Unifying Cybersecurity in State & Local Government

The end-to-end approach to protecting your agency—across any app, any cloud, and any device

Introduction

Today's cybercriminals don't have to look very hard for new places to attack. Government agencies, in particular, keep adding new internet-connected services and technology—often without closing the security gaps. The result is that security threats are increasingly common, with breaches growing in terms of quantity and damage. Studies found that in 2019, there was a surge of ransomware attacks on state and local governments, with 113 notable attacks.[1]

The bad news is that the public sector is highly vulnerable, and the bad actors are taking note. In fact, cyberattacks against state and local government agencies are on the rise.[2] Smaller agencies may be even more at risk due to a lack of security staff and limited funding.

Meanwhile, when it comes to security solutions, the complexity is higher than ever. Thousands of security vendors promise to have the silver bullet for security, and the landscape is awash with a multitude of products and agents to address different threat vectors. Security and IT teams make their decisions in silos—and with no big-picture view of the environment they're trying to protect. It's beyond time for a unified approach.

This white paper will explore why cybersecurity needs to be a team sport, aligning your people, processes, and technology to defend against the latest security threats. We'll look at the key elements needed for a unified approach, and how the comprehensive security platform from VMware can help.

Security Challenges for Today's Agencies

Although breaches at retailers, hotels, and other large enterprises dominate the news, major U.S. cities are experiencing high-profile attacks with damages in the millions of dollars. In fact, all types of city, county, and state government offices are attractive targets. EMS systems, prisons, courts, airports, and election systems are all vulnerable to attack. Many attacks involve ransomware variants and permanent data loss.

For example, the City of Pensacola, Florida was hit with a ransomware attack in early December 2019. The Maze ransomware variant was used, and the hackers threatened to release data if $1M in ransom was not paid. To add insult to injury, this attack occurred days after a shooting at a nearby U.S. Naval Base. Experts estimate that it may take six months to a year for the city, which was mostly shut down, to recover from this hack.[3]

As attacks grow nationwide, government agencies are faced with lots of complexity in securing their infrastructure. Disparate products, agents, and interfaces make it difficult to manage vulnerabilities. The solution sprawl can create more overhead that

TOP 5 CYBERSECURITY BEST PRACTICES

1 **A baseline security assessment** is critical for knowing where vulnerabilities exist, whether you opt for a baseline "Red Team" or "Purple Team" audit and/or cyber hunt exercise. Penetration tests and general audits are also recommended.

2 **Network microsegmentation** is an ideal strategy for limiting lateral movement across the network. Microsegmentation divides your data center into distinct security segments, reducing the reach of an attack if one occurs.

3 **Endpoint detection and response** technology, along with application control (whitelisting) on critical servers, can help detect and remediate advanced attacks. Overall, endpoints are the easiest attack surface for hackers.

4 **Integration of third-party threat analysis** puts your organization in an active position, rather than reactive, and goes well beyond simply responding to alerts. Trusted user communities can also help you get an edge on cybercriminals.

5 **Security training and recruitment/ retention of talent** helps ensure your organization can stay protected, while also knowing how to remediate vulnerabilities.

impacts performance. What's more, key decisions are made by siloed IT and security teams, reacting to threats without a holistic view of the applications, data, infrastructure, and devices that they're trying to protect. Network security is approached differently from endpoint security, which is different from cloud security, and so on.

The interesting thing is that IT and security teams are aligned on the greater goals of preventing breaches, increasing efficiency, and speeding incident resolution. The teams just don't work together very well. According to a recent Forrester study, 77.4% of respondents said their IT and security teams currently have a negative relationship.[1] What's an agency to do?

Strengthening Security with a Unified Approach

To strengthen your agency's cybersecurity posture, your entire organization needs to approach security like a team sport. It's more important than ever to have unified visibility and control across your critical networks, workloads, and endpoints. Your busy IT and security teams need to be able to work together, using a single source of shared truth. The only way to stay ahead of ever-changing threats is with a unified platform—enabling you to zero in on vulnerabilities and mitigate them, before any damage can occur.

Following are three key tactics for building an effective security playbook.

Tactic #1: Security needs to be built-in, not bolted on

Too often, security is approached like a game of "whack-a-mole," with isolated solutions being deployed in response to the latest threats. Many organizations have dozens of security solutions that require independent configuration and monitoring. This increases complexity and risk.

For maximum effectiveness, security should be built into the infrastructure you already have, creating a superior vantage point for threat detection. Your agency should be able to unite around a single platform with a holistic view—reducing the number of products, agents, and interfaces that your teams need to manage, and lowering the chances for error. As a result, you can simplify your policies and have them operationalized across heterogeneous environments, whether running applications in VMs, containers, or bare metal.

Tactic #2: Security needs the context of what you're trying to protect

With the barrage of cybersecurity threats hitting agencies of all sizes, a defensive security strategy is a must. It's vital to stay informed about the latest threats and vulnerabilities. But your security policies are more effective if you also have deeper visibility into your applications and data—and what's "normal" behavior. That way, you can detect anomalous behavior before it can become a threat.

Consider if your security solutions include both endpoint detection and response, along with application control capabilities, to help protect against emerging threats. Continuous diagnostics and mitigation can help you fight the latest malware, ransomware, fileless, and next-generation attacks—on-premises and in the cloud. For added protection, your solutions should also be backed by real-time threat intelligence that suppresses intrusions before they can be deployed.

Tactic #3: Security needs flexibility to support your unique mission

Every agency has its own unique mission, needs, and challenges. Taking a "one-size-fits-all" approach to security simply won't work. Ideally, your organization should have flexible choices for a security stack and prevention protocols. Security solutions need to be effective for your specific workloads, endpoints, networks, clouds, and identity policies—so you can harden potential entry points and proactively immobilize threats.

Your security solutions should also prioritize ease of use and integration. This enables you to break down silos between security and IT teams, while controlling shadow IT and improving manageability. An extensive partner ecosystem is also essential for making the most of your existing security and technology investments.

Transform Security with VMware

In a world of ever-changing threats, VMware is the right partner for protecting your agency and your constituents. VMware helps unify your teams with a comprehensive security portfolio, now including VMware Carbon Black. We provide you with a complete platform approach for continuous diagnostics and mitigation—delivering end-to-end visibility, protection, and system hardening across the network, data center, and endpoint hosts.

Find out how to secure your critical applications, users, and devices, backed by leading threat detection and response capabilities, and be better prepared for what's next.

Sources

[1] VMware Carbon Black, "2020 Cybersecurity Outlook Report," February 2020. https://www.carbonblack.com/resources/threat-research/cybersecurity-outlook-report/

[2] GovTech, "2019: The Year Ransomware Targeted State & Local Governments," December 2019. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2019-the-year-ransomware-targeted-state--local-governments.html

[3] Lee Mathews, "Ransomware Hackers Have Started Leaking City Of Pensacola Data," Forbes, December 31, 2019. https://www.forbes.com/sites/leemathews/2020/12/31/ransomware-hackers-have-started-leaking-city-of-pensacola-data/#46c25d98994b

LEARN MORE

Join us online:

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com