DATA SHEET

Commvault® Cloud Backup and Recovery for Active Directory

Protect AD from cyberattacks, disasters, and operational mistakes

OVERVIEW

Microsoft Active Directory (AD) and Entra ID are central to providing secure authentication for your business. As the control center for identity, access, and security across all systems, Active Directory needs resilient, adaptable protection. In the face of deletion, corruption, and cyberattacks, Commvault Cloud Backup & Recovery for Active Directory delivers fast identity recovery and enables continuous business across the enterprise.

CHALLENGE

Given its importance, it's no surprise that Active Directory is a prime target in 9 out of 10 attacks. The impact of an Active Directory outage or disaster can be far-reaching. Applications, file systems, email services, and databases all rely on AD for proper authentication and secure user access control, so when AD is damaged or taken completely offline, the critical applications and services it supports become inaccessible. Without AD, the business cannot continue.

Fast and secure recovery of Active Directory is foundational to maintaining continuous business. Whether recovering from accidental deletions, corruption, or malicious attacks, recovery with native tools or homegrown solutions is often time-consuming, complex, and prone to error.

9 in 10 cyberattacks target Active Directory.[1]

$4.88M Average global cost of a data breach ($9.3M in the US).[2]

SOLUTION

Commvault Cloud Backup & Recovery for Active Directory provides comprehensive protection and fast recovery for critical AD and Entra ID data and configurations needed to authenticate and provide secure control access to critical applications and services.

With Commvault Cloud, you can:

- Rapidly recover the entire AD forest to a point in time before corruption or attack
- View what's changed in your environment and revert those changes as efficiently as possible
- Recover individual objects like users or groups that were mistakenly deleted
- Roll back unwanted changes to specific object attributes
- Protect AD and Entra ID hybrid environments with a single, unified solution

ROBUST RECOVERY

Rapidly restore entire AD forests, domain controllers, and individual objects and attributes, such as users or groups and their relationships.

INTERACTIVE COMPARISON REPORTING

Compare all changes in the AD domain or Entra ID tenant between two points in time, quickly identify the data that needs to be recovered or reverted, and restore it quickly, directly from the report.

EASY TO MANAGE

Protect Active Directory and Entra ID in hybrid environments with a single, unified solution that also provides data protection for many other on-premises or cloud applications like Microsoft 365, Microsoft Dynamics 365, endpoints, and VMs.

Benefits

- Automate the entire forest recovery process
- Accelerate recovery times and advance resilience
- Enhance cyber readiness with AD recovery testing
- Reduce risks of business productivity downtime
- Eliminate slow and error-prone manual recovery processes

Capability	Features and Benefits
Single-solution protection for Active Directory and Entra ID	• Comprehensive protection across critical AD objects including Group Policy Objects (GPOs), users, groups, and all their relationships • Protect Entra ID roles, conditional access policies, and more • Automated, frequent backups and unlimited retention
Automated Active Directory forest recovery	• Automate the full AD forest recovery process, including the critical hygiene tasks required to verify consistency in the recovered AD • Automated forest recovery runbooks orchestrate the multi-step AD forest recovery process with options to customize steps for fine-grained control • Visual AD topology views enable simple and rapid identification of which domain controllers to restore first and how they should be recovered • Prescriptive runbook views provide full visibility of the recovery progress. See where you are in the process and how long until your AD is back online • Support full-scale, frequent AD recovery testing in a non-production environment
Fast, granular recovery	• Quickly recover only the missing, damaged, or misconfigured objects • Rollback of overwritten or corrupted attributes across many objects at once
Interactive comparison reporting	• Compare all changes in the AD domain or Entra ID tenant between backups or between a recent backup and the live directory and quickly recover deleted or changed objects or attributes directly from the report • Filter by attribute, object, deleted, or modified to narrow search results
Multi-layered security	• Cloud control plane provides resiliency in the face of disaster • Layered security that meets industry standards and supports regulation compliance • At-rest and in-flight data encryption • Role-based, SSO, SAML authentication controls

SUPPORTED PLATFORMS AND APPLICATIONS

Active Directory

Microsoft Active Directory	• On physical or virtual servers, on-premises, or in the cloud
Microsoft Entra ID	

Storage targets

Cloud storage	• Included for Entra ID
On-premises storage	(BYO for Microsoft Active Directory) • Commvault Cloud Air Gap Protect • Azure • Dell EMC Isilon, Data Domain • Hitachi HNAS, VSP, HCP • HPE Primera, Nimble, 3PAR • NetApp E-Series • Pure Storage FlashArray

1. Sheridan, K. (2021, May 3). Researchers Explore Active Directory Attack Vectors. Dark Reading.
2. https://www.ibm.com/reports/data-breach

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