tenable network security

Tenable Delivers Best-of-Breed

Configuration Compliance and Vulnerability Management for U.S. Department of Defense

The Defense Information Systems Agency's (DISA) selection of Tenable Network Security as the foundation of its Assured Compliance Assessment Solution (ACAS) cements Tenable's standing as the undisputed leader in vulnerability management in the U.S. federal government.

The award followed a multiple-month trial of Tenable products, in conjunction with partner HP Enterprise Services, demonstrating the ability to exceed U.S. Department of Defense (DoD) requirements. Tenable's technology is meeting the vulnerability, configuration, and real-time risk management requirements of one of the largest, most demanding government organizations in the world.

In Pursuit of Comprehensive, Enterprise-Class Vulnerability Management

DISA, confronted with a limited capability to quickly and accurately assess the network security of Department of Defense (DoD) enterprise networks, established ACAS to replace the Secure Configuration Compliance Validation Initiative (SCCVI) suite of software previously acquired by DoD. ACAS will fulfill a combination of operational and strategic objectives, including:

- Provide an innovative technical solution with a flexible cost structure.
- Employ a commercial solution that can be easily ordered and quickly deployed across the DoD infrastructure.
- Support enterprise-wide deployment across the Department of Defense (DoD), with the ability to tier system evaluation and management throughout the organization.

Ultimately, DISA sought:

- Fast and accurate enterprise-wide network security assessment; satisfying the goal of increasing the accuracy of risk assessment and standards compliance verification.
- A highly scalable solution easy to deploy at all levels; from the Central Command 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 for Continuous Monitoring.

The Tenable Solution (Tenable – Hewlett Packard Enterprise Services (HPES) Partnership)

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

HPES 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.

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

Ron Gula

CEO, Tenable Network Security

Tenable chose HP Enterprise Services (HPES) because of their extensive DoD experience and the wide-ranging corporate reachback they provide as the industry's largest technology company. HPES has one of the broadest portfolios of products, services, end-to-end solutions, and research and testing in the technology industry. HPES also has a long history in supporting Information Assurance (IA) / Computer Network Defense (CND) programs, and is able to draw upon the IA experience of nearly 2,000 certified professionals.

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 and 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, ability to target operational scanning windows, and managerial reporting requirements.

The Solution

DISA's selection of Tenable followed an extensive evaluation process culminating with a 6-month, multi-site pilot implementation. During this period, Tenable successfully demonstrated the ability to meet and exceed all of DISA's requirements for a modern, enterprise-class configuration assessment and vulnerability management solution.

Tenable's integrated approach to proactive network defense for the DoD is designed to scale easily while maintaining cost effectiveness. It leverages several Tenable components, including:

SecurityCenter™

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

SecurityCenter is the first agent-less scanning solution to be certified by FDCC and SCAP. The SecurityCenter 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.

SecurityCenter ties directly to DISA's Information Assurance Vulnerability Management (IAVM) system. On receipt of a new or updated information Assurance Vulnerability Alert (IAVA), SecurityCenter immediately deploys a new policy to Nessus scanners. That capability eliminates sometimes time-consuming waits for new policies to be manually written, improving security. SecurityCenter 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 Vulnerability Scanner

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. Tenable's Nessus scanner supports more than 55,000 vulnerability checks, and covers more than 22,000 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.

Passive Vulnerability Scanner (PVS)

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. Tenable's Passive Vulnerability Scanner™ (PVS) uniquely overcomes these limitations, effectively extending scanning visibility to resources that would otherwise be missed in assessments. PVS introduces real-time monitoring, identifying devices and systems, applications and services, and network connections and eliminating the restrictions and limitations of traditional, schedule-based scanning. The inclusion of passive vulnerability scanning provides a comprehensive solution for DISA.

A Truly Distributed Enterprise

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

- DoD Combatant Commands
- The four Military Services
- DoD Agencies and Field Activities
- Combat Support Agencies
- Defense Intelligence Agency
- National Geospatial-Intelligence Agency
- National Reconnaissance Office
- National Media Exploitation Center
- National Security Agency
- The US Coast Guard, National Guard, and Reserves

The distributed nature of such an extensive enterprise demands a solution that is not only extremely flexible and easy to use but also highly scalable. Tenable's SecurityCenter addresses these requirements by uniquely supporting multi-tier management, including both local and centralized control, analysis, and reporting.

X-Tool
Converts DISA distributed eXtensible Checklist Configurations Description Format (XCCDF) files into Tenable's Extensible Markup Langauge (XML) format, allowing the files to be imported into SecurityCenter and customized. X-tool also imports and converts Open Vulnerability Assessment Language (OVAL) and DISA generated SCAP content vulnerability files for upload into SecurityCenter.

3D-Tool
Visualization and graphical analysis of network and protocol maps, communication paths, and vulnerability maps.

The Tenable Advantage:
Flexibility – the option to deploy unlimited consoles and scanners allows DISA to build the optimal scanning strategy, reflecting environmental, architectural, and organization requirements.

- **Scalability** – with the ability of individual SecurityCenter 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 55,000 individual plugins 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** – Broad platform support for scanners, no relational database to maintain, and no agents to manage.
- **Continuous Monitoring** – passive scanning capabilities, unique to Tenable, help DISA move from static, point in time assessments.
- **Experience** – the combination of the world's largest technology company with one of the most widely-used vulnerability scanners gives DISA a partner they can trust.

Tenable's 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 their 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.

Conclusion

For DISA and its constituents, ACAS provides the evolution necessary to properly support today's warfighter. Tenable's 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, Tenable's solution provides the sophistication and flexibility needed to satisfy the wide variety of security needs the Department of Defense must support.

Other government agencies and commercial organizations interested in taking advantage of the products and technologies used to deliver ACAS can do so by contacting Tenable at http://www.tenable.com/products/securitycenter or by calling +1.410.872.0555.

About Tenable Network Security

Tenable Network Security is the leader in Unified Security Monitoring. Tenable provides enterprise-class agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure FDCC, FISMA, SANS CAG and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk.

For more information, please visit www.tenable.com.

For More Information

Questions, purchasing, or evaluation:
sales@tenable.com or 410.872.0555, x500
Twitter: @TenableSecurity
YouTube: youtube.com/tenablesecurity
Tenable Blog: blog.tenable.com
Tenable Discussions: discussions.nessus.org
www.tenable.com

tenable™ network security