Commvault

EXPOSED: ACTIVE DIRECTORY SECURITY HEALTH CHECK

While Microsoft Active Directory simplifies the administration of access to key systems across an organization, the harsh reality is that securing it remains particularly challenging. EXPOSED vulnerabilities in this ever-changing pool of users, groups, policies, and app permissions can devastate your identity resilience strategy.

Here's what to think about in protecting it:

Safeguard AD, which is a primary target.

By exploiting blind spots, bad actors can compromise privileged accounts, mimic authorized users, and silently traverse infrastructure, workstations, and applications. Failing to safeguard AD enables attackers with a centralized location to control and sever access to critical business assets. True identity resilience starts with recognizing that AD protection isn't optional – it's essential.

Perform frequent backups.

You need full backups of the entire AD – frequently, automatically, and off-site – with built-in practices around long-term retention.

Automated forest-level recovery cuts recovery time.

AD forest recovery is intricate and complicated, and can take days to weeks when performed manually. In a disaster, every minute counts – the longer it takes to restore AD, the greater the disruption to the business. A solution that automates forest-level recovery accelerates the process, reduces the risk of human error, and enables a faster, more reliable recovery.

An enterprise-grade solution builds identity resilience.

Homegrown solutions and manual recovery processes are time-consuming, complex, and prone to error. Modern threats demand a purpose-built cyber resilience platform that offers simplified management, layered security with encryption, immutable backups, and automated recovery.

Granular recovery saves time and strengthens resilience.

Not every disruption requires a full restore. Fast, granular recovery lets you restore only what's missing, damaged, or misconfigured, reducing downtime and eliminating the need to recover the entire environment.

Craft your disaster recovery plan and test it before it's needed.

Maintaining a well-documented and regularly tested recovery plan is essential for quickly restoring your AD environment to a healthy, pre-attack state. AD recovery testing builds confidence in your recovery process, and gives IT and security teams the opportunity to practice during good times to prepare for the bad times.

Don't leave your identity infrastructure EXPOSED.

Find out how Commvault Cloud can help your organization build identity resilience and protect your most valuable digital assets.

Commvault®

commvault.com | 888.746.3849