cyberDNA

IDENTITY INTELLIGENCE

EXECUTIVE BRIEFING · 2026

Hidden Identity Exposure Checklist

10 questions every security leader should ask — **before attackers do**.

cyberdna.com.au

Identity · Exposure · Visibility

Hidden exposure doesn't always look like weak security.

Many organisations have the controls a mature security programme is expected to have:

- ✓ MFA
- ✓ EDR
- ✓ SIEM
- ✓ Strong compliance

Even mature organisations may still struggle to answer:

01 Which dormant accounts still have access?

02 How many vendor identities are currently active?

03 Are machine identities governed?

04 Which users retain standing privilege?

05 Where does legacy authentication still exist?

> **Identity exposure is not always obvious. Sometimes the greatest risk is the risk you cannot see.**

Ten questions to surface hidden exposure

Answer each honestly. The questions you cannot answer with confidence are often where exposure concentrates.

- [ ] **01 Do you know every privileged identity in your environment?**

  WHY IT MATTERS Excessive or unmanaged privilege increases identity exposure and can expand the impact of a compromised account.

- [ ] **02 Are dormant accounts identified and regularly removed?**

  WHY IT MATTERS Inactive identities that remain enabled can create unnecessary exposure.

- [ ] **03 Is MFA enforced consistently across all critical systems?**

  WHY IT MATTERS Authentication strength remains one of the most important identity security controls.

- [ ] **04 Can you identify all third-party and vendor identities?**

  WHY IT MATTERS External identities often require ongoing governance and access review.

- [ ] **05 Are machine identities inventoried and managed?**

  WHY IT MATTERS Service accounts and API credentials can become overlooked attack paths.

- [ ] **06 Do users retain privileged access longer than necessary?**

  WHY IT MATTERS Standing privilege may increase exposure compared to time-bound or just-in-time access.

- [ ] **07 Does your identity lifecycle automatically remove access when roles change?**

  WHY IT MATTERS Delayed deprovisioning can result in unnecessary permissions remaining active.

- [ ] **08 Do you know where legacy authentication is still used?**

  WHY IT MATTERS Legacy protocols may bypass modern identity protections.

- [ ] **09 Can you visualise identity relationships across SaaS, cloud and on-premises environments?**

  WHY IT MATTERS Fragmented visibility makes identity governance more difficult.

- [ ] **10 Could your security team explain your identity exposure to the board?**

  WHY IT MATTERS Identity security is increasingly a strategic risk discussion, not simply an IT function.

How many did you answer "No" to?

Each "No" represents a question your programme may not currently be able to answer — a place where identity exposure can persist unseen.

0–2

ANSWERED "NO"

Strong visibility

A solid foundation. Continue improving identity governance and close remaining gaps.

3–5

ANSWERED "NO"

Potential Hidden Exposure

Identity visibility gaps may exist. Several areas likely warrant closer review.

6+

ANSWERED "NO"

High Likelihood of Identity Blind Spots

You may have identity risks that traditional security programmes do not fully expose.

This checklist is intended to promote discussion and does not constitute a formal assessment.

The most dangerous identity risks are often invisible.

An organisation may have every expected control in place —

- ✓ MFA
- ✓ Endpoint protection
- ✓ Compliance certifications
- ✓ Security monitoring

— and still struggle with exposure that no control flags:

- Dormant privileged accounts
- Forgotten service accounts
- Vendor access sprawl
- Legacy authentication
- Identity fragmentation

Identity exposure is not always caused by missing controls. It is often caused by missing visibility into identities, privileges, and access relationships that accumulate over time.

Discover the Identity Risks Hidden Behind Mature Security Programs

Using the CyberDNA Identity Risk Index, organisations can evaluate identity exposure across six critical domains.

- Authentication
- Privileged Access
- Identity Lifecycle
- SaaS Governance
- Machine Identities
- Third-Party Access

Request Your Identity Risk Review →

A focused conversation with a CyberDNA identity specialist.

OR SCAN TO BOOK
Identity Risk Review

sales@cyberdna.com.au · cyberdna.com.au