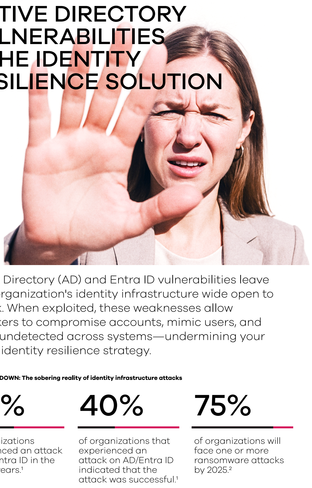
EXPOSED: ACTIVE DIRECTORY VULNERABILITIES + THE IDENTITY RESILIENCE SOLUTION



Active Directory (AD) and Entra ID vulnerabilities leave your organization's identity infrastructure wide open to attack. When exploited, these weaknesses allow attackers to compromise accounts, mimic users, and move undetected across systems—undermining your entire identity resilience strategy.

THE BREAKDOWN: The sobering reality of identity infrastructure attacks

50%

of organizations experienced an attack on AD/Entra ID in the last 1-2 years.[1]

40%

of organizations that experienced an attack on AD/Entra ID indicated that the attack was successful.[1]

75%

of organizations will face one or more ransomware attacks by 2025.[2]

VULNERABILITIES THAT ENABLE ATTACKS

AD's complexity makes it particularly prone to attacks, with several common vulnerabilities, including:

Readable by anyone

Any authenticated user can read the entire AD, so attackers can exploit weaknesses such as configuration errors and privileged accounts.

Inherent trust

Every domain-joined system trusts the directory and is subject to any Group Policy Object (GPO) applied to it.

Cached credentials

Attackers can harvest AD credentials from any connected systems in the network, including privileged service accounts.

Group Policy Objects

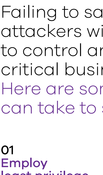
When GPOs are linked at the domain head, they can be used to disable security controls.

Outdated protocols

Legacy protocols are often left enabled to support applications, providing easy access for attackers.

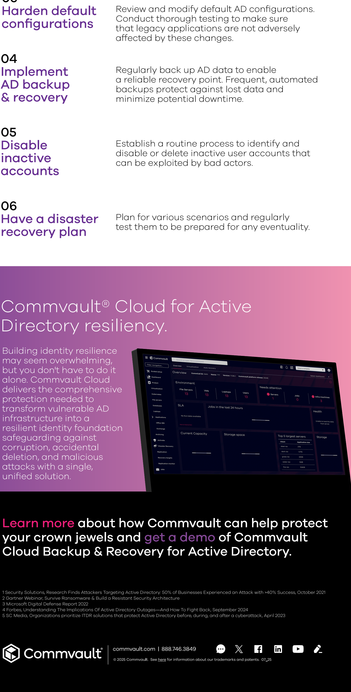
Default settings

Default configurations, such as allowing any domain user to add workstations, can be easily exploited.



These exposed vulnerabilities demonstrate why traditional AD security isn't enough—true identity resilience requires comprehensive protection.

88% of customers impacted by incidents had an "insecure" AD configuration, according to Microsoft Digital Defense.[3]



QUICK AD SECURITY TIPS

Failing to safeguard AD enables attackers with a centralized location to control and sever access to critical business assets. Here are some immediate steps you can take to secure AD:

01 Employ least privilege access

Limit user account permissions to only what is necessary for the tasks they need to perform, reducing the risk of an attacker gaining access.

02 Monitor and audit changes

Keep track of all changes made to AD to quickly detect and address any unauthorized changes or misconfigurations.

03 Harden default configurations

Review and modify default AD configurations. Conduct thorough testing to make sure that legacy applications are not adversely affected by these changes.

04 Implement AD backup & recovery

Regularly back up AD data to enable a reliable recovery point. Frequent, automated backups protect against lost data and minimize potential downtime.

05 Disable inactive accounts

Establish a routine process to identify and disable or delete inactive user accounts that can be exploited by bad actors.

06 Have a disaster recovery plan

Plan for various scenarios and regularly test them to be prepared for any eventuality.

Commvault® Cloud for Active Directory resiliency.

Building identity resilience may seem overwhelming, but you don't have to do it alone. Commvault Cloud delivers the comprehensive protection needed to transform vulnerable AD infrastructure into a resilient identity foundation, safeguarding against corruption, accidental deletion, and malicious attacks with a single, unified solution.

Learn more about how Commvault can help protect your crown jewels and get a demo of Commvault Cloud Backup & Recovery for Active Directory.

1 Security Solutions, Research Finds Attackers Targeting Active Directory, 50% of Businesses Experienced an Attack with >40% Success, October 2021
2 Gartner Webinar, Survive Ransomware & Build a Resistant Security Architecture
3 Microsoft Digital Defense Report 2022
4 Forbes, Understanding The Implications Of Active Directory Outages—And How To Fight Back, September 2024
5 SC Media, Organizations prioritize ITDR solutions that protect Active Directory before, during, and after a cyberattack, April 2023