eBOOK

EXPOSED:
THE TRUTH ABOUT ACTIVE DIRECTORY, IDENTITY RESILIENCE, AND RAPID RECOVERY

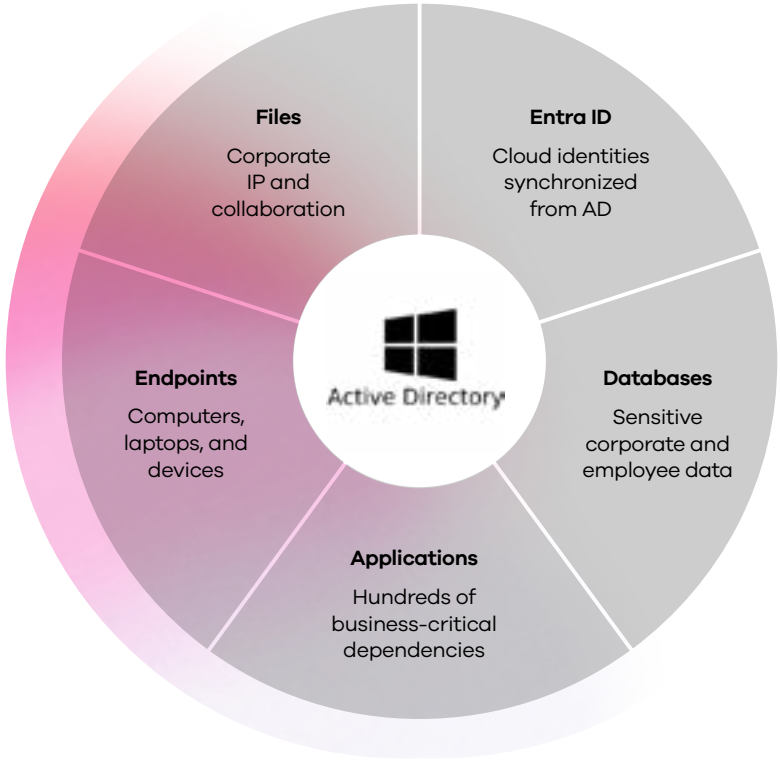
Commvault®

THE HARSH REALITY IS THIS: YOUR ORGANIZATION'S DIGITAL IDENTITY INFRASTRUCTURE IS UNDER SIEGE.

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, making it the ultimate prize for cybercriminals.

But here's what most organizations don't realize: Traditional backup and recovery approaches for AD are fundamentally inadequate in today's threat landscape. The truth about identity resilience goes far beyond simple data protection – it requires a comprehensive strategy that anticipates sophisticated attacks and enables rapid, automated recovery at the speed of business.

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.**

EXPOSED: Why 9 Out of 10 Attacks Target Your Identity Infrastructure

The reality of modern cyber warfare is that identity infrastructure has become the primary battleground. 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.

This is where identity resilience becomes critical. Identity resilience isn't just about backing up your directory – it's about building an identity infrastructure that can withstand, adapt to, and rapidly recover from sophisticated attacks while maintaining business continuity.

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.

The statistics paint a stark picture of the current threat landscape.

AD is involved in an estimated

9/10

attacks[1]

This is not surprising, given AD'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

THE HIDDEN DEPENDENCY: WHY EVERYTHING FAILS WHEN IDENTITY FALLS

Here's what makes AD recovery 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.

Identity resilience recognizes this fundamental dependency. Because nearly everything in modern businesses relies on identity, building resilient identity infrastructure becomes the cornerstone of organizational resilience. This goes far beyond simply restoring AD after an attack occurs.

By establishing identity resilience practices, organizations can better maintain control over their networks and systems even during active attacks, enforce data security and access policies, and provide a stable foundation that supports rapid recovery of other systems and services.

EXPOSED: THE FATAL FLAW IN AD'S BUILT-IN RECOVERY TOOLS

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.

The uncomfortable truth about AD's built-in recovery options: 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.

True identity resilience demands granular recovery capabilities. For comprehensive protection, it's best to have a full and frequent backup of the entire AD that supports precise, object-level recovery operations.

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.

When ransomware strikes, do you have a plan for rapid 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

This case study reveals the critical importance of rapid recovery capabilities within an identity resilience strategy. 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.

THE $300 MILLION LESSON: WHAT MAERSK'S DISASTER REVEALS ABOUT RECOVERY

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

EXPOSED: THE 100-STEP RECOVERY PROCESS THAT'S DOOMED TO FAIL

The reality of AD recovery complexity: 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.

Here's the brutal reality of manual recovery: The recovery process is manual, time-consuming, complex, and prone to error – often taking days to weeks to complete. All the while, business operations cease to function, and users cannot access important applications. This extended downtime directly contradicts the principles of identity resilience, which demands rapid restoration capabilities.

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

THE SOLUTION: HOW TO BUILD STURDY IDENTITY RESILIENCE WITH COMMVAULT

The solution to creating identity resilience: 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 AD recovery and build identity resilience, getting 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.

BEYOND IDENTITY: THE COMPLETE CYBER RECOVERY STRATEGY

Cyber Recovery Is More Than Just AD

Staring down a cyberattack or ransom situation is a harrowing experience. Restoring AD recovery 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.

True identity resilience extends beyond just AD protection – it integrates easily with your broader cyber recovery strategy. 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.

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®