DATA SHEET

Commvault® Cloud Identity Resilience for Active Directory and Entra ID

Help protect and recover Active Directory and Entra ID from cyberattacks, corruption, and operational failures – all from a single platform.

THE CHALLENGE

Active Directory and Entra ID have become primary targets for cyberattacks. Attackers routinely exploit credentials and misconfigurations to gain access, escalate privileges, move laterally, and expand control while evading detection. Yet, many organizations still rely on native tools and manual scripts to protect and restore identity environments, increasing downtime and operational risk. Challenges include:

- Limited visibility into identity risk and misconfigurations
- Inability to detect and respond to malicious or unauthorized changes in real time
- Slow, manual, and error-prone investigation and recovery processes

80% of cyberattacks involve compromised identities.[1]

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

THE SOLUTION: COMMVAULT® CLOUD IDENTITY RESILIENCE

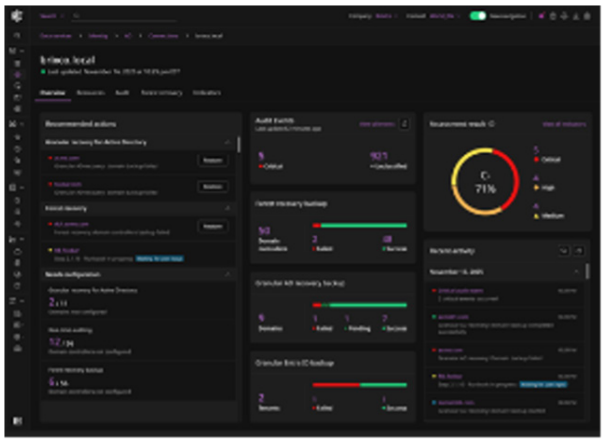
Commvault addresses these challenges with a comprehensive identity resilience solution designed to enable organizations to proactively assess risk, detect and contain threats in real time, and recover Active Directory and Entra ID from cyberattacks, corruption, or operational failures.

PROACTIVELY ASSESS RISK

Help identify and reduce identity risk before it is exploited.

Vulnerability Assessments

Identify misconfigurations and exposures in your AD environment, including excessive privileges, weak delegation, and insecure authentication. Risks are automatically prioritized with remediation guidance, enabling you to proactively reduce attack surface and help prevent compromise before it occurs.



DETECT AND RESPOND TO IDENTITY THREATS IN REAL TIME

Quickly detect, investigate, and contain risky changes to help stop fast moving attacks.

Real-Time Auditing

Monitor AD for high-risk changes, including privilege escalation, persistence techniques, and anomalous behavior. Change events are captured and centralized into a single, searchable timeline of identity activity.

Detailed Audit Trails With Full Context

For each change event, see what changed, who made it, when it occurred, and where it originated, helping differentiate legitimate admin changes from risky activity and reconstruct attack sequences with precision.

One-Click Roll Back of Malicious Changes

Quickly reverse unauthorized or malicious changes directly from the audit event to help contain incidents and minimize impact.

RAPIDLY RECOVER CLEAN IDENTITY STATES WITH PRECISION

Restore identity infrastructure to a clean, trusted state with minimal downtime and disruption for users and applications.

Granular Object-Level Recovery

Perform precise recovery of objects and attributes, plus large-scale rollback when changes affect thousands of identities. Comparison reports highlight differences between backup states or the live environment to help find and fix unwanted changes fast.

Automated Full Forest Recovery

Rapidly recover AD from ransomware or critical failure using intuitive runbooks that orchestrate the full forest recovery process—from domain controller rebuilds to metadata verification, SYSVOL restore, and re-securing replication trust. Recover in place or to a clean environment with fresh OS builds for ransomware-free restoration.

Recovery Testing And Validation

Validate recovery readiness with repeatable runbooks aligned to incident response plans. Safely simulate full forest recovery scenarios, dependencies, and configurations in an isolated environment.

UNIFY HYBRID IDENTITY PROTECTION WITH A SINGLE SOLUTION

Protect your identity estate with a single platform that delivers protection for Active Directory, Entra ID, and Okta, while extending protection across hundreds of other enterprise workloads.

Resilient SaaS-Based Control Plane

Commvault's cloud-based control plane remains accessible even when AD is unavailable or compromised, enabling coordinated response and recovery during critical moments.

Recovery Beyond Identity to Full Business Services

Commvault extends recovery beyond AD across the broader environment—including Microsoft 365, endpoints, virtual machines, and business applications—enabling complete operational recovery after an attack.

Isolated, Immutable Architecture

Identity backups are protected in tamper resistant storage that cannot be modified or deleted by compromised credentials.

1. CrowdStrike, Stop Identity-Based Threats Today
2. 2025 Future of Identity Security Report, ConductorOne

To learn more, visit **commvault.com**

© 2026 Commvault. See here for information about our trademarks and patents. 08_26