eBOOK

PROTECTING THE

Crown Jewels

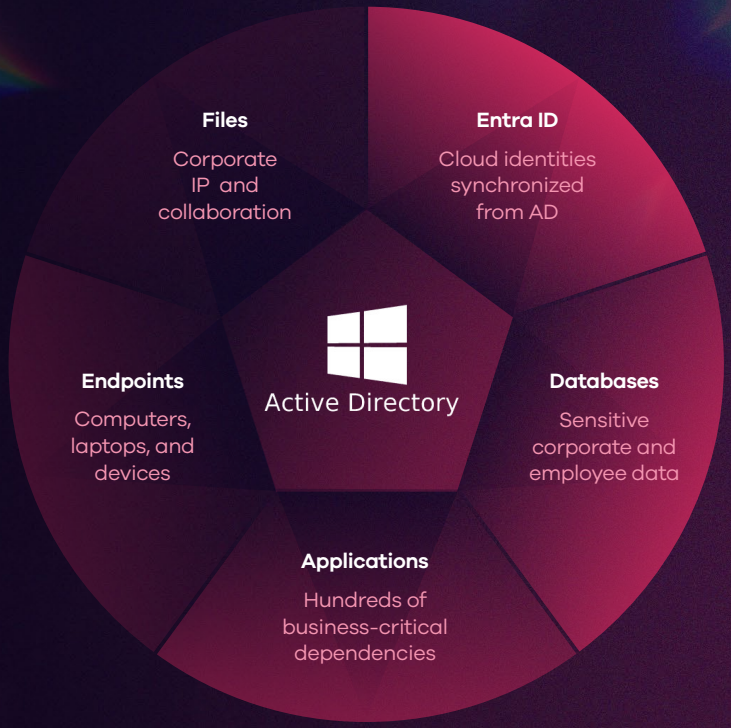
Securing
Active Directory
against cyber threats

Commvault®

The Importance of Active Directory

Microsoft Active Directory (AD) and Entra ID are the **crown jewels** of enterprise identity and access management, authenticating millions of users globally and controlling access to critical business systems. From workstation logins to physical building access, AD enables the seamless operation of your organization.

If AD data becomes corrupted or the directory itself is unavailable, it can severely disrupt line-of-business applications and processes, blocking user access to vital systems and resources.



Without AD, business operations grind to a halt.

Bank staff **can't access customer accounts.**

Doctors and nurses **can't access medical records.**

Coders and developers **can't publish code.**

Managers **can't send emails.**

Teams **can't collaborate or chat.**

Active Directory's importance and complexity makes it a prime target for attacks.

Since AD and identity management are such crucial components of business operations, they present a very appealing target to attackers looking for valuable systems to hold for ransom. For those who simply want to cause chaos, AD is one of the systems that can bring all others to a standstill and devastate the business.

AD is the center of secure authentication and services, and it's critical to maintain its security and recoverability, preparing for the various disasters that could impact it.

Active Directory is involved in an estimated

9/10

attacks[1]

This is not surprising, given Active Directory's importance.

Microsoft Digital Defense reports that

88%

of customers

affected by security incidents had an **insecure AD configuration**, making AD a high value asset to bad actors[2]

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

A recent IBM report highlights a **100%** increase in "kerberoasting" attacks.

This is where attackers try to gain escalated privileges by abusing Microsoft AD[3]

1 Researchers Explore Active Directory Attack Vectors
2 Microsoft Digital Defense Report 2022
3 IBM Report: Identity Comes Under Attack Straining Enterprises' Recovery Time from Breaches

AD Recovery Is the Foundation of Continuous Business

The importance of prioritizing AD recovery is evident when you consider its cascading effect on other workloads. Applications, file systems, email services, and databases all rely on AD for proper authentication and user access.

When AD is damaged or taken completely offline, critical applications and services become inaccessible.

Because nearly everything in modern businesses relies on identity, restoring AD before other workloads is a critical priority.

By restoring AD first, organizations can re-establish control over their networks and systems, verify that data security and access policies are enforced, and provide a stable foundation for the recovery of other systems and services.

MISTAKES HAPPEN

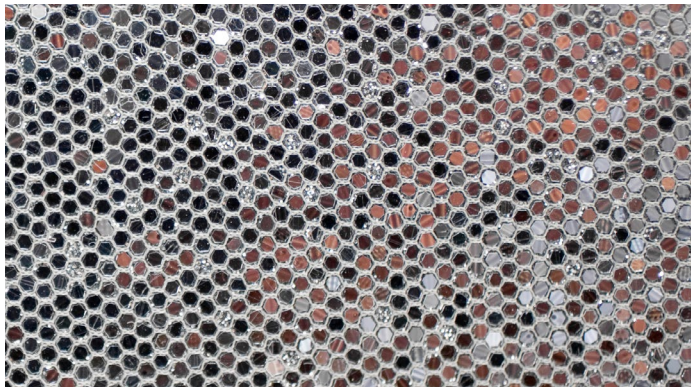
The Need for Granular Recovery

One of the most critical aspects of AD protection is the ability to restore lost or corrupted data quickly. When important data within AD is accidentally or maliciously deleted, changed, or corrupted, you need to be able to quickly identify those changes and restore and recover individual objects and attributes.

While it's helpful that the Recycle Bin in AD can temporarily recover deleted objects, relying on this method is risky. The Recycle Bin only retains deleted objects for a limited time before they are permanently removed. It does not support rolling back changes at the attribute level or reverting modifications to Group Policy Objects (GPOs) or AD configurations.

Sometimes, disasters may not result in the deletion of objects but rather the overwriting of attribute data across multiple objects. For example, a poorly written PowerShell script could cause unexpected changes throughout the directory. When this happens, you need the ability to locate and roll back specific attributes across multiple objects within AD. However, the Recycle Bin cannot undo changes at the attribute level or revert modifications to GPOs or AD configurations.

For comprehensive protection, it's best to have a full and frequent backup of the entire AD. 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 AD environment.



Do you have a plan for recovery?

When ransomware locks down and takes the servers hosting your AD offline, you need the ability to recover the AD environment. This involves rebuilding the directory service, including domains, domain controllers, and associated data, to a pre-attack state.

The impact of an AD attack that disables domain controllers is real and can be devastating. Critical systems stop working. Employees can't log in. Security policies that rely on identity can't be enforced.

"If we can't recover our domain controllers, we can't recover anything."

IT ADMIN, MAERSK

With such threats looming, having a well-documented and frequently tested recovery plan to rebuild and restore your AD environment to a previous, healthy pre-attack state is critical and the key to getting your business back fast.

Ransomware Strikes

In 2017, global shipping giant Maersk fell victim to the NotPetya cyberattack, which encrypted the file systems of:

45K PCs

4K servers

149/150 AD domain controllers

With AD offline, operations instantly ceased, shutting down:

17 global shipping ports

100s of container ships, stranded for **10 days**

In total, the attack cost the company at least:

$300M[4]

4 The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Active Directory Recovery Is a Complex Process

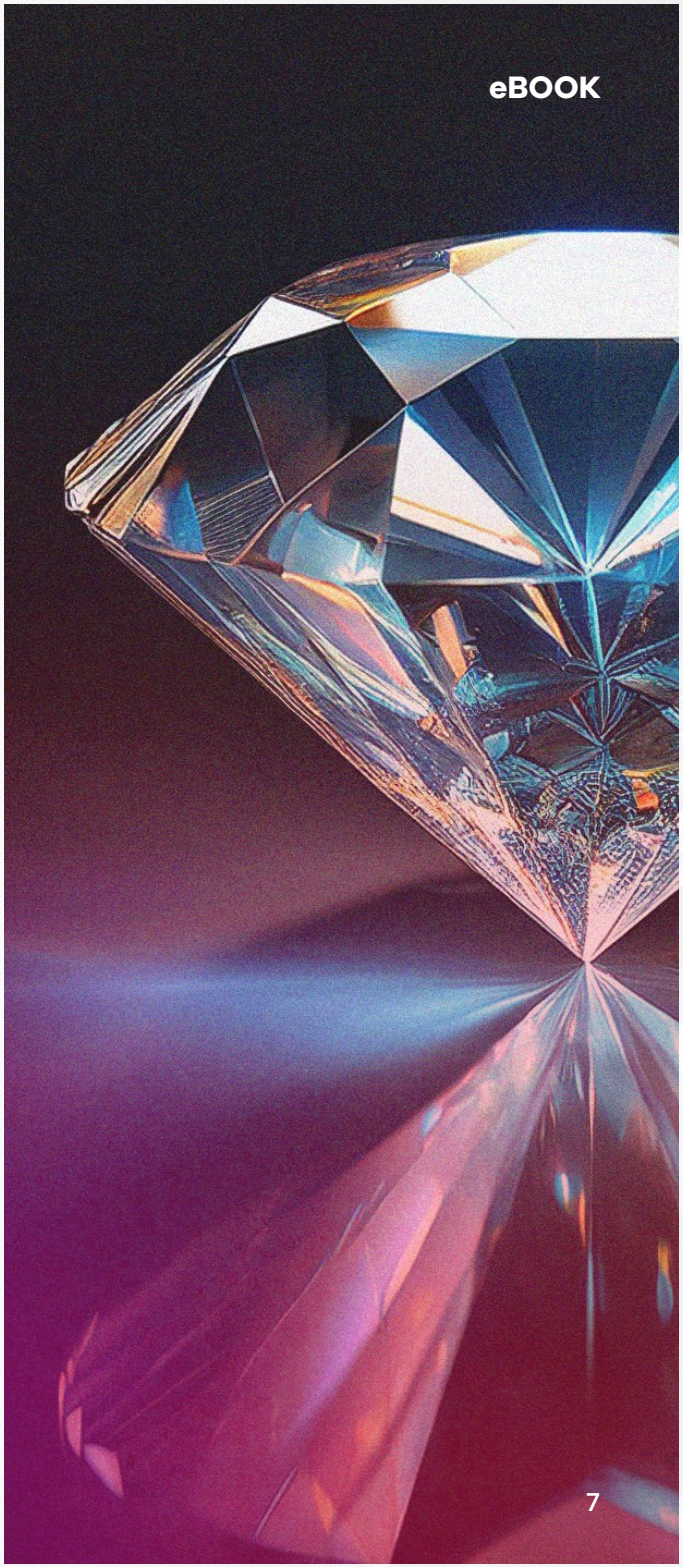
AD forests are complex environments with multiple domains, several domain controllers for each of those domains, and a full hierarchy of users, computers, and access/security settings.

In the case of a cyberattack, it is not enough to simply restore a single domain controller from backup. The recovery and rebuilding process of the environment is incredibly intricate and demands meticulous coordination. Each domain controller must be synchronized and restored carefully to avoid data inconsistencies and potential corruption.

Microsoft's AD Forest Recovery Guide provides a detailed, step-by-step method for this, which can involve anywhere from 50 to 100 or more individual steps, depending on the size of your organization.

The recovery process is manual, time-consuming, and complex – often taking days to weeks to complete. All the while, business operations cease to function, and users cannot access important applications.

Without automating and orchestrating the process, you risk restoring AD to an unusable state, which could further disrupt the business and prolong an outage.



Commvault Makes Your Active Directory Resilient

Commvault Cloud Backup & Recovery for Active Directory allows you to safeguard and accelerate the recovery of AD data in the face of corruption, accidental deletion, and ransomware attacks.

Accelerate Active Directory recovery, and get back to business faster with:

Automated AD forest recovery

Rapidly recover forests to a point-in-time before an attack, allowing you to get back to business in hours rather than days or weeks.

Interactive comparisons

Identify changes to the domain, allowing you to quickly recover mistakenly or maliciously deleted objects or roll back overwritten attributes across the directory.

Flexible, granular recovery

Quickly recover only the missing, damaged, or misconfigured object attributes, and get your business systems or users back online quickly.

Hybrid directory support

Protect critical Microsoft AD and Entra ID objects, including GPOs, users, groups, conditional access policies, roles, and more.

AD recovery testing

Deliver confidence that recoveries can be successful, and allow security and IT teams to practice during good times to prepare for the bad times.

Cyber Recovery Is More Than Just AD

Staring down a cyberattack or ransom situation is a harrowing experience.

Restoring AD is the first step in most cases, and finding ways to automate the otherwise time- and resource-intensive process can help jumpstart the recovery process and bring back the business quickly. Even better is when your AD recovery is built on the same platform the rest of your cyber recovery relies on.

Unifying the cyber recovery and rebuild process on a common platform enables easy coordination, automation, and orchestration that spans more than just identity recovery – you can orchestrate the recovery of apps, data, clouds, and infrastructure. This will help your teams work together to rebuild your systems following cyberattacks and disasters, and build resilience that delivers continuous business.

eBOOK

Request a demo and see how you can restore your entire AD forest in just a few clicks to help maintain continuous business.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®