SONICWALL®

SOLUTION BRIEF

State and Local Government: The Big Cybersecurity Squeeze

State and local tech leaders are under pressure from hackers on one side, work from home on another, and the push toward digital government on another. How can they meet these competing needs with existing headcount while maintaining security?

The days of rolling out digital transformation in small safe phases are a pleasant memory. State and local technology leaders have had to forget about limiting risk and jump into provisioning digital services for their remote workers and constituents with no time to worry about what could go wrong. But, as everybody knows, a lot can go wrong. And it's the tech leader who will have to explain why the agency was attacked, or the workers can't log in, or the constituency is sending angry emails. That's not new. What is new is that IT is no longer running the show from behind the curtains. IT is now center stage, and everyone is paying attention.

Government technology leaders have spoken. Their top priorities are cybersecurity, secure remote access, and connectivity. And state legislators are responding with a host of proposed legislation that will bolster their municipalities' security posture. But while new laws that require or encourage better cybersecurity look good on paper, questions about how new requirements will be met worry technology leaders who understand the scope of the challenge. From ridding offices of outdated workstations to finding and keeping qualified staff, there's a lot of work to be done. Success will begin with a holistic strategy and depend on finding the right partners.

Hackers are looking at you. Here's why.

State and local governments are highly appealing targets for malicious actors. For one thing, there are so many of them — over 90,000, including counties, townships, and town governments. All but the smallest have critical IT systems that store large amounts of personally identifiable information (PII) about constituents, as well as data about the organization's own financial relationships.

Local governments tend to have a lower level of security due to budget constraints, lack of qualified staff, and the continued use of outdated computer systems. Agencies are often aware of their vulnerabilities: for example, the Illinois Attorney General's Office was the target of a triple extortion ransomware attack in February 2021 — an event that occurred after a state audit had alerted the AGO that its cybersecurity protections were inadequate. Other government organizations are also known to be aware of gaps in their defenses that they have not yet been able to repair.

Attackers are paying attention. They target state and local governments because they think they can get the biggest payout for the least effort. That's why there were 44.6 million attacks against government customers in the first half of 2021, a 917 percent increase over the previous year. And until recently, governments were unable to do much to stop them.

However, that is changing. Federal dollars are becoming available to help state and local governments improve their cybersecurity, and state and local decision-makers are assigning more budget to protect their infrastructure. After a ransomware attack hit the school district in Fairfax County, VA, the county shifted $8M to its cybersecurity budget. Now, other municipalities are following suit.

Honey, did we lock the door?

Most state and local tech leaders report they've been pleasantly surprised by their organizations' ability to adapt. Yet 61 percent also say they are still worried about cyberattacks targeting their remote workforces.

The lockdowns happened so fast that a lot of standard security controls were set aside. Technical debt was created that in many cases still exists. Ports and protocols were opened and firewall rules were not updated. Many of these vulnerabilities remain unfixed, leaving open doors for bad actors. But now, the dust has settled. It's time to face that technical debt, and the top priority should be fixing security gaps.

Municipalities can protect themselves with a reliable next-generation firewall that can scale to support a massive number of devices and encrypted connections concurrently while scanning them for threats—but the device has to do all that without impacting performance.

Clean air, clean water, and clean broadband: today's essentials of life

Infrastructure is not a luxury: no municipality can grow without broadband, which correlates to income mobility and overall quality-of-life metrics.

But while state and local governments are eager to provide broadband to their constituencies and federal dollars are on the way, the same technologies that let students get their homework done and parents work from home also provide a way for hackers to execute man-in-the-middle attacks and attacks from compromised devices.

CISOs have to think about security, but users only care about performance. Systems have to respond in real-time and delays are not tolerated. Adding bandwidth is the obvious answer, and the expensive one. A more budget-friendly approach is to implement secure SD-WAN that uses readily-available, low-cost public internet services such as cable, DSL, and 4G.

SonicWall Network Security Manager: Effective, Easy, Affordable

State and local governments can deploy massively scalable protection with SonicWall's Network Security Manager (NSM). NSM is a comprehensive cyber defense system that enables centralized control of your network security, protects network resources on-premise or in the cloud, exposes potential risks, and supports compliance.

- Register, connect, power up, and manage remote locations from a central location
- Orchestrate all firewall operations through a single console
- Expose misconfigured policies and see hidden risks across the infrastructure
- Ease audits with a full audit trail

Learn more about SonicWall NSM

SonicWall Secure Mobile Access: All Endpoints Under Control

Work from home has exploded the number of endpoints you need to protect. SonicWall's Secure Mobile Access (SMA) gives you a zero-trust posture against any remote device attempting to connect with network resources on-premise or in the cloud. SMA's secure access gateway offers streamlined deployment, availability, and support that lowers the total cost of ownership and provides your remote workforce with round-the-clock access that is cost-effective and scalable.

- Get granular with access control
- Authorize devices based on context
- Use the level of VPN that works for you
- Cross BYOD off your list of things to worry about

Learn more about SonicWall SMA

SonicWall Secure Wireless Access Points & High-Speed Switches: Happy Users, Happy CFO

Building out broadband? SonicWall's Secure Wireless Access Points make it easy to deploy, secure, and manage your network at a low total cost of ownership, and high-speed switches deliver the feature-rich, secure connectivity that state and local government needs.

- Give users a superior experience with 802.11ac Wave 2 support, fast roaming, and auto channel selection
- Switch between cloud and firewall management
- Registration and onboarding are convenient with the SonicWiFi app
- SD-Branch ready switches with 10 gigabit connectivity, flexible management, and your choice of deployment options

Learn more about SonicWall's Secure Wireless Access Points and Switches

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

SolutionBrief-TheBigCybersecuritySqueeze-JK-5486