SOLUTION BRIEF

Securing State and Local Government with Fortinet

Protect Digital Assets and Critical Infrastructure Against Growing Advanced Threats

Executive Summary

Technology and data power almost every aspect of our lives and communities. Citizen service delivery and user experiences have been improved by the digitization of processes. But these changes have also increased cyber risk for entities of all sizes—and the frequency, severity, and sophistication of cyberattacks continues to accelerate. Attacks such as ransomware can cause significant financial losses, interruptions of vital services, and loss of citizen confidence and trust.

The Fortinet Security Fabric provides comprehensive and integrated security that helps state and local governments defend against cyberthreats and protect their networks, data, and critical infrastructure. With the Security Fabric, governments are able to secure attack surfaces and increase operational resiliency - the ability to resist, absorb, adapt, and recover from a cyberattack. The Security Fabric converges networking and security tools into a single platform for tighter integrations, increased automation, and faster responses to attacks. A single pane of glass improves visibility and operational efficiency, which helps reduce the burden on lean IT teams. The average downtime following a ransomware attack is over three weeks, so investing in a professional cybersecurity solution has never been more prudent, timely, or valuable.[1]

2,792

U.S. public administration entities were hit by a cyberattack in 2022 alone.[2]

Cybersecurity Challenges Faced by State and Local Governments

State and local governments face a number of different cybersecurity challenges. Top issues include:

Project Slowdowns

Ineffective or inefficient security solutions can slow many of state and local governments' technology initiatives, such as migrating services to the cloud and deploying IoT devices (like sensors) across critical infrastructure. In the past year, some projects have slowed because they have proven to be more complicated, costly, and time-consuming than initially expected. IoT devices often lack adequate built-in security, and a fragmented security architecture can hamper efforts to harden them against attack, slowing or even halting implementation.

Budget Constraints

Ensuring adequate protection of critical data and resources is difficult for organizations with tight budgets. In addition to limited budgets, state and local governments get pushback from citizens, who are usually skeptical about proposed increases in spending. Often, elected officials are reluctant to support major projects or increased headcount because they don't want to alienate voters. As a result, IT staff must be strategic about budget and resource allocation. Risks should be prioritized according to the potential impact on citizens and institutions. At the same time, savvy state and local governments have powerful incentives to act now. Time is running out to take advantage of fiscal assistance from two key federal programs for critical infrastructure cybersecurity. The Coronavirus State and Local Fiscal Recovery Funds (SLFRF) program holds $175 billion in federal funds with a deadline to obligate these funds by December 31, 2024. And the Infrastructure Investment and Jobs Act (IIJA) holds $1.55 billion for Public Utilities, a portion of which has a distribution deadline of five years.

Skills and Training Gaps

Even if budgets allow for increased headcount, a persistent cybersecurity skills gap and lack of workforce training impedes security. In fact, according to recent research, the global cybersecurity workforce shortage tops 3.4 million people.[3] Even if qualified candidates are available, salaries have risen for 47% of cybersecurity professionals with certifications, after rising 29% in 2021.[4] Because public sector salaries often cannot compete with those in the private sector, hiring the available talent is even more difficult for state and local government entities.

Fortinet Solutions Use Cases

Fortinet solutions offer distinct advantages for state and local governments, including:

Meet Compliance Requirements

State and local governments must adhere to regulations regarding personal information, critical infrastructure protection, and environmental standards. Frequent audits slow down strategic initiatives, as staff is often redeployed for manual audit preparation. Fortinet solutions meet government compliance requirements such as FISMA, NIST, and CJIS, and embedded automations make demonstrating compliance faster and easier. In addition to helping organizations meet compliance, Fortinet goes above and beyond by offering complimentary cybersecurity training programs, such as the NSE (Network Security Expert) and the Fast Track Program, aimed at educating IT professionals and bridging the cybersecurity skills gap.

Enable Broad Integration

As the attack surface expands, cybersecurity teams often scramble to fill gaps in security coverage using various point products. Over time, this piecemeal approach builds a siloed security architecture filled with solutions that do not communicate with each other. Architectural fragmentation also results in decreased visibility, delayed threat response, and operational inefficiencies. Siloed, overlapping software and hardware license costs are also expensive. The Fortinet Security Fabric is a flexible, vendor-agnostic platform that consolidates and integrates products, which helps to optimize budgets and reduce complexities for IT teams.

Streamline Security Operations

State and local governments oversee vital infrastructure such as water mains, sewage systems, roads, bridges, and public transportation, and they often use IoT devices to monitor them, extending their IT infrastructure. Coordinated threats to cyber and physical security are evolving faster than some agencies can manage, since it requires including new technologies like facial recognition and weapons detection. The automation in the Fortinet Security Fabric helps streamline security operations and reduce the burden on IT teams.

Centralize Network Security

In addition to providing essential infrastructure and services that directly impact people’s daily lives, state and local governments also handle important functions like local elections, issuance of driver’s licenses and identification, and law enforcement. By centralizing the management of network security, organizations benefit from enhanced visibility, more granular control, and consistent security policies, no matter what services are being provided or from which location(s).

Obtain Contract and Budget Assistance

Cooperative contracts can be an excellent alternative to traditional RFPs. They provide a streamlined process for organizations looking to purchase IT solutions. Fortinet simplifies this process by offering our entire catalog of products and solutions through cooperative contracts, so IT teams don’t waste time and resources conducting their own formal solicitations. In addition, Fortinet and our partners are now offering a comprehensive grant support program. This free program provides public sector agencies with grant information, customized research, and consultation services to help develop project ideas, identify available grant funding for technology-rich projects, and expand initiatives that are already in the works.

Strengthening Cybersecurity for Operational Resilience with Fortinet

The Fortinet Security Fabric detects threats, closes security gaps, and reduces complexity to deliver exceptional operational resilience. Having a common operating picture of activity across your network and devices is the foundation of cyber resilience and can be achieved with a cybersecurity mesh architecture that converges security tools into a single, vendor-agnostic platform. This platform approach offers a single pane of glass view of all network activity. The mesh architecture of the Fortinet Security Fabric spans the attack surface and enables self-healing security and protection of devices, data, and applications.

Private-sector industries are starting to outsource more security operations, while state and local governments often bring them in-house. Internal security operations centers (SOCs) centralize threat detection, analysis, and response, offering actionable insights for network security. Some states provide security operations as shared services to agencies and local governments. For value, SOCs need integrated security architecture, centralized control, and automated reporting and threat response. Multi-tenant infrastructure is essential for entities serving multiple agencies or governments.

> *"We saw demonstrable throughput value in the FortiGate appliances. After two years of research, we decided that Fortinet would be the best partner for the City of Portland and provide the best alignment for the city's next generation of services to our community."*
>
> **Christopher Paidhrin**
> Senior Information
> Security Officer,
> City of Portland

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 Next Generation Firewalls (NGFWs) provide the foundation for this comprehensive architecture. Threat intelligence from FortiGuard Labs provides real-time insight into new threats so that response can be timely. Additionally, security services like Advanced Malware Protection, antivirus, and web filtering can be accessed through several FortiGuard Service Bundles for FortiGate. Built as multi-tenant 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.

Key Takeaways

Government agencies face increasing threats that can impact national security, public safety, and civilian services, so they need robust cybersecurity solutions. Balancing constrained budgets and adopting advanced technology while maintaining transparent communication with citizens is crucial. The Fortinet Security Fabric offers comprehensive cybersecurity to guide operational and defensive strategies for government entities worldwide, regardless of size. For more information about how Fortinet can help resolve your agency's cybersecurity challenges, visit our website.

[1] "Length of Impact After a Ransomware Attack Worldwide, Q1 2020 - Q2 2022," Statista, August 28, 2023.

[2] "DBIR: 2022 Data Breach Investigations Report: Public Sector snapshot," Verizon, May 24, 2022.

[3] "Fortinet 2023 Global Cyber Skills Gap Report Finds More Needs to Be Done to Untap New Talent," Fortinet, March 21, 2023.

[4] "2023 Cybersecurity Skills Gap Global Research Report," Fortinet, November 22, 2023..

April 17, 2024 7:18 PM
2432607-0-0-EN