When Active Directory Works, But Is Not Resilient

By: Jaiz Anuar

7 July 2026 · Cybersecurity · Active Directory · Security Architecture · 6 min read

Many Active Directory environments appear healthy because users can log in, applications authenticate successfully, and domain controllers continue running. But a working Active Directory is not necessarily a resilient Active Directory.

That distinction matters.

In many organisations, Active Directory quietly sits in the background. Users authenticate every morning. Applications bind to LDAP. Group Policies are applied. Passwords are changed. Life goes on.

As long as nothing appears broken, the environment is often considered healthy.

But Active Directory is far more than infrastructure.

It is the identity control plane of the organisation. It determines who can access systems, who receives privileged access, how trust relationships are established, and often where recovery begins after a cyber incident.

The real measure of Active Directory is therefore not whether it works on a normal business day.

The real measure is whether it continues protecting the organisation when conditions become abnormal.

1. A Working Environment Can Create False Confidence

Many organisations judge Active Directory using operational indicators.

Domain Controllers are online. Replication is healthy. CPU utilisation is low. Users authenticate successfully. Applications continue working.

The conclusion becomes obvious.

"Our Active Directory is healthy."

But healthy for what?

Healthy during normal operations does not automatically mean resilient during compromise.

An environment can function perfectly while still carrying architectural weaknesses. Backups may exist but remain inside the same trust boundary. Tier-0 privileges may be permanent. Disaster recovery procedures may never have been exercised. Service accounts may possess excessive permissions that nobody remembers granting.

Operational success should never be confused with architectural resilience.

The better question is not whether Active Directory works today.

The better question is:

What happens when Active Directory becomes the target?

2. Active Directory Is More Than Another Server

One of the biggest architectural mistakes is treating Domain Controllers like ordinary infrastructure servers.

They are not.

Active Directory is a Tier-0 asset.

It authenticates identities. It applies security policy. It establishes trust. It controls privileged access across the enterprise.

If an attacker compromises Active Directory, many downstream security controls become significantly less effective.

This changes how the environment should be protected.

Administrative access should originate from dedicated privileged workstations. Standing privileged access should be minimised. Administrative sessions should be monitored. Emergency accounts should be tightly governed. Privileged identities should exist only for as long as they are genuinely required.

The greatest danger is not simply administrator error.

It is an attacker inheriting administrator privilege.

Permanent privilege creates permanent opportunity.

3. Backup Is Not Recovery

Almost every organisation claims it has Active Directory backups.

That may well be true.

But backup and recovery are not the same capability.

A backup is merely a copy.

Recovery is the ability to restore business operations under pressure.

Modern ransomware has fundamentally changed this conversation.

Attackers increasingly target backup infrastructure before encrypting production systems. Administrative credentials may already be compromised. Recovery environments may depend upon the very identity platform that has been attacked.

This means organisations should regularly prove—not simply assume—that they can restore Domain Controllers, Group Policy Objects, DNS, SYSVOL, and ultimately the Active Directory forest itself.

The critical question is no longer:

Do we have backup?

Instead, it becomes:

Can we recover Active Directory quickly, cleanly, and confidently?

4. Service Accounts Quietly Increase Risk

Service accounts rarely receive the same attention as human identities.

Yet they often possess significant privilege.

Applications depend upon them. Backup systems use them. Monitoring platforms authenticate through them. Integration services rely upon them every day.

Over time, they accumulate.

Some no longer have owners. Others continue operating long after the original application has disappeared. Passwords remain unchanged for years. Privileges continue expanding.

Unlike employees, service accounts never resign.

A resilient Active Directory requires every service account to have a clearly identified owner, defined business purpose, appropriate privilege, monitored activity, and lifecycle management.

Every non-human identity should still have human accountability.

5. Disaster Recovery Is More Than Another Site

Many organisations believe they have solved Active Directory resilience simply because Domain Controllers exist at a disaster recovery location.

Unfortunately, resilience involves much more than geography.

The disaster recovery environment must continue supporting authentication, DNS, Kerberos, LDAP, Group Policy processing, administrative recovery activities, VPN authentication, and business-critical applications under production workload.

Recovery procedures should be exercised under realistic conditions rather than existing only as documentation.

An architecture that succeeds only on diagrams may fail when people depend upon it most.

6. Hybrid Identity Changes Everything

Active Directory no longer exists in isolation.

Many organisations now operate hybrid identity environments where on-premises Active Directory synchronises with Microsoft Entra ID and cloud services.

Identity recovery therefore extends beyond Domain Controllers.

Recovery planning must also consider synchronisation services, password hash synchronisation, Conditional Access dependencies, privileged cloud identities, Microsoft 365 services, and authentication sequencing between cloud and on-premises environments.

Recovery should reflect the actual identity architecture—not yesterday's infrastructure boundaries.

Final Thought

A working Active Directory can hide architectural fragility.

It may successfully support authentication, policy enforcement, administration, and business operations every single day.

But resilience is revealed only when conditions become abnormal.

When privileged credentials are stolen.

When ransomware targets identity.

When disaster recovery becomes production.

When backup must actually be restored.

When hybrid identity behaves differently than expected.

That is when the architecture is truly tested.

Active Directory should therefore never be designed simply to work.

It should be designed to withstand compromise, recover from failure, sustain business continuity, and protect the trust foundation of the organisation.

Because in the end, Active Directory resilience is not merely an infrastructure concern.

It is a security architecture concern.

Question assumptions. Share knowledge. Build trust.