Charting New Horizons

Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy Policy Discussion Paper – Trend Micro Overview Response

---

Trend Micro is a global leader in cyber security, with more than 35 years of experience delivering proactive protection, industry-leading threat intelligence, and world-class incident response. Our capabilities include advanced threat research, vulnerability discovery through the Zero Day Initiative (ZDI), and deep expertise across consumer, SMB, NFP, enterprise, government, AI, cloud, operational technology, and critical infrastructure sectors.

We have been on the ground in Australia for over 20 years, investing in local partnerships, development, and customer support. Our team includes Australian developers and threat researchers, complemented by dedicated R&D initiatives in the region. In addition, our SaaS services are IRAP-assessed and hosted in Australia, underscoring our commitment to sovereign capability and trusted service delivery.

Trend Micro's ongoing investment globally and across Australia, New Zealand, and the Pacific reflects our long-standing partnership with governments, enterprises, and communities in building resiliency across all levels of the Australian economy.

Horizon 2 Response

Overview

Australia is at a turning point in its national cyber security strategy. Horizon 2 presents an opportunity to move beyond compliance checklists and fragmented initiatives towards a risk-based, outcome-driven approach that protects citizens, strengthens businesses of all sizes, secures critical infrastructure, embraces advanced cyber tooling and enhances regional resilience.

Trend Micro is in a unique position with genuine breadth across this entire landscape. We are active and engaged at every level that government must consider:

- **Citizens and consumers:** We have decades of experience and work through our Internet Safety for Kids & Families program, consumer protection products, and scam awareness campaigns.

- **Small and medium businesses and NFPs:** We have global reach and local presence to design and scale managed security services that smaller organisations could never build themselves. As statistics bear out, these organisations employ a significant number of Australians. Whether directly or via our MSP/MSSP partners, Trend is already actively helping the smaller businesses across Australia reach cyber maturity.

- **Large enterprises and government:** The Trend Micro platform is IRAP-assessed, and SaaS hosted in Australia with local research and engineering teams and long-standing partnerships across all sectors and levels of government. We are committed to supporting our customers in this space that have modern proactive cyber maturity needs and those with additional requirements of legacy, airgap and sovereign capability that can be completely hosted on Government premises.

- **Operational Technology & Critical Infrastructure:** Trend Micro has delivered OT, IoT and connected ecosystems through TXOne (Operational Technology), VicOne (automotive and connected vehicle security) and CTOne (private 5G and OT/IoT security). We are tackling the emerging risks that will shape the next decade of critical infrastructure resilience.

- **Regional & Global leadership: t**hrough deep engagement with governments in Southeast Asia, the Pacific, Five Eyes Partners and more, we are providing threat intelligence, workforce training, and cyber capacity building.

This breadth, combined with over 35 years of global leadership and more than 20 years of continuous investment in Australia, gives us a unique perspective: We see the entire threat landscape from the family home to the nation-state adversary, design practical solutions to address the entirety of the challenge and are considered a trusted partner to our customers worldwide.

Shield Alignment

Trend Micro is strongly aligned with the Governments goals for the 2030 Cyber Security Strategy and heavily invested in the success of this project across the region. The table below gives a brief high-level overview of what expertise, advice, industry insight or existing partnerships and strengths we can contribute to each of the shields.

Desired Outcome	Trend Micro Capability
Shield 1 - Strong Businesses & Citizens - Consolidated awareness, resilience uplift for citizens, SMB, NFP, and enterprise	Consumer footprint in AU (millions protected) & Internet Safety for Kids & Families program (education). SMB/NFP managed security via MSP/MSSP partnerships; model for gov-funded bundles. Risk-based resilience for enterprise/government: CREM*, exposure metrics, deployment models.
Shield 2 - Safe Technology - Secure edge devices, OT, IoT, vendor risks	VicOne (automotive/connected vehicles). CTOne (private 5G/OT/IoT). TXOne, TippingPoint IPS for OT & legacy protection.
Shield 3 – World-class Threat Sharing & Blocking - Intelligence sharing, active defence, block threats at scale	Global threat intel unmatched breadth (consumer → SMB → enterprise → gov). Zero Day Initiative (ZDI) = #1 global vulnerability disclosure program. Pwn2Own (leverage for AU based edition). TippingPoint IPS for inline blocking at gateways, ISPs, MSPs.
Shield 4 – Protect Critical Infrastructure - Effective, proportionate SOCI obligations, resilience uplift	Outcome-based CREM* approach to risk/exposure. IRAP assessed SaaS in AU. OT/ICS protection via VicOne/CTOne/TXOne.
Shield 5 – Sovereign Capability - Workforce, research, sovereign ICT	20+ years in AU with local R&D and sovereign-hosted SaaS. Skills programs (family, school, SMB). Partnerships with universities/think tanks. Training and enablement across SEAPAC/ANZ region.
Shield 6 – Strong Region and Global Leadership - Regional uplift (SEA, Pacific), diplomacy, norms	Active in Fiji, Tonga, Vanuatu, PNG and supporting the broader Pacific Rim. On-the-ground IR, training, capacity-building. Able to extend RAPID with intel/skills packages. Trusted global player in standards (AI, data, OT).

*CREM: Cyber Risk Exposure Management

From Controls to Risk

Australia's current posture is in our opinion too control centric. Frameworks like the Essential Eight have value as baselines, but they are too often reduced to tick-box compliance exercises that consume resources without materially reducing risk.

Our market intelligence and customer conversations lead us to believe Horizon 2 must reorient towards exposure and risk management, with measurable outcomes such as:

- Prioritisation of cyber risks across the entire attack surface including vulnerabilities, identities, data, APIs, misconfigurations and more.
- Shorter time-to-detect and time-to-contain.
- Faster recovery of essential services.
- Reduced scam and fraud losses for citizens.
- Proactive and predictive cyber security risk visibility

Trend Micro has been leading this shift globally, developing metrics, tooling, and managed services that directly measure and reduce cyber exposure. Our published research[1] and conversations with our customers show that the right tooling not only brings better job satisfaction and reduces stress and staff turnover but also has a measurable and demonstratable reduction in the likelihood to suffer a breach or cyber incident or the damage when one occurs. We can bring this perspective and capability to bear in support of the Australian cyber strategy.

Scaling Protection for Citizens, NFPs and SMB

Citizens and small entities are disproportionately impacted by cybercrime and scams. Scam losses to individuals now exceed business cybercrime losses, and SMBs, which employ more than 5 million Australians, frequently lack the skills or resources to protect themselves.

Government should move beyond awareness campaigns alone and create funded, standardised managed services for SMBs and NFPs, delivered via accredited local MSPs. These programs should also make use of recent advances in AI for security where skills and capability gaps or shortages can be bridged by new AI tooling. Trend Micro is one of the few organisations with the scale, technology, and partnerships to make this a reality.

[1] Proactive Security: The Role of Exposure Management and Detection-Response Capability. Bakuei Matsukawa (Principal Threat Researcher). July 02, 2025

Education is also an essential component of cyber uplift. Through long-running programs for families and schools, Trend Micro has proven experience in raising digital literacy. We are excited to continue the education of Australia in partnership with the Government via channels with appropriate reach. This might include Super Funds, Community Organisations, Local Councils, etc.

Large Business, Critical Infrastructure, and Government

For larger entities, the biggest challenge is regulatory duplication and fragmentation. SOCI, Privacy reforms, Essential Eight, and sectoral regulators create overlapping demands that often lead to "compliance theatre" instead of resilience.

We recommend a shift to outcome-based regulation tied to risk metrics, with harmonised reporting across frameworks. For government agencies, there is a continuous decline in Essential Eight compliance. This highlights the need for centralised remediation funding and risk-based assurance, not just audits.

Modern cyber security tooling has evolved to a point where cyber risk across the entire attack surface and toolset can be assessed, quantified and prioritised in near real-time. These modern tools provide a path to true cyber security maturity instead of fixating on Essential Eight. Having controls such as Essential Eight is a small step to a baseline style approach, however we see many organisations lull themselves into a false sense of "safety" following this which in reality means they are unknowingly ignoring the attack surface not covered in the E8 maturity model. This is frightening and an all-too-common reality in our experience.

Our initiatives such as TXOne, VicOne and CTOne show how we are addressing the convergence of IT, OT, IoT, and cloud in future-proofing CI resilience in energy, transport, and telecommunications. These models can inform Australia's approach to securing next-generation critical systems.

Vulnerability & Threat Intelligence

Our Zero Day Initiative (ZDI), the world's largest vendor-agnostic bug bounty program, plays a pivotal role by identifying and responsibly disclosing zero-day vulnerabilities, fostering collaboration with security researchers and vendors to prevent exploits before they can be weaponised. Through events like Pwn2Own, we uncover vulnerabilities in software, hardware and critical systems, including AI ecosystems and consumer devices, enhancing proactive defence.

We recommend that the Government work with ZDI to launch an Australian vulnerability disclosure program leveraging ZDIs trusted reputation and established and mature processes for responsible disclosure. This could include hosting local events like Pwn2Own that would encourage Australians to pursue vulnerability research for the right reasons and could enhance the ability of Australia to detect attacks early and block at scale.

Our threat intelligence is strengthened by our comprehensive security solutions spanning cloud, web, email, network, endpoint, identity, IoT environments and more, providing extensive visibility into attack surfaces and ongoing malicious activities via hundreds of millions of global sensors.

As a global leader in threat research and intelligence, Trend Micro draw on over three decades of cybersecurity expertise and a network of more than 450 dedicated researchers across 14 global threat research centres to deliver unparalleled insights into the evolving cyberthreat landscape.

Our collaboration with global law enforcement, including the Australian Federal Police (AFP), INTERPOL, FBI, NSA, EUROPOL to name a few plus our involvement in numerous global takedowns demonstrates and underscores our commitment to utilising our threat intelligence and combating cybercrime.

We recommend a closer collaboration between Trend Micro and the Australian Government around the utilisation of our Threat research, intelligence and insights to better secure the nation.

Regional Leadership

Australia's national resilience depends on the resilience of the wider region. Horizon 2 should expand initiatives like Cyber RAPID to become platforms for regional threat intelligence, training, and managed resilience packages for Southeast Asia and the Pacific.

Trend Micro is already working with governments across the region; assisting in cyber maturity uplift, sharing threat intelligence, building capacity, and helping shape policy. This experience positions us as a trusted collaborator for Australia's regional cyber diplomacy and uplift.

While our major successes in the region have centred around the larger nations that have the talent and capability to invest in cyber maturity, we also have engagement with some of the smaller nations to help provide uplift despite these challenges. We welcome the chance to partner more closely with the Australian government to continue our cyber uplift and training efforts in the Pacific.

Conclusion

Horizon 2 is a once-in-a-generation opportunity. To succeed, it must:

- Pivot from control-centric compliance to risk-based exposure management.
- Deliver managed solutions for SMBs and NFPs that make resilience accessible.
- Harmonise regulation for large enterprises and critical infrastructure while driving measurable outcomes.
- Invest in education and digital literacy across society.

- Lead in regional cyber capacity building, amplifying Australia's role in Southeast Asia and the Pacific.

Trend Micro is already a trusted partner of business and government around Australia and the world, and we stand ready to partner and collaborate with the Australian Government to inform policy, shape strategy, and where appropriate, co-develop and deliver solutions. Because of our deep commitment to Australia and our long history of investment here, we are prepared to dedicate significant resources to support this process.

We believe we are uniquely placed to help government navigate this next phase of national cyber resilience, and we would welcome the opportunity to demonstrate this further with the Department.

Key Recommendations

1. **Shift from controls to risk (Shields 1, 2, & 4)**

Move beyond compliance-driven approaches like Essential Eight toward a risk-based national framework with common scoring and exposure metrics that apply consistently across government, industry, and citizens.

2. **Scale protection for those most at risk (Shields 1, 2, 3 & 5)**

Establish government-backed managed security services for SMBs and NFPs, and provide citizens with access to scam protection and education - ensuring resilience for the parts of the economy and community most frequently targeted.

3. **Build sovereign capability & regional strength (Shields 1 - 6)**

Create an Australian vulnerability disclosure and bug bounty program (leveraging ZDI expertise) and invest in Pacific cyber resilience programs - extending Australia's leadership by enabling block-at-scale defences and uplifting regional partners. Securing our citizens, critical infrastructure and businesses at all levels.

An additional submission has been made that answers most of the 50 questions from the discussion paper across all 6 shields in more depth. However, Trend has more to offer than can be contained in these responses and we make ourselves available for further discussion and consultation around these issues.