zscaler™

ThreatLabz

ANZ Executive Perspective

AI Security 2026

Security Maturity in a World of Machine-Speed Corporate Risk

AI adoption in Australia and New Zealand (ANZ) has moved from 'new' to 'normalised'. Accordingly, the 2026 cybersecurity landscape across ANZ has shifted from human-led skirmishes to **autonomous, AI-fuelled, machine-speed warfare.** While organisations are rapidly integrating AI into their infrastructure, security maturity is not keeping pace.

The challenge facing ANZ's executive leadership is clear: while AI drives productivity, protecting your business's brand and bottom line just got harder. Traditional 'perimeter' and 'binary' security models are obsolete. 2026 is the year **Zero Trust** becomes a mandatory operational standard, not just a technical goal. It is central to aligning business and technology trust with customer and employee experiences, and board expectations.

This report is a snapshot of the latest data from Zscaler's ThreatLabz AI Security Report 2026, with a laser focus on ANZ. It looks at the key AI drivers in ANZ to date, predictions for the future, and critical actions to manage your corporate risk and build organisational trust.

ANZ AI/ML TRANSACTIONS IN 2025

(June-December 2025)

AI SYSTEM VULNERABILITIES AND FAILURE RATES*

Critical vulnerabilities identified in

100%

of AI systems tested

90% of systems failed wihin

1 hour 27 minutes

Median time to first critical vulnerability:

16 minutes

Fastest observed failure:

1 second

* Based on Zscaler red team testing—authorised adversarial simulations where ethical hackers emulate real-world threat actors.

3 Strategic Themes Critical for 2026

Threat reports are great, but executives and boards must match threats with actions. Here are three critical themes for your 2026 security strategy to succeed.

1. Sanctioned Risk: Data Leakage at Scale

Productivity tools like **Grammarly (38.7% of AI/ML transactions globally) and ChatGPT (14.2%)** are the most used AI apps[1]. However, without strict governance, these apps create high-volume data leakage pathways where sensitive inputs can result in a 'Notifiable Data Breach' under **Australian Privacy Law.** Risk of exposure is already playing out at scale, with 18,033 terabytes of data transferred to AI/ML applications globally in 2025[2].

This has become a board-level issue as AI touches core service delivery and core data, requiring audits to measure your setup against benchmarks such as the **ACSC's Essential Eight** mitigation strategies, anchored in increased visibility, risk modification, qualification and treatment plans, and lifecycle governance for AI use, not just ad hoc policy.

2026 Outlook

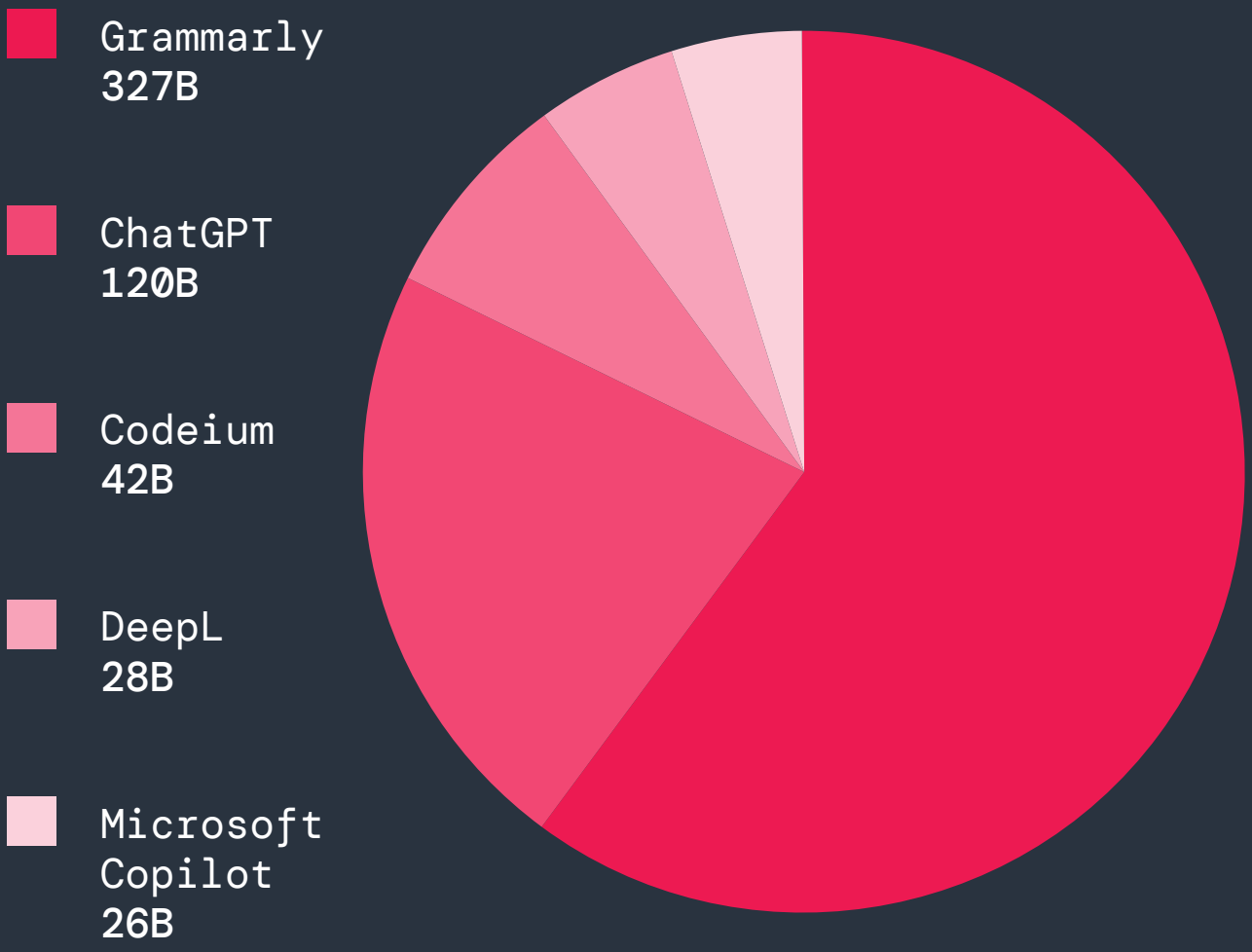
Securing AI will no longer be optional or confined to technical teams. As organisations move from GenAI pilots to full deployments, attackers will target data stores behind GenAI apps, giving them greater visibility into internal decision-making cycles.

Leadership and boards will be expected to have clear visibility into AI risk and security policies across their entire business and ecosystem.

[1] Zscaler ThreatLabz 2026 AI Security Report
[2] Zscaler ThreatLabz 2026 AI Security Report

TOP 5 APPS GLOBALLY FOR AI OR ML RELATED TRANSACTIONS

(June-December 2025)



While ANZ's app landscape varies, major concerns are shared around sensitive source code and Personally Identifiable Information (PII) leaking into LLMs at record speed[3]. 60% of Oceania tech leaders identify **AI-driven social engineering** as their top threat for 2026[4].

[3] Zscaler ThreatLabz AI Security Report 2026
[4] ISACA/Technology Decisions: "ISACA reports on what's keeping tech leaders up at night for 2026"
[5] Zscaler ThreatLabz AI Security Report 2026

2. AI as Infrastructure: The New Crown Jewels

AI is no longer just a tool; it is **always-on infrastructure.** Engineering and IT departments now account for over **80% of total AI transactions** as they focus on building and delivering enhanced services[5].

AI adoption is outpacing oversight. Attackers are shifting from targeting users to **tampering with AI models and datasets** directly. Increasingly, this includes AI embedded within enterprise applications and development platforms, extending beyond what organisations can directly see or control. A single compromised vendor integration can become a shortcut to an **organisation's 'crown jewels'** via ungoverned data paths and unmonitored copilots.

2026 Outlook

Attacks on AI supply chains will **target core components powering organisation-wide AI systems.**

Attackers will focus on **tampering with AI models and datasets,** taking advantage of embedded AI across software supply chains to steal information and move laterally.

[3] Zscaler ThreatLabz AI Security Report 2026
[4] ISACA/Technology Decisions: "ISACA reports on what's keeping tech leaders up at night for 2026"
[5] Zscaler ThreatLabz AI Security Report 2026

3. Machine Speed: Breaking AI Systems in Minutes

Security controls designed for human reaction times cannot stop AI-driven attacks. Zscaler red teaming found that **100% of enterprise AI systems** had critical flaws, with a median time to first failure of just **16 minutes.**

At the same time, attacks are becoming more precise and convincing, moving from generic scams to voice deepfakes and AI-generated emails that flawlessly mimic trusted organisations across **government, utilities and major banks.**

2026 Outlook

As agentic AI attacks, both autonomous and human-orchestrated, are embedded into AI workflows, **rogue agents will become harder to spot.**

This will drive attacks that combine **phishing, automated decision-making, and high-speed data theft at machine speed.**

Industries in the Crosshairs

Industry	Why they are targeted	Primary AI Threat
Financial Services	High direct financial gain	AI-driven credential stuffing and deepfake fraud
Healthcare	Sensitive PII for ransom or extortion	AI-driven credentials compromise
Government & Defence	Strategic intelligence and citizen data	AI-driven spear-phishing and state-sponsored espionage
Critical Infrastructure	Essential services (power, water, and telecommunications)	Autonomous malware designed to disrupt physical systems
Retail & E-commerce	High volumes of credit card data	AI bots that scrape data or perform ‘inventory hoarding’

Financial Impact and Regulatory Escalation

The financial stakes for ANZ organisations have reached record highs as cybercrime becomes industrialised. In Australia, **large businesses have seen a staggering 219% increase in average cybercrime costs;** the average cost of a cyberattack for a large Australian business now exceeds **$202,000**, while medium-sized firms face nearly **$100,000** per incident[6]. In New Zealand, **the average cost of a data breach for an SME has climbed to NZD $173,000**[7]. And the regulators are responding.

[6] Australian Signals Directorate: "Annual Cyber Threat Report 2024-2025"
[7] National Cyber Security Centre: "Businesses in Aotearoa need to prioritise cyber security."

	Australia	New Zealand
Approach	Risk-based guardrails; mandatory for Government	'Adopter nation' and innovation focus; light-touch, voluntary
Lead Authorities	Australian Government Australian Signals Directorate Australian Government Digital Transformation Agency	MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT HĪKINA WHAKATUTUKI National Cyber Security Centre
Strategies, Policies & Mandates	PSPF 2025 formally mandates **Zero Trust** Guidance for AI Adoption (GfAA) as essential practices for developers and deployers Policy for the responsible use of AI in government	Responsible AI guidance for businesses New Zealand's Cyber Security Action Plan 2026 - 2027
Regulatory 'Hammer'	Penalties up to **AU$50 million** or **30% of annual turnover** for serious breaches	**NZ$5 million** or **2% of annual turnover**, alongside **director penalties of up to NZ$500,000**
Key Deadline	New mandatory AI policy requirements (June 2026)	Biometric Processing Privacy Code (late 2025)

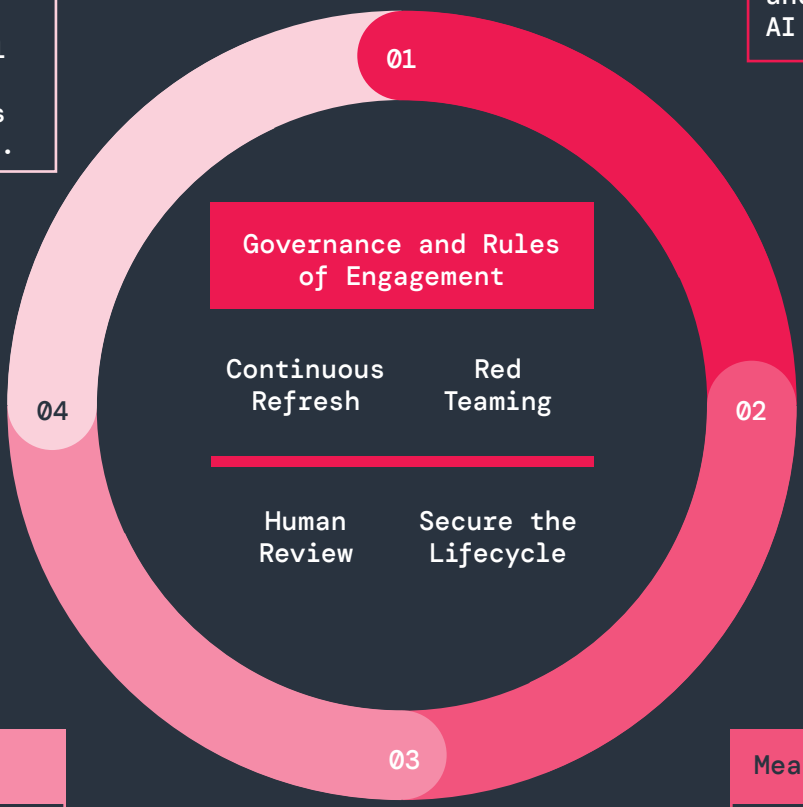
AI Security Cycle: Executive Action Checklist

Govern

Define your internal “rules of engagement” and move oversight from IT to board-level accountability. Ensure inline inspection of all AI/ML traffic to prevent malicious data exfiltration.

Discover

Create a continuous catalog of all GenAI and SaaS tools with AI features.



Manage

Implement least privilege access for every user, service, and system interacting with an AI model.

Measure

Disable risky AI defaults and pause functionality until risk reviews are complete.

Trust by Design. Simplicity by Default.

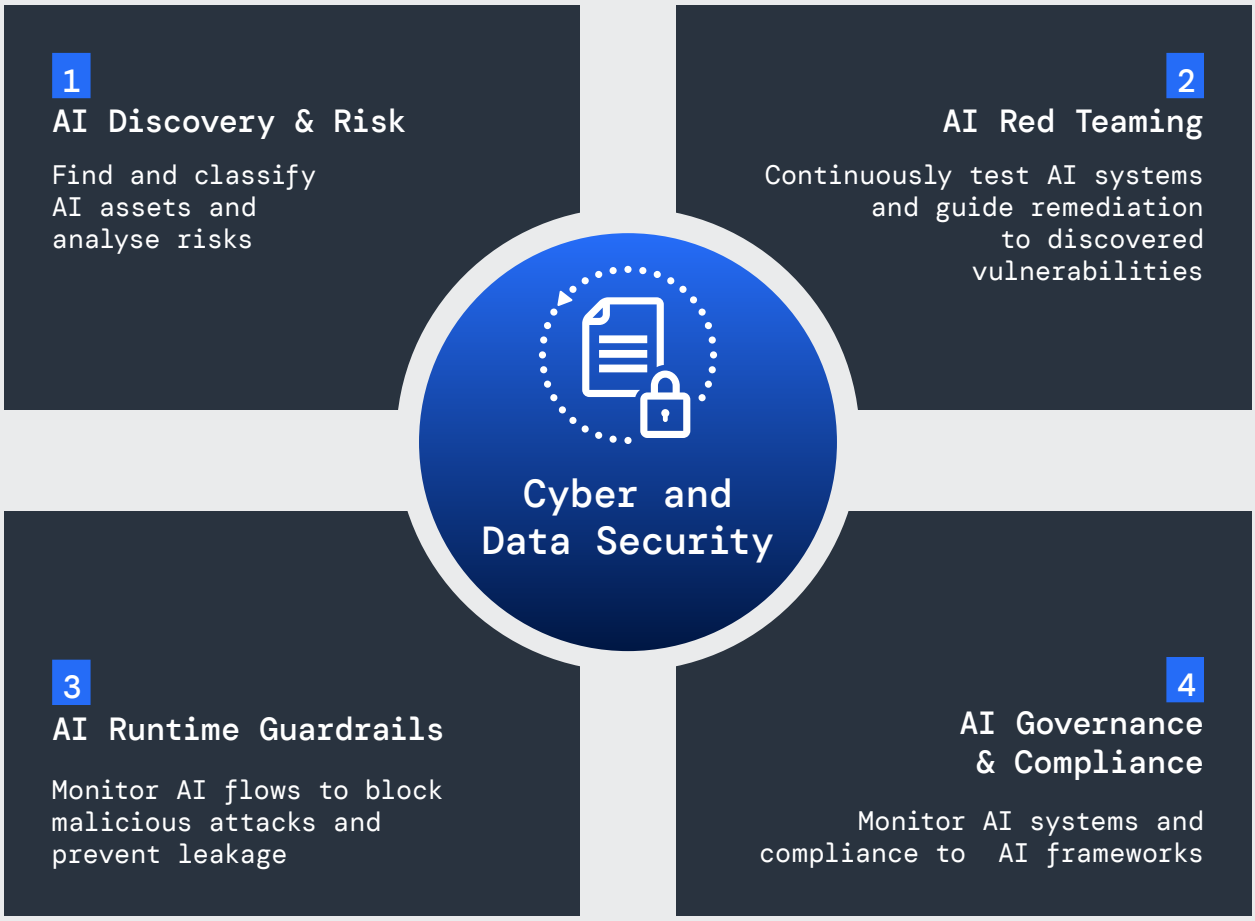
As AI adoption transitions from novel experimentation to a foundational operational requirement across ANZ, the regional threat landscape has fundamentally shifted toward machine-speed warfare.

The data is clear: with critical vulnerabilities being identified in AI systems in as little as 16 minutes, traditional perimeter-based security is no longer a viable defence. To protect their brand and the bottom line, ANZ organisations must move beyond ad hoc policies and embrace Zero Trust as a mandatory operational standard.

This shift ensures that while AI drives productivity, it does not simultaneously become an unmonitored gateway to the 'crown jewels' of corporate data.

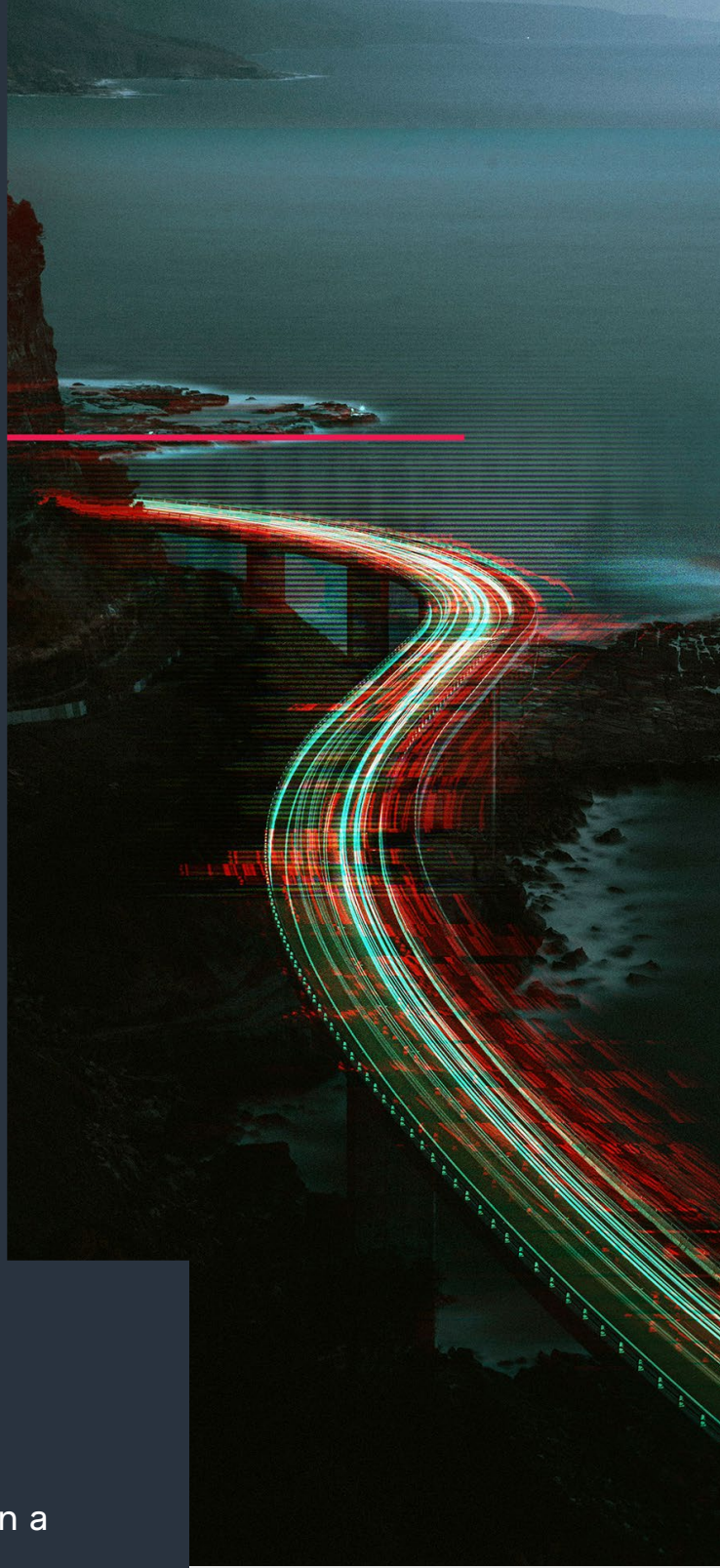
Building organisational trust in 2026 depends on the ability to outpace attackers not just with better tools, but with superior visibility and a relentless commitment to secure, AI-driven infrastructure.

Ultimately, managing corporate risk in this autonomous era requires board-level accountability and a proactive, enterprise-wide governance framework. The Zscaler AI Security Platform delivers end-to-end protection, from AI asset discovery and risk posture assessments to continuous red teaming and runtime guardrails, enabling AI governance and cCompliance at scale.



With regulators now locked in, the cost of inaction has never been higher. By shifting from reactive blocking to proactive, AI-driven defense, ANZ leaders can securely accelerate their AI transformation while staying ahead of evolving threats and regulatory mandates.

Learn More



Dive deeper into the ways AI is expanding the enterprise attack surface in the ThreatLabz 2026 AI Security Report.

Download

Learn how Zscaler AI Security combines visibility, governance, and inline protection across the full AI lifecycle.

Read Now

Unlock real-world examples of how organisations are building digital trust in a world of escalating cyber threats.

Explore

zscaler™