

SECURING THE CORE

ACTIVE DIRECTORY VULNERABILITIES + HOW TO FIX THEM

Active Directory (AD) and Entra ID are vital for network access control, making them prime cyber threat targets.


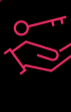


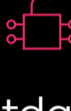

Exploiting vulnerabilities, attackers can compromise accounts, mimic users, and move undetected across systems.

THE BREAKDOWN



VULNERABILITIES THAT ENABLE ATTACKS

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

 <h3>Readable by anyone</h3> <p>Any authenticated user can read the entire AD, so attackers can exploit weaknesses such as configuration errors and privileged accounts.</p>	 <h3>Inherent trust</h3> <p>Every domain-joined system trusts the directory and is subject to any Group Policy Object (GPO) applied to it.</p>	 <h3>Cached credentials</h3> <p>Attackers can harvest AD credentials from any connected systems in the network, including privileged service accounts.</p>
 <h3>Group Policy Objects</h3> <p>When GPOs are linked at the domain head, they can be used to disable security controls.</p>	 <h3>Outdated protocols</h3> <p>Legacy protocols are often left enabled to support applications, providing easy access for attackers.</p>	 <h3>Default settings</h3> <p>Default configurations, such as allowing any domain user to add workstations, can be easily exploited.</p>



WITHOUT AD, BUSINESS OPERATIONS GRIND TO A HALT



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 eventualities.

COMMVAULT® CLOUD FOR ACTIVE DIRECTORY RESILIENCY

Protecting Active Directory may seem 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.



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