



Balancing Security Efficiency and Effectiveness in Endpoint Protection

MARKET TRENDS REPORT



Executive Summary

Government agencies face growing pressure to cut costs while also navigating an increasingly complex threat landscape. Cyber incidents are on the rise while, at the same time, security teams are struggling with tool sprawl and a lack of visibility into their environments. Efficiency has become a major topic of conversation, increasing the pressure on security teams to do more with less.

Confronting a growing number of alerts and tighter resources, government agencies must evaluate their existing security deployments in endpoint prevention, detection and response for opportunities to reduce costs and leverage the right technology for more efficient endpoint security.

With the incorporation of automation and machine learning (ML), current solutions have the potential to reduce false positives and ease the pressure on IT and security teams. The right endpoint detection and response and application control solutions can help drive both efficiency and effectiveness in government security efforts.

This increased efficiency is sorely needed. “In the government sector, resources keep getting cut, and you’re still being asked to do more and more, at a time when we are seeing a lot of high-profile, government-related attacks happening,” said Paul Miller, Security Strategist in Broadcom’s Enterprise Security Group.

By The Numbers

Cyber incidents on the rise:

2023 saw 32,211 incidents reported to US-CERT. This included incidents due to, among others:



12,261
improper usage



6,198
email/phishing



5,687
other/unknown
attack vectors



3,569
web-based attacks

2024 data is not available yet, but agencies are operating under “high risk” conditions.



Tool sprawl within agencies:

Two-thirds of state and local agencies (and more than 1/3 of federal) report using **six or more tools** to manage IT risks, and only

- **43%** of federal respondents and
- **22%** of state respondents

feel strongly confident that they can identify the number and type of connected endpoints.

\$27.5 billion

the cybersecurity budget in FY2025 across all federal agencies, including:

\$3.7 billion + **\$22 billion**
for products (13%) for staff & contractors

┌────────── a 4:1 labor-to-tech ratio ─────────┐

1,083

the number of proposed cuts to CISA’s workforce during FY2026 — from 3,732 employees down to 2,649

“The threat landscape is rapidly evolving with the onset of AI-related innovation, regulatory disruption, and job loss radicalization. This, coupled with their own major organizational and funding changes, leaves agencies vulnerable. The mission and challenge to keep systems, data, employees, and citizens secure has not changed.”

Source: Forrester — [Government Leaders: Prioritize Cyber Efficiency Amid Federal Volatility](#)

Choosing the Right Approach to Endpoint Protection

The Challenge: High Threat Levels, Inefficient Security Strategies

Government is a high-profile cybersecurity target: The Government Accountability Office classifies agencies as operating under “high risk” conditions. But agencies have fewer resources to combat threats, and that presents challenges.

Endpoint security inefficiencies: Many organizations rely only on a negative security model, which blocks known bad software from running, but does nothing to prevent zero-day threats. A truly effective security posture also includes a positive security model, which allows only trusted software to run. Failure to include both approaches leads to security gaps that increase inefficiencies, attack surface and the need for skilled human intervention.

“Without automation and machine learning to classify those alerts into known entities that can be dismissed automatically, there’s no efficient way to reduce noise,” Miller said. Defenders are stretched thin chasing down alerts, and “bad actors gain elevated access to environments simply by attempting to overwhelm analysts with volume,” he said.

Product selection: Buying the wrong tools, or too many, adds inefficiencies and reduces security. “If you are in a government agency, chances are some of your assets are unsupported, and if you’re selecting an EDR or prevention solution that can’t cover your legacy operating system, you’re leaving attack surface available for threat actors,” Miller said.

The traditional approach to product selection compounds the problem. “It’s becoming harder for agencies to select endpoint solutions,” he explained. “Agencies should pivot toward vendors who have a more comprehensive suite of solutions.”

Balancing budget and compliance: Cybersecurity defense budgets are shrinking, with the latest budget legislation cutting spending across civilian agencies by \$1.23 billion ([CSO Online](#)), in addition to millions already cut from CISA’s budget.

At the same time, however, cybersecurity risks continue to rise, and agencies are expected to adhere to security and compliance mandates, such as the Office

of Management and Budget (OMB) requirement for endpoint detection and response (EDR) solutions or the security controls outlined by NIST.

The Solution: Improved Endpoint Security, Application Control

Agencies must spend smarter to be more efficient and realize that prevention, detection and response capabilities can vary between vendors, that there may be differences in device and operating system support, configurability and control, and even detection fidelity.

Detection fidelity is a significant concern: Alerts must be accurate and reliable to support investigation and threat hunting, and response and remediation. “Fewer false positives reduces response teams’ cognitive load, helping ensure better outcomes,” said Miller.

Buyers should also consider the scalability needed for government use cases, criteria such as control over where and how data is stored, and an ability to integrate across the security stack.

When it comes to application control, a solution based on a **positive security model** can enhance agency protection. “A positive security model allows only known, trusted software to run in your environment,” Miller said. “If you have legacy systems, you can see into them, restrict what runs on them. That means you have greater compliance and visibility.”

Buyers should consider how an application control solution can help them meet specific security goals — and how quickly. Such solutions can be time consuming to adopt but using trust mechanisms can simplify policy creation and maintenance.

Some application control solutions encompass additional elements, such as device control, file integrity monitoring, and memory and registry protection. These capabilities in one solution provides an unprecedented ability to inventory software in the environment and simplifies purchasing.

When evaluating any solution, **vendor selection matters**. “Agencies must set out their goals: advanced endpoint protection, telemetry collection and correlation for detection. You need that same platform to have tooling that reduces the false-positive workload coming into your analysts’ queue,” Miller said.

Best Practices

To optimize endpoint security, several best practices can drive new levels of security efficiency.



Visibility into security environment.

The function of a platform, first and foremost, is to enable analysts. “It really is important to understand that the analysts and threat hunters making the decision at the end of this workflow are the ones who matter,” Miller said.

Visibility helps to both empower analysts and ease their workload. “Visibility gives you near real-time or in some cases predictive capabilities. That’s how you do threat detection and response and mitigate context switching for an analyst, reducing cognitive fatigue,” he explained.

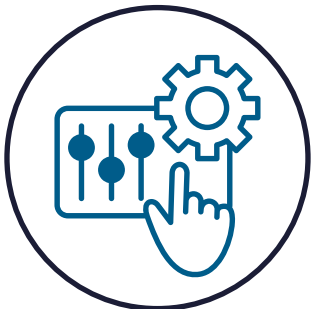


Use automation to speed up workflows.

Detection and response solutions often use automation to improve analyst efficiency — automating tasks that are traditionally labor intensive and time consuming. An example of this would be triaging alerts. Automating filtering through alerts can help responders focus on those that really matter.

Tools can and should be used for classification of threats in the background before they even become generated alerts. Automation and ML can look for anomalous patterns, flagging likely malicious intent and enabling analysts to mitigate threats.

Finally, some automated responses “will be able to stop attacks as they’re going on, and alert after the fact,” Miller said. By making full use of such capabilities, agencies can evolve their incident response while simultaneously making their thinly stretched human resources go further.



Implement a robust application control solution.

The right application control solution can help drive more efficient protection. When policies are enforced to ensure that only trusted applications can run, the solution can help block malware, tame shadow IT, and keep unauthorized software out of play.

“With application control, you’re preemptively reducing the risk of a threat actor executing code in your environment,” Miller said. “High compliance in application control puts you into a position where threat actors will not be able to run anything in your environment that you haven’t approved.”

With application control in high enforcement mode, “you’re reducing the response and recovery time because you don’t allow the incident to happen in the first place,” he said. “You are preventing attacks.”

Case Study

An attack on public-sector resources helps demonstrate the value of using the right tool for the job at hand.

The war in Ukraine had many public-sector organizations on high alert. “We were told to be on the lookout for attacks on bus companies and energy generation facilities,” Miller said. “That was interesting. It was like, ‘Energy generation, that’s always under attack. But bus companies? That’s a weird one.’”

Carbon Black, an endpoint security solution by Broadcom, helped prove out the warning. “One advantage to having a particularly large install base with tools like Carbon Black is that we have broad visibility,” Miller said. “Later that week, we could see multiple attacks firing off — using the same tactics, within seconds of each other, in multiple customer environments.”

Sure enough, the bad actors were going after the transportation sector, as well as energy resources. “We saw them trying to drop modified firmware to potentially allow backdoors to very sensitive environments,” he explained, “and we stopped that attack.”

For government agencies, the incident elevates a number of key learnings. First, the threat is very real. Agencies have valuable holdings, from personal data to nuclear control systems. “All those things are very tempting targets,” Miller said.

The incident also shows the value in “having a partner that has a wide field of vision, that is able to see new and emergent threats happening across the globe in real time,” he said. In the present era of heightened geopolitical conflict, “threat actors are not going to be backing down. So choosing a vendor that has experience dealing with cybercriminals as well as Nation State threat actors is a wise move.”

HOW BROADCOM HELPS

As a well-established leader in the government space, Broadcom offers an unmatched security portfolio that includes two brands with long, rich legacies in endpoint security — Symantec and Carbon Black. Between these brands, government agencies can leverage industry-leading endpoint protection, detection and response.

Broadcom’s mission is to redefine the level of security available to organizations by delivering full-stack, enterprise-grade protection at an unprecedented cost-value ratio, and in a form factor that makes it accessible to all.

“We’re one of the few organizations in this space that can provide the full spectrum of protection,” Miller said. “Our experience, along with the breadth of our product offerings, allows us to be holistically aware of threats, from email to networks to endpoints to Threat Intel. All these domains are mission critical, and we can cover them all.”

Learn more: <https://www.carahsoft.com/broadcom>



ABOUT BROADCOM

The most targeted organizations in the world secure their environments with Symantec and Carbon Black, which now form the Broadcom Enterprise Security Group. Fueled by Broadcom's commitment to R&D, the company aims to always innovate its solutions to keep you ahead of the next novel assault or sophisticated attack.

<https://www.carahsoft.com/broadcom>

[@symantec](#)
[@carbonblack](#)
[@broadcom](#)
[@carahsoft](#)

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.



1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop

