SECURING THE STATE: FORTINET'S SECURITY SOLUTIONS FOR STATE GOVERNMENTS

KEY SECURITY CHALLENGES FOR STATE GOVERNMENTS

State governments are undergoing digital transformation to increase efficiencies and reduce costs. One top goal of many states is to develop and deliver consistent security strategies, standards, and governance models across state and local agencies, including delivering security services to local 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.

Because of the sensitive data they house and the critical infrastructure they control, states are popular targets for hackers. And, like businesses, they are facing more sophisticated cyber threats than ever before. On the bright side, state governments do understand how critical cybersecurity is. "The most recent surveys from the Center for Digital Government show that cybersecurity is the No. 1 priority for state and county CIOs."[1]

Another challenge for many state governments is that agencies and departments reside in IT silos. This reduces security teams' visibility into security events across the network, and limits their ability to enforce controls.

In addition, complex legacy networks comprised of myriad point products, and demonstrating compliance without automation, waste a lot of IT time and resources. Given IT security skills shortage and budget constraints, it's important to address inefficiencies.

STATE GOVERNMENTS: SOLUTION REQUIREMENTS

To implement the ideal security posture to address the challenges above, as well as ensure scalability for the future, state governments need to keep a number of criteria in mind.

To effectively secure the entire attack surface, state governments need security solutions that integrate local and global threat intelligence from a proven source throughout the entire network. These solutions must be able to communicate and automatically respond to threats to achieve near-real-time prevention, detection, and mitigation of attacks.

Since departments, agencies, and residents demand an always-available, fast network, security controls that slow down the network are unacceptable. Ensuring high-performance solutions is another critical criterion.

While IT silos are not conducive to efficient security, segmentation of users, applications, and the network helps thwart intrusions and stop threats from spreading through the network. Centralized visibility of network events and coordination of threat response across all segments must be readily available.

There's also a significant need within public agencies for a streamlined security infrastructure. Thus, the security architecture needs to minimize the amount of time staff spend administering and monitoring security systems. Centralized management through a single pane of glass is key. Automated compliance reporting is another important consideration.

FORTINET DELIVERS COMPREHENSIVE SECURITY FOR STATE GOVERNMENTS

FORTINET'S STRATEGIC DIFFERENTIATOR—THE FORTINET SECURITY FABRIC

Fortinet delivers a unique approach to security. The architecture, called the Fortinet Security Fabric, integrates Fortinet and Fabric-ready Partner products to enable easier management, better protection, and automation of time-consuming tasks.

As part of the Fabric ecosystem, Fabric-Ready Partner solutions can be integrated with the Fortinet Security Fabric. State governments can leverage their existing investments while still gaining the time savings and stronger security of an integrated security architecture.

FORTINET'S SIMPLIFIED, PROVEN SOLUTIONS ARE IDEAL FOR STATE GOVERNMENTS

Fortinet provides integrated security solutions to protect the whole network:

Network Security. Protects the network from known and unknown threats. FortiGate Next-Generation Firewalls include multiple security and networking controls, as well as a Wi-Fi controller in a single platform for reduced complexity, ease of management, and lower total cost of ownership (TCO).

Multi-Cloud Security. Reduces complexity by protecting the expanded attack surface across Software-as-a-Service (SaaS) applications, as well as private and Infrastructure-as-a-Service (IaaS) cloud deployments, all with a single solution.

Endpoint Security. Detects and blocks malicious objects from web, email, network, and personal storage that target endpoint devices.

FortiClient delivers easy-to-manage, automated, fully customizable endpoint security for a wide range of devices.

Email Security. Inspects email for unwanted and malicious messages and inappropriate/sensitive content. FortiMail provides comprehensive security for both incoming and outgoing messages and is easy to deploy, operate, and manage.

Web Application Security. Protects web applications from threats targeting known and unknown exploits. FortiWeb (web application firewall) uses the latest threat intelligence to protect web applications from sophisticated attacks while lowering management and operational costs.

Advanced Threat Protection. Detects intrusions that have evaded conventional, established defenses. FortiSandbox isolates and inspects any suspicious files detected by security tools to stop them before damage is done.

Management and Analytics. Enables visibility and management of Fortinet and partner products for smooth operation and greater insight. Reduced cost and complexity with centralized control of the entire network from a single console drive a lower TCO. Automated reporting helps track compliance.

Unified Access. Fortinet's secure access solutions deliver comprehensive security and access control for secure Wi-Fi and enable secure user/admin connectivity.

WHY FORTINET IS THE PREFERRED CHOICE FOR STATE GOVERNMENTS

With more than 340,000 customers, Fortinet is the fastest-growing enterprise network security company in the world and the #1 most adopted network security solution.

Fortinet's solution for state governments delivers everything needed for reliable, effective security: top-rated technology and threat intelligence, faster performance, and a unique Fabric approach to cover all attack surfaces and reduce complexity. In addition, Fortinet is committed to regular independent third-party testing to validate product effectiveness and performance.

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.

To ensure top protection from the latest threats, Fortinet's 200+ 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.

To validate product effectiveness and performance, Fortinet frequently participates in third-party tests, consistently earning top scores. Fortinet has earned "Recommended" ratings for nine different products in tests by NSS Labs, an independent research and testing organization. This is more than any other network security vendor. Fortinet also regularly receives certifications from ICSA Labs, Virus Bulletin, and more. These unbiased validations let customers know which products perform the best and deliver the lowest TCO, helping them make informed decisions.

Research and advisory firm Gartner provides insights on technology and vendors to help business leaders make purchasing decisions. Multiple Fortinet solutions can be found in Gartner Magic Quadrants, including Enterprise Network Firewall, UTM, Wired and Wireless LAN, and Web Application Firewall.

PROVEN SECURITY SOLUTIONS FOR STATE GOVERNMENTS

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 state 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 state governments.

[1] "Survey Highlights Cybersecurity Gaps Between Government and Private Sector," Government Technology, August 25, 2017.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

173011-0-A-EN May 7, 2018 4:16 PM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:SB-State-Govt-Solution-Selection-for-Business:sb-state-govt-solution-selection-050718-416pm