

WHITE PAPER

Strengthening Cybersecurity in Local Government



Protecting the Community with Fortinet Solutions

The local government sector faces numerous challenges in the digital age, from managing critical infrastructure (CI) like wastewater systems to embracing the smart city revolution. Ensuring the security of open data initiatives and addressing the cybersecurity skills shortage adds to these complexities. Local Governments often operate under tight budgetary constraints, struggling to deliver quality services and maintain infrastructure with limited financial resources. Subsequently, balancing budgets while meeting growing demands for services and infrastructure upgrades continues to be significant challenge.

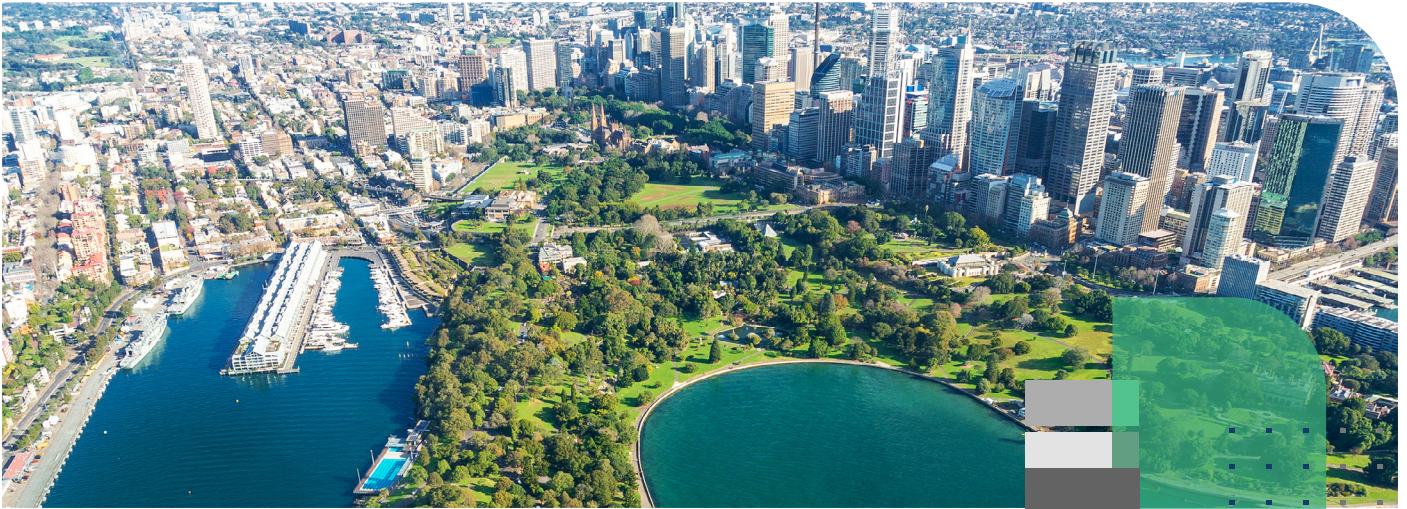
As government services increasingly rely on digital platforms, the risk of cyber attacks has dramatically increased. It's not just about protecting sensitive data; it's also about maintaining public trust and ensuring the continuity of critical public services.

The Australian Signals Directorate 2022/23 cyber threat report showed that the average cost of cybercrime increased by 14 per cent from the previous year. In addition, there were almost 94,000 cybercrime reports, up by 23 per cent from the previous year, and that 12.9 per cent of these cyber incidents came from the state and local government sector.¹

As a global leader in broad, integrated, and automated cybersecurity solutions, Fortinet is uniquely positioned to address these challenges. Fortinet provides comprehensive security solutions that align with crucial standards, including the Essential Eight mitigation strategies and the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 family of standards. This paper outlines how Fortinet's solutions can be leveraged by Australian local governments to secure their digital transformation journey effectively and efficiently.

Fortinet cybersecurity solutions help local governments better prepare for potentially damaging cyber attacks with a holistic, integrated security architecture that unifies cyber and physical security. This approach empowers entities to respond to future attack vectors without needing to replace their security infrastructure every few years. It also optimises the use of taxpayer funds by increasing operational efficiency and streamlining security operations.





Local Government Cybersecurity Challenges

Local governments face several cybersecurity challenges, including:

1. Cost optimisation

Local governments operate on limited budgets, which sometimes results in reluctance from officials to support investment in replacing ageing IT infrastructure. As a result, IT staff must be strategic about budget and resource allocation, with risks prioritised according to the potential impact on citizens and services. As the volume and velocity of cyber attacks increase, local governments often do not have the option of adding headcount to address the issue. Even if new positions are approved, the cybersecurity skills shortage makes talent very expensive. Fortinet offers a unified approach to cybersecurity, integrating multiple security functions into a single platform. This consolidation reduces the need for multiple, disparate security solutions, leading to significant cost savings on both hardware and software. By streamlining security infrastructure, local governments can reduce maintenance costs and simplify management.

2. Targeted threats

Local governments are heavily targeted with common and dangerous threats such as ransomware, which is a type of malware that holds data and devices hostage until a ransom is paid. While some entities refuse to pay the ransom, others have no choice. Consequently, adversaries will continue to target them in this way for the foreseeable future. Smaller entities often lack both the budget and the expertise to fight back, and larger organisations might face extremely high remediation costs if they choose not to pay the ransom. Fortinet provides real-time threat intelligence solutions that continuously monitor and analyse global threat data to identify and respond to ransomware attacks swiftly. By leveraging artificial intelligence (AI) and machine learning (ML), Fortinet's solutions can detect ransomware patterns and behaviours before they can inflict significant damage.

3. Enhancing critical infrastructure security

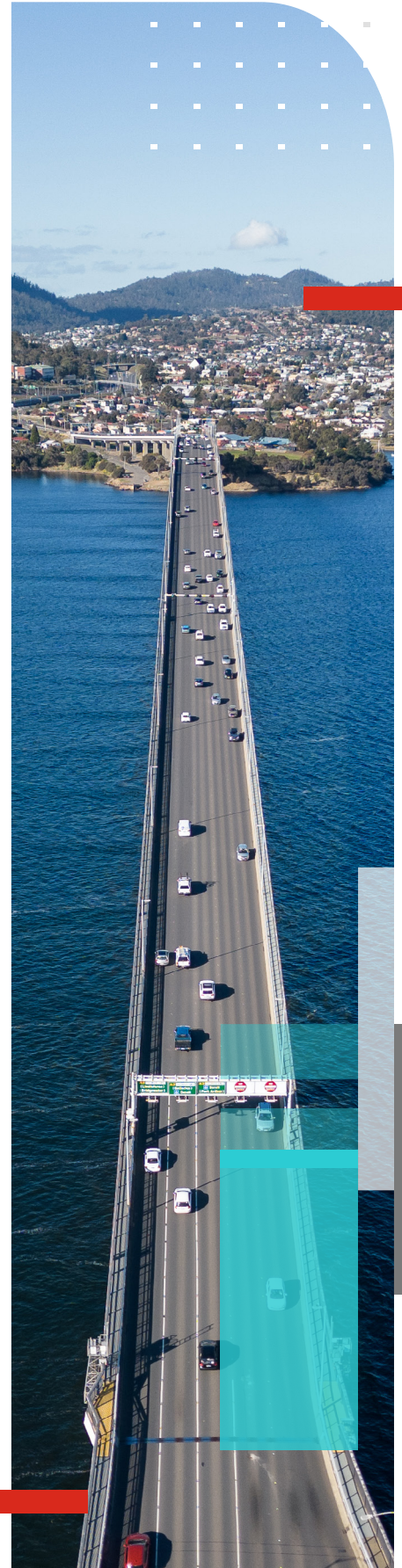
Local governments are responsible for critical infrastructure, such as water, wastewater systems, and traffic management. These essential services face increasing cyber threats that can lead to disruptions, service outages, and even physical damage, posing significant risk to public safety and economic stability. Fortinet's solutions offer advanced threat protection by integrating features such as intrusion prevention, web filtering, and deep packet inspection. These capabilities help detect and block sophisticated cyber threats at the network perimeter, preventing unauthorised access and potential attacks on CI.

4. Empowering smart cities

The smart city initiative requires a secure, scalable network infrastructure to support various technologies, including Internet of Things (IoT) devices, sensors, and connected systems. Local governments face challenges in ensuring the confidentiality, integrity, and availability of data collected and processed by these IoT devices, as well as maintaining interoperability among diverse systems. Fortinet's integrated security solutions ensure the confidentiality, integrity, and availability of data collected and processed by IoT devices, facilitating the secure adoption of smart city technologies.

5. Digital service platforms

Open data initiatives, essential for transparency and innovation, and online portals that let residents access a wide range of services, such as paying bills, lodging requests, and obtaining information, pose significant security risks if not properly managed. These risks include unauthorised data access, data breaches, and service disruptions. Coupled with mobile applications that provide residents with convenient access to local government services on their smartphones, these initiatives require robust security measures. Fortinet's comprehensive security suite ensures that data shared with the public is protected against unauthorised access and manipulation.



6. Addressing the skills shortage

The cybersecurity skills shortage is a global issue, significantly impacting local governments. Managing cybersecurity becomes increasingly complex with limited skilled personnel, making it difficult to keep up with evolving threats and technologies. Fortinet's automated and integrated solutions reduce the complexity of managing cybersecurity, making it easier for existing staff to manage the security posture effectively. Additionally, Fortinet's training and certification programs can help local governments upskill their staff in cybersecurity.

7. Essential Eight and ISO/IEC 27000

Local governments must comply with critical cybersecurity standards to protect their information assets and ensure the confidentiality, integrity, and availability of their services. Fortinet's solutions are designed to help organisations comply with critical cybersecurity standards. The Essential Eight mitigation strategies, recommended by the Australian Cyber Security Centre (ACSC), are a core part of Fortinet's approach to cybersecurity, ensuring a baseline of security hygiene. Similarly, Fortinet's emphasis on information security management systems aligns with the ISO/IEC 27000 family of standards, providing a comprehensive framework for managing and protecting information assets.

Managing cybersecurity becomes increasingly complex with limited skilled personnel, making it difficult to keep up with evolving threats and technologies.





Use Cases

Local governments can use Fortinet solutions to address various use cases such as:

Secure access

Local governments often have a complex web of users and device types accessing the network at any given time. In addition, staff, contractors, and other third parties often have access to certain systems, introducing significant risk.

Ensuring that each login is authorised is a key priority; however, simply requiring a username and password is not enough, as threat actors often gain initial access to a network using stolen credentials from a third party. To provide secure access in a world where trust is not static, a multilayered approach is necessary. While multi-factor authentication (MFA) provides a much more secure way for authorised users to access network resources, additional layers of verification must be applied to both users and devices trying to log in, and the network must be intelligently segmented to only allow access to authorised users.

Fortinet provides these levels of verification as a part of an integrated security architecture. FortiAuthenticator and FortiToken identity and access management (IAM) tools offer multiple checks for users, while FortiNAC monitors devices attempting to access network resources. FortiInsight user and entity behaviour analytics (UEBA) detect anomalies that might indicate compromised user accounts or devices. FortiPresence analytics technology pinpoints where wireless devices are located when access is requested, and FortiDeceptor lures adversaries into revealing themselves. Intent-based segmentation features in FortiGate next-generation firewalls (NGFWs) segment the network according to evolving business needs, ensuring that users have access only to what they need to do their jobs.

Ensuring that each login is authorised is a key priority; however, simply requiring a username and password is not enough.

Integration of voice, cyber, and physical security

Local governments maintain thousands of kilometres of wastewater systems, roadways, bridges, traffic management, and other CI, much of which is controlled and monitored by IoT devices. These connected sensors geographically extend a government's IT infrastructure and its attack surface. Like other CI, these systems can be targeted by cyber criminals and nation-state actors intending operational disruption, economic losses for the community, or even loss of life.

Such infrastructure can also be subject to coordinated cyber and physical attacks. Therefore, protecting it necessitates an integrated approach to both cyber and physical security. Adding voice communications to the integrated architecture improves operational efficiency and enhances security.

The Fortinet Security Fabric empowers local governments to integrate cybersecurity, physical security, wireless networking, and Internet Protocol (IP)-based voice communications infrastructures for comprehensive protection. FortiAP and FortiSwitch deliver secure wireless networking, while analytics tools like FortiAnalyzer, FortiPresence, and FortiSIEM provide reporting and analysis on this entire infrastructure. Additionally, FortiNAC monitors and verifies all these devices to protect the network.

The Fortinet Security Fabric empowers local governments to integrate cybersecurity, physical security, wireless networking, and Internet Protocol (IP)-based voice communications infrastructures for comprehensive protection.



Security operations

For local governments, the Security Operations Centre (SOC) must deliver value in terms of enhanced security and cost-effectiveness. Its services should be powered by an integrated security architecture that offers broad protection, centralised visibility and control, and the ability to automate reporting and threat detection and response. The Fortinet SecOps platform helps local governments tackle various challenges in securing the organisation from constantly evolving cyber threats, despite the volume and complexity of security alerts. This is where Fortinet's SecOps platform, built on AI and automation to reduce cyber risk, is critical. Today's cybersecurity model must go beyond the time-consuming, highly manual process of detect and respond to reduce threat actor dwell time and cyber risk.

Fortinet Advisor is the new generative AI (GenAI)-based security assistant that uses natural language processors (NLP) and GenAI to guide, simplify, and automate security analyst activities. Fortinet Advisor is seamlessly integrated into the user experience of FortiSIEM and FortiSOAR SecOps products to help optimise threat investigation and response, security information and event management (SIEM) queries, security orchestration, automation, and response (SOAR) playbook creation, and more.

Today's cybersecurity model must go beyond the time-consuming, highly manual process of detect and respond to reduce threat actor dwell time and cyber risk.



Fortinet Differentiators

Fortinet offers local governments a series of distinct advantages, including:

1. Integrated platform

Fortinet delivers a flexible platform for building an end-to-end, integrated security architecture. This integration can span a local government's CI to its public services, from the data centre to the endpoint to multiple clouds, and from physical security and voice communications to cybersecurity. It includes an open application programming interface (API) and Fabric Connectors to integrate third-party security tools.

2. Remote location networking and security

Fortinet offers a comprehensive software-defined wide area network (SD-WAN), networking, and cybersecurity infrastructure for branch locations and field sites that provides optimal security and improves network performance. Network traffic can securely travel over the public internet, helping local governments avoid the high cost of multiprotocol label switching (MPLS) connections.

3. Insider threat protection

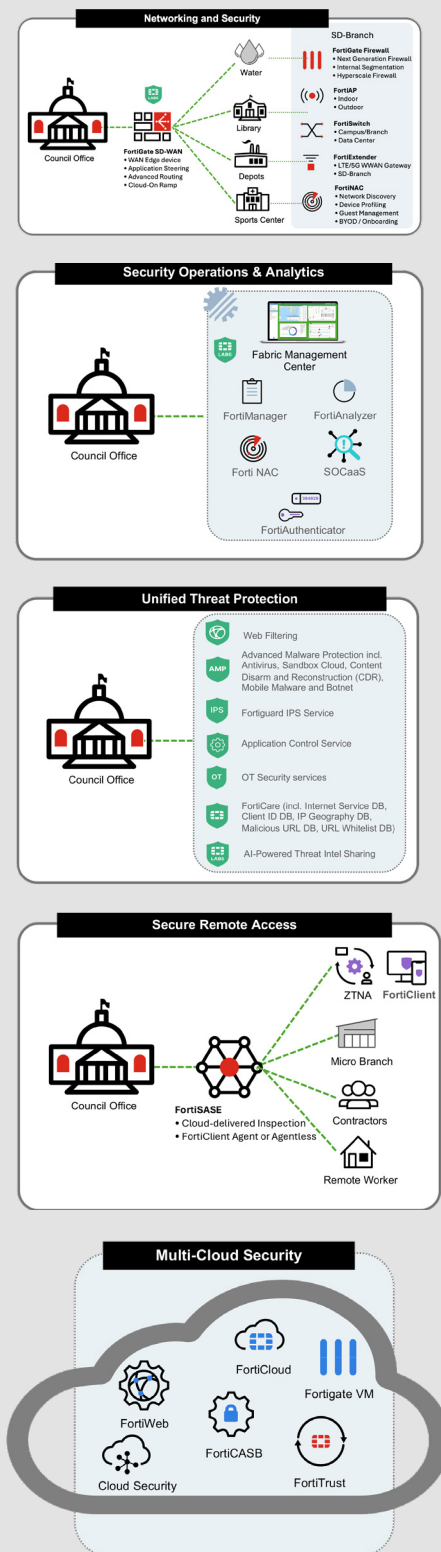
Local governments face especially high risk from third parties and insiders who perpetrate accidental and deliberate attacks. Fortinet delivers a comprehensive solution to guard against these threats with identity and access management tools supplemented by NAC, intent-based segmentation, deception technology, and UEBA.

4. Robust threat intelligence

FortiGuard Labs delivers comprehensive intelligence from a large global network of NGFWs, sandboxes, and an AI-powered security event detection system (SED) that has refined its algorithms using years of machine learning (ML) training. The result is extremely accurate detection of new threats with almost no false positives.

5. Industry leadership

Fortinet, one of the most validated cybersecurity companies in the world, is consistently positioned in leadership positions across 80+ research reports from major industry analyst firms like Gartner, IDC, and Forrester, and is included in eight Gartner Magic Quadrants.

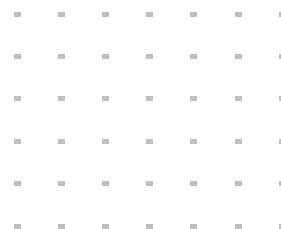


Protecting the Community with Fortinet Solutions

As Australian local governments navigate the complexities of digital transformation, cybersecurity remains a paramount concern. Fortinet's suite of solutions offers a comprehensive, integrated approach to cybersecurity that not only meets the current challenges, but is also scalable for future needs. By leveraging Fortinet's technologies, local governments can secure their CI, embrace smart city initiatives, protect open data, and address the cybersecurity skills shortage, all while complying with essential cybersecurity standards. Fortinet is more than a provider of cybersecurity solutions; it's a partner in ensuring the secure and successful digital transformation of Australian local governments.



i <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023>



www.fortinet.com

Copyright © 2024 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. Certain offerings mentioned herein may not be generally available, and 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.