rubrik

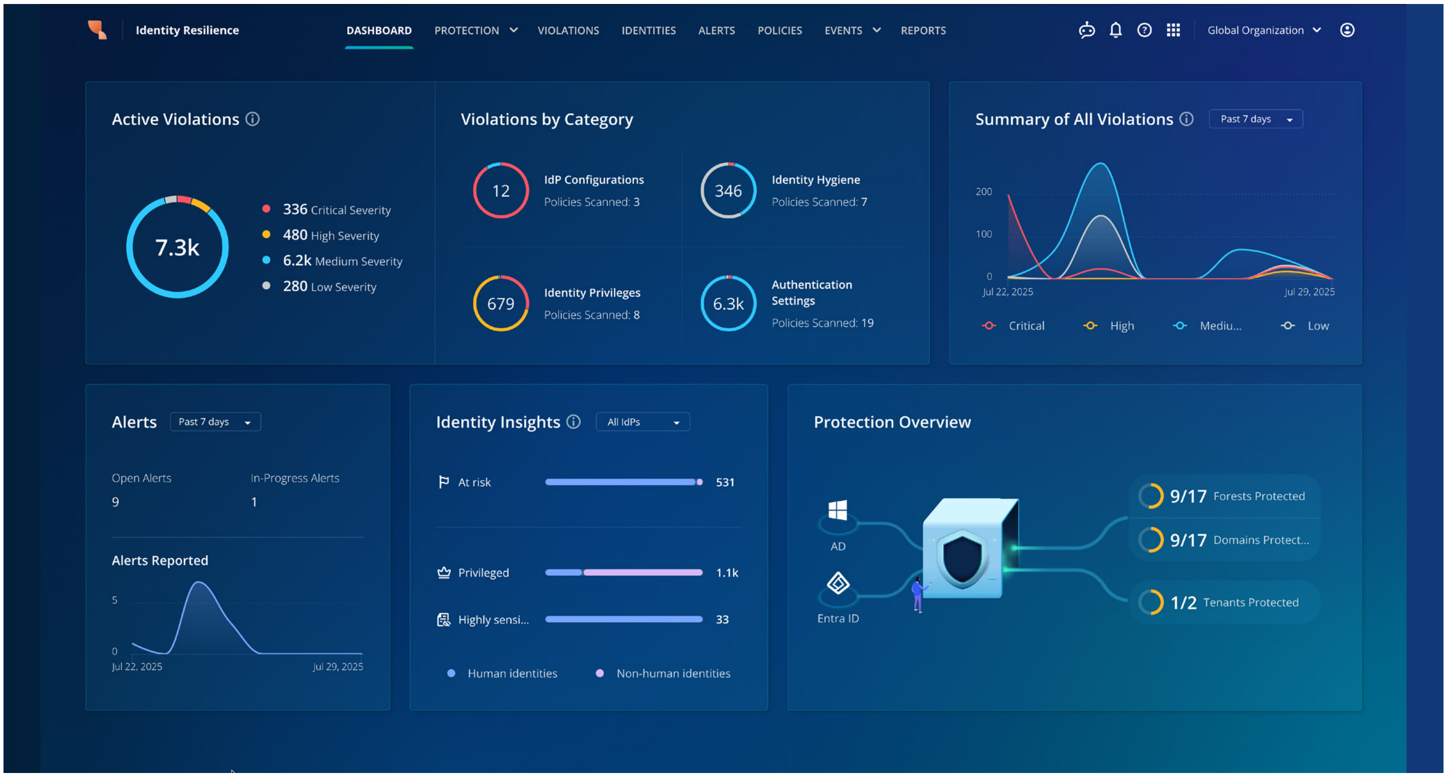
# Rubrik Identity Resilience

## Technical Brief

Your identity infrastructure is under attack.

Rubrik Identity Resilience empowers organizations to protect and recover their identity systems before, during, and after an attack. By bringing visibility, real-time detection, and orchestrated recovery into a single, integrated platform, Rubrik helps organizations remediate risks, rollback critical changes, and recover quickly, keeping your business resilient against identity-based attacks.

Active Directory (AD) and Entra ID form the foundation of enterprise access, yet securing these systems, especially across hybrid and multi-cloud environments, has become increasingly complex. Relying on fragmented tools, scripts, and point-in-time assessments create gaps that leave you vulnerable to identity-based threats. Manual investigation of threats and attempts to identify and rollback the backdoors and weakness left by the attackers may allow adversaries to remain undetected in your environment. Meanwhile, manual recovery processes prolong downtime, putting your business at greater risk.



Identity-based attack vectors dominate the current threat landscape, with over 80% of cyber intrusions leveraging compromised credentials, privilege escalation, or misconfigured access controls to breach systems, propagate laterally, and disrupt business operations. Advanced threat groups such as Scattered Spider specifically exploit these configuration blind spots and gaps in detection to navigate within networks while evading traditional security tools.

A critical challenge stems from the fragmented nature of existing IT security stacks, which often lack integrated, real-time telemetry and cross-platform visibility into identity state and behavior. Furthermore, most solutions do not provide mechanisms for rollback or recovery from unauthorized identity configuration changes or access grant abuse. As a result, identity recovery workflows often rely on manual processes, potentially compromised system backups, or incomplete and mutable audit logs.

Without an integrated, resilient identity security framework combining continuous policy enforcement, tamper-resistant monitoring, and orchestrated recovery capabilities, organizations remain vulnerable to escalating identity-related threats, operational interruptions, and extended breach dwell times.

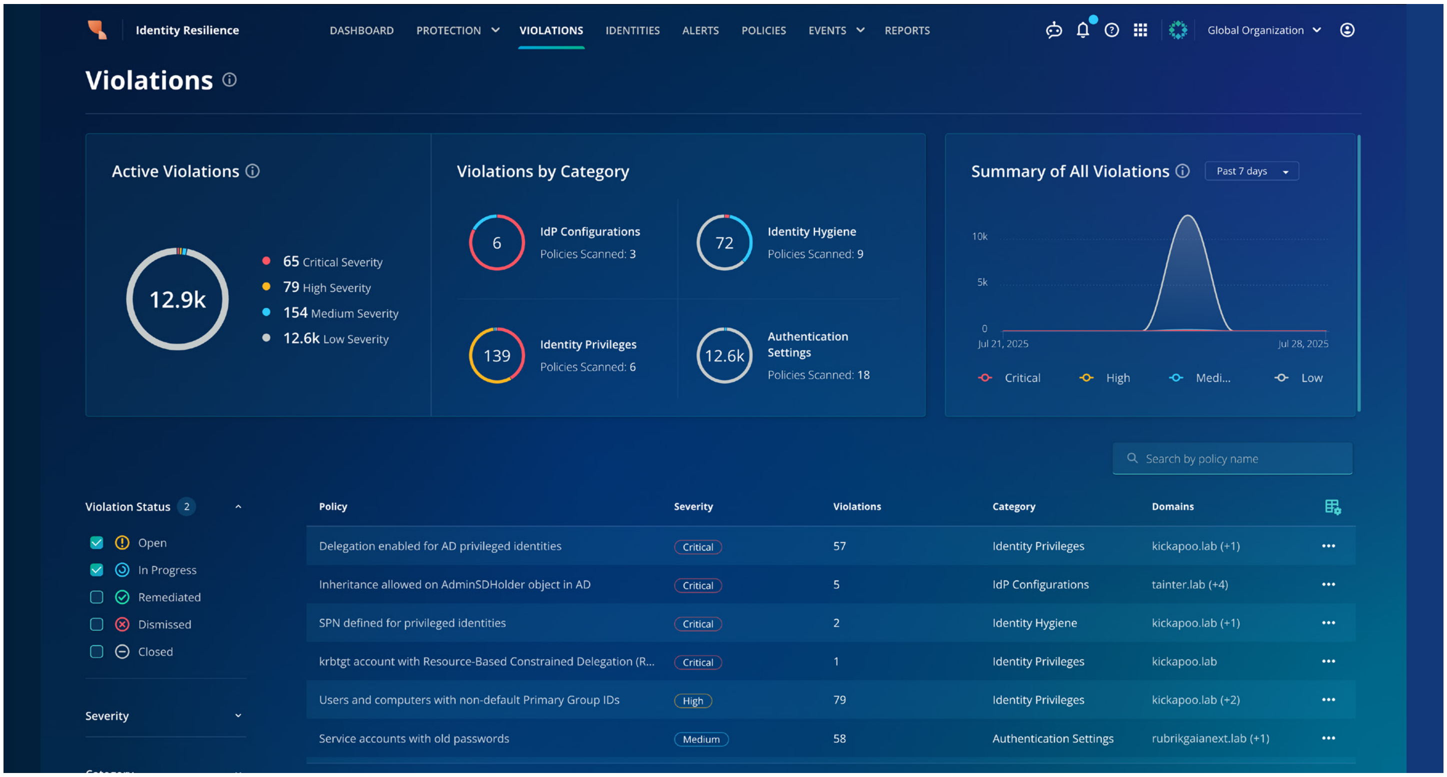
Rubrik Identity Resilience addresses these gaps by delivering comprehensive visibility into the most vulnerable points threats actors exploit. It continuously monitors and detects critical changes, such as those used for lateral movement and privilege escalation, in near real-time, empowering organizations to quickly remediate risks, close exposure gaps and evict bad actors before they can cause more harm.

## UNIFIED IDENTITY INVENTORY

With the growth in use of systems in and across clouds, while many organizations still retain heavy investments in on-premises infrastructure, it is not uncommon for identity systems to be spread across multiple providers. Rubrik Identity Resilience provides a single, unified identity inventory that provides visibility into identities (both human and non-human), and the associated risks and alerts across onboarded IdPs. Additionally, when used in conjunction with Rubrik DSPM, details of sensitive data that an identity has access to are also presented, allowing you to prioritize identities based on not only their privileges in the IdP, but also the degree of sensitive data access they have.

## POLICY-DRIVEN IDENTITY RISK DETECTION

Rubrik Identity Resilience builds out a comprehensive identity inventory, showing all identities across all onboarded IdPs, including both human and non-human identities (NHIs). Once created, the inventory is automatically updated with every snapshot. A powerful policy engine then monitors configuration details, continuously scanning for compliance with defined policies. Identity Resilience ships with many policies out of the box, mapped to well-known security and best-practice frameworks, such as MITRE ATT&CK, D3FEND, OWASP, and ANSSI. These policies are unified across IdPs where relevant. Some examples of these policies are privileged identities with delegation enabled, users with weak or no MFA enforced, and service accounts with old passwords, which might indicate that credentials are not being effectively rotated.



Violations

Active Violations

12.9k

- 65 Critical Severity
- 79 High Severity
- 154 Medium Severity
- 12.6k Low Severity

Violations by Category

| | |
|---|---|
| 6 | IdP Configurations<br>Policies Scanned: 3 |
| 72 | Identity Hygiene<br>Policies Scanned: 9 |
| 139 | Identity Privileges<br>Policies Scanned: 6 |
| 12.6k | Authentication Settings<br>Policies Scanned: 18 |

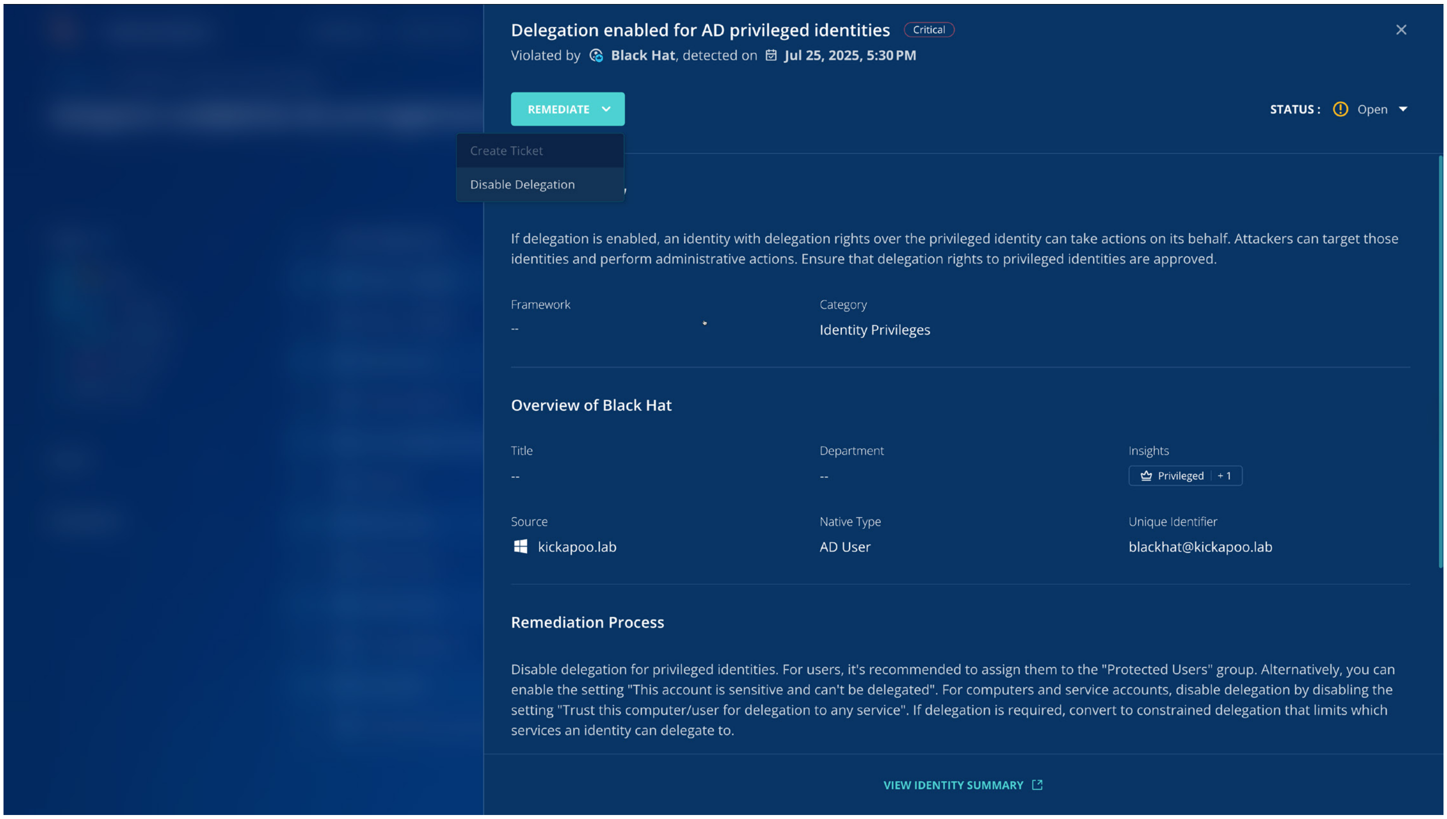
Summary of All Violations

Violation Status 2

☑ Open
☑ In Progress
☐ Remediated
☐ Dismissed
☐ Closed

| Policy | Severity | Violations | Category | Domains |
|---|---|---|---|---|
| Delegation enabled for AD privileged identities | Critical | 57 | Identity Privileges | kickapoo.lab (+1) |
| Inheritance allowed on AdminSDHolder object in AD | Critical | 5 | IdP Configurations | tainter.lab (+4) |
| SPN defined for privileged identities | Critical | 2 | Identity Hygiene | kickapoo.lab (+1) |
| krbtgt account with Resource-Based Constrained Delegation (R... | Critical | 1 | Identity Privileges | kickapoo.lab |
| Users and computers with non-default Primary Group IDs | High | 79 | Identity Privileges | kickapoo.lab (+2) |
| Service accounts with old passwords | Medium | 58 | Authentication Settings | rubrikgaianext.lab (+1) |

Where violations of policy are detected, they are highlighted in the user interface, with options to raise a ticket in an ITSM tool such as ServiceNow, and, where feasible, remediate the violation directly in the IdP. Additionally, security violations can be sent to SIEM and SOAR tools via webhooks, enabling the automated triggering of workflows from these tools.



Delegation enabled for AD privileged identities

Violated by **Black Hat**, detected on **Jul 25, 2025, 5:30 PM**

STATUS : Open

If delegation is enabled, an identity with delegation rights over the privileged identity can take actions on its behalf. Attackers can target those identities and perform administrative actions. Ensure that delegation rights to privileged identities are approved.

Framework: --

Category: Identity Privileges

Overview of Black Hat

Title: --

Department: --

Insights: Privileged +1

Source: kickapoo.lab

Native Type: AD User

Unique Identifier: blackhat@kickapoo.lab

Remediation Process

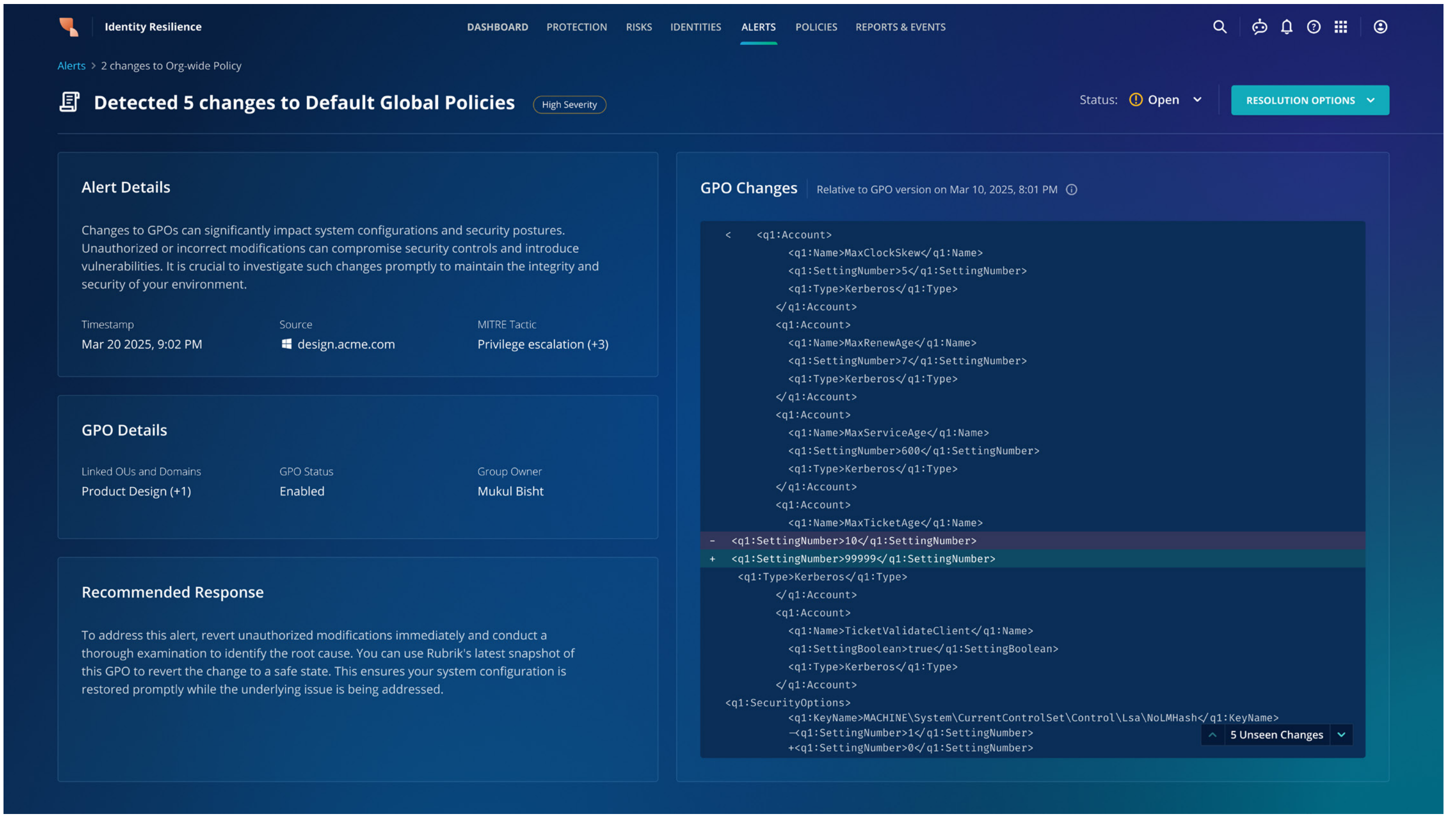
Disable delegation for privileged identities. For users, it's recommended to assign them to the "Protected Users" group. Alternatively, you can enable the setting "This account is sensitive and can't be delegated". For computers and service accounts, disable delegation by disabling the setting "Trust this computer/user for delegation to any service". If delegation is required, convert to constrained delegation that limits which services an identity can delegate to.

## NEAR REAL-TIME MONITORING FOR CRITICAL CHANGES

Some monitoring tools scan the Windows event log or rely on Windows Event Forwarding (WEF) for detecting suspicious activity. Unfortunately, bad actors are aware of this, and they also know that log files can be easily overwritten with any data they prefer or simply cleared when they need to cover their tracks. Without robust event tracking, it can become nearly impossible to detect malicious activities.

Rubrik Identity Resilience continuously monitors Active Directory independently of the Windows event logs. This unique approach is tamper-resistant, making it significantly more difficult for an adversary to remain undetected. Once event data is written from the IdP to the Rubrik platform, it is immutable in the same way as the data backups, assuring the integrity of event data.

Where suspect activity, such as privilege escalation, or the editing of Group Policy Objects (GPOs) is detected, an alert is triggered for triage and remediation.



Detected 5 changes to Default Global Policies

High Severity

Status: Open

RESOLUTION OPTIONS

Alert Details

Changes to GPOs can significantly impact system configurations and security postures. Unauthorized or incorrect modifications can compromise security controls and introduce vulnerabilities. It is crucial to investigate such changes promptly to maintain the integrity and security of your environment.

| Timestamp | Source | MITRE Tactic |
|---|---|---|
| Mar 20 2025, 9:02 PM | design.acme.com | Privilege escalation (+3) |

GPO Details

| Linked OUs and Domains | GPO Status | Group Owner |
|---|---|---|
| Product Design (+1) | Enabled | Mukul Bisht |

Recommended Response

To address this alert, revert unauthorized modifications immediately and conduct a thorough examination to identify the root cause. You can use Rubrik's latest snapshot of this GPO to revert the change to a safe state. This ensures your system configuration is restored promptly while the underlying issue is being addressed.

GPO Changes | Relative to GPO version on Mar 10, 2025, 8:01 PM

```
<    <q1:Account>
         <q1:Name>MaxClockSkew</q1:Name>
         <q1:SettingNumber>5</q1:SettingNumber>
         <q1:Type>Kerberos</q1:Type>
       </q1:Account>
       <q1:Account>
         <q1:Name>MaxRenewAge</q1:Name>
         <q1:SettingNumber>7</q1:SettingNumber>
         <q1:Type>Kerberos</q1:Type>
       </q1:Account>
       <q1:Account>
         <q1:Name>MaxServiceAge</q1:Name>
         <q1:SettingNumber>600</q1:SettingNumber>
         <q1:Type>Kerberos</q1:Type>
       </q1:Account>
       <q1:Account>
         <q1:Name>MaxTicketAge</q1:Name>
-  <q1:SettingNumber>10</q1:SettingNumber>
+  <q1:SettingNumber>99999</q1:SettingNumber>
    <q1:Type>Kerberos</q1:Type>
       </q1:Account>
       <q1:Account>
         <q1:Name>TicketValidateClient</q1:Name>
         <q1:SettingBoolean>true</q1:SettingBoolean>
         <q1:Type>Kerberos</q1:Type>
       </q1:Account>
  <q1:SecurityOptions>
         <q1:KeyName>MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash</q1:KeyName>
         -<q1:SettingNumber>1</q1:SettingNumber>
         +<q1:SettingNumber>0</q1:SettingNumber>
```

5 Unseen Changes

## Alerting and Response

**Near Real-Time Alert Generation:** Suspicious events trigger alerts with detailed context, including the identities of involved parties, timestamps, affected resources, and recommended response actions.

**Integration to ITSM platforms:** Threats and Security Violations can both be triggers to raise a ticket for investigation in an ITSM platform. Out of the box, Rubrik has an API-level integration with ServiceNow ITSM.

**Webhook Integration:** Alerts and events can be sent using Webhooks to SIEM and SOAR tools, where workflows for further triage and remediation can be triggered.

## RECOVERY OF IDENTITY PROVIDERS

While Identity Resilience focuses on reducing risk and detecting suspicious activity to prevent bad actors from taking damaging action, it is clear that a robust strategy is required, including an assume breach mindset. Rubrik Identity Recovery, included with Identity Resilience, provides comprehensive recoverability of Active Directory and Entra ID, including hybrid configurations. By taking this strategic approach, organizations are well-positioned to minimize risk through the proactive management of their identity attack surface, while ensuring they have the ability to recover in the event of an attacker compromising and destroying this critical component of their infrastructure.

## SOLUTION ARCHITECTURE AND DEPLOYMENT CONSIDERATIONS

### Security and Compliance

- Granular RBAC can additionally be used to grant access to only Identity Resilience (with no access to other Rubrik capabilities, for IAM and GRC teams) and vice versa (so that backup admins have no access to Identity features).
- Certified, compliant platform and support team. To learn more about compliance in Rubrik Security Cloud, see https://www.rubrik.com/compliance-program.

- Encryption of data at rest and in transit is enforced, alongside strict role-based access controls (RBAC) for administrators.
- Backup data is immutable once written to the platform, providing assurance of recoverability

### Hybrid Environment Support

- The Rubrik Backup Service is deployed to Domain Controllers to collect AD data (and also take Active Directory backups as required) without exposing sensitive login credentials, or requiring extensive network changes.
- AD event data processed on-cluster within your datacenter, with metadata sent to Rubrik Security Cloud for further processing.
- For Entra ID, onboarding can be done through a single Administrative login to create a service principal (Enterprise App) with the minimum required privileges.
- Security policy definitions and alerts are unified irrespective of location, simplifying governance across on-premises, hybrid, and multi-cloud deployments.
- Active Directory recovery is orchestrated across multiple clusters, so that you can backup locally and recover from a single UI.

### Simple, Global Control Plane

- Award-winning, simple-to-use interface to manage identity and data security posture, plus the protection and recovery of data and identity.
- End-to-end, orchestrated recovery of your critical services, from identity to data, in the event of an attacker being successful.
- Enterprise-grade cyber resilience, trusted by over 4000 customers to protect identity services worldwide.

## PACKAGING

Rubrik has been protecting identities for its customers for several years, with over 4,000 customers trusting Rubrik for their identity services. The chart below details the capabilities provided across the Rubrik portfolio, including Identity Resilience.

| | Rubrik Foundation / Business / Enterprise Edition | Rubrik Identity Recovery | Rubrik Identity Resilience (Includes Identity Recovery) |
|---|---|---|---|
| Protect and recover Active Directory users, groups, and Domain Controllers | ✓ | ✓ | ✓ |
| Protect and recover Entra ID users, groups, and roles | ✓ | ✓ | ✓ |
| Granular recovery of objects for AD and Entra ID | ✓ | ✓ | ✓ |
| Orchestrated full AD Forest Recovery | | ✓ | ✓ |
| AD Object Attribute Comparison & Recovery | | ✓ | ✓ |
| Hybrid Recovery Workflow for AD and Entra hybrid environment | | ✓ | ✓ |
| Unified identity inventory of human and non-human identities across all IdPs. | | | ✓ |
| Policy-based detection of risks in IdP and identity configuration | | | ✓ |
| In-app remediation of detected risks | | | ✓ |
| Near-real-time alerting for critical changes or suspicious activity, with tamper-resistant monitoring | | | ✓ |

## SUMMARY

Identity Resilience leverages a comprehensive, policy-driven engine, coupled with robust, tamper-resistant event monitoring techniques, to provide multi-layered protection for enterprise identities in Microsoft Active Directory and Entra ID environments.

By continuously validating configuration compliance, detecting anomalous activity in near real-time, and providing actionable insights and in-app remediation capabilities, Identity Resilience empowers organizations to proactively manage identity risk, secure their most critical attack surface, and ensure resilient business operations.

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

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

Rubrik (NYSE: RBRK) is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

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.

brf-rubrik-identity-resilience / 20250730