

Media Alert

Embargoed until Monday, 12 October 2026 at 9:00 am AEDT

Cisco Report: The biggest threat to your security team might be your own organisation

AI is making threats faster, but approval delays, data silos and disconnected teams are slowing Australian defenders down

News summary:

- **AI is raising the stakes.** 93% of Australian organisations suffered a material, business-disrupting cyber incident in the past 12 months. More than 37% involved an AI-enhanced attack.
- **The biggest blocker is organisational, not technical:** When asked what would most improve their cyber defences, around 63% of practitioners in Australia pointed to organisational friction, such as coordination delays, slow approvals, and data access issues—rather than technology as cyber defence blockers.
- **More budget doesn't equal more protection:** While 89% of Australian enterprises increased security spend over the past two years, nearly half (45%) saw incidents stay the same (33%) or rise anyway (12%).
- **The best defenders organise better.** Among organisations that increased security spending, Relentless Defenders – the global top 8%, were nearly twice as likely to see incidents fall (71% vs. 41% overall).

12 October 2026 – If an organisation can't coordinate a human response in a day, it will struggle to govern autonomous agents that act in seconds. New research from Cisco, finds that the organisations best at defence do not rely on one strength, but instead combine broad coverage, fast response and a team working as one, without operational bottlenecks.

The **Relentless Defence Report** from Cisco, a key builder of critical infrastructure in the AI era, examines how security practitioners are adapting to a threat landscape that is being reshaped by AI. The report scored organisations on the breadth and consistency of their security coverage across all environments; how quickly they can detect, respond, remediate a threat, and what slows them down. Australia scored 62 out of 100 on the Cisco Defence Index (placing the market in the 'Reactive' tier), slightly behind the global average of 64 out of 100. The best and most resilient cyber professionals are what Cisco calls “Relentless Defenders”, making up only 8% of organisations globally, and just 5% in Australia, highlighting the urgent need for a culture of proactive, unified defence in the AI era.

Where security teams lose time

The report identifies organisational friction as a key barrier to stronger cyber defence but recognises that security teams can't solve this problem alone. Ownership, approvals and silos sit across IT, procurement and executive leadership, which is why they persist. When teams cannot operate as one, decision rights are unclear and data is fragmented, deploying and governing AI becomes increasingly more complex.

- **Coordination:** 46% of Australian organisations say security, networking and IT teams operate as one team with shared visibility and tooling.
- **Executive influence:** 40% say what they measure is too technical to persuade executives, 42% struggle to translate business metrics into information that can influence decision making, and 30% have no consistent way to measure security performance at all.
- **Data access:** 40% spend more time collecting and correlating data across systems than addressing the actual threat, and 42% say critical insights are missed because data sits out of reach.
- **Australia's cyber-Achilles heel:** For Australia, the landscape is impacted heavily by lower executive cyber and AI fluency with 42% of Australian cybersec professionals struggling to translate business metrics into information that can influence decision making, with almost one in two (42%) stating that critical insights are missed because data sits out of reach.

AI is making defenders faster, but security concerns delay adoption

More than 88% of Australian practitioners report detection and response gains of at least 25%, with more than one in three (35%) saying it is significantly reducing operational burden.

Yet fewer than half (39%) of the organisations surveyed have extensively deployed AI-powered security capabilities. Adoption is highest in network security and lowest in security operations and investigation – the areas where AI could most directly reduce the burden on security teams. Over one-third (40%) have extensively deployed AI agents in security operations. They are held back by concerns over data exposure, compromised systems, and third-party handling. Only 62% of Australian organisations are very confident they could detect and respond to a compromised AI agent.

“AI adoption in the network was inevitable because human reaction time couldn't keep pace with packet-level threats years ago. The network became machine-speed by necessity. Security operations are now hitting that exact same inflection point. The organisations pulling ahead aren't treating AI as a separate chatbot in the SOC; they are treating the network fabric as the sensor

and enforcement engine for the entire security stack,” said **Carl Solder, Cisco Chief Technology Officer, Australia and New Zealand**.

What Relentless Defenders do differently

Relentless Defenders (the global top 8% (and top 5% in Australia) scoring 80/100 on the Cisco Defence Index) do more to reduce friction and control the AI they are developing. They are also more likely to report stronger AI outcomes in security operations, not because they spend more, but because they lead across the organisational dimensions that enable security teams to act quickly:

- 83% **operate as a single coordinated security team** with shared visibility and tools across security, network and infrastructure, versus 37% of all other defenders.
- 86% apply consistent **controls to AI agents** and non-human identities, versus 37%. 77% are very confident they **could detect and respond to a compromised AI agent**, versus 51%
- 25% report **AI helped improve threat-detection speed by more than 100%**, versus 7%.
- Among organisations that increased security spending, the Relentless Defenders were **nearly twice as likely to see incidents fall** (71% vs. 39%).

END

About the report

The Relentless Defence Report draws on a double-blind survey of 8,000 security professionals across 30 markets, conducted in April and May 2026. It scores organisations across coverage – how completely they can protect their environment; speed – how quickly they can detect, respond and remediate threats; and friction – what slows them down; survey, analysis and report were conducted in partnership with Satori Experience and Sandpiper.

Resources

Microsite: [Microsite](#)

Report: [Link](#) to global report