

SECURING THE CORE

ACTIVE DIRECTORY /ULNERABILITIES + HOW TO FIX THEM

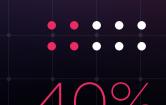
access control, making them prime cyber threat targets. Exploiting vulnerabilities, attackers can compromise accounts, mimic

Active Directory (AD) and Entra ID are vital for network

users, and move undetected across systems.



experienced an attack on AD/Entra ID in the last 1-2 years!



THE BREAKDOWN

experienced an attack on AD/Entra ID indicated that the attack was successful.1

of organizations that

of organizations will

face **one or more** ransomware attacks by 2025.2



AD's complexity makes it particularly prone to attacks,

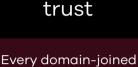
with several common vulnerabilities, including:



entire AD, so attackers can exploit weaknesses such as configuration errors and privileged accounts.

Any authenticated

user can read the



system trusts the

Inherent

directory and is subject to any Group Policy Object (GPO) applied to it.



credentials

Attackers can harvest

AD credentials from

any connected systems in the network, including privileged service accounts.



When GPOs are linked at the domain head, they can be

used to disable

security controls.



often left enabled to

support applications,

Outdated

providing easy access for attackers.



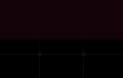
easily exploited.

Default configurations,

such as allowing any

domain user to add

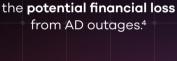
workstations, can be



WITHOUT AD, BUSINESS OPERATIONS GRIND TO A HAULT

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

PER HOUR



QUICK AD SECURITY TIPS Failing to safeguard AD enables attackers with a centralized

DAYS TO

the time it takes organizations to

recover from an attack on AD/Entra ID.5

Employ least privilege access Limit user account permissions to only what is necessary for the tasks

location to control and sever access to critical business assets.

Here are some **immediate steps you can take** to secure AD:

they need to perform, reducing the risk of an attacker gaining access.

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

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

Monitor and audit changes

affected by these changes.

minimize potential downtime.

Harden default configurations

Implement AD backup & recovery

Disable inactive accounts

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

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



prepared for any eventuality.

Plan for various scenarios and regularly test them to be

Have a disaster recovery plan

COMMVAULT® CLOUD FOR ACTIVE DIRECTORY RESILIENCY

overwhelming, but you don't have to do it alone. Commvault Cloud delivers dedicated protection to safeguard

Active Directory and Entra ID data from corruption, accidental deletion, or malicious attacks with a single, unified solution.

Protecting Active Directory may seem

Learn more about how Commvault can help protect your crown

for Active Directory.

jewels and get a demo of Commvault Cloud Backup & Recovery

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



commvault.com | 888.746.3849





in



© 2024 Commvault. See here for information about our trademarks and patents. 11_24