Government

ForeScout CounterACT®: The smart approach to Command Cyber Readiness Inspections (CCRI)

Every day, government agencies process vast amounts of sensitive information vital to U.S. national security. Loss of this sensitive data or unauthorized access to the systems and networks it resides on can have serious national security consequences, ranging from privacy issues and public embarrassment to global economic and political turmoil. It is essential that civilian and defense IT organizations safeguard this information and the networks that house it, while making it readily available when and where appropriate.

To ensure an apt and consistent level of security, government IT organizations must demonstrate and maintain compliance with a large and growing number of regulations, directives and standards. The main objective is to eliminate intrusions, protect sensitive information and mitigate exposure to cyberattacks. To achieve these goals, the Defense Information Security Agency (DISA), under the direction of U.S. Cyber Command, has begun conducting Command Cyber Readiness Inspections (CCRI) of key Department of Defense (DoD) agencies and sites, including those that support the Net-Centric Environment (NCE) and Global Information Grid (GIG).

CCRI is a comprehensive review of a DoD entity's cyber posture that includes a detailed assessment of its Information Assurance programs, the non-classified and classified IP networks, and the critical cyber and physical assets that support these networks. CCRI criteria are based on several key standards and directives including the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) directives 6211.02D and 6510.01F. DoD entities are given short notice (typically 30 to 60 days) prior to a CCRI audit to ensure their assets will pass the inspection.

CCRI Adherence Challenges

The DISA STIGs provide an extensive set of recommendations and checklists to ensure that all DoD cyber assets meet a minimum acceptable level of security. However, implementation of the STIG checklists presents significant challenges for DoD IT organizations because the process is time-consuming, resource-intensive and error-prone. Compliance policies for all cyber assets need to be defined, audited, reviewed, fixed and reported on a regular basis. Failure to adhere to the STIG standards can have serious repercussions, including possible disconnection from the GIG.

Without the help of compliance automation solutions, the process to prepare for a CCRI audit involves a series of tedious manual tasks that require IT administrators to write and run scripts, verify their results and then ensure non-compliant assets are remediated by running additional scripts. Furthermore, attempting to aggregate and analyze results from separate security systems is cumbersome, costly and less than foolproof. As a result, attaining reliable and continuous compliance to the CCRI criteria across an entire DoD IT organization can be ineffective and inefficient insofar as it can affect IT administrators' operational activities in order to satisfy a CCRI audit.

CounterACT Security Platform

The ForeScout CounterACT security platform provides real-time monitoring, control and policy-based remediation of managed, unmanaged and non-traditional devices to serve as a cornerstone for CCRI. Here's how:

See

- Discover devices the instant they connect to your network without requiring agents
- Profile and classify devices, users, applications and operating systems
- Continuously monitor managed devices, BYOD* and IoT* endpoints

Control

- Allow, deny or limit network access based on device posture and security policies
- Assess and remediate malicious or high-risk endpoints
- Improve compliance with industry mandates and regulations

Orchestrate

- Share contextual insight with IT security and management systems
- Automate common workflows, IT tasks and security processes across systems
- Accelerate system-wide response to quickly mitigate risks and data breaches

Attaining reliable and continuous compliance to the CCRI criteria across an entire DoD IT organization can be ineffective and inefficient insofar as it can affect IT administrators' operational activities in order to satisfy a CCRI audit.

To address these challenges, DoD IT organizations require policy-based compliance automation solutions that provide a methodology to rapidly assess and improve the security posture of critical cyber assets in accordance with DISA STIGs and CJCSI directives. These automated solutions ensure that the entire process of identification, remediation and reporting of non-compliant cyber assets is conducted in a repeatable manner, thereby achieving continuous compliance without consuming significant IT resources.

ForeScout Expedites CCRI Audit Processes

Preparing for a CCRI audit requires a combination of trained staff, strong policies and industry-leading technology. While there is no “silver bullet” that covers all the required criteria, there are solutions that can contribute significantly to achieving adherence. ForeScout offers a policy-based security platform for endpoint compliance automation that can help DoD IT organizations to create, monitor and enforce endpoint security policies in accordance with DISA STIGs and CJCSI directives, all with minimal effort.

ForeScout CounterACT® is a virtual or physical appliance that deploys seamlessly within existing network, security and endpoint infrastructure and provides a highly scalable, cost-effective CCRI solution without the need to upgrade or re-architect the network. Endpoint identification, classification, policy-based control and remediation functions do not require the use of agents and fully support embedded devices. The CounterACT appliance installs out-of-band, avoiding latency or potential for network failure, and can be centrally administered to dynamically manage thousands of endpoints from one console. As a result, the system enables rapid deployment and low total cost of ownership.

The plug-and-play architecture allows for seamless integration with configuration and policy management systems, vulnerability assessment and host-based security systems, ticketing and systems management, and security information event management systems to yield a closed-loop platform for continuous monitoring and compliance. Consequently, commanders can ensure their IT organization will satisfy CCRI audit requirements and achieve continuous compliance while enabling the IT staff to focus on more mission-critical activities.

As shown in the following table, ForeScout CounterACT provides DoD entities with the capacity to automate several endpoint compliance controls required by DISA STIGs and CJCSI directives.

	CCRI Criteria	ForeScout CounterACT
Visibility and Asset Management	Establish and maintain a hardware asset inventory for various types of devices connected to the IP network. Establish and maintain a software asset inventory, including OS and application versions and patch levels.	CounterACT maintains a comprehensive asset inventory of devices attached to the network. The inventory can be searched and organized by various hardware and software attributes. Inventory reports can also be generated.
Authentication and Access Control	Block or disconnect IS or device if a directed task(s) cannot be implemented or mitigated as directed by CC/S/A authority.Deploy protection mechanisms at layered or internal enclave boundaries as required for networks handling unclassified and classified information. Use commercial wireless networks and devices in accordance with DoD Wireless STIG. Ensure Authorizing Official-approved wireless devices, services and technologies.	CounterACT can block or restrict access to devices when they become non-compliant. It enforces role-based access control to provide users and devices access to different parts of the network or specific IT resources. CounterACT can enforce remote access policies through integration with multiple vendors' VPN products. It provides additional controls for enforcing wireless compliance through integration with wireless infrastructure.
Compliance Monitoring and Remediation	Devise a list of authorized software that is required for each type of system. Monitor for unauthorized software installed on each machine.Secure configurations for hardware and software on laptops, workstations and servers. Run current versions of software and make sure they are fully patched. Remove outdated and older software from the system. Conduct vulnerability assessments, Blue Team vulnerability evaluations, cybersecurity inspections and Red Team operations to provide a systemic view of enclave and IS security posture. Ensure subordinate organizations implement DoD Standard Security Configuration. Use DoD-provided automated tools/solutions such as the Host Based Security System (HBSS) or CC/S/A-procured tools/solutions developed in accordance with DOD data exchange standards to ensure interoperability with DOD-provided solutions for remediation of vulnerabilities. Implement USSTRATCOM warning and tactical directives/orders through the use of available automated tools.	CounterACT can perform a wide range of compliance checks, including monitoring for required software, unauthorized software, software versions and patch versions, device configuration and endpoint vulnerabilities, just to name a few. It integrates with other DoD-provided tools such as HBSS or vulnerability scanners to obtain additional compliance information for managed devices. When compliance violations are detected, CounterACT can respond based on the severity of the violation by simply alerting or notifying IT staff, or auto-remediating, quarantining or blocking non-compliant endpoints.
Compliance Notification and Reporting	Provide cybersecurity inspection, evaluation, and assessment findings and results through existing command and technical management channels. Implement warning and tactical directives/ orders that correspond to hardware and software within CC/S/A IT resources and assets inventory.	A wide variety of compliance assessment reports can be scheduled or generated upon demand to fulfill audit requirements, as well as provided to command and technical management. CounterACT policies allow notifications and reports to be sent to IT staff regarding the compliance status of cyber assets.

Solution Benefits

- Dynamic Network Asset Intelligence
- Policy-based Compliance Control
- Automated Remediation
- Reduced Risk and Vulnerability Profile
- Expedited Audit Process
- Lower Operational Cost

Learn more at
www.ForeScout.com

ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591
Fax 1-408-371-2284

CounterACT Highlights

Active Asset Management. Dynamically generated hardware and software asset repository of what's on the network: devices, hardware, operating systems, applications, patch levels, processes, open ports, peripheral devices, users and more.

Policy-based Access Control. Limit access to information systems by authorized users and devices, and to authorized types of transactions. Use either 802.1X port-based access control or alternative network authentication and access control mechanisms.

Continuous Monitoring. Assess the security and compliance posture of endpoints in real-time before and after they connect to the network. Detect endpoint configuration violations and malicious behavior and tailor the response to the violation's severity.

Automated Remediation. Automate remediation of non-compliant endpoints by triggering actions such as auto-update of host-based configuration and protection systems, patches and updates, and installing, activating or disabling applications or peripherals.

Compliance Reporting. Leverage a fully integrated reporting and notification engine to monitor the level of policy compliance, satisfy audit requirements and produce real-time inventory reports.

HBSS Integration. Increase situational awareness and incident response by automatically detecting and remediating endpoints with missing or broken Host Based Security System (HBSS) agent, and grant, deny or limit network access based on compliance with STIG and FDCC standards assessed by HBSS.

Guest Access. Create individualized access control policies for foreign nationals and contractors to limit access to authorized secret networks and systems (such as SIPRNet) and non-classified networks and systems (such as NIPRNET) in accordance with DoD and CJCSI directives.

Mobile and Wireless Controls. Detect and enforce security controls on mobile devices such as smartphones and tablets. Enforce wireless compliance based on STIG standards and CJCSI directives through integration with wireless network infrastructure.

Non-disruptive Deployment. Deploy within existing network infrastructure without the need to re-architect the network, deploy in-line, upgrade the switching fabric or require agents. Enforce access policy from any level of switch/network hierarchy, including access, distribution or core layer.

IT Interoperability. Leverage integration with existing IT infrastructure such as **directories** (Active Directory and OpenLDAP) and patch management, endpoint protection, ticketing, vulnerability assessment, security information and event management, and mobile device management systems.

Cost Savings. Eliminate manual processes associated with assessing, reviewing, remediating and reporting on compliance to STIG and CJCSI standards. Increase IT efficiency by reducing the time spent preparing for CCRI audits, allowing IT administrators to focus on critical daily operational activities.

*Bring Your Own Device (BYOD), Internet of Things (IoT)
**As of November 2015

Version 4_16