

THE IDENTITY RESILIENCE



IMPERATIVE

Identity is now the primary attack surface, and the foundation of operational continuity.

Identity resilience is an organization's ability to maintain trusted access despite identity-based threats. It is a proactive approach that focuses being able to rapidly detect and contain threats, and restore identity systems to a clean, trusted state with minimal downtime and disruption to business operations.

WHY IT MATTERS: THE IDENTITY ATTACK SURFACE IS EXPANDING - AND ACCELERATING

Identity Is the Primary Attack Vector

80% of all modern breaches involve compromised identities¹ to gain access, move laterally, and cause widespread business disruption.

82% of organizations report experiencing at least one identity-based attack in the last year.²

Visibility Into Identity Is Incomplete

69% of leaders admit they lack full visibility into identity vulnerabilities, and

55% lack visibility into admin access across their organization.⁴

AI Is Compressing Attack Timelines

With AI-driven attack automation, adversaries can begin lateral movement within as little as 4 minutes,³ leaving organizations with less time than ever to detect, contain, and recover.

Gaps in Recovery Readiness

Existing recovery methods are slow, manual, error-prone, and often risk reinfection.

1 CrowdStrike, Stop Identity-Based Threats Today
 2 ConductorOne, 2025 Future of Identity Security Report
 3 ReliaQuest, Annual Cyber Threat Report, 2026
 4 Cisco Duo, 2025 State of Identity Security

THE REALITY: IDENTITY COMPROMISE = FULL CONTROL

IDENTITY IS THE CONTROL PLANE

When identity is compromised, attackers don't just gain access – they gain full control.

Attack Paths Already Exist Inside Your Environment

Attackers don't need to break identity systems – they exploit what's already there:

- Over-permissioned accounts
- Misconfigurations and policy drift
- Hidden relationships

In **47%** of incidents, attackers secured high privileges before ever touching the network.

Attacks Are Stealthy and Hard to Detect

By impersonating legitimate users, adversaries blend into everyday activity, making threats hard to detect and easy to persist.

- Use of valid credentials
- Activity that looks like normal admin behavior
- Gradual, low-noise escalation

A single compromised credential can expose multiple privilege paths, enabling attackers to move from:

USER → ADMIN → FULL CONTROL often without detection.

THE POTENTIAL COSTS OF IDENTITY COMPROMISE

- Operational paralysis due to loss of authentication systems
- Increased ransomware impact and recovery complexity
- Regulatory exposure and reputational damage

BUILDING IDENTITY RESILIENCE ACROSS THE FULL LIFECYCLE

As identity-based attacks grow in speed and sophistication, the ability to assess risk, detect and stop attacks, and recover cleanly is critical.

ASSESS: Know Your Risk

Identify misconfigurations that enable attacks before they happen.

- Uncover configurations and misconfigurations
- Understand blast radius and prioritize risk
- Establish a baseline for your identity security posture

DETECT: Identify and Contain Threats Early

Detect, investigate, and respond to identity-based attacks.

- Track identity changes and prioritize in real time
- Reconstruct incidents with full context – who did what, when, and where
- Roll back unauthorized or malicious changes instantly

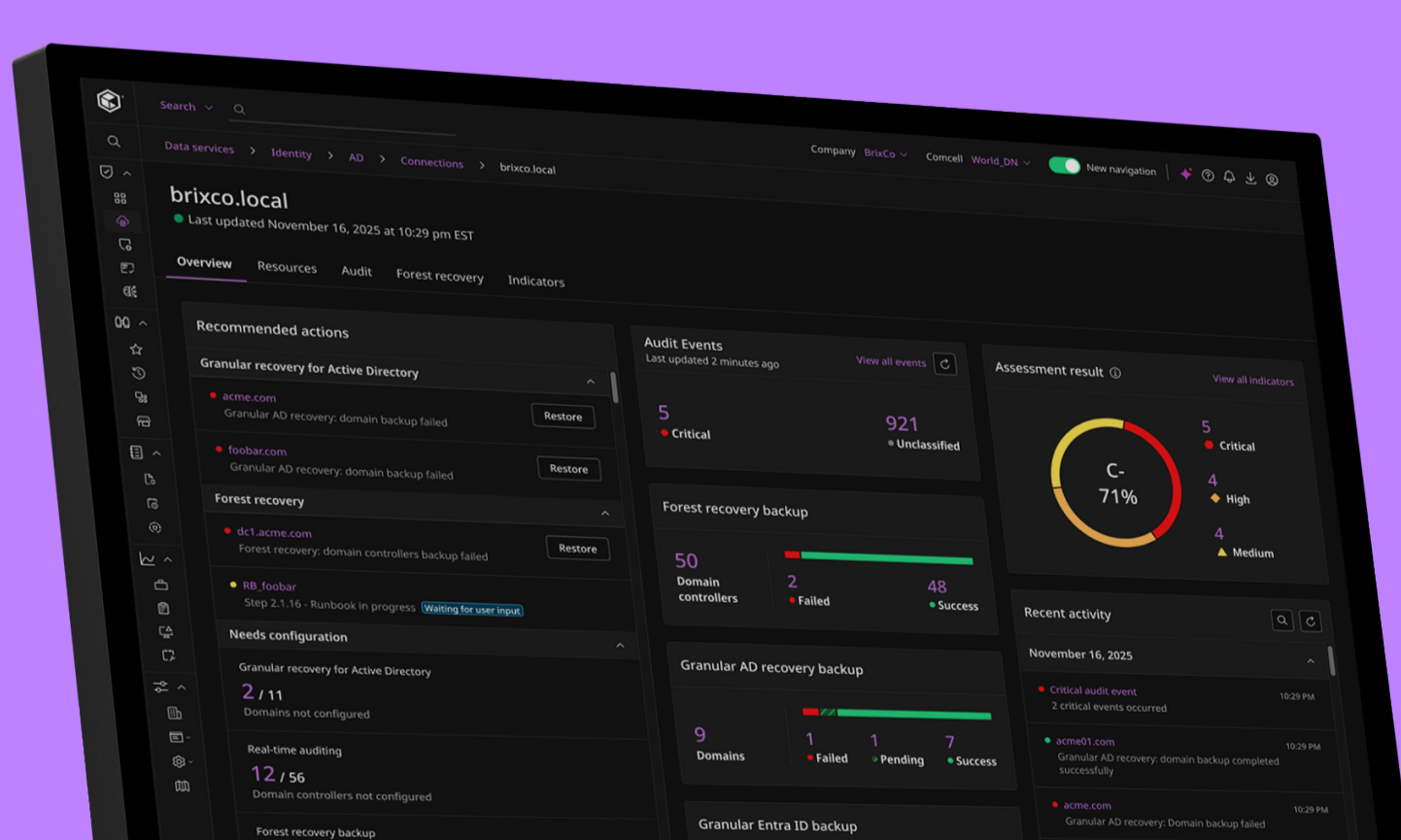
RECOVER: Get Back to a Clean State With Confidence

Recover identity systems without reintroducing risk.

- Rapidly recover identity systems to a clean state
- Validate recovery points to avoid reinfection
- Minimize downtime across dependent systems

HOW COMMVAULT® CAN HELP

Commvault is designed as a comprehensive identity resilience solution to help organizations proactively assess vulnerabilities, monitor and detect suspicious changes, and rapidly recover identity systems from cyberattacks, corruption, or operational failures.



Protect against risk. Detect threats faster. Recover with confidence.

Explore Commvault Identity Resilience capabilities [here](#).

Get a personalized demo, [here](#).