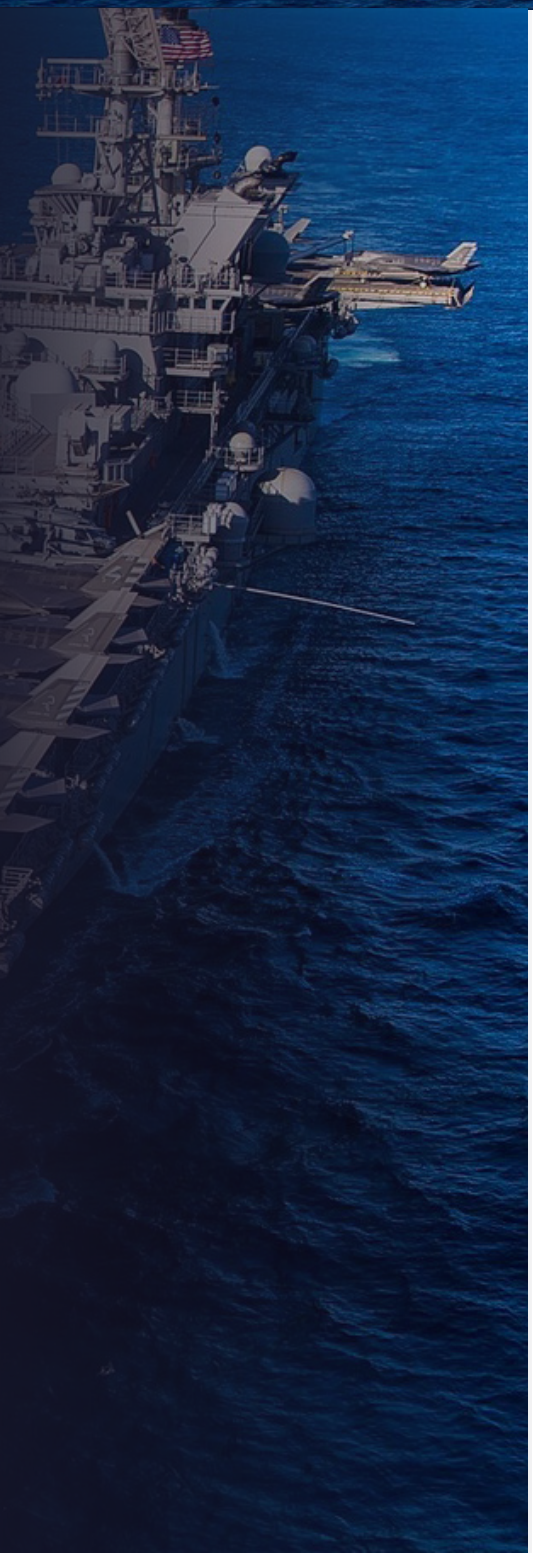
Symantec by Broadcom | Carbon Black. by Broadcom | carahsoft

Transforming Endpoint Security Across U.S. Navy Networks

A CASE STUDY IN EFFICIENCY AND COST AVOIDANCE



Executive Summary

In recent years, the U.S. Navy has made significant strides in modernizing its cybersecurity infrastructure, particularly around endpoint protection. A key development in the Navy's cybersecurity evolution has been the move away from legacy Host-Based Security Systems, such as Trellix ENS, toward Microsoft Defender for Endpoint. While this shift brings certain advantages in connected and cloud environments, it also introduces challenges, particularly in isolated air-gapped environments where many core Microsoft Defender capabilities are limited or non-functional.

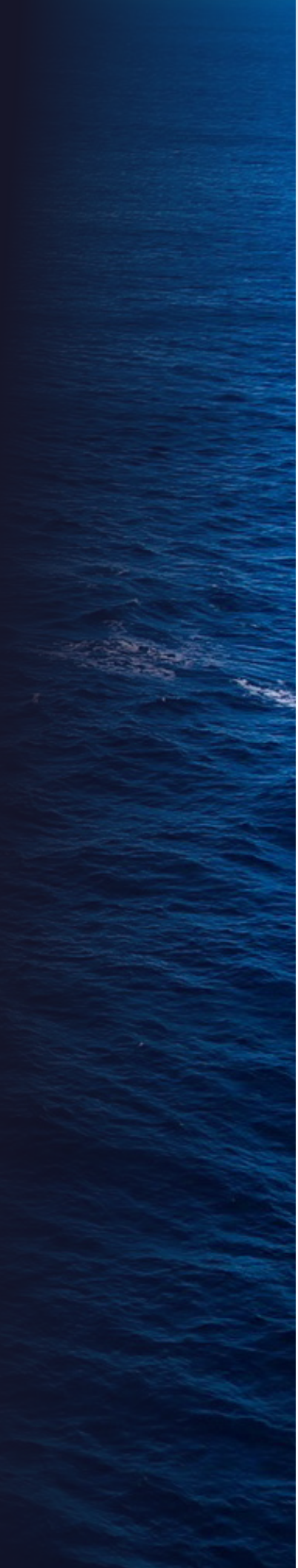
At the same time, the rise of artificial intelligence (AI) has prompted the Department of War (DoW) to re-evaluate the cost implications of on-premises versus cloud-based deployments. AI workloads often require significant and unpredictable CPU resources, which can lead to sudden spikes in usage. In pure cloud environments, even a single unintentional AI simulation or query can result in substantial, unexpected costs. In such cases, on-premises and air-gapped deployments remain the preferred approach for both cost control and operational security.

To address these gaps and maintain consistent security across all operational domains, the Navy (NETWARCOM and PEO-Digital) collaborated with Carahsoft, Leidos and Broadcom, selecting the Symantec platform as a unified endpoint protection solution across the broader naval enterprise. This strategic change has resulted in substantial improvements in security posture, system performance and long-term cost efficiency across a wide range of naval networks.

Modernizing the SMIT Network

One of the most significant transitions within the Navy occurred in the Service Management, Integration, and Transport (SMIT) environment, which supports approximately 650,000 users. In this initiative, the Navy undertook a full replacement of the Trellix endpoint agents, implementing a streamlined deployment of Symantec Endpoint Protection (SEP).

The implementation of a single SEP agent across Windows, macOS and Linux systems consolidated multiple agents previously required by Trellix. Additionally, the shift eliminated the need for the ePolicy Orchestrator (ePO), simplifying endpoint management significantly. With the introduction of a lightweight management console, the Navy virtualized its endpoint infrastructure, enabling faster provisioning, easier updates and reduced cost of administration. This transformation improved the operational efficiency of the cybersecurity team and delivered measurable performance benefits to end users.



Endpoints experienced reduced CPU and memory consumption. Symantec's lightweight solution addressed the performance impact on endpoints, particularly during concurrent high-demand situations, including the operating systems transition, Patch Tuesdays, and DoW-wide broadcast events. Additionally, Symantec's features such as location awareness, host integrity monitoring, tamper protection, adaptive & predictive protection, and endpoint deception technologies represented an upgrade from the previous solution, aligning with the Navy's evolving security requirements.

Extending Protection Across Legacy, Excepted and Specialized Naval Networks

Beyond SMIT, the Carahsoft, Leidos and Broadcom teams are working with the Navy to extend the adoption of Symantec's endpoint suite to several other critical Navy infrastructures, including the Naval Air Systems Command (NAVAIR), Navy Shipyards and both the Surface and Undersea Warfare Centers under NAVSEA. These environments, which handle sensitive or mission-critical data, benefit from consistent and centralized endpoint protection measures.

The transition was facilitated through the Navy's Portfolio Licensing Agreement (PLA), which ensures that Symantec's full suite of endpoint and networking tools are available to all Navy and Marine Corps without incurring additional software licensing costs. This contractual framework enhances the Navy's ability to scale its cybersecurity infrastructure while maintaining fiscal responsibility. By leveraging the PLA, the Navy avoided substantial expenses that would otherwise stem from other cybersecurity vendors. For example, as Microsoft phases out support for older operating systems, associated End-of-Life (EOL) operating systems charges can become exponentially costly for the Navy. Similarly, recent price increases from several cybersecurity vendors—reportedly as high as 300% over previous years for the same solution—posed a potential budgetary constraint on Navy's technical debt. The shift to Symantec under the multi-year PLA contract mitigates both financial risks, enabling a proactive and cost-effective security strategy.

Modern Tools for Modern Threats

This multi-phase implementation represents more than a software migration; it reflects a shift in how the Navy approaches cybersecurity across its digital landscape. By prioritizing lightweight centralized management, scalable architecture and efficient resource use, the Navy has positioned itself to respond more effectively to emerging threats, reduce system vulnerabilities and operate within a more predictable budget. This was made possible by the power of Leidos, whose expertise was instrumental in delivering a seamless, secure and fast deployment in a demanding industry such as the Navy.

This deployment may set a precedent for other government entities facing similar modernization challenges. The value of portfolio licensing agreements for broad deployments and the importance of selecting holistic platform vendors with integrated cybersecurity solutions that offer comprehensive, forward-compatible capabilities at reduced cost are demonstrated in this implementation.

The content of this white paper has been reviewed, verified, and approved by Leidos and the Navy PAO for public dissemination.

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

Broadcom Navy Case Study January 13, 2026