carahsoft

Symantec by Broadcom

Carbon Black. by Broadcom

Building Efficient Endpoint Protection

Infographic

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider®** supporting a broad portfolio of industry-leading technologies through GSA, NASPO ValuePoint, The Quilt and a wide range of other contract vehicles.

As the **Master Government Aggregator®**, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Symantec and Carbon Black by Broadcom, we provide technology solutions that drive modernization, strengthen operations and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/SymantecResources
carah.io/CarbonBlackResources

Join Events & Webinars:
carah.io/SymantecEvents
carah.io/CarbonBlackEvents

Discover Technology Solutions:
carah.io/SymantecSolutions
carah.io/CarbonBlackSolutions

Learn About Procurement:
carah.io/SymantecContracts
carah.io/CarbonBlackContracts

Connect With Our Team:
Broadcom@carahsoft.com
571-662-3260

Building Efficient Endpoint Protection

Faced with growing pressure to reduce costs despite a more complex threat landscape, agencies must evaluate their existing approach to preventing, detecting and responding to endpoint breaches, finding ways to reduce costs and leverage the right technology for more efficient security.

Agencies Face High Threat Levels and Inefficient Security

CYBER INCIDENTS ON THE RISE

In fiscal 2023 agencies reported 32,211 incidents to the Cybersecurity and Infrastructure Security Agency (CISA) Computer Emergency Readiness Team.

TOOL SPRAWL

Two-thirds of state and local agencies — and more than one-third of federal agencies — use **six or more tools** to manage IT risks.

PROLIFERATION OF ENDPOINTS

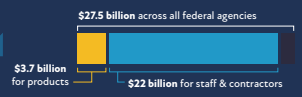
Only 43% of federal respondents and 22% of state respondents feel strongly confident that they can identify the number and type of connected endpoints.

FEWER HANDS TO HELP

1,083: the number of proposed cuts to CISA's workforce during FY 2026, from 3,732 employees down to 2,649.

TOO LITTLE AUTOMATION

The federal cybersecurity budget in FY 2025 reflects a 4:1 labor-to-tech ratio:



Fight Back With Efficient Endpoint Security

Endpoint security requires several essential elements, including:

DETECTION FIDELITY

Alerts must be accurate and reliable to support detection, response and remediation. Reducing false positives diminishes cognitive load for analysts and provides better outcomes.

A POSITIVE SECURITY MODEL

Allowing only known, trusted software to run in your environment protects systems from malware, shadow IT and unauthorized software. If you have legacy systems, you can see into them and restrict what runs on them, giving you greater compliance and visibility.

THOUGHTFUL VENDOR SELECTION

Choose a platform that offers advanced endpoint protection, telemetry collection, correlation for detection, and tooling to reduce false positives.

Best Practices

Drive new levels of security efficiency by following these best practices:

Gain visibility into your security environment.
Analysts and threat hunters need real-time or even predictive capabilities to detect and respond to attacks. Visibility empowers analysts and reduces their workload.

Use automation and machine learning.
Automated alert filters that assess anomalies in the background help responders focus on threats that really matter and can stop some attacks automatically.

Implement a robust application-control solution.
The right application control solution can help drive more efficient protection by keeping unauthorized software out of play. Preventing incidents means organizations can spend less time — and fewer taxpayer dollars — on response and recovery.

Case Study: Ukraine



As the war in Ukraine heated up, an alert went out: Watch for cyberattacks aimed at an unusual target — transportation — in addition to more typical threats to energy facilities. Broadcom's Carbon Black endpoint security solution spotted bad actors going after energy resources, attempting to install modified firmware and insert backdoors to sensitive environments. And they saw hackers hitting an RV rental company that the Ukrainian government was using to move civilians to safety. Broadcom stopped the attacks. That's the value of a vendor with a wide field of vision that can identify new and emerging threats in real time.

Broadcom Meets the Need for Efficient Endpoint Protection

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. That includes:

- An unmatched security portfolio — Symantec and Carbon Black
- A rich legacy in endpoint security
- Industry-leading endpoint protection, detection and response

Learn more: www.carahsoft.com/broadcom

govloop · Symantec by Broadcom · Carbon Black. by Broadcom · carahsoft