

AUSTRALIAN MARKET INTELLIGENCE

# Australia's cybersecurity gap is *Israel's opportunity*

Australia faces an escalating threat environment, a structural talent shortage, and AU\$7.5B in annual security spending. Israeli deep-tech has built precisely what Australian organisations need.

THE MARKET

# Australia spends AU\$7.5B on cybersecurity in 2026. The market grows at 9.5% per year.

**AU\$7.5B**

Projected security spend in 2026, up 9.5% year-on-year

**AU\$3.7B**

Security services alone , consulting, managed and professional services

**88%**

Of ANZ CIOs rank cybersecurity as top technology investment priority ,  
2nd year running

**13.3%**

Projected CAGR to 2035 , market expected to reach AU\$36B

## Australia is under sustained *cyber attack*

### **84K** Cybercrime reports in FY2024-25

One report every 6 minutes to the ACSC. Average business cost of a cyber incident rose 50% in a single year to AU\$80,500.

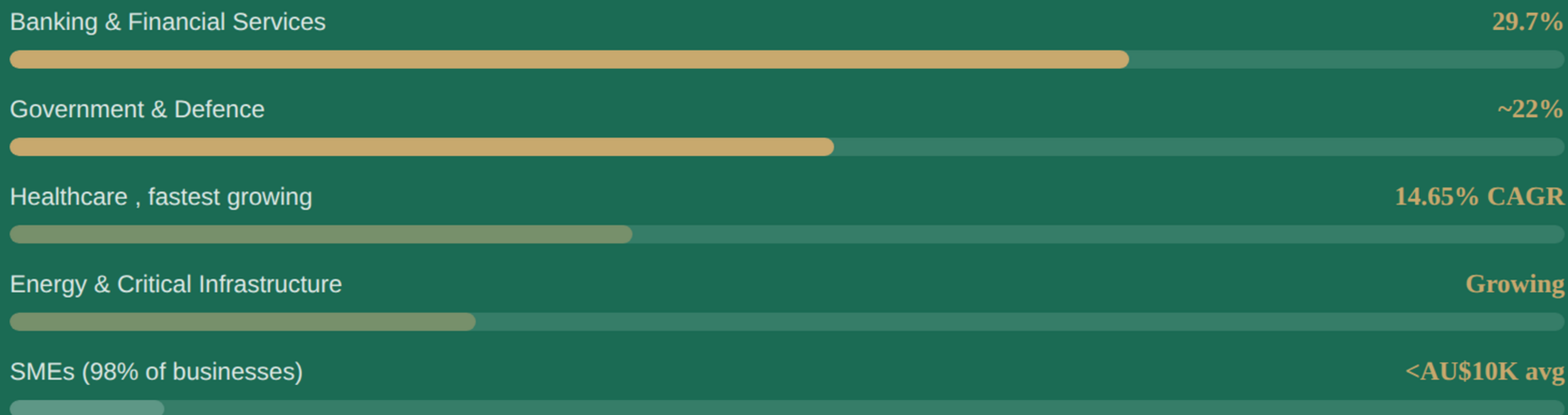
### **111%** Rise in attacks on critical infrastructure

13% of all ACSC incidents involved critical infrastructure. State-sponsored actors from China and Russia explicitly targeting Australian networks.

### **83%** Increase in threat notifications

ACSC notified entities over 1,700 times of malicious activity, up 83% year-on-year. Ransomware reports climbed 23%.

## Where Australian security budget flows



Healthcare is the fastest-growing sector at 14.65% CAGR , driven by the MediSecure breach and systemic vulnerabilities exposed across the sector.

## THE STRUCTURAL PROBLEM

**Australia cannot hire its way out of this. The talent simply does not exist.**

## SHORTFALL BY 2026

**30,000**

Unfilled cybersecurity positions forecast across Australia

## WORKFORCE TODAY

**70,900**

DB admins and ICT security specialists currently employed

54% of Australian cybersecurity teams are understaffed. 58% have unfilled positions. **One cyber professional for every 240 Australian businesses.** The talent pipeline cannot close this gap. Technology must.

**WHY ISRAEL**

# 500+ active cybersecurity companies. 36% of all Israeli tech investment. The world's deepest cyber ecosystem.

- **AI-driven threat detection and automated response**

Replacing headcount with intelligence. Built for organisations that cannot hire fast enough.

- **OT and critical infrastructure security**

Protecting energy, water, and transport systems, directly mapped to Australia's SOCI Act obligations.

- **Zero-trust architecture and identity security**

Credential theft drives 40% of Australian breaches. Israeli identity and access solutions address the root cause.

- **Cloud-native data security and posture management**

As Australian enterprises migrate to cloud, Israeli data security companies are the global benchmark.

## THE ENTRY WINDOW

## Three reasons Australian doors are open right now

- 1 Mandatory reporting is forcing procurement**  
Australia's new ransomware reporting regime (May 2025) and the SOCI Act are pushing boards to act. Budget has been released. Decisions are being made now.
- 2 Domestic supply cannot meet demand**  
30,000 unfilled positions. 54% of teams understaffed. Australian organisations are actively looking offshore for technology that replaces the headcount they cannot find.
- 3 The Israeli corridor is still uncrowded**  
US and UK vendors have deep Australian relationships. Israeli companies largely do not, yet. The companies that establish reference customers now will be first movers in a AU\$36B market by 2035.



SIGMA VENTURES ADVISORY

## Meeting in *Tel Aviv* this June?

We are meeting Israeli cybersecurity and deep-tech companies in mid-June. If Australia or APAC is on your roadmap, let's talk fit, GTM, and demand.

[sigmaventures.co](https://sigmaventures.co) ↗

*"Where Israeli deep-tech meets Asia-Pacific opportunity"*