Closing the Gap: How a Major Defense Organization Standardized Enterprise Cybersecurity with Symantec

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

A major defense organization successfully transitioned from fragmented security solutions to a comprehensive, enterprise-wide Symantec deployment, achieving significant cost savings while strengthening cybersecurity posture across complex, air-gapped environments. This transformation addressed critical security gaps left by the transition from Host-Based Security System (HBSS) to Microsoft Defender for Endpoint. Through Symantec's implementation, the organization achieved centralized management and enhanced protection capabilities across their entire enterprise.

The Challenge

The organization faced multiple cybersecurity challenges that hindered its ability to achieve information superiority:Advanced web filtering, content analysis, and deep file inspection capabilities

- **Security Coverage Gaps:** The transition from HBSS to Microsoft Defender for Endpoint created vulnerabilities in their defense posture
- **Vendor Fragmentation:** Multiple security vendors across different IT security domains created management complexity and inconsistent coverageTrade Agreements Act (TAA)-compliant solutions to meet Federal procurement requirements
- **Complex Environment Requirements:** Need for unified security across on-premises, cloud and disconnected/disadvantaged networks
- **Compliance Demands:** Strict adherence to Risk Management Framework (RMF), Cybersecurity Maturity Model Certification (CMMC) and CORA 3.0 requirements

The Solution

The organization chose Symantec as its standardized enterprise security platform, leveraging Broadcom's comprehensive cybersecurity suite to address its complex requirements through a unified approach that eliminated the fragmentation of its previous multi-vendor environment.

Unified Security Architecture

Symantec delivered a centralized security framework built around a single agent deployment that operates seamlessly across Windows, Mac and Linux environments. This unified architecture provides enterprise-wide visibility and control through a centralized management console, ensuring feature parity across on-premises, cloud and air-gapped networks. The single-platform approach eliminated the complexity of managing disparate security tools while maintaining consistent protection standards across all network segments.

Comprehensive Protection Layers

The solution incorporates multiple layers of advanced security capabilities, including artificial intelligence (AI) and machine learning-driven behavioral analysis for threat detection and prevention. Integrated components such as firewall protection, intrusion prevention systems and application control work in concert with memory protection, browser security and exploit prevention technologies. Built-in deception technology and endpoint detection and response capabilities provide additional layers of defense, creating a comprehensive security posture that addresses both known and emerging threats.

Modular Deployment Flexibility

Recognizing the organization's existing technology investments, Symantec's modular architecture allows for complementary integration with its current Microsoft Defender for Endpoint deployment. This flexibility enables the organization to select specific Symantec components based on their unique security requirements while leveraging out-of-the-box intrusion prevention capabilities for operating systems and applications. The modular approach ensures optimal resource utilization while maximizing security effectiveness across the enterprise.

Key Results and Benefits

Financial Impact:

- Millions in cost savings through strategic procurement agreements
- Reduced network complexity and vendor consolidation
- Predictable spending with guaranteed protection levels
- Rapid return on investment with the lowest cost of endpoint administration

Operational Excellence:

- Streamlined IT security operations across worldwide network infrastructure
- High efficiency with low false positive rates
- Enhanced incident response capabilities through centralized intelligence
- Simplified compliance reporting and audit readiness

Security Enhancement:

- Strengthened information advantage aligned with Department of War (DoW) objectives
- Comprehensive endpoint security for traditional and mobile devices

- Global threat intelligence network integration
- Regulatory compliance support for federal requirements

Partnership Value

The organization's 20+ year relationship with Symantec, supported by Carahsoft's Public Sector expertise, has enabled:

- Strategic procurement through Blanket Purchase Agreements (BPAs) and Enterprise License Agreements (ELAs)
- Streamlined technology acquisition and deployment processes
- Interactive product demonstrations and feature exploration
- Ongoing support for enterprise-wide adoption initiatives

Looking Forward

The organization continues expanding its Symantec deployment to achieve complete enterprise-wide standardization across all agency operations. Their strategic roadmap focuses on completing the agency-wide migration to Symantec products, building upon the successful implementation to ensure comprehensive security coverage throughout their global network infrastructure.

Moving forward, the organization plans to further consolidate its vendor relationships to reduce operational complexity while enhancing its overall security posture through deeper integration of Symantec's cybersecurity technologies. This continued partnership approach ensures ongoing alignment with evolving compliance requirements and positions the organization to maintain its information superiority objectives as threat landscapes and regulatory frameworks continue to evolve.

Ready to strengthen your agency's cybersecurity posture? Contact us at info@scoppcyber.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 DoW Air-Gaps Case Study v2 February 18, 2026