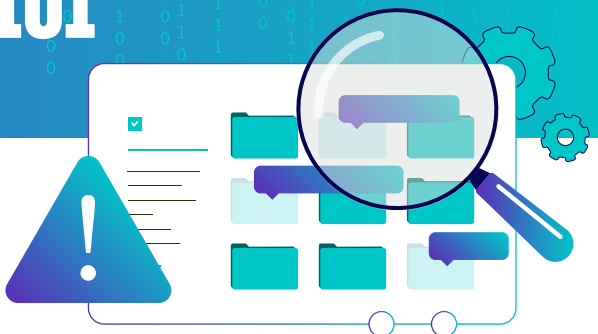
Identity Resilience 101



What is Identity Resilience?

Identity Resilience is the ability of an organization's identity and access management (IAM) system to withstand, adapt to, and rapidly recover from a cyberattack or other disruptive event.

It's a proactive approach that goes beyond simply preventing attacks. Instead, it assumes that a breach is inevitable and focuses on building a system that can absorb the shock of an attack, quickly identify and contain the damage, and restore a clean, functional state with minimal downtime and impact on business operations.

Why It Matters

Identity is #1 attack vector
Over 80% of cyberattacks exploit compromised identities to gain unauthorized access, move laterally, exfiltrate data, and shut down business operations.

Complexity increases risk
Hybrid IT environments, privileged misconfigurations, and fragmented security tools leave organizations exposed.

Blind spots from siloed tools
Security and IT teams lack unified visibility into identity risks, access permissions, and recovery readiness.

Lack of resilient recovery
Existing recovery methods are slow, complex, and vulnerable, often forcing organizations to recover from compromised backups or to rebuild manually.

Top Risks for Enterprises

Ransomware Attacks: Malicious software that encrypts data and holds it for ransom, creating the dual threat of system inaccessibility and long-term identity theft from stolen data.

Insider Threats or Malicious Deletion: A person with authorized access intentionally destroying or manipulating data, which severely compromises the integrity of all records and makes identity recovery extremely difficult.

Operational Failures: Unintentional incidents caused by system malfunctions or human error, which can result in the loss of data and a delay in identity recovery services until records are restored from a backup.

Data Breach Response: Sensitive data is exposed, leading to a complex and long-term response of damage control, including a widespread effort to mitigate the risk of identity theft for all affected individuals.

Key Benefits

- **Identity Posture Management** with a user 360° visibility into identity risks across human and non-human identities, detecting privilege escalations, misconfigurations, risky access patterns, and dormant accounts, before attackers do.
- **Data-Aware Risk Prioritization** – Rubrik links identity risks to the data they can access, enabling smarter, faster remediation.
- **Remediation & Risk Mitigation** – Proactively detect and disable suspicious accounts, expired NHIs, and exposed credentials. Apply controls to reduce the attack surface and preempt lateral movement.
- **Change Monitoring & Rollback** – monitor every critical identity change across AD and Entra ID, including roles, policies, and group memberships. Investigate malicious changes and instantly roll them back.
- **Active Directory & Entra ID Cyber Recovery** – Rapid clean-room recovery of AD forests, domains, objects, and attributes. Full tenant recovery of Entra ID, as well as granular restoration of Entra ID and hybrid objects, while retaining vital object interrelationships, ensuring minimal downtime.
- **Cross-Tenant & Hybrid Recovery** – Recover Entra ID objects to alternate tenants or across hybrid environments. Orchestrate cross-IdP recovery for seamless restoration of access across multiple IdP environments.

Actionable Steps

Ask Yourself These Questions

How do we maintain business continuity if our primary identity system becomes unavailable?	Have we established and validated a realistic Recovery Time Objective and Recovery Point Objective for our most critical identity systems?	What are our immutable recovery strategies to restore our IDP to a known, verified-good state following a compromise?	How do you leverage identity security platforms to detect critical activity, like GPO changes, and enhance your IdP's security posture?