Commvault

eBOOK

Four Things to Consider with Active Directory Protection

Dedicated security and recoverability for your Microsoft AD and Entra ID data

eBOOK

Commvault

The Keys to the Castle

As a widely adopted authentication tool for small, medium, and enterprise businesses, Microsoft Active Directory (AD) and Entra ID are the gatekeepers of authorization processes for networks, applications, and environments. User account attributes like names, addresses, phone numbers, passwords, and more are grouped, providing administrators with simplified control over user access. While AD simplifies the lives of administrating access to key systems, securing it can be particularly challenging. It controls an ever-changing pool of users, groups, policies, and app permissions. A single misstep—be it a misconfiguration, a compromised password, or a dormant account—can enable a bad actor to elevate privileges and steal, corrupt, or deny access to critical applications and data, ultimately leading to unplanned downtime of production services.

With Active Directory at the center of secure authentication and services, protecting and securing this data is critical for businesses today. Having the ability to know what has changed in the environment and reverting those changes is paramount.

A data protection solution for Active Directory can help mitigate the risk of data loss and quickly get your business back online.

Here are four things to consider when keeping your AD data secure and protected:

#1

FREQUENT BACKUPS

Best practices shouldn't just apply to company data and databases – but AD as well. Frequent, automated backups save you the agony of dealing with lost domain information and more. While using tombstone for temporarily recovering deleted items can be helpful, relying on this method is risky as tombstone lifespans are limited. Having a full and frequent backup of the entire Active Directory is best. Backup as a Service solution allows for frequent backups, off-site secure storage, and simplified management — with built-in best practices around long-term retention.

#2

BUILDING YOUR OWN – CAN VS. SHOULD

Sure, there are ways to script and other installable services that help you protect Active Directory, but should you build it? Home-grown solutions may seem rewarding, but they are time-consuming with maintenance, additional patching, and the added burden on IT. Instead, opting for an enterprise-grade and secure data protection solution delivered as SaaS eliminates

the need for in-house development and support. With just a few clicks, you can be protected in minutes with simplified management, layered security with encryption, and protection from ransomware.

#3 RECOVERING ATTRIBUTES

Administrators often invest considerable effort in organizing an Active Directory structure, making sure the right items are in the correct Organizational Units (OUs) and with the right permissions. Having this level of granularity of a directory object is critical to a finely tuned IT organization. Without a data protection solution, any disruption would necessitate a complete rebuild of the OUs. A dedicated data protection solution allows for granular recovery, restoring only the missing, damaged, or misconfigured object attribute. This granularity can quickly get the business systems or users back online without needing a full restore of an entire Active Directory environment.

#4 RANSOMWARE HAPPENS

As a core element of centralized management, Active Directory has become a primary target and pathway to execute ransomware attacks. By exploiting blind spots, bad actors can compromise privileged accounts, mimic authorized users, and silently traverse infrastructure, workstations, and applications to establish their foothold. Failing to safeguard AD enables attackers with a centralized location to control and sever access to critical business assets. Now more than ever, it's critical that today's businesses consider AD protection in their overarching security and ransomware response strategies. Combatting ransomware takes a multi-layered approach to data security, with recovery readiness playing a critical role.

50% of organizations experienced an Active Directory attack in the last two years.[1]

CLOSING THE DATA RECOVERY GAP

Modern businesses need robust, dedicated protection of their critical Microsoft AD and Entra ID data. Optimized to meet the needs of today's businesses, purpose-built solutions for AD offer unmatched simplicity.

Benefits of dedicated protection

- Air-gapped, isolated data backups
- Robust tools for recovery and compliance
- Advanced user control to undo damaging and unwanted changes
- Layered security and early threat detection ransomware protection

COMMVAULT® CLOUD, POWERED BY METALLIC AI

Commvault Cloud delivers industry-leading security and protection for Active Directory and Entra ID data—proven to keep your business safe, compliant, and recoverable from threats. Minimize data exposure, drive visibility into threats, and confidently respond using the industry's most advanced data resiliency platform.

With broad coverage across data centers, clouds, SaaS apps, and more, the Commvault Cloud offers one platform to safeguard entire data estates, all from a single pane of glass.

Safeguard your hybrid directory by protecting critical Microsoft AD and Entra ID objects, including group policy objects, users, groups, conditional access policies, roles, and more.

Interactive comparisons identify all changes to the domain or tenant, allowing you to quickly recover mistakenly or maliciously deleted objects or roll back overwritten attributes across the entire directory.

Virtually air-gapped backup copies, zero-trust access controls, and early detection capabilities isolate data copies for advanced ransomware protection.

BENEFITS

Mitigate ransomware risk, keep data compliant, and rapidly recover with integrated cloud storage from Commvault.

Optimize operations
with automated and high frequency backups

Preserve content
with immutable and tamper-proof data copies

Compare and rapidly recover data
with in-place and out-of-place restore options

Seed, replicate, and retain
sandbox environments for development and testing

Mitigate risk
with data isolation, decoupled from source environments

Minimize cyber attacks
with AI-powered detection, monitoring, and data defense

Maintain SLA compliance
with unlimited storage and retention built-in

Protect it all
with single-solution, multi-platform protection

NEXT STEPS

Protecting Active Directory may seem overwhelming, but you don't have to do it alone. Commvault is here to help you every step of the way.

Sign up for a 30 day free trial today.

1 EMA Research Report – The Rise of Active Directory Exploits

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