Commvault®

ACTIVE DIRECTORY SECURITY HEALTH CHECK

While Microsoft Active Directory simplifies administrating access to key systems across an organization, securing it can be particularly challenging. It controls an ever-changing pool of users, groups, policies, and app permissions.

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.

✓ Perform frequent backups.

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

✓ An enterprise-grade solution saves headaches.

Homegrown solutions are time-consuming and burdensome for your IT staff. A SaaS solution offers simplified management, layered security with encryption, and protection from ransomware.

✓ Granular recovery saves time.

It takes considerable effort to organize an AD structure with the right items in the correct Organizational Units and with the right permissions, but it's critical. Spare yourself a complete rebuild after a disruption with a dedicated solution that can restore only the missing, damaged, or misconfigured object attribute.

✓ Craft your disaster recovery plans.

If Active Directory is down, business operations grind to a halt, and users cannot access important applications. Having a well-crafted and regularly tested recovery plan is essential to getting your business back online fast when disaster strikes.

✕ Don't leave your AD vulnerable.

Find out how Commvault Cloud can help your organization protect one of your most valuable assets.

Commvault®

commvault.com | 888.746.3849