FORTINET

SOLUTION BRIEF

Why Hardware-as-a-Service from Fortinet Makes Sense for State and Local Governments

Executive Summary

In some areas of state and local government in the United States, data is vulnerable.[1] Cyber defenses may be less robust than cybersecurity professionals would prefer due to challenges around budgets, a skills gap in hiring new talent, and the increasing volume and velocity of cyber threats.[2] A new model for procuring best-in-class security solutions overcomes all three limitations.

The Hardware-as-a-Service (HWaaS) approach gives public entities a way to pay for hardware and software as operational expenditures (OpEx) rather than capital expenditures (CapEx). This can reduce costs, streamline procurement processes, and enable governments to maintain a modern security infrastructure even as pressures to cut CapEx budgets continue to mount.

The HWaaS Option Helps State and Local Governments:

- Deploy top-tier security solutions with no CapEx investment
- Streamline procurement approval processes for hardware, software, and services
- Potentially reduce overall spending on security infrastructure
- Establish a cadence of regular security-technology upgrades, to stay ahead of rapidly evolving threats
- Modernize without adding staff for new security expertise

Barriers to IT Innovation in State and Local Governments

Many state and local government budgets exist in a perpetual tightening cycle. This creates a formidable barrier to modernization of the technology infrastructure. Obtaining CapEx funding may be feasible for public-facing solutions, but investment dollars tend to be very hard to come by for behind-the-scenes functionality, even mission-critical security capabilities.

Staffing issues exacerbate the problem. Experts predict that there will be 3.5 million unfilled cybersecurity jobs in the U.S. by 2021.[3] State and local governments across the country are feeling the impact of this skills gap. Those governments that do invest in top-tier security technologies might have difficulty optimizing the benefits from their investments if they are experiencing gaps in cybersecurity skills or headcount.

Another factor affecting governments' ability to keep systems secure is the lightning-fast rate of change in both threats and security technologies. Even when CapEx money is available, the length of the typical government procurement process makes it difficult to maintain a cutting-edge infrastructure. By the time request for proposal (RFP), purchase, and implementation processes are complete, the deployed solution might no longer be the latest version.

Efforts to modernize the security infrastructure in state and local governments face significant obstacles—but they are absolutely imperative. Ransomware, data breaches, and other cyberattacks are becoming increasingly prevalent.[4] Some experts believe local and state governments are now cyberattackers' preferred targets.[5] In July 2019, the governor of Louisiana declared a state of emergency in response to a ransomware outbreak.[6] Government IT teams wanting to avoid a similar fate must find a way to keep their security infrastructure up to date. That is where HWaaS comes in.

How Does HWaaS Work?

HWaaS is a consumption-oriented procurement model that enables businesses, governments, and other organizations to access technologies that may not fit in their CapEx budgets. Many top-of-the-line Fortinet security solutions are available via HWaaS, including FortiGate next-generation firewalls (NGFWs), FortiSwitch secure access switches, FortiAP access point security solutions, FortiNAC network access control appliances, and even FortiSIEM security information and event management software.

To access these technologies as a service, a state or local entity would enter into an agreement with a participating Fortinet partner. The partner would deploy the hardware, either on-premises in the government data center or in the partner's data center with cloud-based access for government IT staff.

The government entity would then make recurring payments to the partner for a term such as 12 or 36 months. At the end of the term, the client would have three options: purchase the equipment outright, renew the HWaaS contract, or end the agreement.

HWaaS in Action

Consider the example of a state agency that has 20 satellite offices. It is currently paying $10,000 per month for multiprotocol label switching (MPLS) connectivity between these sites. To improve the speed of the satellite offices' internet connections and to save money, the agency wants to replace its MPLS connections with software-defined wide-area networking (SD-WAN) using a new FortiGate NGFW.

The NGFW's list price is $213,000. A Fortinet partner is selling it for $105,500, but that price still represents a significant upfront investment. Eliminating the $10,000 monthly charge for MPLS is appealing, but the agency does not have room for the NGFW in its CapEx budget.

	Legacy MPLS-Based Network	SD-WAN via NGFW Purchase	SD-WAN via HWaaS
Monthly Charge for MPLS	$10,000	$0	$0
Monthly Charge for SD-WAN	$0	$0	$5,200
CapEx Investment	$0	$105,500	$0
ROI of Transition	N/A	10.5 months	1 month

The agency chooses instead to pursue an HWaaS arrangement. It gains access to the same FortiGate NGFW, via a monthly recurring payment of $5,200 and no CapEx spending at all. This decision spares the agency from the painful RFP process that is typical for state governments' CapEx allotments, and it provides a full return on investment (ROI) as soon as the agency stops paying the $10,000 monthly MPLS charge.

Benefits of the HWaaS Model

Moving security technologies to HWaaS offers state and local governments several benefits. One is that the OpEx cash flows of an HWaaS contract can usually be slotted into the existing annual budget. The upfront costs are much lower than with CapEx investments, and approval processes for OpEx purchases tend to be less onerous. Thus, OpEx funds are generally easier to secure than CapEx.

In the example above, shifting from a legacy solution with a higher monthly recurring charge to a modern, lower-cost solution should be seamless. The agency might even be able to leverage the $4,800-per-month cost savings to deploy other HWaaS solutions that further enhance its security infrastructure.

Another HWaaS option is to modernize by engaging a managed security service provider (MSSP) to run the new hardware in its own data center. This approach saves the state or local government from having to add security expertise, because the Fortinet partner organization is fully responsible for deployment and maintenance of the solution.

A final benefit of HWaaS lies in the flexibility the public entity has at the end of the contract. Upgrading hardware when the contract term expires is simple, especially compared with a lengthy CapEx procurement process. This means the HWaaS approach helps state and local governments keep their security technologies up to date when budgets for CapEx spending are tight (or nonexistent).

Top-tier Security Solutions Made Attainable

Fortinet security solutions are regularly recognized by independent reviewers as best in class. As an example, FortiGate NGFWs have received "Recommended" ratings from NSS Labs for the past six years. In addition to providing leading-edge functionality within their individual markets, Fortinet solutions integrate into a Security Fabric, facilitating real-time coordination of threat detection and response.

HWaaS makes Fortinet security solutions attainable even for state and local governments facing continuously constricting limits on CapEx spending. As governments prioritize both IT security and IT modernization, the HWaaS model provides an opportunity to achieve both objectives—and to reduce the chances that they will be the next victim of a headline-grabbing cyberattack.

[1] Megan Reiss, "When it comes to cybersecurity, states are the weak link," Newsday, January 26, 2019.

[2] Michelle Moore, Ph.D., "Inside the Government Cybersecurity Landscape: Federal vs. State Level Challenges," Tripwire, May 1, 2019.

[3] Dave Barton, "The Cybersecurity Talent Gap = an Industry Crisis," Security Magazine, April 30, 2019.

[4] Benjamin Freed, "Report: Ransomware attacks against state and local government are on the rise," StateScoop, May 13, 2019.

[5] Aroosa Ashraf, "What Are The Biggest Security Threats To State And Local Governments?" Infosec Institute, accessed September 9, 2019.

[6] Catalin Cimpanu, "Louisiana governor declares state emergency after local ransomware outbreak," ZDNet, July 25, 2019.