CYBERDNA

The Ultimate Guide to Eliminate AD & Entra ID Risks in Just 90 Days

The step-by-step framework for IT and security leaders who need results, not theory.

WHAT YOU'LL LEARN INSIDE

- Why Active Directory and Entra ID are the #1 target in 9 out of 10 cyberattacks
- The 7 most dangerous identity risks hiding in your environment right now
- A proven 90-day framework to find, fix, and monitor your biggest identity risks
- The attack paths attackers use — and how to close them before they do
- How to build the business case for identity security investment

This guide is designed for:

IT Managers, Security Managers, CISOs, and CIOs at organisations running Active Directory or Microsoft Entra ID (Azure AD) with 50–5,000 employees.

cyberdna.com.au

Managed Identity Risk • Managed Cloud Risk • Managed Breach Risk

Table of Contents

Introduction: The Identity Crisis No One Talks About

You probably have a firewall. You probably have antivirus. You might even have a SIEM. But there's one area most organisations ignore until it's too late: identity.

80% of cyberattacks involve compromised credentials or identity misconfigurations. Not malware. Not zero-days. Identity.

Active Directory (AD) and Microsoft Entra ID (formerly Azure AD) are the backbone of almost every organisation's IT environment. They control who can access what — which makes them the most valuable target in any network.

The problem? Most organisations set them up years ago, keep adding to them, and never step back to audit the risk that has been building up silently.

Stale admin accounts. Over-privileged service accounts. Legacy protocols that bypass MFA. Misconfigured delegation settings. Credentials leaked on the dark web. These aren't theoretical risks — they're findings we see in almost every identity assessment we run.

> *The average attacker spends 207 days inside a network before they're detected. In the vast majority of cases, they used compromised identity — not malware — to get in and stay hidden.*

This guide gives you a practical, 90-day framework to find your biggest identity risks, fix the most critical ones, and build the foundation for a sustainable identity security program.

You don't need to be a security expert to follow this guide. You need to be willing to look at what's in your environment, and commit to 90 days of structured action.

Let's get started.

Chapter 1: Why AD & Entra ID Are Attackers' Favourite Targets

Active Directory has been the backbone of enterprise identity for over two decades. Entra ID extended that to the cloud. Together, they control access to virtually everything in your organisation: files, systems, applications, email, and infrastructure.

That's exactly why attackers love them.

1.1 The Scale of the Problem

Consider what Active Directory and Entra ID control in a typical mid-size organisation:

- Every user's login credentials
- Access to file servers, email, cloud apps, and VPNs
- Privileged accounts that can reset passwords, modify Group Policy, or replicate the entire directory
- Service accounts running critical business systems
- Trust relationships with partner organisations

When an attacker compromises one privileged account — or finds a single misconfiguration — the blast radius is enormous. They don't need to break through your firewall. They just need to find one unlocked identity door.

1.2 The Most Common Identity Attack Patterns

These are the attack techniques our team sees most frequently in the wild:

Attack Technique	What It Does
Kerberoasting	Extracts service account hashes from AD and cracks them offline. No special privileges required.
DCSync	Impersonates a Domain Controller to steal all password hashes in AD. Gives attacker full domain control.
Pass-the-Hash	Reuses stolen NTLM hashes to authenticate as another user without knowing their password.
AS-REP Roasting	Targets accounts with Kerberos pre-auth disabled. Extracts crackable hashes with no credentials required.
Credential Stuffing	Uses leaked username/password pairs from dark web breaches against your Entra ID tenant.
Token Theft	Steals OAuth tokens from compromised devices to access cloud resources, bypassing MFA entirely.

None of these techniques require exotic skills. They're taught in free online courses and automated by tools that are publicly available. The barrier to launching these attacks is lower than most security teams realise.

1.3 Why Traditional Security Misses Identity Attacks

Most security tools are designed to detect malware and network intrusions. They look for suspicious files, weird network traffic, or known attack signatures.

Identity attacks look different. An attacker using a legitimate admin account to browse file servers doesn't look like an attack — it looks like normal admin work. Without identity-specific detection, these attacks are invisible.

> **Key Insight:**
> A firewall stops traffic. A SIEM alerts on signatures. But neither one tells you which of your admin accounts has a password from a 2019 data breach, or which service account can replicate your entire directory. Only identity-specific visibility does that.

Chapter 2: The 7 Most Dangerous Identity Risks in Your Environment

After running hundreds of identity assessments, these are the seven risks we find most often — and the ones attackers exploit first.

Risk 1: Stale Privileged Accounts

Domain Admins who left the company six months ago. Service accounts for applications that were decommissioned two years ago. Admin accounts created for a one-off project and never disabled.

Every one of these is an open door. An attacker doesn't need to create a new account if there's already a Domain Admin account sitting dormant with no monitoring.

What to look for: Accounts with Domain Admin, Enterprise Admin, or Schema Admin rights that haven't logged in within 90 days.

Risk 2: Excessive Privilege (Privilege Creep)

Over time, users accumulate permissions. A developer gets admin access for a project and keeps it. An IT technician is added to Domain Admins temporarily and never removed. A service account is given broad AD rights because it was "easier at the time."

The result is an environment where far too many accounts have far too much access — and any one of them becoming compromised is a catastrophic event.

What to look for: Users with privileged group memberships that exceed their job role. Service accounts with Domain Admin rights.

Risk 3: MFA Not Enforced on Privileged Accounts

It surprises most people: even in 2024, a significant number of organisations still have Domain Admins or Global Admins in Entra ID without MFA enforced. Sometimes it's a legacy exclusion. Sometimes it's a break-glass account that was never properly secured. Sometimes it just fell through the cracks.

A privileged account without MFA is a single compromised password away from a full domain takeover.

What to look for: Privileged accounts in Entra ID not covered by Conditional Access policies requiring MFA. Local admin accounts with no additional controls.

Risk 4: Kerberoastable Service Accounts

Service accounts in Active Directory are often configured with weak or never-expiring passwords, and many are registered as Service Principal Names (SPNs). Any authenticated user can request a Kerberos service ticket for these accounts and attempt to crack the password offline.

A weak service account password can be cracked in minutes. If that account has elevated AD rights — as many do — the attacker now has domain-level access.

What to look for: Accounts with SPNs registered that have passwords older than 1 year, or weak password complexity.

Risk 5: Leaked Credentials on the Dark Web

Your employees use their corporate email addresses to sign up for external services. Those services get breached. The email/password combinations end up for sale on dark web marketplaces.

If an employee reuses their corporate password on an external site, and that site is breached, an attacker now has valid credentials for your Entra ID environment. This happens constantly — and most organisations have no visibility into it.

What to look for: Corporate email addresses appearing in known data breach datasets. Users whose breached passwords match their current corporate password.

Risk 6: Legacy Authentication Protocols

Legacy authentication protocols (NTLM, Basic Auth, legacy SMTP) don't support modern MFA. When these protocols are enabled, an attacker can use them as a side door to bypass your Conditional Access policies entirely.

Microsoft has been pushing organisations to disable these for years. Most have not fully done so.

What to look for: NTLM authentication still active in your environment. Sign-in logs showing authentication via legacy protocols. Applications still using Basic Auth.

Risk 7: Misconfigured Delegation in AD

Kerberos delegation allows one system to authenticate to another on behalf of a user. When configured correctly, it's a normal part of enterprise applications. When misconfigured — specifically when "Unconstrained Delegation" is enabled — it allows an attacker to capture the Domain Controller's authentication ticket and gain full domain control.

Unconstrained delegation was the default in older versions of AD and was often enabled for convenience. Many environments still have it.

What to look for: Computers or user accounts with Unconstrained Delegation enabled, especially if they're not Domain Controllers.

> **Reality Check:**
>
> *In a recent identity assessment, we found all seven of these risks present in the same environment. The organisation had a SOC, an EDR, and a SIEM. None of those tools flagged a single one.*

Chapter 3: The 90-Day Identity Risk Elimination Framework

This framework is designed to be executable by an internal IT or security team, with or without additional tooling. It's structured in three phases of 30 days each, moving from visibility to action to resilience.

Phase	Days 1–30: Discover	Days 31–60: Remediate	Days 61–90: Monitor
Focus	Get full visibility into your identity risks	Fix critical risks, harden your environment	Build ongoing detection & response capability

Phase 1: Days 1–30 — Discover & Assess

You cannot fix what you cannot see. Phase 1 is about getting a complete, honest picture of your identity attack surface. No assumptions. No guesses. Data.

Week 1: Privileged Account Inventory

Run a complete audit of all accounts with privileged AD group memberships. This means Domain Admins, Enterprise Admins, Schema Admins, Backup Operators, Account Operators, and any custom groups with elevated AD rights.

For each account, record:

- Account type (user, service account, or computer account)
- Last login date
- Password last changed date
- Whether MFA is enrolled (for Entra ID accounts)
- The business owner responsible for this account

Week 2: Entra ID Conditional Access Audit

Review every Conditional Access policy in your Entra ID tenant. Map which users, applications, and conditions are covered — and more importantly, what's excluded.

Common exclusions that create risk:

- Emergency access accounts excluded from all CA policies
- Legacy application service accounts excluded from MFA

- Break-glass accounts with no monitoring
- Gaps where legacy authentication is still permitted

Week 3: Service Account & SPN Review

Enumerate all service accounts in Active Directory. For each, document the SPN registrations, password age, group memberships, and the system or application it runs. Flag any service account with:

- Domain Admin or equivalent privileges (almost never justified)
- A password older than 1 year
- No known business owner

Week 4: Dark Web Credential Check & Legacy Protocol Audit

Check whether corporate email addresses appear in known credential breach datasets. This can be done manually using free tools like HaveIBeenPwned for individual checks, or via an automated identity intelligence service for bulk checking at scale.

Simultaneously, run an audit of authentication logs in both AD and Entra ID to identify any sign-ins using legacy protocols (NTLM, Basic Auth, POP3, IMAP).

> **Phase 1 Output:**
> A risk register with every finding categorised by severity (Critical / High / Medium). This becomes your remediation backlog for Phase 2.

Phase 2: Days 31–60 — Prioritize & Remediate

With your risk register in hand, Phase 2 is about systematic remediation — starting with the risks that give attackers the most leverage and working down.

Remediation Priority Order

1. Disable or review all stale privileged accounts (especially Domain Admins with no recent login activity)
2. Enforce MFA on all privileged accounts in Entra ID via Conditional Access
3. Reset passwords on all Kerberoastable service accounts. Consider migrating to Group Managed Service Accounts (gMSA) which rotate passwords automatically
4. Disable Unconstrained Delegation on any non-Domain Controller computer or user accounts

5. Block legacy authentication protocols via Conditional Access in Entra ID
6. Reset credentials for any corporate accounts that appear in dark web breach data
7. Remove Domain Admin rights from service accounts that don't require them

Change Management Tips

Some of these changes carry operational risk if done carelessly. Before remediating:

- Communicate changes to impacted application owners and system owners
- Test in a non-production environment first for changes to delegation or service accounts
- Implement a rollback plan for each change
- Document every change made with a date, rationale, and approver

> **Pro Tip:**
> Don't try to fix everything at once. An aggressive remediation without proper change management can break applications and create outages. Prioritise the five highest-severity findings in week 5, then work through the list systematically.

Phase 3: Days 61–90 — Monitor & Mature

Fixing known risks is not the end of the program. New accounts are created. Applications are onboarded. Configurations drift. Phase 3 builds the ongoing capability to detect and respond to identity threats as they emerge.

Build Your Identity Monitoring Baseline

Define what "normal" looks like for your environment:

- Which accounts log in outside business hours?
- Which accounts typically authenticate from which locations?
- What is the normal volume of failed authentication attempts?
- Which privileged accounts are used for which tasks?

Key Alerts to Configure

At minimum, configure alerts for the following events in your SIEM or identity monitoring tool:

- New account added to Domain Admins or Global Admins
- Privileged account login outside business hours from unexpected location

- Account created and used to access sensitive resources within 24 hours
- Mass file access or deletion from a user account
- Kerberos TGT requested for account that hasn't been used in 90 days
- Legacy authentication sign-in attempts on accounts that should only use modern auth

Establish a Quarterly Identity Review

Schedule a quarterly review of:

- New privileged accounts created since the last review
- Service accounts with aging passwords
- Conditional Access policy coverage gaps
- New applications integrated with Entra ID and their access scope
- Any new findings from dark web credential monitoring

> **Phase 3 Output:**
> A sustainable, repeatable identity security program. Not a one-time project. Identity security is not a destination — it's an ongoing practice.

Chapter 4: Common Identity Attack Paths & How to Close Them

Understanding how attackers move through an environment helps you prioritise your remediation efforts. Here are the most common attack paths in AD and Entra ID environments.

Attack Path 1: Kerberoasting → Domain Compromise

Step 1: Attacker gains any valid domain user account (phishing, credential stuffing, or physical access).

Step 2: They query AD for accounts with SPNs registered (this requires no special privileges).

Step 3: They request Kerberos service tickets for those accounts.

Step 4: They take the encrypted tickets offline and crack them with tools like Hashcat.

Step 5: If the service account has Domain Admin rights or weak passwords, they now have elevated access.

How to close it: Ensure all service accounts have strong, 25+ character passwords. Migrate to gMSA wherever possible. Remove unnecessary SPNs. Remove Domain Admin rights from service accounts.

Attack Path 2: Credential Stuffing → Entra ID Tenant Access

Step 1: Attacker purchases corporate email/password pairs from a dark web breach dataset.

Step 2: They test credentials against your Entra ID tenant via legacy authentication endpoints (which bypass Conditional Access and MFA).

Step 3: Successful logins give them access to email, Teams, SharePoint, and any SaaS applications connected to Entra ID.

How to close it: Block legacy authentication via Conditional Access. Enable and enforce MFA for all users. Monitor Entra ID sign-in logs for authentication from unusual locations or via legacy protocols. Run dark web monitoring to proactively identify compromised credentials.

Attack Path 3: Unconstrained Delegation → Domain Controller Impersonation

Step 1: Attacker compromises a server or workstation with Unconstrained Delegation enabled (often a file server or application server).

Step 2: They wait for a privileged user — or the Domain Controller itself — to authenticate to that server.

Step 3: Their Kerberos ticket, including the Domain Controller's TGT, is cached on the compromised server.

Step 4: Attacker extracts the TGT and uses it to perform a DCSync attack, replicating all password hashes from AD.

Step 5: Game over. Full domain compromise.

How to close it: Audit and disable Unconstrained Delegation on all non-Domain Controllers. Migrate to Constrained or Resource-Based Constrained Delegation. Mark privileged accounts as "Account is sensitive and cannot be delegated."

Chapter 5: Building the Business Case for Identity Security

You know the risk. Now you need to get the budget and the organisational support to fix it. Here's how to make the case to your board or executive team.

5.1 Translate Technical Risk into Business Impact

Your board doesn't think in terms of Kerberoasting or Unconstrained Delegation. They think in terms of:

- Business disruption: How long would operations stop if we had a ransomware incident?
- Financial exposure: What would a breach cost us in recovery, regulatory fines, and lost revenue?
- Regulatory risk: What are our obligations under Privacy Act, ISO 27001, or cyber insurance requirements?
- Reputational risk: What happens to customer trust if our data is stolen and published?

Frame your identity security program in these terms. For example:

> ***Instead of:***
>
> *"We have 12 accounts with Unconstrained Delegation enabled."*
>
> **Say:**
>
> "We have 12 configurations in our environment that, if exploited, would give an attacker complete control of our Active Directory within hours. Recovery from a full AD compromise typically takes 3–7 days minimum and costs between $250,000 and $1M+ in our sector."

5.2 The Cost of Doing Nothing

The cost of identity security investment needs to be compared not to zero, but to the cost of a breach. Industry data is consistent:

Metric	Typical Figure
Average cost of a data breach (IBM, 2023)	USD $4.45 million globally
Average time to identify a breach	207 days
Average time to contain a breach	70 days

Percentage of breaches involving credentials	~80%
Percentage of attacks using identity as entry point	>90% in ransomware cases

5.3 The Board-Level Three-Point Framework

When presenting to executives, structure your case in three points:

8. Where we are today: the current state of our identity risk (use findings from your Phase 1 assessment). Present the number of critical findings, not the technical details.
9. What it means if unaddressed: the realistic business impact if the top three findings are exploited. Quantify where possible.
10. What we're doing about it: your 90-day plan, the investment required, and the risk reduction outcome.

This framing respects the board's time, speaks their language, and positions you as a proactive leader — not someone asking for budget after a problem has already occurred.

Chapter 6: Tools & Technologies for Identity Security

You don’t need an enterprise security budget to run this program. There are free and commercial tools at every level.

Free & Built-in Tools

- Microsoft Entra ID Portal: Conditional Access, Sign-in logs, Identity Protection (P2 licence required for full features)
- Microsoft Defender for Identity (MDI): Detects identity attacks in AD environments. Available in Microsoft 365 E5.
- BloodHound Community Edition: Visualises AD attack paths. Used by attackers AND defenders. Free and invaluable.
- PingCastle: Free AD health assessment tool. Scores your AD against hundreds of risk checks.
- HaveIBeenPwned API: Check corporate email addresses against known breach data.
- PowerShell (Active Directory module): Native AD querying for auditing accounts, SPNs, delegation settings.

Commercial Identity Security Platforms

As your program matures, manual tools become insufficient for continuous monitoring. Commercial platforms provide:

- Continuous monitoring of AD and Entra ID for new risks as they emerge
- Automated dark web credential monitoring at scale
- Identity threat detection and real-time alerting on attack behaviour
- Identity disaster recovery — the ability to restore AD to a known-good state after a compromise

CyberDNA’s Managed Identity Risk (MIR) service is built on the Dela Security platform, which provides all four of these capabilities in a single managed service. It connects to your AD and Entra ID environment in under 30 minutes and surfaces your full identity risk picture immediately.

Conclusion: What to Do Right Now

You've now got a clear picture of the identity threat landscape, the seven most dangerous risks, a 90-day framework to address them, and the business case to get it funded.

Here's the honest truth: most organisations know they have identity risk. What they lack is a clear starting point, a prioritised action plan, and the internal capacity to execute it.

That's where CyberDNA can help.

What a Managed Identity Risk (MIR) Assessment Looks Like

Our MIR service starts with a free Breach Likelihood Assessment. In under 30 minutes, we connect to your Active Directory and Entra ID environment, run a comprehensive risk scan, and give you a prioritised report of your top findings.

You'll see:

- Which accounts represent your highest-severity risks right now
- Whether any corporate credentials have appeared in dark web breach data
- Your AD health score benchmarked against similar organisations
- A prioritised remediation roadmap

No long engagement. No commitment required. Just visibility.

This assessment is designed for organisations with 50–5,000 employees running Active Directory or Microsoft Entra ID. It's not intended for home users or organisations without Microsoft identity infrastructure.

READY TO SEE YOUR IDENTITY RISK?

Book your free Breach Likelihood Assessment with CyberDNA.

30 minutes. No commitment. Your full identity risk picture.

Book Your Free Assessment → cyberdna.com.au

About CyberDNA

CyberDNA is an Australian cybersecurity services company specialising in identity security, managed security services, and vulnerability management. We protect organisations running Active Directory and Microsoft Entra ID across Australia and New Zealand.

cyberdna.com.au | MIR • MCR • MBR

