carahsoft

Symantec

Symantec Endpoint Protection Capabilities for U.S. Federal and DoW

Case Study

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 Broadcom (Symantec), 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

Join Events & Webinars:
carah.io/SymantecEvents

Discover Technology Solutions:
carah.io/SymantecSolutions

Learn About Procurement:
carah.io/SymantecContracts

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

Symantec Endpoint Protection Capabilities for U.S. Federal and DoW

CASE STUDY

CHALLENGES

- Security coverage gaps
- Vendor fragmentation created management complexity and inconsistent coverage
- Complex environment requirements across cloud and on-premises
- Strict compliance demands to RMF, CMMC and CORA 3.0 requirements

BROADCOM SOLUTIONS

- Symantec Endpoint Protection
- Symantec Protection Engine
- Symantec Message Gateway
- Symantec Secure Web Gateway

BENEFITS

- Millions in cost savings and rapid return on investment
- High efficiency with streamlined IT security operations, low false positives and simplified compliance reporting
- Strengthened information advantage with Symantec's Global Intelligence Network

Executive Summary

In today's cyber threat environment, basic endpoint malware products are no longer enough to stop attacks. Consider this: most of the successful headline-generating ransomware attacks that wreaked havoc on companies and federal agencies were successful against systems protected by market-leading endpoint protection products. Yet attackers were successful at disruption, damage, and theft. It would be smart to ask ourselves why.

Advantages of Symantec over Trellix ESS

The simple fact is that adversary tradecraft has evolved to circumvent prevention-centric endpoint protection technologies. While modern EPP solutions are effective at stopping commodity malware, determined human-operated attacks rely on techniques that blend in with legitimate network activity and take advantage ofbelow-the-radar techniques. Their success hinges on exploiting the inherent visibility gaps in a prevention-only security model.

- **Unified, Lightweight Agent.** Symantec employs a single, lightweight agent that provides comprehensive endpoint protection across Windows, macOS, and Linux operating systems. This design minimizes system overhead and simplifies deployment and maintenance activities.
- **Centralized Management Console.** A single management console provides unified visibility and control across cloud, hybrid, on-premises and DDIL (Disrupted, Degraded, Intermittent, and Limited) air-gapped environments. Unlike Trellix, Symantec's console can be virtualized and does not rely on ePO, enabling seamless interoperability across diverse infrastructures.
- **Operational Efficiency and Cost Reduction.** By consolidating endpoint management and security functions, Symantec significantly improves operational efficiency while reducing administrative complexity and total cost of ownership (TCO).
- **Enhanced Security Capabilities.** Symantec incorporates advanced features such as location awareness, host integrity monitoring, tamper protection, proactive and adaptive security, and endpoint deception technologies. These capabilities strengthen an organization's security posture against sophisticated and evolving threats.

Better Together with Microsoft

Symantec's endpoint security solutions are designed to complement and enhance Microsoft Defender capabilities, particularly in complex or constrained operational environments.

- **Proactive Protection Against Zero-Day Threats.** Symantec's Intrution Prevention System (IPS) delivers real time protection against operating system and application zero-day vulnerabilities. In contrast, Microsoft Defender for Endpoint (MDE) requires a full Windows update to leverage the latest Microsoft security technologies, a process that may be impractical or impossible when systems are compromised.
- **Support for Isolated and Air-Gapped Environments.** Symantec provides full functionality in isolated, air-gapped, or restricted networks, where many Microsoft Defender core capabilities are limited or non-functional. Using the on-premises Symantec Endpoint Protection Manager (SEPM), organizations can manage all environments seamlessly. MDE, by contrast, must revert to Group Policy Object (GPO)-based management, increasing administrative effort and cost.
- **Modular Deployment for Flexible Integration.** Symantec Endpoint Protection is modular, allowing organizations such as the Department of War (DoW) to selectively deploy components that best complement or extend Microsoft Defender capabilities.
- **Transparent Licensing Model.** Symant Symantec maintains a straightforward, all-inclusive licensing structure with no hidden costs or tiered pricing. All features, including EDR, server protection, vulnerability management, and cross-platform support, are included without additional fees.

Ready to strengthen your agency's cybersecurity posture? Contact us at Broadcom@carahsoft.com to explore how your agency can leverage Carahsoft's unique licensing model with Government and education-specific pricing and discounts.

For more information, visit our website at: www.carahsoft.com/broadcom

Symantec SEP for DoW Reseller One-Pager December 8, 2025