Commvault + HCLTech

SOLUTION BRIEF

# Strengthening Identity Resilience with Commvault and HCLTech

Restoring trusted access faster when cyberattacks strike

## THE IMPORTANCE OF IDENTITY RESILIENCE

Identity is the gatekeeper to an organization's critical data, applications, and systems. When identity platforms are compromised, access to critical systems is immediately disrupted—and quickly grinds your business operations to a halt. This makes Microsoft Active Directory and Entra ID prime targets for cyberattacks. As AI adoption accelerates—especially with agentic AI, where machines autonomously request, grant, and act on permissions—the value and exposure of identity systems continue to grow. Because identity compromises often remain undetected for months, silently altering permissions and enabling persistent control across both human and machine identities, organizations should protect, validate and recover these systems to maintain trust, reduce risk, and enable rapid business recovery.

Active Directory is involved in an estimated

**9/10 attacks**[1]

Gartner reports that

**85% of identity related breaches**[2]

can be attributed to hacked machine identities such as service and automation accounts

For attackers, AD is a one-stop shop for elevating privileges and stealing, corrupting, or denying access to critical applications and data.

**100%**

increase in "kerberoasting" attacks where attackers try to gain escalated privileges by abusing Microsoft AD[3]

## CHALLENGES TO BUSINESS & OPERATIONS

The distributed, multi-master nature of Active Directory and Entra ID provides for high availability and resiliency but introduces complexity that makes the process of recovering AD from a disaster or cyberattack complicated. This is especially true for enterprise AD environments consisting of multiple domains and geographies. Whether recovering from accidental deletion, corruption, or a ransomware attack, using native methods and tools or homegrown solutions is often a time-consuming, complex, and manual, error-prone process. And the longer it takes to restore AD back to a working state, the greater the disruption to the business.

- Extended downtime due to complex, manual recovery process
- Lack of visibility across hybrid environments
- Loss of trust in identity raises risk of attacker persistence

.

## THE NEED FOR COMPLETE RECOVERY

Without unified visibility and orchestration, teams lack the ability to quickly assess risk, reverse unwanted identity changes, and execute recovery with confidence across hybrid environments. Active Directory forests are highly complex environments, spanning multiple domains, domain controllers, and interconnected users, devices, and security policies. When ransomware takes an AD forest offline, each domain controller must be recovered and reintroduced in the correct sequence using validated, clean identity data to help prevent reintroducing compromised changes from replicating across the environment.

Manual AD forest recovery is slow and error-prone under crisis conditions. Without automated and orchestrated recovery, human error can introduce new corruption, reopen security gaps, and extend downtime. Complete recovery demands a cyber-resilient approach that unifies Active Directory and Entra ID protection, automates recovery workflows, and restores trusted identity services at the speed the business requires.

## A UNIFIED CYBER RESILIENCE FRAMEWORK

Together, Commvault and HCLTech bring industry-leading technology and cyber resilience capabilities to safeguard your identity infrastructure n—from proactive risk assessment and rapid threat response to confident recovery of Active Directory and Entra ID.. Through a single dashboard, organizations can detect malicious or unwanted changes in real time, uncover hidden vulnerabilities before they're exploited, and rapidly roll back directory changes across hybrid environments—recovering your identity systems cleanly—in hours, not weeks.

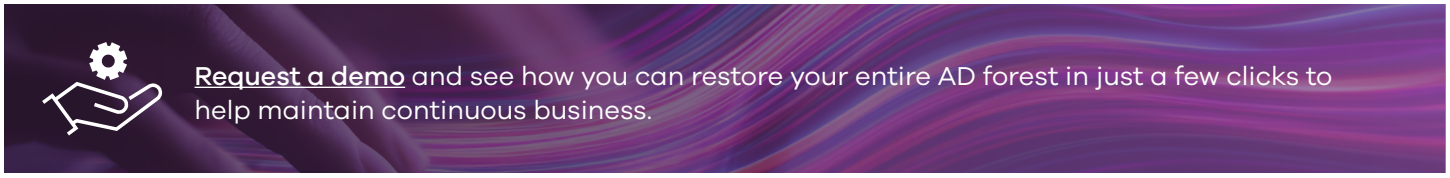
This holistic approach provides:

- **Industry insight and strategic guidance** from HCLTech identity and security experts to design, test, implement, and sustain a resilient AD environment aligned with Zero Trust principles and support regulatory data-resilience obligations. This includes identifying AD vulnerabilities, recovery gaps and compliance risks, continuously testing and monitoring AD backup and recovery scenarios, creating runbooks, and testing recovery readiness.
- **Proactive identity risk assessments and monitoring -** With AI-driven insights and clear recommendations, regularly remove excess access and risky configurations, rapidly detect and contain suspicious anomalies and accidental directory modifications, and enable 24×7 monitoring to stop threats before they escalate.
- **Comprehensive, orchestrated AD forest recovery** with automated DR runbooks to streamline the multi-step process or object-level restoration to reverse malicious or accidental changes without restoring the entire directory—each cutting recovery times from weeks to hours.
- **Recover AD to clean VM** by leveraging AI-enabled Commvault Synthetic Recovery to rapidly create consistent point-in-time recovery images, and then isolate, test, and validate recovery of identity providers in Commvault Cleanroom Recovery. Generate runbooks automatically for building out, orchestrating, and automating the steps required for a identity recovery.
- **Unified hybrid identity protection** through one interface for Microsoft Active Directory and Entra ID, provides consistent visibility, risk insights, automated rollback and recovery workflows across the identity landscape while reducing tool sprawl.

## KEY BUSINESS OUTCOMES

By leveraging the joint HCLTech and Commvault solution, your organization can:

- Reduce downtime and financial loss through reliable, fast, automated recovery.
- Improve compliance posture with auditable, tested recovery plans.
- Enhance identity resilience against ransomware and unplanned disruptions.
- Build confidence in data integrity to support resilient operations and protect brand reputation.




[1] Researchers Explore Active Directory Attack Vectors, 2021
[2] Gartner Top Trends for 2025, 2025
[3] IBM Report: Identity Comes Under Attack, Straining Enterprises' Recovery Time from Breaches, 2024

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