cyberDNA

IDENTITY INTELLIGENCE

EXECUTIVE BRIEFING · 2026

# 2026 Identity Attack Trends Guide

How modern adversaries exploit identity, credentials and access to breach enterprises.

# Identity has become a critical attack surface.

Organisations continue to invest in the controls a mature security programme is expected to have:

- ✓ EDR
- ✓ SIEM
- ✓ Vulnerability Management
- ✓ Cloud Security

Yet adversaries increasingly pursue identity rather than infrastructure:

- Credentials
- Tokens
- Privileged accounts
- Session hijacking
- Service accounts

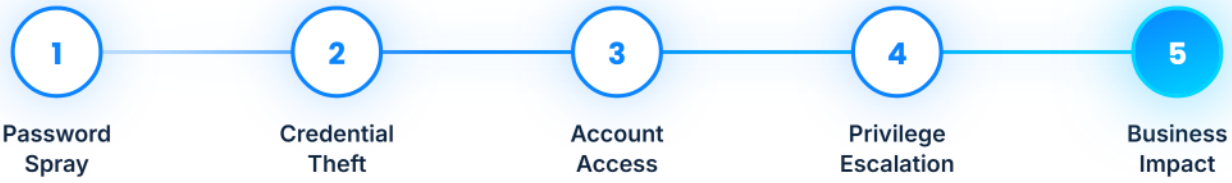
> **Modern attacks frequently begin with identity.**

# 1 Credential theft continues to drive breaches

Credentials remain among the most sought-after assets. Rather than exploiting infrastructure, adversaries frequently obtain valid credentials and log in.

- Password spraying
- Credential stuffing
- Phishing
- Session theft
- Token abuse




KEY MESSAGE

**Compromising identity often provides easier access than exploiting infrastructure.**

INFORMED BY Microsoft Verizon DBIR

# 2 Privileged access remains a high-value target

Elevated access concentrates risk. Once inside, adversaries seek the accounts and roles that expand what a single compromise can reach.

Admin accounts | Standing privilege | Shared accounts | Privileged SaaS roles


Compromise value concentrates toward the top tiers.

KEY MESSAGE

**The impact of compromise often depends more on privileges than on the initial intrusion itself.**

INFORMED BY Verizon DBIR CISA

# 3 Machine identities are expanding the attack surface

Modern enterprises increasingly depend on non-human identities — often outnumbering people, and frequently without clear ownership.

Service accounts | Secrets | Certificates | API keys


KEY MESSAGE

**Many organisations understand their users, but lack visibility into machine identities.**

INFORMED BY CISA NIST

# 4 Third-party access creates hidden exposure

External relationships extend the identity perimeter. Vendor, contractor and partner access is rarely scoped as tightly as internal access.

Vendors | Contractors | Partners | External identities


Access relationships expand over time →

KEY MESSAGE

**External access often persists longer than intended.**

INFORMED BY CISA | Identity governance best practices

# 5 Legacy authentication continues to increase risk

Older protocols remain in use across many environments, quietly widening the set of paths an attacker can take.

Lacks MFA | Weaker authentication | Expanded attack paths

| Modern Identity | | Legacy Authentication |
|---|---|---|
| ✓ MFA | vs | ✗ MFA gaps |
| ✓ Strong authentication | | ✗ Older protocols |
| ✓ Conditional access | | ✗ Expanded attack paths |

KEY MESSAGE

**Security maturity does not always mean identity maturity.**

INFORMED BY Microsoft NIST

# The most dangerous identity risks are often invisible.


Identity exposure often develops gradually. Many organisations discover hidden risks only after a security event — or a dedicated identity assessment.

# What should security leaders ask?

Hidden identity exposure often starts with questions like these.

01 ☐ Where are privileged identities concentrated?

02 ☐ Which dormant accounts remain active?

03 ☐ Are machine identities inventoried?

04 ☐ How is third-party access governed?

05 ☐ Where does legacy authentication still exist?

06 ☐ Is identity exposure visible across cloud, SaaS and on-premises systems?

> **Organisations do not always discover identity exposure through incidents. Often, they discover it through visibility.**

cyberDNA

YOUR NEXT STEP

# Discover the Identity Risks Hidden Behind Mature Security Programs

Using the CyberDNA Identity Risk Index, identify identity exposure across six critical domains.

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

**Request Your Identity Risk Review →**

A focused conversation with a CyberDNA identity specialist.

SCAN TO BOOK INSTANTLY

**Identity Risk Review**

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