge, particularly during a cyber incident. Rubrik Security Cloud simplifies this process with a guided, wizard-driven approach that orchestrates full forest recovery to a preferred point in time. By managing Active Directory recovery at both the forest and domain controller levels, Rubrik accelerates the return to business, offering flexible restore options to the same host or alternate environments, including VMs, bare metal, or cloud instances.

For more granular recovery, Rubrik enables object-level search and restoration of users, computers, groups, and Group Policy Objects. Administrators can easily search across backups for a specific point in time, select the desired objects, and let Rubrik handle the rest. More than just restoring objects, *Rubrik preserves critical relationships between them—ensuring attributes and dependencies remain intact without requiring manual intervention.*

Following Microsoft Active Directory best practices, Rubrik leverages wbadmin for application-consistent protection and orchestrates recovery through a simple, five-step wizard. This automation eliminates the tedious process of manually rebuilding object relationships and trusts, providing a faster, more secure path to identity recovery.

Object Comparison & Attribute Recovery

Each object in Active Directory comprises a number of different attributes, both native to Active Directory and those created by extensions to the AD schema. Changes to each attribute can have wide-ranging implications in terms of access to data and applications, so it is important to be able to identify changes over time. Rubrik Identity Recovery can compare an object from a point-in-time snapshot with the current state of the object and its attributes, so that you can easily identify how it has changed, providing the ability to easily recover only selected attributes of that object.

Rubrik Identity Recovery for Entra ID

Entra ID

Entra ID, formerly known as Azure Active Directory, is a cloud-native identity and access management platform with unique recovery challenges. Many organizations rely on the Entra recycle bin for object recovery, but in a cyber incident, there is no guarantee those objects will still be available. To ensure resilience, Rubrik provides a logically air-gapped, immutable backup of Entra ID, allowing organizations to recover identities with confidence.

With Rubrik's intuitive, shopping-cart-style recovery wizard, organizations can easily select specific snapshots and objects to restore, ensuring seamless protection for hybrid environments where Entra Connect synchronizes on-premises AD objects to your Entra Directory. Beyond users, groups, and roles, Rubrik Identity Recovery also safeguards Enterprise Apps and App Registrations, enabling fast recovery of business-critical applications and their service principals to a trusted, known-good state.

Identity Recovery for Cyber Resilience

Without resilient identity services, organizations face prolonged downtime, operational disruption, and heightened security risks. Rubrik Identity Recovery provides fast, orchestrated restoration of Active Directory and Entra ID, ensuring business continuity even after cyber incidents. With an emphasis on security, immutability, and hybrid recovery, Rubrik enables organizations to protect, recover, and strengthen their identity infrastructure against evolving threats on a single platform.