Executive Summary

Local governments are undergoing digital transformation to increase efficiencies and reduce costs. One top goal of many counties and cities is to develop and deliver consistent security strategies, standards, and governance models across their agencies. However, new technologies adopted for these initiatives, such as cloud computing, mobile devices, and Internet of Things (IoT), expand the attack surface and can open the door to new threats. In 2019, more than 104 ransomware attacks targeted state and local government organizations. The Fortinet Security Fabric enables end-to-end integration of a local government’s security architecture, and a broad suite of security solutions that address today’s most critical use cases.

Cyber Criminals Increasingly Target State and Local Governments

With a relative lack of cybersecurity expertise and a need to stay operational at all times, state and local governments have become a favored target of cyber criminals (especially ransomware operators). The reason for this is simple—smaller government agencies are more likely to pay a ransom because of the intense pressure to resume normal operations and serve the public. With the sensitive data they house and the critical infrastructure they control, regional governments now face cyber threats that are growing in number and sophistication. The high number of government employees who rapidly transitioned to telecommuting as a result of the COVID-19 pandemic have introduced new network vulnerabilities and expanded the network attack surface even further.

One of the key challenges for many governments is that their agencies and departments reside in IT silos. This obscures a security team’s visibility into network activity and often limits their ability to enforce controls. In addition, these complex legacy networks comprised of myriad point products cannot support automated workflows (such as compliance auditing and reporting processes). These unnecessary manual workflows waste tremendous resources (both time and money) on an annual basis. Given the ongoing worldwide shortage of skilled IT staff, and a rising crisis in terms of budget constraints, these kinds of operational inefficiencies must also be addressed.

Solution Requirements for Local Governments

To address the challenges above and ensure security scalability for the future, local governments need to keep a number of criteria in mind. Local governments need integrated security solutions across the organization to protect their increasingly distributed network attack surfaces. This includes different departments, multiple agencies, and telecommuting staff. Security that works as a collective unit throughout the organization is able to communicate, share threat intelligence in real time, and then automatically respond to threats. Security integration is a foundational requirement because it enables instantaneous actions for prevention, detection, and mitigation of cyberattacks.
Performance is also an important consideration. Departments, agencies, and public users demand a reliably available and responsive network. Therefore, security controls must not create performance bottlenecks in the process of securing network traffic or enforcing access controls.

Segmentation of users, applications, and the network helps thwart insider threats and limits hackers and malware (including ransomware) from spreading through the network. Centralized visibility of network events and coordination of threat responses across all segments must also be readily available.

In addition, there is a significant need within public agencies for greater simplicity when it comes to security infrastructure. The security architecture should minimize the amount of time staff spends deploying, orchestrating, and monitoring security systems. To this end, single-pane-of-glass management is a key requirement. Automated compliance reporting is another valuable feature to consider.

The Fortinet Security Fabric: Simplified Protection for Public Sector Networks

Fortinet’s unique Security Fabric architecture provides local governments with better network protection, simplified management, and seamless automation of time-consuming tasks. The Security Fabric incorporates both Fortinet solutions and third-party partner products so that governments can leverage their existing security investments while still gaining the critical advantages of an integrated security architecture.

Proven Solutions, Comprehensive Security

Fortinet offers comprehensive solutions to protect local government networks, addressing cybersecurity needs covering all attack vectors.

Network Security. FortiGate next-generation firewalls (NGFWs) provide scalable, comprehensive protection without slowing network traffic. Purpose-built, application-specific integrated circuit (ASIC) chip processing results in exceptionally high performance—even when large amounts of encrypted traffic are inspected. Intent-based segmentation capabilities ensure that network resources are adequately divided for appropriate access control. Secure software-defined wide-area networking (SD-WAN) features offer secure and efficient services to both remote users and distributed offices of different departments/agencies.

Cloud Ready. As local governments move more resources to the cloud, they can be assured of integrated, comprehensive protection. FortiCWP cloud workload protection tools extend this integration to a hybrid cloud network, and feature native integration with each major public cloud provider and a coordinated approach to securing all of them.

Endpoint Security. FortiClient and FortiEDR advanced endpoint security help detect and remediate attacks on devices before they can spread through the network. FortiInsight user and entity behavior analytics (UEBA) technology watches for anomalies in behavior, while FortiDeceptor helps lure attackers into revealing themselves.

Zero-trust Access. In combination with FortiGate segmentation, Fortinet identity and access solutions deliver comprehensive protection and control. FortiToken and FortiAuthenticator enable multi-factor authentication (MFA) of remote employees. Network access control (FortiNAC) is able to enforce bring-your-own-device (BYOD) policies even over remote virtual private network (VPN) connections, allowing the organization to control what types of devices can connect and what access they receive.

Wireless Connectivity. FortiAPs provide secure wireless access at remote work locations with full integration and configuration management in a single pane of glass.

Telephony. FortiFone is a secure, Voice-over-IP (VoIP) telephony solution, whose traffic is secured, managed, and monitored by a FortiGate NGFW. It is available in soft client and several hardware options.

Data Loss Prevention (DLP). FortiGate and FortiWiFi provide DLP functionality for remote workers, which is essential when these employees have access to sensitive company data.

Management and Analytics. The Fortinet Security Fabric supports a more proactive, consistent approach to security across local government deployments. FortiManager, FortiAnalyzer, and FortiSIEM provide centralized visibility, control, and reporting with maximum automation.
Why Fortinet Is the Preferred Choice for Local Governments

Fortinet solutions for local governments deliver everything needed for reliable, effective security: top-rated technology and threat intelligence, faster performance, and a uniquely integrated architecture that covers all attack surfaces while reducing complexity. In addition, Fortinet is committed to regular independent third-party testing to validate product effectiveness and performance—including NSS Labs, ICSA Labs, and Virus Bulletin.8

Fortinet invests heavily in research and development (R&D) and holds four times more patents than any other network security vendor. One key benefit of in-house R&D is the custom, purpose-built security processors that radically boost performance, enabling Fortinet firewalls to deliver the best price per performance in the industry.9

To ensure top protection from the latest threats, FortiGuard Labs’ in-house threat intelligence experts work around the clock to discover and analyze threats and to deliver countermeasures in the form of continuous updates to the Fortinet Security Fabric.

Reducing Risk While Boosting Efficiency

Fortinet marries effective security with efficient security management, integrating multiple capabilities with the Fortinet Security Fabric. This consolidation of security functionality is crucial in providing the end-to-end security coverage that local governments require, while reducing resource needs.

Fortinet already has a large installed base of government customers and a history of supporting complex public-sector environments, making Fortinet a premier security partner for local governments.

---

2 Ibid.
3 Jim Richberg, *Pandemic underscores the importance of security, agility for remote work,* GCN, August 10, 2020.
5 *IT functions suffering from skills shortages according to IT leaders worldwide in 2017 and 2019,* Statista, September 24, 2020.
8 *Certifications,* Fortinet, accessed October 6, 2020.