tenable

SOLUTION BRIEF

ASSURED COMPLIANCE ASSESSMENT SOLUTION (ACAS), POWERED BY TENABLE

ACHIEVE AND EXCEED DOD COMPLIANCE

The sophistication and frequency of cyberattacks continues to increase exponentially. In parallel, the evolution of the IT landscape has exploded to include much more than physical and virtual machines, and the landscape continues to transform. As more assets, systems, devices and users come online, more complexity, uncertainty and reactive security are sure to follow. Poor visibility into the IT environment, data overload and a lack of effective communications put your missions at risk.

To address these challenges, the Defense Information Systems Agency (DISA) selected Tenable's technology to power the Assured Compliance Assessment Solution (ACAS) program. The ACAS mission is simple: Assess DoD enterprise networks and connected IT systems against DoD standards, as well as identify any known system vulnerabilities.

With ACAS and Tenable, you can both meet and exceed DoD compliance while also participating the Cyber Exposure revolution. As the network and threats to it grow, Tenable solutions grow in parallel, enabling you to anticipate, prioritize and neutralize threats across any infrastructure, any device and at any time – helping you know and respond to your Cyber Exposure. It's that powerful.

THE TENABLE ACAS SOLUTION

ACAS provides complete visibility and prioritized, actionable data through customized reporting. Recently, new capabilities were added to the ACAS contract with the addition of Nessus® Agents, supporting even more compliance capabilities.

The solution today includes the following IT security platform necessities: Tenable.sc™ (formerly SecurityCenter®) for on-prem Vulnerability Management, Nessus® scanners controlled by Tenable.sc, Nessus Network Monitor® (formerly Passive Vulnerability Scanner® or PVS), Nessus® Agents, and LCE® (Log Correlation Engine). The Tenable solution is Security Content Automation Protocol (SCAP) 1.2 compliant and provides advanced capability to configuration compliance and auditing.

Information on additional solution components and enhancements can be found at https://www.ask-acas.info/.

Solution Component	ACAS Provided
Tenable.sc™ (formerly SecurityCenter)	Yes
Nessus® (scanners controlled by Tenable.sc)	Yes
Nessus Network Monitor® 1GB	Yes
Nessus Agents	Yes

Solution Component	ACAS Provided
Tenable.ot™	Recommended
Nessus Network Monitor 10GB	Recommended

KEY BENEFITS

With ACAS and Tenable.sc, you have the resources needed to harness the IT security transformation and meet and exceed DoD compliance.

- **Complete Vision**: The most comprehensive view of deployed assets and potential weaknesses in the IT environment
- **Situational Awareness**: Contextual insight and actionable intelligence so you can prioritize targets and destroy threats
- **Fast Communications**: Share customized reports, statuses, assessments and discoveries easily and quickly
- **Risk Measurement**: Measure risk against mission objectives with powerful reporting for total operational excellence
- **Continuous Compliance**: Know the network you'reresponsible for, achieve DoD compliance and then exceed it.

TENABLE.SC: ANTICIPATE, PRIORITIZE AND CLOSE THE CYBER EXPOSURE GAP

The Tenable.sc platform provides the most comprehensive and integrated view of security posture to reduce risk and exceed DoD compliance. This next generation vulnerability analytics component for ACAS includes: Assurance Report Cards, Advanced Analytics/Trending, Customizable Dashboards/Reports and Cumulative Scan Results.

ASSURANCE REPORT CARDS

Continuously measure effectiveness of security policies based on strategic objectives

ADVANCED ANALYTICS & TRENDING

Assess insights and actionable information to prioritize security issues associated with the security posture of all deployed assets

HIGHLY CUSTOMIZABLE DASHBOARDS/REPORTS

Satisfy the specific visibility needs of all roles in your security operations team

CUMULATIVE SCAN RESULTS

Consolidate data from multiple on-prem Nessus® scanners and provide remediation trending information

UNDERSTANDING CYBER EXPOSURE WITH TENABLE.SC

Cyber Exposure is an emerging discipline for managing and measuring cybersecurity risk in the digital era. Cyber Exposure transforms security from static and siloed visibility into cyber risk to dynamic and holistic visibility across the modern attack surface. Cyber Exposure translates raw vulnerability data into business insights to help security teams prioritize and focus remediation based on business risk. Cyber Exposure provide leadership and cybersecurity professionals with a way to objectively measure cyber risk to help guide strategic decision-making. Just as other functions have a system of record, including ITSM for IT and CRM for Sales, Cyber Exposure solutions will provide Security with a system of record to help them effectively manage and measure cyber risk.

Tenable.sc is the on-prem solution that brings together unique sensors for vulnerability management, all of which are now available to the DoD as part of ACAS. Starting with active scanning (Nessus), passive network monitoring (Nessus Network Monitor), Agent scanning and event data (LCE), unit commanders are able to visualize up-to-date vulnerability and threat intelligence information. With Tenable.sc, you have even more power to continuously discover all assets, identify all vulnerabilities, monitor all networks in real time for advanced threats, gather contextual insight to rapidly respond to security breaches and ensure compliance.

NESSUS AGENTS: CLOSE THE CYBER EXPOSURE GAPS

The ACAS solution now includes Nessus Agents which enables you to deploy clients across the enterprise, extending the coverage for the DoD mandated vulnerability scanning, assessment and management capabilities. Nessus Agents close the gap in reporting for assets on the move or removes the requirements for credential management. Nessus Manager collects the Agent vulnerability data and reports back to Tenable.sc's advanced vulnerability analytics engine. Tenable.sc retrieves agent results, and correlates the data so you can accurately assess risk and prioritize remediation workflows.

Nessus Agents used via Tenable.sc enable you and your teams to achieve:

- **Effective resource allocation to improve efficiency**
- **Expanded scan coverage across the entire IT environment**
- **Improved risk analysis by integrating context from existinginfrastructures and partner framework**

NESSUS NETWORK MONITOR: MODERN VIEW FOR THE MODERN CYBER SECURITY PROFESSIONAL

Periodic scanning is no longer an acceptable IT security defense tactic given the nature and proliferation of threats. Point in time scanning leads to uncertainty and gaps in coverage, which is the Cyber Exposure Gap. Tenable Nessus Network Monitor (NNM) exposes these problems by delivering real-time asset discovery and network monitoring for continuous scanning and assessment of DoD enterprise-level networks. NNM is a critical element to effectively creating and managing a more modern view of the IT infrastructure you're tasked with defending. Information on additional solution components and enhancements can be found at https://www.ask-acas.info/

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies.