FORTINET

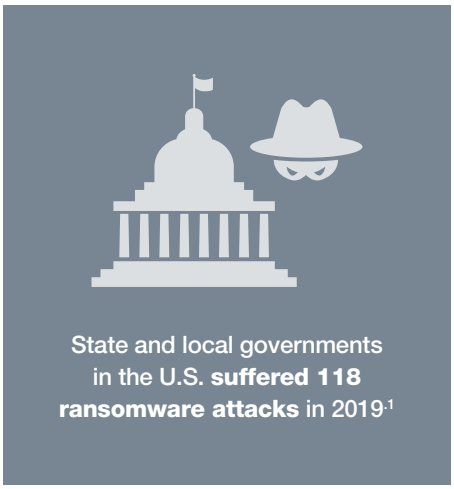
WHITE PAPER

Fortinet State-Local Government Cybersecurity Solutions

Protecting Digital Assets and Critical Infrastructure Against Growing Advanced Threats

Executive Summary

State and local governments are often overshadowed by the federal government in public consciousness, but they provide vital services that are missed when they experience interruptions. Cities, counties, and states have recently been targeted with more frequent attacks, notably with ransomware, catching entities off guard and costing them millions of dollars. Fortinet cybersecurity solutions help governments to better prepare for potentially damaging attacks with a holistic, integrated security architecture that brings cyber and physical security under a single umbrella. Such an approach enables entities to respond to future attack vectors without ripping and replacing their security infrastructure every few years. It also optimizes the use of taxpayer funds by increasing operational efficiency and streamlining security operations.



Although the news media typically focuses much of its attention on the activities of the federal government, state and local governments are responsible for a variety of services that impact the everyday lives of every resident. Critical infrastructure like roads, bridges, water and sewage systems, and public transportation are operated by state and local entities. Elections—even for federal offices—are administrated locally. Driver's licenses and other forms of identification are issued by the state government. And a vast majority of law enforcement personnel are employees of state and local entities.

This broad array of service offerings makes state and local governments attractive to a variety of cyber criminals.[2] Specifically, critical infrastructure is attractive to nation-state actors looking to create chaos and sow discord. The fact that personal information from every resident can be found in state databases is of interest to cyber criminals seeking to sell that information on the dark web. Hacktivists can wreak havoc with state and local government IT systems to make a political point.[3]

Adversaries can also shut down the IT systems of local governments in order to extract ransoms from desperate entities.[4] Ransomware targeting state and local governments is on the rise, with an average of more than two successful attacks on U.S. state and local governments per week in 2019.[5] With the help of federal and state resources, some entities, such as the city of Baltimore and 22 small local governments in Texas, have managed to avoid paying the ransom—but spent much more than the ransom amount to restore systems. Other entities, such as the cities of Riviera Beach and Lake City in Florida, had no choice but to pay.[6] This means the incentive for more ransomware attacks will remain—especially as long as there is a perception that state and local governments are unprepared for attacks.

Entities funded by taxpayers almost always operate on limited budgets, and many use some legacy technologies as a result. But many state and local governments have embraced digital technology to provide better service—and more transparency—to their citizens. As a result, innovative models of shared services between governments, innovation labs,[7] and new approaches to Internet-of-Things (IoT)-enhanced public services[8] are now on the agenda. These advancements promise to improve customer service, public engagement, and community cohesiveness. But they also expand the attack surface.

Key State-Local Government Cybersecurity Challenges

State and local governments face a number of different cybersecurity challenges:

Cost Optimization

State and local governments operate on limited budgets, and citizens are usually skeptical about proposed increases in spending. This sometimes results in reluctance on the part of elected officials to support major projects, not wanting to incur the wrath of voters. As a result, IT staff must be strategic about budget and resource allocation, with risks prioritized according to the potential impact on citizens and institutions. As the volume and velocity of attacks increase, state and local governments often do not have the option of adding headcount to address the issue. And even if new positions are approved, the cybersecurity skills shortage makes talent very expensive.[9]

Targeted Threats

State and local governments are heavily targeted with threats like ransomware. While some entities refuse to pay the ransom, others have no choice but to pay up. As a result, adversaries will target them in this way for the foreseeable future. Smaller entities often lack both the budget and the expertise to fight back, and larger governments might face extremely high remediation costs if they choose not to pay the ransom.

Digital Government Transformation

Many state and local governments are implementing digital transformation (DX) strategies,[10] notably migration of some or all services to the cloud and deployment of IoT devices such as sensors across critical infrastructure. However, these projects have slowed in the past year, and entities indicate that their migration strategies have proven more complicated, costly, and time-consuming than initially expected. Further, they need help with proper selection of service and deployment models and scalable and elastic IT-enabled capabilities provided as a service. IoT devices often lack adequate built-in security, and a fragmented security architecture can hamper efforts to harden them against attack.

Integration of Security Architecture

As the attack surface expands for a state or local government, cybersecurity teams often scramble to fill coverage gaps with point products. Over time, this results in a highly siloed security architecture filled with solutions that do not integrate or communicate with each other. This architectural fragmentation results in decreased visibility, delayed threat response, and operational inefficiencies. It also creates cost inefficiencies due to siloed, overlapping software and hardware license costs.

Compliance Reporting

Governments are accountable to the public, and compliance information is often a matter of public record. They must achieve and report compliance with regulations about the handling of personal information, protection of critical infrastructure, and environmental standards. Audits are frequent enough that redeploying staff to manual audit preparation each time will significantly slow the strategic initiatives they are working on with the remainder of their time.

Use Cases

State and local governments can use Fortinet solutions to address various use cases that include:

Secure Access

State governments often have a complex web of users and device types using the network at a given time. Contractors and other third parties often have access to certain systems, and this introduces significant risk to state and local governments. As a result, ensuring that each login is authorized is a key priority. But simply requiring a username and password is not enough. Threat actors often gain their initial access to a network using stolen credentials from a third party.[12]

To provide secure access in a world where trust is not static, a multilayered approach is necessary. Multi-factor authentication provides a much more secure way for authorized users to access network resources. But additional layers of verification must be applied to both users and devices trying to log in. And the network must be intelligently segmented to restrict each portion of the network to those who need to see it.

Fortinet provides these levels of verification as a part of an integrated security architecture. **FortiAuthenticator** and **FortiToken** identity and access management tools provide multiple checks for users, and **FortiNAC** network access control (NAC) keeps track of devices that try to access network resources. **FortiInsight** user and entity behavior analytics (UEBA) watches for anomalies in behavior that might indicate compromised user accounts or devices. **FortiPresence** presence analytics technology pinpoints where wireless devices were located when access was 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 job.

Security Operations

While some private-sector industries are outsourcing more of their security operations, growing numbers of state and local governments are bringing them in-house. An internal security operations center (SOC) makes sense for many entities, as it centralizes management of threat detection, analysis, and response while providing actionable insights about the best strategies for keeping the network secure going forward. As a further development of this trend, some state governments provide security operations as a shared service to individual state agencies and local government entities within their jurisdiction.

For the SOC to deliver value in terms of enhanced security and cost-effectiveness, its services must be powered by an integrated security architecture with broad protection, centralized visibility and control, and the ability to automate reporting and threat detection and response. For entities acting as a service provider to other agencies or governments, ensuring that the infrastructure is designed for multitenant use is crucial.

"For now, these [ransomware] attacks on local governments appear to be the result of cyber crime. However, these same targets are also vulnerable to acts of cyber warfare or attacks perpetrated by nation-states."[13]

The **Fortinet Security Fabric** provides an end-to-end, integrated security architecture that supports comprehensive SOC operations for entities using the in-house or service provider models. **FortiGate NGFWs** provide the foundation for this comprehensive architecture, and threat intelligence from **FortiGuard Labs** provides real-time insight into new threats so that response can be timely, and security services like **Advanced Malware Protection, antivirus,** and **web filtering** can be accessed through several **FortiGuard Service Bundles for FortiGate.** Built as multitenant from the ground up, **FortiManager** and **FortiAnalyzer** provide robust management and analytics tools for centralized visibility, control, and reporting on the overall security posture of each entity being served.

Integration of Voice, Cyber, and Physical Security

State and local governments maintain thousands of miles of water mains, sewage systems, roadways, bridges, public transportation lines, and other critical infrastructure—many of which are controlled and monitored with IoT devices. These connected sensors and cameras geographically extend a government's IT infrastructure—and its attack surface. Like other critical infrastructure, these systems can be the target of cyber criminals and nation-state actors whose goal is operational disruption, economic losses for the community, or even loss of life.

Such infrastructure can also be subject to coordinated cyber/physical attacks. As a result, protecting it involves an integrated approach to both cyber and physical security. Such integration will become increasingly important as emerging facial recognition and weapons detection technology comes online—and begins to be used by adversaries as well. Adding voice communications to the integrated architecture improves operational efficiency and enhances security.

The **Fortinet Security Fabric** enables state and local governments to integrate cybersecurity, physical security, wireless networking, and IP-based voice communications infrastructures for comprehensive protection. **FortiCamera, FortiRecorder, FortiVoice,** and **FortiFone** add surveillance and voice communications capabilities to the Fortinet Security Fabric. FortiAP wireless access points and FortiSwitch switches enable secure wireless networking to be added to the mix. Analytics tools like **FortiAnalyzer, FortiPresence,** and **FortiSIEM** can provide reporting and analysis on this entire infrastructure. And **FortiNAC** network access control monitors and verifies all these devices to protect the network.

Secure Remote Sites

Even smaller local governments have multiple locations from which different kinds of services are delivered in their communities, and larger ones have hundreds or thousands of assorted facilities. Providing connections between these branches and the main IT infrastructure has historically required expensive multiprotocol label switching (MPLS) infrastructure that is difficult to scale according to fluctuations in traffic, and the increasing use of cloud-based services often results in increased network traffic—and latency.

In response to these problems, software-defined wide-area network (SD-WAN) technology has moved into the mainstream in the past few years.[14] SD-WAN enables network traffic to travel on the public internet. To keep such a network secure, SD-WAN technology should ideally be integrated with the cybersecurity infrastructure—and with the networking infrastructure at the remote location.

Fortinet Secure SD-WAN is built into **FortiGate NGFWs**, enabling a highly secure SD-WAN solution without adding additional hardware. It allows network traffic to travel not only on the public internet but also over a virtual WAN (vWAN) within select public clouds. At the remote locations, **Fortinet SD-Branch** solutions extend the **Fortinet Security Fabric** to the access layer at each branch. **FortiNAC** network access control verifies devices connecting to the network, and **FortiAP** wireless access points and **FortiSwitch** switches enable secure Wi-Fi at branches.

Advanced Threat Detection

The threat landscape for state and local governments is increasing in volume, velocity, and sophistication. Manual threat response during business hours is no longer sufficient, and even 24-hour manual coverage cannot keep up with threats that move at machine speed. State and local governments need access to robust, real-time threat intelligence with automated response policies to combat unknown, including zero-day threats, and targeted attacks.

FortiGuard Labs collects threat intelligence from a large global network of sensors, and has maintained an artificial intelligence (AI)-powered self-evolving detection system (SEDS) for nearly eight years. For all this time, the SEDS has refined its algorithms using machine learning (ML), resulting in extremely accurate, real-time identification of unknown threats across the entire **Fortinet Security Fabric. FortiSandbox** and **FortiIsolator** use AI to provide additional layers of zero-day threat detection. Further, the Fortinet **Advanced Malware Protection** service provides broad protection against malware-based attacks.

"Better to prepare a way to protect and restore the data without paying off criminals, but this must be done in advance of an incident."[15]

7 in 10 state IT leaders will devote most of their IT investments toward private, public, or hybrid cloud models over the next three years.[16]

Digital Government

The way citizens interface with their state and local governments has been transformed over the past decade, with everything from utility payments to fishing licenses available via mobile app or other online processes. IoT devices provide information on everything from traffic conditions, to water quality, to the wait time at smog check stations. These services are often powered by applications residing in a hybrid cloud infrastructure. These multiple clouds have come to contain much of the sensitive data held by an entity, and must be seen as a part of the government's overall network.

As entities adopt more and more services across this distributed architecture, the default is to use the native cybersecurity tools offered by each public cloud provider. However, these solutions do not communicate with each other. The result is multiple silos in the security architecture, necessitating a lot of manual work on the part of busy cybersecurity team members in reporting and threat response. As state and local government networks get more complex and the threat landscape becomes more advanced, it is increasingly important to simplify the security architecture by achieving integration and consistent policy management across the infrastructure.

Fortinet **Dynamic Cloud Security** solutions, part of the **Fortinet Security Fabric**, deliver this integration by providing a single-pane-of-glass view of the entire cloud infrastructure. They feature *native integration* with all major public cloud providers, *broad protection* to cover all elements of the attack surface, and *management and automation* features that enable consistent, timely threat detection and response through automation.

Fortinet Differentiators

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

Integrated Platform

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

Remote Location Networking and Security

Fortinet offers a comprehensive 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 state and local governments avoid the high cost of MPLS connections.

Insider Threat Protection

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.

Robust Threat Intelligence

FortiGuard Labs delivers comprehensive intelligence from a large global network of NGFWs, sandboxes, and an AI-powered SEDS that has refined its algorithms using ML training for nearly eight years. The result: extremely accurate detection of new threats with almost no false positives.

"[S]tate governments must take digital transformation and security transformation seriously, particularly as endpoints expand and attacks become increasingly frequent, volumetric, and complex."[19]

Industry Leadership

Fortinet is recognized as a Leader in the Gartner Magic Quadrant for Network Firewalls.[17] The company has also achieved nine "Recommended" ratings from NSS Labs and achieved the best score in its NGFW Security Value Map.[18]

Conclusion

State and local governments are increasingly targeted by cyber criminals, and they must be prepared to fight back against potentially devastating attacks. The Fortinet Security Fabric helps unify an entity's security architecture, simplifying security operations while providing real-time, multilayered threat response.

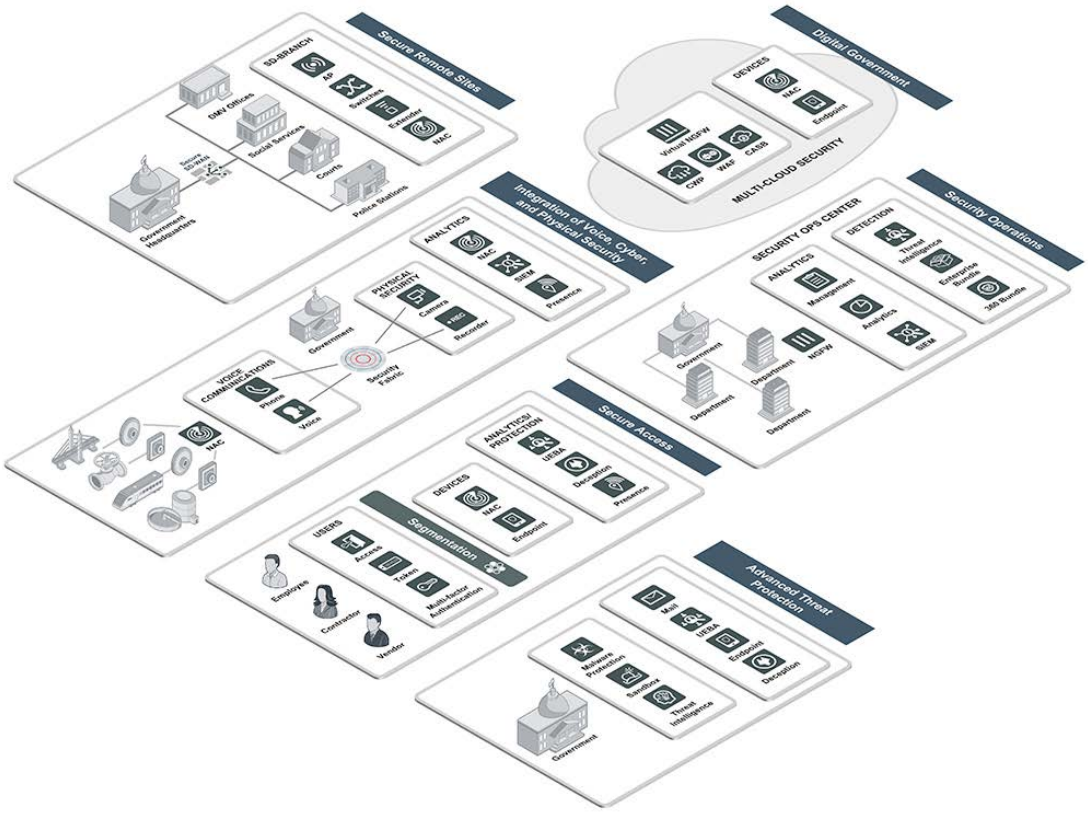


Figure 1: State and local government cybersecurity solutions from Fortinet address multiple use cases with a broad, integrated, and automated approach to security.

[1] "For state and local government, 2019 was the year of ransomware," StateScoop, December 20, 2019.

[2] "What Makes Local Government an Enticing Cyber Target?" Fortinet, August 19, 2019.

[3] "What Are The Biggest Security Threats To State And Local Governments?" Infosec, accessed January 16, 2020.

[4] Dan Lohrmann, "2019: The Year Ransomware Targeted State & Local Governments," Government Technology, December 23, 2019.

[5] "For state and local government, 2019 was the year of ransomware," StateScoop, December 20, 2019.

[6] "Threat Landscape Report, Q2 2019," Fortinet, 2019.

[7] Karen J. Bannan, "Local Governments Experiment with Innovation Labs," StateTech, June 27, 2019.

[8] Ryan Johnston, "Texas moves 'beyond IoT' in new state technology strategy," StateScoop, November 19, 2019.

[9] Phil Muncaster, "Cybersecurity Skills Shortage Tops Four Million," Infosecurity, November 7, 2019.

[10] "How Digital Transformation Is Revolutionizing Government," Forbes, March 29, 2019.

[11] "Ransomware Attacks Targeting Local Governments, What CISOs Need to Know," The CISO Collective, Fortinet, September 11, 2019.

[12] Claire Zaboeva, et al., "Public Sector Security Is Lagging—How Can State and Local Governments Better Defend Against Cyberattacks in 2020?" Security Intelligence, December 11, 2019.

[13] Chloe Demrovsky, "Why Ransomware Attacks on Local Government Matter," Forbes, August 27, 2019.

[14] Andy Patrizio, "Enterprises Are Moving to SD-WAN Beyond Pilot Stages to Development," NetworkWorld, May 7, 2018.

[15] Chloe Demrovsky, "Why Ransomware Attacks On Local Government Matter," Forbes, August 27, 2019.

[16] "State agency leaders focusing more on cloud IT investments, survey says," StateScoop, January 22, 2019.

[17] "Gartner recognized Fortinet a Leader in the 2019 Magic Quadrant for Network Firewalls," Fortinet, accessed January 15, 2020.

[18] Ibid.

[19] Shawn McCarthy and Ruthbea Yesner, "Developing Your Security Fabric: A Transformational Approach for State Government," IDC and Fortinet, May 2019.

January 30, 2020 3:42 AM

517025-0-0-EN

D:\Fortinet\White Paper\Vertical Marketing - State and Local\wp-fortinet-state-local-government-cybersecurity-solutions-V1-1302020-342AM