FEDERAL GOVERNMENT WHITE PAPER

Introduction

Today’s cybercriminals don’t have to work very hard to launch new attacks. Advanced hacking tools and services are increasingly for sale on the dark web, and there’s also unprecedented collaboration among nation states. The result is that cyberattacks are growing in volume and effectiveness. Studies found that in 2019, there was a surge of ransomware attacks on government entities, often driven by state-sponsored groups.\(^1\)

The bad news is that the public sector is highly vulnerable, and bad actors are taking note. Federal agencies reported 35,277 cyber incidents in 2017 alone. In the past few years, robust agencies such as the Internal Revenue Service, United States Postal Service, and even the White House have all reported breaches.\(^2\)

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

Cyberattacks are increasing for government agencies, with geopolitical tensions playing a major role. In fact, China and Russia account for 41% of all incident response (IR) investigations, while North Korea, Iran, and Brazil were also found to be the origin of a significant number of investigations.\(^3\) Targets often include financial assets, intellectual property, and state secrets, but election-focused attacks are also growing more common.

Cyberattacks on election infrastructure are supported by a thriving market on the dark web, where 20 different state voter databases were recently found for sale.\(^3\) Sophisticated hacking tools are also cheaper and more accessible than ever. Voting machines, voter rolls, and state election websites are all perceived to be at risk. In a recent survey of IR professionals, 65% believed that the 2020 presidential election will be influenced by a cyberattack.\(^2\)

With attacks on the rise, 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
Unifying Cybersecurity in Federal Government

**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.

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.

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. With a purpose-built internal firewall, you can also secure and inspect lateral traffic with a “zero trust” approach, that is, all traffic is considered untrusted until proven otherwise.

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

With cybersecurity threats ranging from lone hackers to nation states, a proactive 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 on-premises security solutions include both endpoint detection and response, along with application control capabilities, to help protect against emerging threats. Continuous diagnostics and monitoring can help you fight the latest malware, ransomware, fileless, and next-generation attacks. With cybersecurity training simulations, your agency can also improve staff readiness for responding to attacks.
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, 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. You should be able to integrate with existing products, at your own pace.

Transform Security with VMware
In a world of ever-changing threats, VMware is the right partner for protecting your agency and the public at large. 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