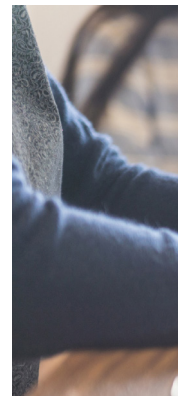


The United States of Cyber Security:

Securing State and Local
Government Networks





All organizations have an obligation to act as caretakers of the personal data they accept. From the smallest retail store to the largest and most complex healthcare systems – there is an expectation that credit card processing and personal information collecting are done so with utmost care.

Perhaps two of the most significant ways that state and local government differ is in the scope of the data itself and the consequences experienced if it's lost. State and local governments collect and store a great deal of sensitive information about citizens, often more than even the federal government. But because it also has a fundamental duty to protect not just its data, but more critically its people, the matter of cyber security becomes much more than an IT issue – it becomes an issue of public safety.

The challenges in maintaining the security of state and localized networks are complex, from evading election hacking to protecting against insider threats. But thankfully, WatchGuard solutions are uniquely architected to be the industry's smartest, fastest and most effective network security products. WatchGuard solutions enable IT pros to keep sensitive data – and citizens – secure.

KEY CHALLENGE

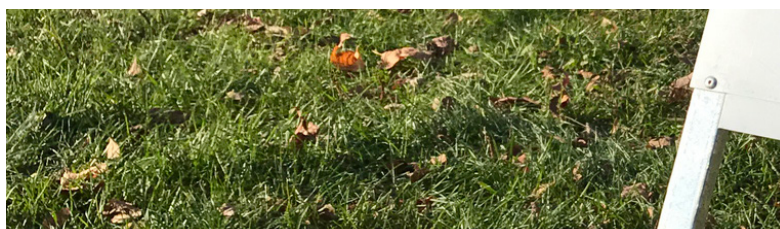
ELECTION HACKING

One of the biggest threats to the security of state and local elections may not be as obvious as a menacing cyber hacker in a dark hoodie – it might be an unassuming but ill-prepared election clerk. In an election system with more than 10,000 unique jurisdictions, the responsibility of security often rests on the shoulders of local officials who are not up to date on the latest security threats or robust cyber security training. Exacerbating the issue is a critical shortage of dedicated cyber security staffing – in fact, it's estimated that there will be a **1.5 million global shortage of cyber security professionals by 2020.**

All it takes is one clerk absent-mindedly clicking on a link in a seemingly legitimate email for a hacker to penetrate a county or state system. These phishing attempts – where hackers attempt to obtain sensitive information such as usernames and passwords by disguising themselves as a trustworthy entity in an electronic communication – are becoming more and more prominent. In fact, 90% of cyber attacks start with a phish.

Given the opportunity, hackers could break into online voter registration databases to either steal personal information or change names and addresses, creating mass confusion on Election Day. Hackers could even take over social media accounts to broadcast false results from seemingly trusted sources, or falsely announce that polls are closing earlier or later than normal. But perhaps one of the greatest costs that follows a successfully executed election hack is the potential to undermine public confidence in the system.





Paper Ballots. Some election advocacy groups say the single most important move that jurisdictions can make is switching to paper-based systems, which can help restore people's trust in election outcomes. With paper ballots, officials can verify vote counts by comparing digital tallies with the paper record.



Risk Assessments. 42% of government officials have not performed a network security audit within the past 12 months, but just like any other organization, local governments should regularly assess the effectiveness of their information security efforts. Often, it's helpful to bring in an outside expert who may be better able to spot potential risks, gaps in compliance, and areas where security could be improved. A WatchGuard MSSP can provide valuable guidance and may see vulnerable security gaps that your internal teams cannot.



Employee Education. Even the most fastidiously trained staff member could make a mistake; maybe they're clicking through morning emails pre-coffee, or maybe they happen upon a particularly well-crafted phishing. WatchGuard DNSWatch enables you to not only protect against a hapless click, but also provide immediate training prompts to reinforce phishing awareness.

KEY CHALLENGE

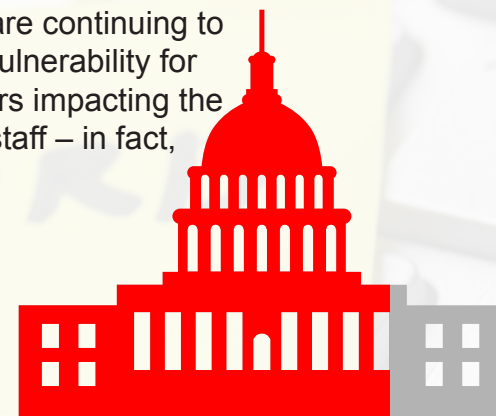
OUTDATED LEGACY TECHNOLOGY

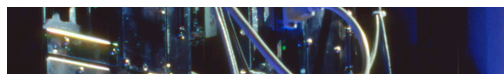
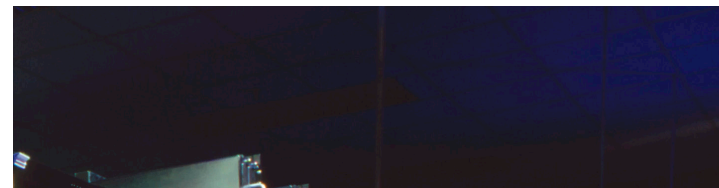
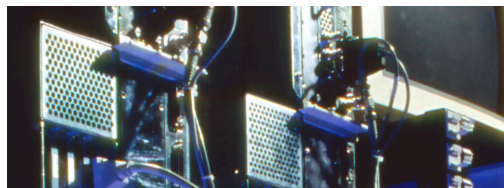
Today's network security does not have the luxury of being 'set it and forget it.' Because hackers are continuing to evolve and perfect their attacks methods, security that doesn't evolve with them creates a major vulnerability for state and local systems. Unfortunately, legacy solutions are easily one of the most prevalent factors impacting the efficacy of government networks today. Often this is a result of budgetary restrictions and limited staff – in fact,

80% of state governments say that funding is their top challenge in government information security.

Take the Office of Personnel Management computer systems for example. The agency blamed their notorious breach, which impacted millions of individuals, on its aging IT infrastructure. During this incident, hackers gained access to personnel files from 4.2 million past and present government employees, as well as 5.6 million digital images of employee fingerprints.

Perhaps one of the most harmful – and common – legacy technologies today is authentication systems centered only on what you know – your credentials. Because these resources can so easily be compromised, the strongest approach to identification should require users to provide both information they know (username and password), along with information provided on something they have (a mobile phone or other device).





WatchGuard MSSPs (Managed Security Service Providers) are armed with the experience to effectively support government IT departments. These service providers are skilled at dealing with budgeting constraints and are able to find and implement the latest solutions that turn IT projects from an inflexible capital expense into a flexible and affordable operating expense.



A relatively easy way to upgrade existing infrastructure – without needing to rip and replace an entire existing system at once – is with **WatchGuard wireless access points**. Each appliance has the flexibility to operate as both an access point and a dedicated WIPS (Wireless Intrusion Prevention System) security sensor. This means that when deployed as dedicated WIPS sensors, the devices work with your existing access points (Cisco, Aruba, Ruckus, Ubiquiti, etc.) to add enterprise-grade wireless security protection to your network.



A stateful packet firewall, while essential, isn't enough anymore. The reality is that every network needs a full arsenal of scanning engines to protect against spyware and viruses, malicious apps and data leakage – all the way through ransomware, botnets, advanced persistent threats, and zero day malware. **WatchGuard's Total Security Suite** provides the most complete package of unified security controls on the market today, all in one cost-effective and easy-to-deploy license.



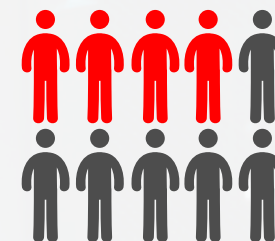
Because passwords alone are easily compromised, **WatchGuard's AuthPoint** service implements MFA (multi-factor authentication) using the AuthPoint app to facilitate user authentication. Any external login attempt creates a secure push notification to the user's smartphone, showing who and from where someone is trying to authenticate. When this message is part of their own login process, they simply accept and quickly gain access to the authorized network resources and Cloud apps. When not, then the authorization attempt is rejected, causing criminals to be blocked from gaining access – even when they are using the correct credentials.

KEY CHALLENGE

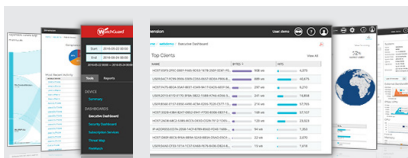
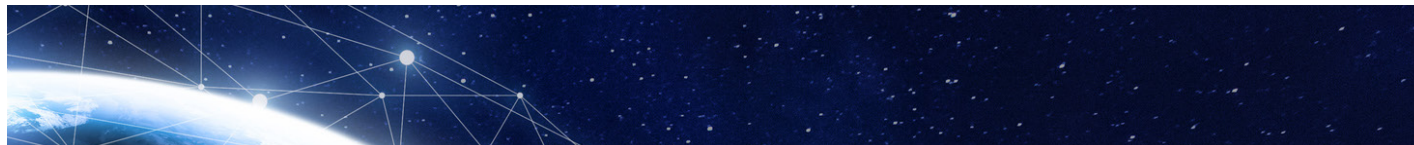
VISIBILITY ACROSS DECENTRALIZED NETWORKS

State and local networks are often far more decentralized than federal networks, creating a great deal of risk. Because there is still a high level of interconnectivity between municipal and state networks, that back and forth communications present many opportunities for cyber criminals to gain access to sensitive data.

When an organization's network infrastructure is so distributed, granular visibility into all activity – across all networks – is critical. Unfortunately, **four in ten state and local IT leaders** say they lack the tools they need to identify and report cyber security vulnerabilities in their networks. When combined with a lack of security intelligence tools that prioritize risks, technology gaps make it harder for government security personnel to optimize their time and effectiveness.



Officials also say a lack of understanding about technologies and risks, and difficulty understanding security metrics, are the biggest challenges they face in communicating security risks to top government leaders and elected officials.



Visibility across all networks can be achieved with **WatchGuard Dimension**. This built-in tool, which comes standard with every WatchGuard Firebox® appliance, provides intuitive reporting methods (such as real-time dashboards) that make it easier to communicate threat activity and remediation to senior government leaders and elected officials.



Government agencies require not only visibility into both network and endpoint event data, but also the ability to quickly leverage actionable insight to remove threats. **ThreatSync**, a key component of WatchGuard's Threat Detection & Response service, collects event data from a WatchGuard Firebox, its Host Sensor, and enterprise-grade threat intelligence feeds, analyzes this data using a proprietary algorithm, and assigns a comprehensive threat score and rank. This powerful correlation engine enables Cloud-based threat prioritization to empower IT teams to quickly respond to threats.

The challenge of securing state and local government networks goes beyond that of a typical IT issue to one of inherent public safety. Thankfully, WatchGuard solutions address the critical challenges impacting government agencies today to keep sensitive data – and citizens – secure.



PROTECT YOUR BUSINESS • PROTECT YOUR ASSETS • PROTECT YOUR PEOPLE

Cyber security is more relevant than ever before. The number of worldwide cyber attacks are at an all-time high with no signs of slowing down, as small to midsize businesses continue to fall victim with serious impact to their business operations and continuity. WatchGuard is here to provide the layered protection you need against the most advanced types of malware, and deliver it in way that is simple to maintain. You face the same threats as enterprise organizations, shouldn't you have the same level of security?

Global Headquarters United States

Tel: +1.800.734.9905

Email: sales@watchguard.com

European Headquarters The Netherlands

Tel: +31(0)70.711.20.85

Email: sales-benelux@watchguard.com

APAC & SEA Headquarters Singapore

Tel: +65.3163.3992

Email: inquiry.sea@watchguard.com

©2018 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, AuthPoint, DNSWatch, Dimension and Firebox are trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No WGCE67105_091918

