cyberDNA

CONVERSATION ASSET — IDENTITY ARCHITECTURE

Identity Architecture Risk Report

What technology leaders should know about hidden identity risk.

Modern identity environments are becoming increasingly complex.

As organisations adopt cloud services, SaaS applications, automation, hybrid identity platforms, and distributed infrastructure, identity architecture grows organically over time.

Permissions accumulate, service accounts multiply, trust relationships expand, and visibility becomes more difficult.

The result is often an identity environment that functions operationally but **contains hidden architectural risk.**

This executive briefing highlights common identity architecture patterns technology leaders should understand.

BEYOND ACTIVE DIRECTORY

Why Identity Architecture Matters

Modern identity environments extend far beyond Active Directory.

TODAY'S IDENTITY ARCHITECTURE OFTEN SPANS

- Active Directory
- Entra ID
- SaaS applications
- Cloud infrastructure
- Service accounts
- Automation platforms
- Third-party integrations

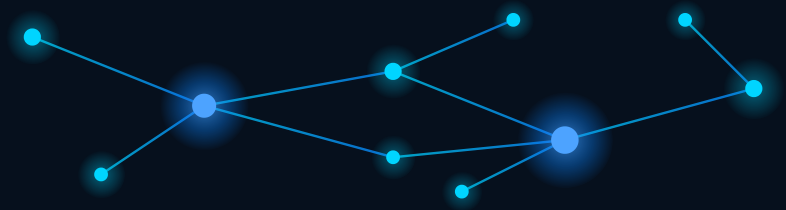
As complexity increases, governance often struggles to keep pace.

Architectural weaknesses may remain invisible for years until they contribute to operational disruption, security incidents, or recovery challenges.

> Technology leaders need visibility not only into individual risks, but into how identity relationships, permissions, and dependencies connect across the environment.

ON-PREMISE & DIRECTORY

CLOUD & SAAS IDENTITY



Access & Hybrid Identity

PATTERNS **01–02** OF 04

01

ARCHITECTURE PATTERN 01

Permission Sprawl

Access is often granted faster than it is removed.

Over time, users accumulate permissions through role changes, project assignments, temporary access requests, and inherited group memberships.

QUESTIONS TO CONSIDER

- How often are permissions reviewed?
- Are inherited privileges understood?
- Can excessive access be identified quickly?
- Is privilege accumulation measured?

ARCHITECTURAL RISK Reduced visibility and excessive access exposure.

02

ARCHITECTURE PATTERN 02

Hybrid Identity Gaps

Many organisations operate across both Active Directory and Entra ID.

While hybrid identity delivers flexibility, it also introduces complexity through synchronisation, trust relationships, duplicated administration, and inconsistent governance.

QUESTIONS TO CONSIDER

- Are identity responsibilities clearly defined?
- Are privileged roles aligned across environments?
- Are trust relationships understood?
- Is visibility consistent across platforms?

ARCHITECTURAL RISK Cross-environment exposure and governance blind spots.

Accounts & Relationships

PATTERNS **03–04** OF 04

03

ARCHITECTURE PATTERN 03

Service Account Growth

Service accounts frequently expand faster than governance processes.

Many organisations discover service accounts that:

- Lack ownership
- Support retired applications
- Have excessive permissions
- Remain active long after their original purpose

QUESTIONS TO CONSIDER

- Are service account owners documented?
- Are dependencies understood?
- Are permissions regularly reviewed?
- Can dormant accounts be identified?

ARCHITECTURAL RISK Hidden operational and security dependencies.

04

ARCHITECTURE PATTERN 04

Identity Relationship Complexity

Modern identity environments create thousands of interconnected relationships.

Groups, nested permissions, delegated administration, service identities, and cloud roles can create pathways that are difficult to visualise.

QUESTIONS TO CONSIDER

- Can critical identity relationships be mapped?
- Are attack paths understood?
- Are privileged chains visible?
- Can identity dependencies be analysed quickly?

ARCHITECTURAL RISK Hidden pathways and decision-making complexity.

COMMON FINDINGS

What Independent Identity Architecture Reviews Commonly Reveal

Independent reviews commonly uncover:

- Permission accumulation over time
- Service account ownership gaps
- Dormant privileged identities
- Inconsistent governance between AD and Entra
- Unclear recovery dependencies
- Privileged access relationships that are poorly understood
- Excessive administrative access
- Architectural complexity that has grown organically

> **Most findings are not the result of negligence.** They are often the natural consequence of growth, operational demands, mergers, cloud adoption, and evolving technology environments.

SELF-ASSESSMENT

Identity Architecture Review Checklist

How many of the following can you confidently answer "Yes" to?

- ☑ We understand our critical identity dependencies
- ☑ Service account ownership is documented
- ☑ Hybrid identity governance is clearly defined
- ☑ Permissions are regularly reviewed
- ☑ Privileged relationships are visible
- ☑ Identity architecture has been independently reviewed
- ☑ Identity recovery dependencies are understood
- ☑ Architectural complexity is actively managed

Complexity is not the problem. Unseen complexity is.

If helpful, we'd be happy to have an initial discussion about your current identity architecture and areas where hidden complexity may warrant closer attention.

Request an Initial Conversation →

OR

CONTACT

sales@cyberdna.com.au

WEBSITE

www.cyberdna.com.au