CASE STUDY

United States Department of Defense Combat Support Agency

> *"DISA's security and compliance requirements are ahead of the curve and should be applied across both commercial and government organization responsible for delivering critical infrastructure."*

AMIT YORAN
CEO, Tenable

DISA

The Defense Information Systems Agency (DISA), is a United States Department of Defense (DoD) combat support agency composed of military, federal civilians, and contractors. With a vision to provide "information superiority in defense of our Nation," the Defense Information Systems Agency, a U.S. Department of Defense combat support agency, provides IT and communications support to national leaders, joint warfighters and other key mission and coalition partners who contribute to the defense of our country.

Recognizing its limited capability to quickly and accurately assess the security of enterprise networks, DISA established the Assured Compliance Assessment Solution (ACAS) to replace the Secure Configuration Compliance Validation Initiative (SCCVI) software suite previously acquired by DoD. ACAS fulfills a combination of operational and strategic objectives, including:

- Providing an innovative technical solution with a flexible cost structure
- Employing a commercial solution that can be easily ordered and quickly deployed across the DoD infrastructure
- Supporting enterprise-wide deployment, with the ability to tier system evaluation and management throughout the organization

CHALLENGES

DISA sought a flexible, accurate and scalable vulnerability management solution that was easy to deploy at all levels. It had to deliver real-time visibility and risk assessment across all DoD networks, enabling decisive, risk-based management decisions consistent with federal guidelines, to address a broad combination of operational and strategic objectives, including:

- Fast and accurate enterprise-wide network security assessment
- Increased accuracy of risk assessment and standards compliance verification
- High scalability and ease of deployment at all levels, from the Geographic Commandant Commander to the warfighter on the front lines
- Real-time risk assessment across DoD networks to provide essential situational awareness and enable true, risk-based management decisions consistent with existing and emerging federal guidelines

Because of its extensive DoD experience and the wide-ranging corporate reachback Perspecta (formerly HPES) provided as the industry's largest technology company, Tenable found a viable partner to satisfy the DISA ACAS need. Historically, Perspecta had one of the broadest portfolios of products, services, end-to-end solutions, and research and testing in the technology industry. It also had a long history in supporting Information Assurance (IA) / Computer Network Defense (CND) programs, and was able to draw upon the IA experience of nearly 2,000 certified professionals.

Perspecta assessed several technical approaches and vulnerability tools in order to find the right solution/partner. This comprehensive assessment was driven by several key criteria, including knowledge and understanding of DoD enterprise networks, ability to meet Security Content Automation Protocol (SCAP) compliance and Common Criteria standards, implementation speed and flexibility, ability to meet ACAS requirements, operator ease of use and ability to meet long-term DoD enterprise needs.

Unlike many security software solutions, Tenable built its licensing and deployment architecture with one goal in mind: to allow customers' security monitoring strategies to be defined by their needs, not by license and cost restrictions. For DISA, that approach facilitates flexible scanner usage across the DoD infrastructure, enables an improved security posture, and enhances satisfaction of organizational requirements such as fault tolerance, the ability to target operational scanning windows and managerial reporting.

A TRULY DISTRIBUTED ENTERPRISE

ACAS is the DoD's enterprise-wide solution for vulnerability management and configuration compliance. The enterprise it spans includes:

- DoD Combatant Commands
- Four Military Services
- DoD Support Agencies
- Defense Intelligence Agency
- National Geospatial-Intelligence Agency
- National Reconnaisance Office
- National Media Exploitation Center
- National Security Agency
- The U.S. Coast Guard, National Guard and Reserves

The distributed nature of such an extensive enterprise demands a solution that is extremely flexible and easy to use, but also highly scalable. Tenable.sc™ (formerly SecurityCenter®) addresses these requirements by uniquely supporting multi-tier management, including both local and centralized control, analysis and reporting.

SOLUTION

Tenable and Perspecta, established an exclusive partnership to offer DISA an integrated software solution that is accurate, thorough, scalable, reliable, intuitive and easy to use. It can be easily deployed via download to all DoD components – without the need to procure and install appliance devices. No other tool can match the unique tiering ability Tenable offers, which allows DISA to aggregate security data in one central location to support its mission. This team united two key market leaders, which combined complementary skills and experience to offer a superior ACAS solution to DISA and the restof DoD.

Tenable.sc™ (formerly SecurityCenter®), integrated with Nessus® Network Monitor and Nessus®, combined active and passive scanning technology and a flexible, fluid architecture. This proactive, automated solution provided DISA with essential situational awareness and context, enabling true, risk-based management decisions that comply with both current and emerging federal guidelines.

The Tenable Solution: Comprehensive, Enterprise-Class Vulnerability Management:

DISA's selection of Tenable followed an extensive evaluation process culminating with a six-month, multi-site pilot implementation. During this period, Tenable successfully demonstrated its ability to meet and exceed all DISA requirements for a modern, Enterprise-class vulnerability management and configuration compliance solution. Tenable provided an integrated approach to proactive network defense for the DoD, designed to scale easily while maintaining cost effectiveness. It leverages several Tenable components, including:

tenable.sc™

Tenable.sc provides continuous asset-based security and compliance monitoring, unifying the processes of asset discovery, vulnerability detection and configuration auditing. It delivers a central point for discovering assets, detecting vulnerabilities and data leaks, managing events and conducting configuration and compliance audits.

Tenable.sc is the first agent-less scanning solution to be certified by FDCC and SCAP. The Tenable.sc console works with Nessus scanners to look for policy changes every time a scan is requested. This provides the ability to assess an organization's vulnerability and compliance posture, as well as delivering analysis and workflow tools that allow the user to easily perform reporting, auditing and remediation tasks.

Tenable.sc ties directly to DISA's Information Assurance Vulnerability Management (IAVM) system. Upon receipt of a new or updated information Assurance Vulnerability Alert (IAVA), Tenable.sc immediately deploys a new policy to Nessus scanners. That capability eliminates often time-consuming waits for new policies to be manually written, improving security. Tenable.sc also has a built-in reporting engine which already produces the common reports DISA needs – without advanced scripting. ACAS users quickly gain access to relevant data to efficiently create meaningful reports.

nessus® Professional

A high-quality, full-function scanner covers a breadth of vulnerability and configuration checks across a broad range of different workstation, server and network devices. The Tenable Nessus scanner supports more than 87,428 plug-ins and covers more than 38,439 unique Common Vulnerabilities and Exposures (CVEs). The scanner is fast and accurate, giving clients the greatest possible visibility into the status of connected devices and systems. The popular Nessus scanner has been downloaded more than ten million times.

nessus® Network Monitor

Traditional active scanning systems miss transient devices – like smartphones – as well as many cloud-based services, resulting in dangerous gaps in coverage and visibility. So sophisticated security professionals complement active scanning with passive scanning. Nessus Network Monitor (formerly Passive Vulnerability Scanner or PVS) uniquely overcomes these limitations, effectively extending scanning visibility to resources that would otherwise be missed in assessments. It introduces real-time monitoring, identifying devices and systems, applications and services, and network connections, as well as eliminating the restrictions and limitations of traditional, schedule-based scanning. The inclusion of passive vulnerability scanning provides a comprehensive solution for DISA.

BENEFITS

For DISA and its constituents, ACAS provides the evolution necessary to properly support today's cyber warfighter. The Tenable solution delivers a holistic, highly automated and accurate approach to real-time continuous monitoring. Combining active and passive scanning technologies within a fluid, flexible architecture, the Tenable solution provides the sophistication and flexibility needed to satisfy the wide variety of security needs the Department of Defense must support.

By meeting and exceeding the vulnerability, configuration and real-time risk management needs of one of the largest and most demanding government organizations in the world. The selection of Tenable as the foundation of the Assured Compliance Assessment Solution (ACAS) helps cement Tenable as the undisputed leader in vulnerability management in the U.S. federal government

Solution benefits include:

Flexibility
The option to deploy unlimited consoles and scanners enables DISA to build the optimal scanning strategy, reflecting environmental, architectural and organization requirements.

Scalability
With the ability of individual Tenable.sc consoles to scan hundreds of thousands of IPs, scanning architectures are based on mission requirements, not technology constraints.

Accuracy
The comprehensive Nessus library of more than 87,428 individual plug-ins helps eliminate missed events (i.e., false negatives), while the popularity of Nessus provides an immediate feedback loop and extra layer of quality assurance.

Easy to deploy, use and maintain
The broad platform support Tenable provides for scanners has no relational database to maintain and no agents to manage

Continuous Monitoring
Passive scanning capabilities, unique to Tenable, help DISA move beyond static, point in time assessments.

Experience
The combination of one of the world's largest technology companies with one of the most widely-used vulnerability scanners gives DISA a partner it can trust.

The Tenable software-only approach means components are easily procured and deployed on industry-standard architecture hardware, not proprietary appliances. This means DoD can expand and adapt its scanning architecture as required by operational demands, without the delays and costs associated with buying, shipping and maintaining appliance inventory. Additionally, our solution can run on the government's existing platform, minimizing disruptions during transition.

For DISA and its constituents, ACAS provides the evolution necessary to properly support today's cyber warfighter. The Tenable solution delivers a holistic, highly automated and accurate approach to real-time continuous monitoring. Combining active and passive scanning technologies within a fluid, flexible architecture, the Tenable solution provides the sophistication and flexibility needed to satisfy the wide variety of security needs the Department of Defense must support.

By meeting and exceeding the vulnerability, configuration and real-time risk management needs of one of the largest and most demanding government organizations in the world. The selection of Tenable as the foundation of the Assured Compliance Assessment Solution (ACAS) helps cement Tenable as the undisputed leader in vulnerability management in the U.S. federal government.

To learn more, visit: **tenable.com** and **https://www.disa.mil/Cybersecurity/Network-Defense/ACAS**
Contact Us: **marketing@tenable.com**