

WHITEPAPER

# Government and Industry: Partnering on Cybersecurity to Strengthen Data Security





# TABLE OF CONTENTS

The Cyber Threat and Geopolitics:  
New Risks..... 3

Strong Private and Public Sector Engagement to Protect  
Critical Infrastructure and Systems ..... 7

Six Reasons to Partner with Fortinet..... 11

Protecting Data Sovereignty with Strong Partnerships:  
Next Steps..... 14



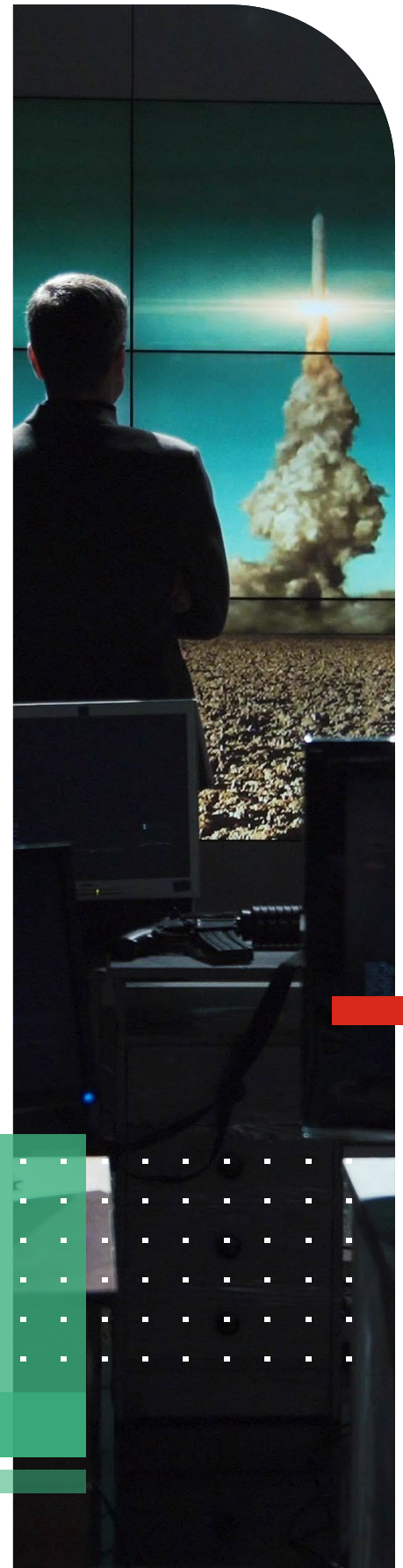
## The Cyber Threat and Geopolitics: New Risks

From Russia's cyberattacks against Ukraine's critical infrastructure and government to increasingly sophisticated cybercrime threats, the developing cyber threat landscape is creating greater havoc globally. Hybrid warfare – meaning conflict short of direct military action as well as a capability of military projection – is the new reality, creating risks for individuals, businesses, and governments. Geopolitics and cybersecurity are now inextricably linked.


The Australian Strategic Policy Institute states that: “Modern warfare and geopolitical competition will be marked not just by military action and conventional deterrence, but by ‘hybrid threats’—cyberattacks and data theft, disinformation and propaganda, foreign interference, economic coercion, attacks on critical infrastructure, and supply chain disruption, among others.”<sup>i</sup>

Conflict on the scale of Russia's attack on Ukraine has not been seen since the end of the Second World War. Geopolitical tensions present the most dangerous risk the western world has faced in decades. Cyber weapons are now part of national armouries as well as in the toolkit of organised crime, showing that business enterprise security and risk cannot be managed solely by the chief information security officer (CISO) and their teams. Everyone from individual employees to top-level management, customers, and supply chain partners must help to contain cyber risks.

The geopolitical landscape around Australia in the Indo Pacific region is changing dramatically, with a heavily contested South China Sea, competitions for influence in the Pacific and Indian Oceans, increasing strain on global supply chains, the dramatic impacts of climate change, and ageing critical infrastructure (CI) that is vulnerable to natural and manmade disruptions. Australia faces a wave of nation state-backed cyberattacks against national security and economic interests as tensions continue to escalate.







**“We’re already in a Cold War, with an elevated risk of conflict in the Indo Pacific within the next three to five years. Unfortunately, we’re shockingly underprepared and need an urgent rethink of national security and defence policy.”**

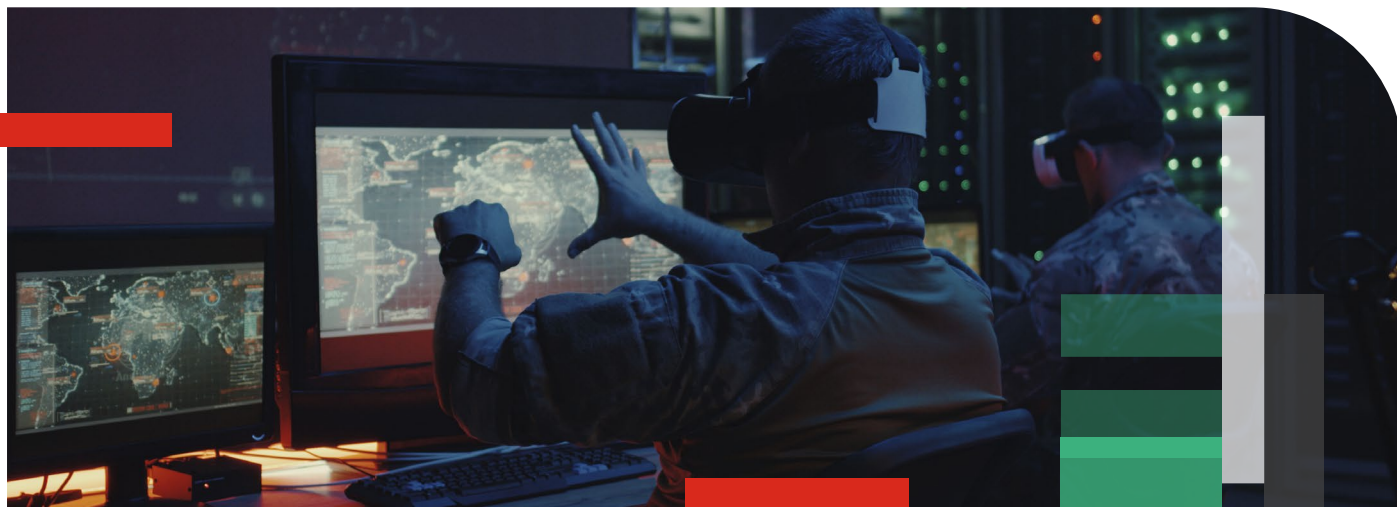
*Peter Jennings, Fortinet Public Sector Advisory Council (PSAC) member, former Australian Strategic Policy Institute Executive Director and Defence Deputy Secretary for Strategy*

The Australian government has responded to geopolitical instability by hardening public sector government networks against cyberattacks and by updating legislation strengthening the security and resilience of critical infrastructure. Further, a new strategic review focused on the Australian Department of Defence is considering priority investment in defence capabilities, including in the cyber domain and on trusted supply chain resilience initiatives.

### **Hybrid warfare and nation state actors**

Russia’s continuing invasion of Ukraine shows how cyber technology is now a central and increasingly effective component of modern warfare. Moscow has sought to disable Ukrainian IT networks, attacked critical infrastructure, and sought to disrupt the command-and-control systems of the Ukrainian military. For its part, Ukraine has shown the value of agile and well-defended IT and critical infrastructure networks.





While there is no single definition of hybrid warfare, the term shows that countries can advance strategic aims by military and non-military means as well as additional tools of influence, coercion, and interference. Attacking a country's critical infrastructure such as the power grid, ports, airports, hospitals, and communications systems can do profound damage to national resilience. Today the 'battlespace' can combine military and non-military targets and include 'grey zone' activities, like espionage and information operations, that may not quite meet the threshold of an act of war. Targeting western critical infrastructure far from the theatre of conflict for cyberattack is consistent with Russia's broader military doctrine of 'escalate to de-escalate' and distract adversaries or force them to the negotiating table.

The new strategic geopolitical challenges mean that Australia must defend against elements of hybrid warfare. We must protect critical infrastructure from such threats that can be remotely delivered, such as malware arriving hidden in an email, or enabled through some element of human intervention (the so-called insider threat), or by conventional military means.

Beyond the risk of cyberattacks by nation states, organised crime and even lone cyber hackers have the intent and capacity to threaten businesses and individuals. The security message is clear: whatever their origin, cyber threats present substantial new risks to individuals, businesses, governments, and nations. Developing stronger security against such threats is an essential requirement.

The speed at which one nation can target another nation's vulnerabilities by cyber means is rapidly increasing. When a vulnerability is discovered, there are often weeks, months, or more before businesses identify the risk by seeing proof of concept (PoC) exploits. This gives organisations less time to patch and prepare their IT defences. In fact, according to Fortinet's *2022 Networking and Cybersecurity Adoption Index*, fewer than 49 per cent of Australian and New Zealand organisations said they could detect a security breach in less than 90 days, with 23 per cent taking between two and three months.<sup>ii</sup>

Surprisingly, many high-profile, well-resourced, and cyber mature businesses can be more badly affected by ransomware than smaller entities. For example, in 2021, large, well-funded organisations such as JBS Foods, Colonial Pipeline, CNA Financial, and Frontier Software, and an external payroll software provider for the South Australian government, all fell victim to destructive cyberattacks, be they the product of organised crime, nation states, or a combination of the two. The key point is that the cyber threat is not just affecting the smaller end of the market; some sectors already quite mature in cyber defence are also being compromised.

Ransomware attacks are normally quite obvious and immediate as they dramatically impact the availability of critical services. The attacker wants to cause as much disruption as possible to compel the victim to pay the ransom; however, a sophisticated, motivated nation state intent on espionage or data destruction masked as badly executed ransomware is hard to identify.

As it stands, it's almost certain that nation state malware is present and undetected in many government departments and agencies, managed service providers (MSPs), electricity distributors, and other critical infrastructure entities. That malware may be lying dormant waiting to be activated or quietly stealing sensitive data from the compromised network. With the illicit access already achieved, such malware could be used in the future to conduct more destructive activities such as destroying all data in its path through use of wiper malware.





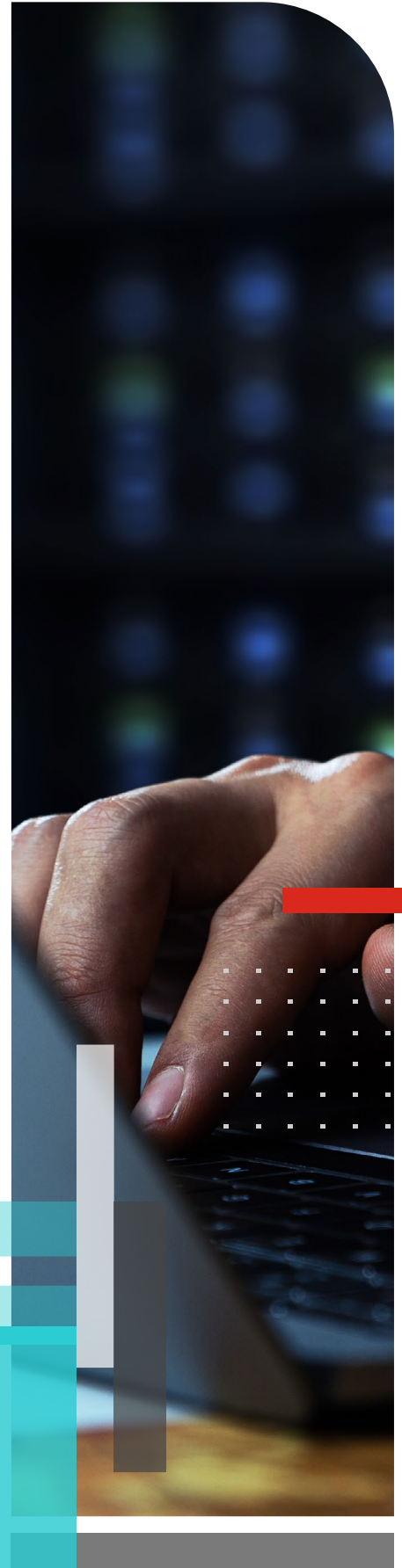
## Strong Private and Public Sector Engagement to Protect Critical Infrastructure and Systems

Given the growth of cyber threats, it has never been more important for the Australian government to coordinate with a much broader group of stakeholders, partnering to protect our shared interests. It is now clearly understood that securing cyber and physical infrastructure is a shared responsibility. The Albanese government has appointed the first-ever Cyber Security Minister, Hon Claire O'Neil, who has tasked her department with re-casting the cybersecurity strategy first published in 2020. Minister O'Neil has stated that this will involve significant industry engagement and wants a more consultative approach to building the strategy.

The Australian government's Critical Infrastructure Resilience Strategy intends to increase resilience across critical infrastructure assets, address vulnerabilities across physical, cyber, supply chain, and personnel domains, provide a wholesale uplift in critical infrastructure security, and provide practical ways to confirm that critical infrastructure assets are safeguarded against risks.<sup>iii</sup> Delivering on this plan will require extensive industry engagement and a new level of trusted cooperation between the public and private sectors.

The Australian government is developing a much more detailed and comprehensive understanding of critical infrastructure, its security vulnerabilities, and any gaps in that must be addressed. Additional analysis will identify links and interdependencies in critical infrastructure that an adversary may seek to exploit in an attack.

We need to leverage the greater strength that will come from closer private and public sector security cooperation, working together on a shared protective mission. Greater cooperation between public and private entities will deliver better visibility into threats through shared intelligence, better use of scarce cyber specialists, and better management of incident response.



## Private sector strengths

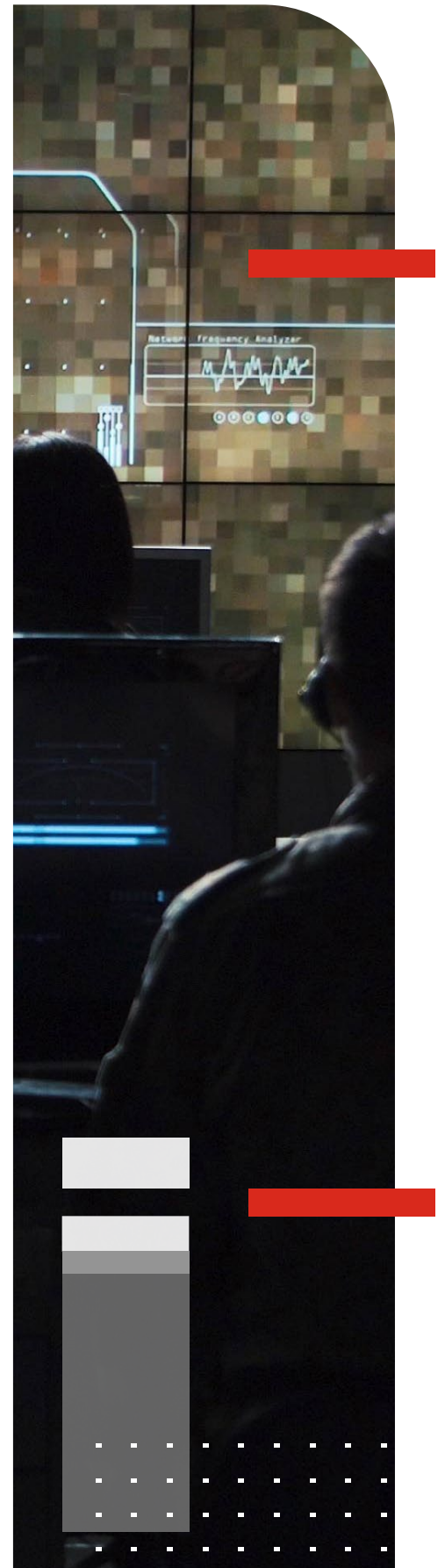
### 1. Global cyber intelligence and research

An increasingly risky threat landscape is forcing organisations to strengthen their guard against new cyber threats and breaches. Securing cyber-enabled equipment and networks and the data that flows between them is vital in our hyper-connected world. Investment in research and development is essential to build a safer cybersecurity future and is a key part of the government's ability to reduce cyber threats to critical infrastructure and supply chains. However, governments can't mitigate all incoming threats alone. Instead, the onus on building cyber resilience should be shared with critical infrastructure operators, service providers, and cybersecurity companies sharing the breadth of their knowledge and understanding of threats. Strong public-private partnerships are essential in protecting Australia's critical infrastructure and will offer more focused, practical, and cost-effective new technology.

### 2. Strong and trusted global supply chains

To secure Australia's tactical advantage, organisations within government, defence, national security, as industries covered under critical infrastructure legislation, must be using mission-critical technology while maintaining cyber resilience. These sectors face growing challenges relying on increasingly complex supply chains and inherent cyber vulnerabilities from multiple angles. Australia's geographic location and size limits our capability to locally design, manufacture, and distribute high-end cyber goods and services. Defending Australia and its national interests requires partners with strong and trusted global supply chains and the ability to draw on globally scalable production capabilities.

In this context, 'trusted' means that governments and businesses have a verified record of the performance of a cybersecurity adviser that meets the nation's highest national security standards. This trust must build on the accreditation schemes such as Common Criteria (CC). While CC is a powerful system, the diversity of systems in areas like critical infrastructure beyond classified government systems, mean that CC cannot always ensure the most secure solution. CC can be expensive, rigid, and has a lead time for cyber technology to make the list. In certain cases, the latest generation of off-the-shelf technology, carrying all the latest security patches, can be a better fit.





### 3. Significant experience in protecting critical infrastructure

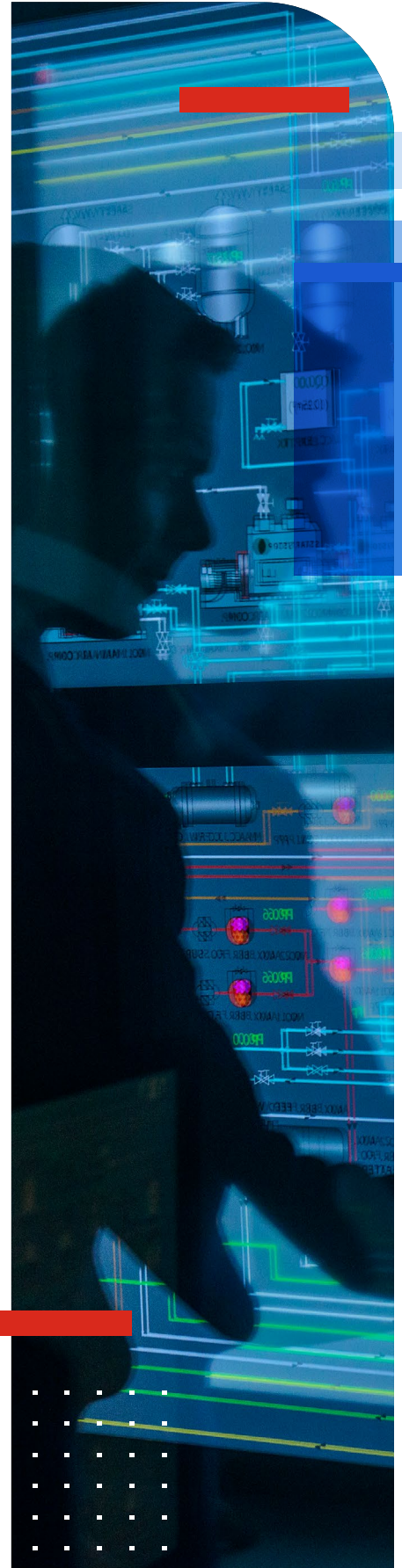
Critical infrastructure is under 24/7 attack from sophisticated cybercriminals and nation state actors. Recent cyberattacks demonstrate the need for stronger cyber resilience across critical infrastructure supply chains. In 2021, Colonial Pipeline, the largest fuel pipeline in the US, was compromised by ransomware, causing the company to suspend operations for days and seriously disrupting many communities along the US east coast.<sup>iv</sup> Here, Australia's critical infrastructure sector is urgently working to address the growing risk of attacks on ageing operational technology (OT) systems.

Partnering with a global cybersecurity leader with deep experience in protecting OT can help governments and businesses better understand and defend against cyber threats. A trusted partner will focus on building cyber resilience that combines advanced segmentation, which is the separation and protection of each component of a complex network, with access control and malware protection. These elements are needed to build an overarching security architecture to defend a complex OT network. A trusted partner will also focus on building cyber resilience that leverages network segmentation, rigorous access control, and malware protection that provides threat visibility to deliver ease of operation and machine-speed response for dealing with threats at enormous scale.

### 4. A partner able to deal with all aspects of cyber threats

Historically, Australian governments and critical infrastructure entities have approached cybersecurity from a product perspective. The contemporary threat requires a more integrated approach; something that manages components as a full system. We need our defence systems to work together at machine speed and to better support the scarce cyber defenders tasked with building, integrating, and operating these complex systems.

Adding to this complexity is the increasing requirement for government and private sector to work together more closely in providing services to the Australian people. Recent high-profile attacks against Australian infrastructure show how federal and state government agencies will inevitably be drawn into responding to threats that compromise data from many sources.



Best practice cybersecurity at a national level requires a holistic approach that protects against cyber threats at every point in complex businesses, critical infrastructure, and government operations. Multiple layers of defence are needed; working together to mitigate the risk of attacks. By thinking about cyber defence as an interconnected mesh, threats can be better and more quickly identified and addressed. The cybersecurity mesh is a modern approach to security architecture that enables a complex distributed enterprise to deploy and extend security where it's most needed.<sup>v</sup> It also enables the use of emerging technology like artificial intelligence and machine learning. This enables rapid detection of threats and automated orchestration that will identify and contain threats as well as automatically heal impacted systems without human intervention.

## 5. Access to advanced cybersecurity training

Human skills and ingenuity are the most important part of cybersecurity. By itself, technology cannot provide the answer to cyber threats. As such, training is a vital part of cyber defence to ensure stronger data protection by increasing understanding of the latest threats and possible solutions. It is also increasingly essential that cyber training moves out of the IT department and becomes a foundational requirement for all employees. Cyber training must be made relevant and engaging for our current and future workforce.<sup>vi</sup> Australians will only become more IT connected, so basic cyber awareness should become more of a foundational skill instilled across all age groups. Cyber security training should also be extended to all parts of our economy. That means business partners and subcontractors—essential partners in delivering a working economy, critical infrastructure, and national security infrastructure—must be trained and committed to protect data from cyber threats. Working with a highly qualified partner with comprehensive cybersecurity training will help prepare Australia to deal with risks and threats in its systems, networks, and devices.





## Six Reasons to Partner with Fortinet

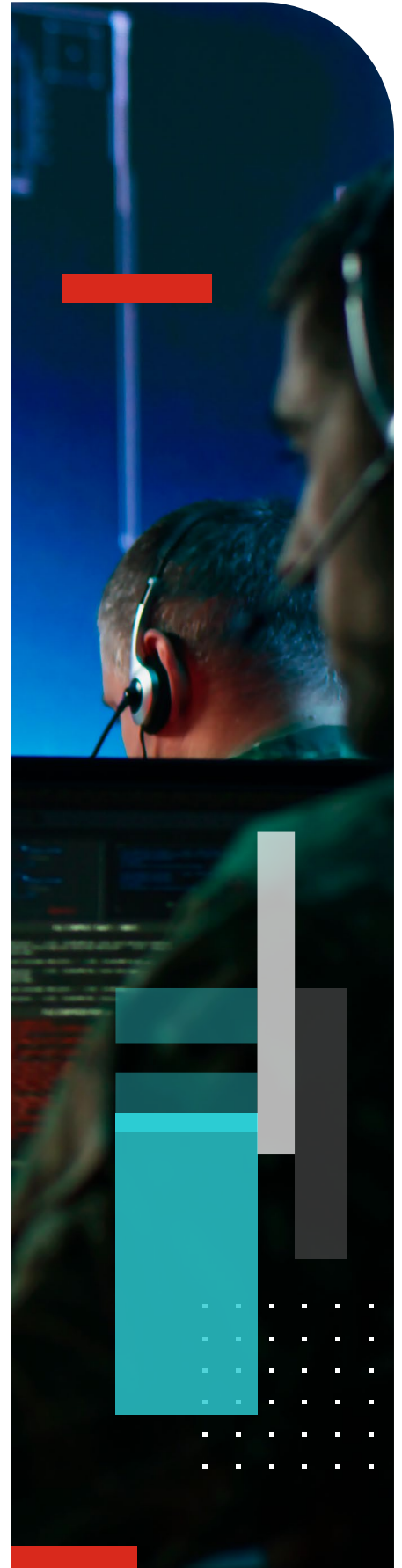
### 1. Fortinet is a trusted partner in national security and defence

As the cyber threat becomes more pervasive, Australian critical infrastructure operators and government agencies must have the most comprehensive cybersecurity solution available, provided by a partner they can trust. Trusted international partners with the necessary global expertise and intellectual property (IP) are essential to best protect Australia's national security interests and alliance relationships. Advanced nations face similar problems regardless of their size and location and common standards facilitate the development and delivery of cyber solutions that evolve at the speed of threat actors and IT. Fortinet partners closely with the United States and Australian governments to ensure product certification and regulatory compliance and have a dedicated Certifications Resource Centre. It is committed to adhering to such standards as ISO27001, TAA, FIPS certification, Common Criteria, and the DoDIN APL, to name a few.

Fortinet has also formed the Public Sector Advisory Council (PSAC) to engage with public sector organisations in developing responses to the increasingly risky international cyber threat environment. The Fortinet PSAC is chaired by Gary Locke, former U.S. Ambassador, U.S. Secretary of Commerce, and Governor of Washington state. Gary is joined by members who have excelled in a variety of government roles and missions including Peter Jennings, who was most recently the executive director of the Australian Strategic Policy Institute and a former Deputy Secretary for Strategy with the Defence Department. The Fortinet PSAC expands the company's commitment to securing public sector organisations within the Five Eye community of trusted defence and intelligence partners in the United States, United Kingdom, Australia, Canada, and New Zealand.

### 2. FortiGuard Labs

Fortinet's FortiGuard Labs threat intelligence and research organisation provides threat intelligence services that help organisations identify risk and strengthen security. Our threat research and response team is made up of more than 200 expert analysts globally who identify new or unknown threats and develop ways to detect them before they become entrenched in customer networks. FortiGuard Labs has discovered more than a thousand 'zero day exploits', which are attack techniques that were previously unknown. FortiGuard Labs has a growing presence in Australia, with security-cleared personnel who deeply understand the defence and national security cyber threat landscape.







### 3. Fortinet is focused on a trusted supply chain

The Australian government continues to strengthen the security of supply chains. In a deeply interconnected world, the challenge is to build supply chain resilience and reduce risk. A completely sovereign cyber system, if such a thing could be possible, would be less effective. The answer is to make use of onshore and offshore trusted partners as part of supply chain management as well as to diversify supply chains geographically to reduce risk from cyber disruptions. With a measured and verified approach to developing trusted partners, Australia can draw on the strengths of global supply chains, accessing the best partners with a global perspective. Fortinet has a growing presence in Australia and a robust global supply chain with the ability to tap into its American-based global support structure, creating more options for sourcing components and opportunities to handle more inventory with lower overhead costs.

### 4. Fortinet has a breadth of experience

Fortinet has a significant presence across Australian industries with a strong track record protecting critical infrastructure. Its aim is to help critical infrastructure operators create long-lasting cyber resilience in the face of escalating cyberattacks. With this breadth of engagement and cross-sector understanding, Fortinet can apply local knowledge to deal with specific cyber risks and local requirements. Much of this experience is maintained and strengthened through international exercises, so when something does happen, Fortinet knows what to do by drawing on its multinational work force. For example, in April 2022 Fortinet assisted NATO's Cooperative Cyber Defence Centre of Excellence with Exercise Locked Shields, the largest and most complex international live-fire cyber defence exercise in the world for cybersecurity professionals to practice defending national IT systems and critical infrastructure under the pressure of a severe cyberattack.<sup>vii</sup>

## 5. Fortinet offers broad cybersecurity protection

As more industrial systems converge with similar IT networks, previously siloed and protected OT systems are now more vulnerable to the same threats typically targeted towards IT systems. Organisations must defend against increasing threats from malicious and state-sponsored or state-linked attackers. Fortinet is the only vendor that can deliver a truly integrated security fabric that covers the OT security best practices and requirements for the entire converged IT-OT network. Fortinet has a strong track record protecting critical infrastructure and understands the unique needs of certain sectors. For example, ruggedised FortiGate next-generation firewalls (NGFWs) are built to secure sites with extreme heat, cold, vibration, and electrical interference.

Fortinet's industrial control system (ICS) and supervisory control and data acquisition (SCADA) solution integrates OT security solutions with best-of-breed protection for IT environments that extend from the data centre to the cloud to the network perimeter. In the age of hybrid warfare, partnering with an international company that brings deep experience, trusted and verified capability, secure supply chains, and interoperability, is critical.

## 6. Fortinet is a cyber awareness and technical training specialist

The Fortinet Training Institute is committed to developing experts in the field of cybersecurity through training and certification. The Training Institute's certification program enables people to learn about cybersecurity at all levels, ranging from awareness to foundational to expert level knowledge. Supported by Fortinet's strong network, the Training Institute has issued more than one million certifications to date.

Fortinet's Academic Partner Program and Education Outreach Program work with higher education as well as non-profit and government initiatives. Through these programs, Fortinet offers training and certification opportunities for women, veterans and military spouses, students, and economically disadvantaged individuals in order to cultivate a more diverse, equitable, and inclusive cybersecurity workplace. Fortinet offers all its self-paced training courses for free, which includes over 300 hours of curriculum. To continue its work to help close the cybersecurity skills gap, Fortinet has pledged to train one million people over the next five years (2022-2026).



# Protecting Data Sovereignty with Strong Partnerships: Next Steps

Threats against Australia's critical infrastructure are becoming more complex, more prolific, and more frequent. As it stands, the scope and scale of the problem is too large for any single governmental organisation to tackle alone. Building sovereign capability and critical infrastructure resilience is vital to national interest; however, it cannot mean total self-reliance, particularly for Australia, which is highly trade-dependent, has strong alliance relationships, and close security links with many international partners. Australia needs to bolster its national security capabilities to protect data by working with trusted partners who maintain the expertise and the IP necessary to defend complex economies and societies.

The complexities of our interconnected world and increasing geopolitical uncertainties mean it's more important than ever for government and industry to work together and create strategic partnerships to strengthen Australia's resilience to cyber threats.

## Authors

Glenn Maiden

Director of Threat Intelligence, FortiGuard Labs ANZ

Nicole Quinn

Head of Government Affairs APAC



- 
- <sup>i</sup> <https://www.aspistrategist.org.au/the-real-potential-of-aukus-is-about-far-more-than-submarines>
  - <sup>ii</sup> <https://global.fortinet.com/apac-lp-anz-networking-wp-index-report>
  - <sup>iii</sup> <https://www.cisc.gov.au/what-is-the-cyber-and-infrastructure-security-centre/critical-infrastructure-resilience-strategy>
  - <sup>iv</sup> <https://www.energy.gov/ceser/colonial-pipeline-cyber-incident>
  - <sup>v</sup> <https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021>
  - <sup>vi</sup> <https://www.ibm.com/downloads/cas/3R8N1DZJ>
  - <sup>vii</sup> <https://www.ccdcoe.org/exercises/locked-shields/>



[www.fortinet.com](https://www.fortinet.com)

Copyright ©2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.