# SOLUTION BRIEF: HOW STATE AND LOCAL GOVERNMENTS CAN SECURE THEIR NETWORKS

## Abstract

State and local governments are increasing productivity and delivering more and better services by deploying technologies such as wireless networks, mobile applications, collaboration tools, virtualization and cloud computing. But innovation creates risks. How can government agencies keep their networks secure, easy-to-manage and compliant with regulations during digital transformations?

This brief describes how state and local governments can innovate and secure their networks using an integrated, easy-to-manage set of networking and security solutions from SonicWall.

### New Challenges for Security and Network Management

New technologies are enabling state and local governments to bring greater value to citizens and improve the productivity of employees. But every digital initiative exposes agencies to new types of risk. The table below summarizes some of the opportunities and the associated dangers.

### High Availability, Compliance and Flat Budgets

Digital initiatives and multiplying cyberthreats aren't the only challenges facing state and local agencies. IT organizations must:

- Support hundreds of distributed locations.
- Provide high levels of performance and availability for critical applications, including law enforcement, medical and emergency response systems with life-or-death outcomes.
- Cope with an expanding list of regulations and standards, including FIPS, Common Criteria, HIPAA, PCI DSS, the NIST CyberSecurity Framework, and privacy and data breach disclosure laws.
- Manage capital investments, operating expenses and staffing with little or no increase in budgets.

| INITIATIVES | ADVANTAGES | SECURITY CHALLENGES |
|---|---|---|
| Web portals and self-service applications | Provide citizens with fast, convenient access to government services | Malware, DDoS attacks and other web-based threats |
| Wireless networks and mobile applications | Enable agency employees to provide services in communities | Man-in-the-Middle attacks, lost and stolen devices, attacks on the core network from trusted devices |
| Cameras, sensors, controllers, other internet-connected devices | Provide data and manage infrastructure in real time | Attacks on critical infrastructure, DDoS attacks from compromised devices |
| Cloud-based collaboration and productivity tools | Increase the productivity of agency staffs | Lack of monitoring, oversharing of confidential information, exposure to rogue insiders and unsecure third parties |
| Virtualization, SaaS applications, cloud platforms | Reduce the costs of data centers and IT operations while increasing flexibility | Lack of visibility, control, and management tools for virtual and cloud environments |

### Needed: Integrated Security Solutions That Span Networks and Computing Environments

How can government agencies with limited resources address so many challenges?

The key is adopting integrated solutions that can secure traditional, cloud, and wireless networks.

That protect against many types of threats.

That secure multiple computing environments, including conventional (bare metal) servers and virtual machines in data centers, cloud-based SaaS (software as a service) and storage applications, and public and private cloud platforms,

That enables state and local agencies to:

- Define and enforce network security policies centrally
- Drive end-to-end visibility and share intelligence across computing environments
- Protect against both known and unknown threats
- Obtain contextual awareness so security teams can respond to attacks faster and more accurately
- Simplify compliance efforts and audits
- Deliver more services to constituents and communities without increasing risk

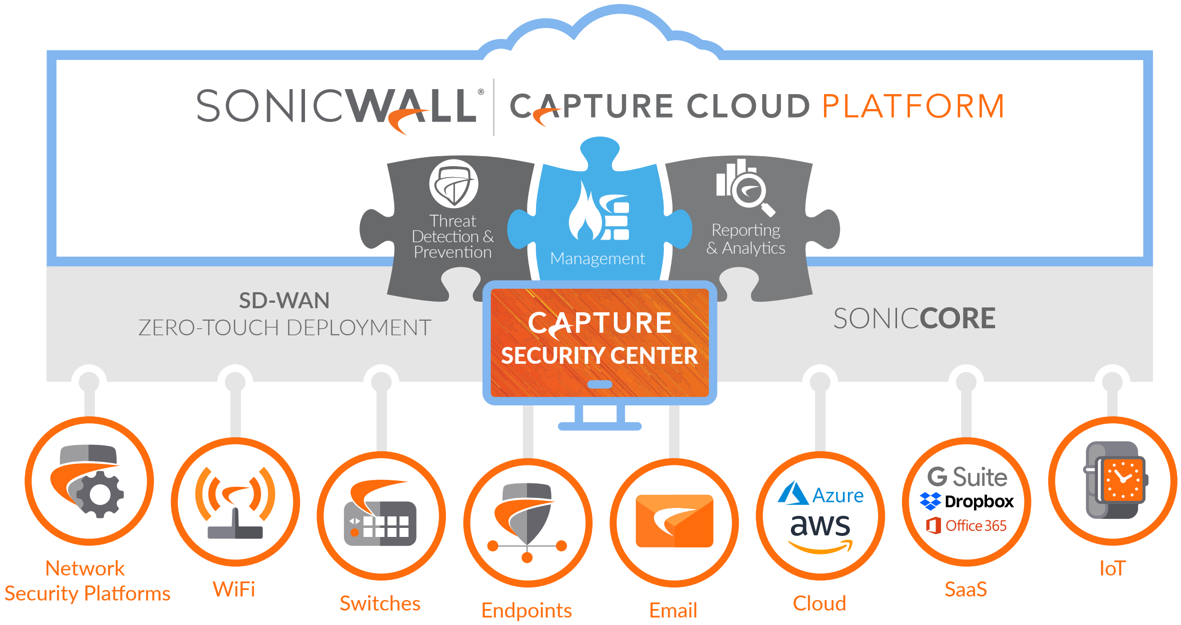
## Integrated Solutions for State and Local Governments

SonicWall offers a series of security products and services that work together to maximize security and productivity, unified through the SonicWall Cloud Capture Platform.

### Network Security Solutions

SonicWall offers a range of network security solutions: Network Security virtual (NS*v*) series virtual firewalls, TZ Series entry-level firewalls, Network Security appliance (NS*a*) series mid-range next-generation firewalls, Network Security services platform (NS*sp*) series next-generation firewalls, and SonicWall WAF series web application firewalls.

SonicWall's firewalls enable state and local governments to provide citizens with secure access to government services through industry-leading threat detection and security policy enforcement features. These include intrusion, application, and protocol protection, patented Reassembly-Free Deep Packet Inspection (RFDPI®), cloud-based malware detection and multi-engine sandboxing with patent-pending Real-Time Deep Memory Inspection (RTDMI™), cloud-based multi-engine sandboxing and malware detection, and defense against OWASP Top Ten web application security risks.



These network security solutions help agencies leverage virtual environments to decrease costs, and they can improve compliance with government regulations and industry standards by segmenting and restricting access to systems with confidential personal and financial information.

In addition, SonicWall's firewalls have the power and high availability features to support thousands of cameras, sensors, and other internet-connected (IoT) devices, and to sustain the performance of critical applications in the face of DDoS attacks.

### Wireless Access Points and Security

SonicWall products to support and secure wireless networking include SonicWave wireless access points, the WiFi Cloud Manager (WCM) WiFi network management system, and the WiFi Planner wireless site survey tool.

These products permit state and local governments improve the security of employee communication and allow clients and constituents to use wireless applications in controlled "guest" mode. They offer capabilities such as wireless intrusion detection and prevention, content filtering, scanning to detect rogue access points, and integration with SonicWall's Capture ATP cloud-based sandboxing.

SonicWall's technology also allows agencies to roll out secure, high-performance wireless networks faster. For example, a mobile app allows non-technical employees to register new mobile access points in remote offices, after which SonicWall firewalls can automatically detect and provision those devices.

### Endpoint Security

SonicWall enables agency employees to bring their work out of the office and into the community by protecting mobile endpoints with the Capture Client unified client security platform and the Content Filtering Client (CFC). These services continuously monitor system behavior and use SonicWall's threat intelligence to provide dynamic whitelisting and blacklisting of URLs, IP addresses, and websites. They work with SonicWall's Capture ATP sandboxing service with RTDMI to detect and block malware, including ransomware, viruses, worms, Trojans, and rootkits. Capture Client can even erase the effects of ransomware and other malware by rolling back Windows PCs and servers to a previously-known good state.

### Security for Email, Collaboration, Cloud-Based File Sharing, and SaaS Applications

State and local government agencies are working hard to increase communication and collaboration with constituents, other local government and non-government organizations, regulators and federal agencies. They seek to increase the productivity of their staffs by using cloud-based email, collaboration, file storage and file sharing services, and popular SaaS applications. However, although these services and applications simplify collaboration and increase productivity, they also make it harder to enforce security and privacy policies.

SonicWall has answers for agencies that use on-premises email servers, Microsoft Office 365, Google G Suite, cloud file storage and file sharing services, and popular SaaS applications. SonicWall's Cloud App Security service, Email Security appliances and cloud-based Hosted Email Security service provide best-in-class advanced threat protection to stop targeted phishing attacks, never-before-seen attacks and email fraud such as business email compromise attacks and account takeovers. They also provide visibility into inbound and outbound email traffic and files, and help prevent unauthorized file uploads and file sharing.

### Securing Applications on Public and Private Clouds

When state and local agencies move applications to cloud platforms, they reduce capital and operating expenses and can move IT staff from routine work to strategic roles. But without visibility into public and private cloud environments, this migration is very risky.

For public clouds, SonicWall's Network Security virtual (NSv) series virtual firewalls enable agencies to protect applications running on Amazon Web Services (AWS) and Microsoft Azure platforms. They can detect previously unknown threats, block ransomware, viruses and other malware, find threats in encrypted network traffic and block communication with malicious websites. They also provide administrators with single-pane-of-glass visibility into traffic to and from the platforms and between zones within them.

For application workloads running in private clouds, the NSv series firewalls provide visibility into traffic between virtual machines, defend against never-before-seen vulnerabilities and the unauthorized takeover of virtual systems. They can also block malicious actions such as spreading malware, file system browsing, and command and control (C&C) communication to malicious websites, as well as enabling micro-segmentation to isolate sensitive data and comply with regulations.

### Security Management, Reporting and Analytics

SonicWall's Capture Security Center is a scalable cloud-based security management system. It provides unified management, reporting, and analytics for network, endpoint, and cloud security through a convenient, secure, cloud portal.

The Capture Security Center:

- Reduces security information silos to give state and local governments deeper insights into their cyber risks.
- Lowers operational costs through capabilities like Zero-Touch operations that dramatically simplify the installation, configuration, and provisioning of firewalls at remote and branch office locations.
- Increases operational efficiency by automating workflows so agencies can programmatically deploy and update security policies with ease and assurance.
- Simplifies compliance by addressing the firewall change management and auditing requirements of standards such as PCI DSS, HIPAA, and GDPR.
- Enables SOC and incident response teams to respond to incidents and remediate vulnerabilities faster by integrating real-time, actionable threat intelligence from SonicWall Analytics, and by providing an interactive dashboard with graphics and tools for monitoring, reporting, and analyzing security and network data.

### Integrated Security That Spans Networks and Computing Environments

State and local governments are under pressure to deliver more value without increasing budgets or staffs. The only way to accomplish that goal is to unify the management of network security.

The Cloud Capture Platform integrates:

- The SonicWall portfolio of network, wireless, email, and endpoint security solutions
- The company's cloud-based Capture ATP (advanced threat protection) service
- Threat intelligence from SonicWall Capture Labs and Capture Threat Network
- The Capture Security Center's unified security management, reporting, and analytics

SonicWall's Cloud Capture Platform gives agency security staffs secure access with single sign-on to a wide range of tools to manage network security policies and monitor and analyze network security traffic.

## Conclusion

State and local government agencies are working hard to serve their constituents better in the face of escalating threats, limited resources, and regulatory requirements. To grasp the opportunities offered by new technologies, they need to find integrated, easy-to-manage security that spans all their networks and platforms. They also need technology suppliers who have a track record of meeting their requirements today and anticipating their needs tomorrow.

**Learn more** at www.sonicwall.com/slg, and contact us to explore how we can help your agency.

**About Us**

SonicWall has been fighting the cybercriminal industry for over 27 years, defending small, medium-sized businesses and enterprises worldwide. Our combination of products and partners has enabled an automated real-time breach detection and prevention solution tuned to the specific needs of the more than 500,000 organizations in over 215 countries and territories, so you can do more business with less fear. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
**www.sonicwall.com**