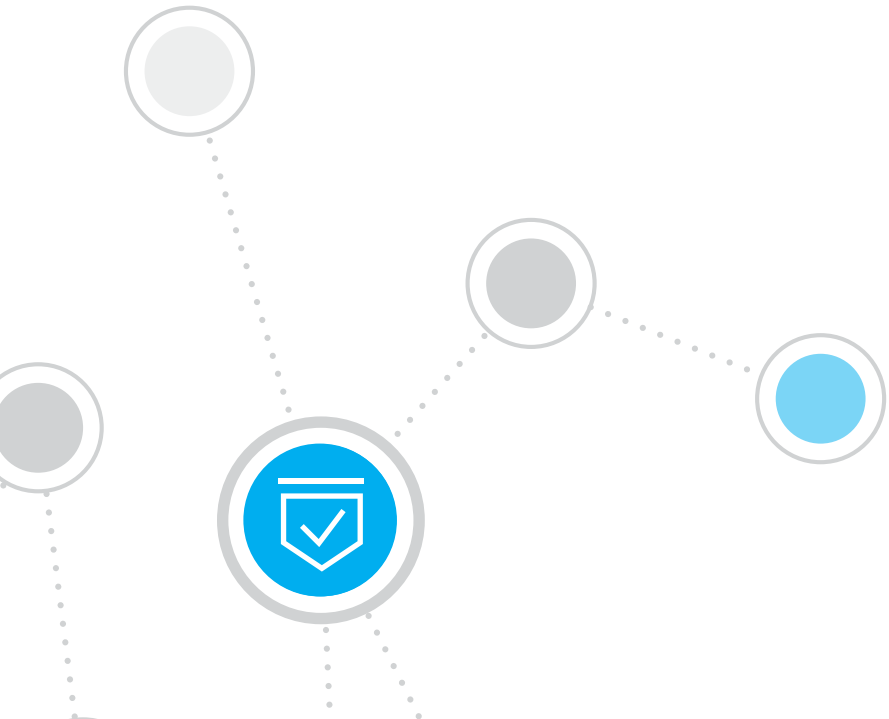
ForeScout

White Paper

Comply to Connect with the ForeScout Platform



ForeScout CounterACT® can provide visibility, hygiene, mitigation and control across technical, management and operational assets in accordance with the U.S. Government's 800-53 and NIST SP 800-171 standards. CounterACT is the agentless visibility and control solution that:

- Maps directly to 10 of 18 primary controls, 38 specific controls and over 150 supporting controls
- Integrates with leading third-party tools to help ensure further compliance that supports additional controls
- Supports these controls in real time to boost compliance with Continuous Diagnostics and Mitigation (CDM) requirements

Executive Summary

Comply to Connect (C2C) is a United States Department of Defense (DoD) security framework designed to dramatically improve the level of assurance for authentication, authorization, compliance assessment and automated remediation of devices connecting to the enterprise network. Within the C2C framework, devices are authenticated and assessed for compliance against DoD security policy prior to being authorized and granted access to enterprise network resources. Compliant devices gain full access to the network. Non-compliant devices receive limited access to network services and are automatically remediated, reassessed as compliant and granted network access once compliant. Unauthorized devices are restricted and unable to access the network.

Critical Characteristics of an Infrastructure Security Framework

A C2C framework requires four critical characteristics to maximize effectiveness and efficiency:

- **Extensive Network-Based Visibility, Discovery and Classification of Devices** – Comprehensive discovery and classification of hardware connecting to an enterprise network is foundational to securing that network. Solutions relying on agents, sensors, or network scans cannot provide that level of complete visibility, as agents are bound to fail, sensors are difficult to fully deploy across all network segments and rogue devices evade network scans in order to remain hidden. To know what devices are on the network, one must interrogate the network infrastructure. C2C requires the authoritative and complete visibility provided only by full network interrogation to see and enumerate devices connecting to the network. This discovery and classification must also include where devices are connected to your network.
- **Redundant Manageability and Control of Devices** – Solutions relying on a single method to manage and control devices, whether agent-based or agentless, risk introducing a manageability gap where agents are not installed/running or agentless inspection isn't configured correctly across 100 percent of the devices on the enterprise network. C2C requires the redundancy of both agent-based and agentless manageability and control of devices to fully mitigate this risk.
- **Orchestration with Mandated Security and Network Management Solutions** – Compliance and remediation of DoD devices are tightly coupled with security solutions mandated by DoD policy. Remediation of non-compliant devices depends on integration with fielded software and patch management solutions. C2C requires out-of-the-box, certified and bi-directional integration with both mandated and fielded solutions delivering security and network management services.
- **Continuous Monitoring and Automated Remediation** – Compliance enforcement of devices connecting to the enterprise network does not end once a device has been deemed compliant and granted network access. C2C requires devices remain compliant in order to remain connected to the network, promptly and automatically triggering remediation when devices fall out of compliance while connected.

How ForeScout Helps You See More

ForeScout combines the techniques below with heterogeneous network integration and an advanced device categorization taxonomy that classifies traditional and IoT/OT devices by operating system, vendor and model, allowing you to make intelligent, policy-based security decisions.

1. Poll switches, VPN concentrators, access points and controllers for a list of connected devices.
2. Receive SNMP traps from switches and controllers.
3. Monitor 802.1X requests to built-in or external RADIUS server.
4. Monitor DHCP requests to detect when a new host requests an IP address.
5. Optionally monitor a network SPAN port to see network traffic such as HTTP traffic and banners.
6. Run Network Mapper (Nmap) scan.
7. Use credentials to run a scan on the device.
8. Receive NetFlow data.
9. Import external MAC address classification data or request LDAP data.
10. Monitor virtual machines in public/private cloud.
11. Classify devices using PoE with SNMP.
12. Use optional agent.

ForeScout has a proven ability to implement a C2C framework with sophisticated capabilities as a risk mitigation platform that provides network access control and continuous monitoring. With its vast set of Extended Modules for orchestration with mandated and other common DoD cybersecurity tools, as well as its unique ability to deliver the four critical characteristics cited above, ForeScout provides the core foundation in any C2C implementation for security as it relates to traditional information technology (IT), non-traditional operational technology (OT), platform IT (PIT) and Internet of Things (IoT) devices connecting to DoD networks.

The Comply to Connect Workflow and Phases

The security of a C2C framework is delivered by a workflow of four closely coordinated phases in which devices connecting to the network are evaluated against policy, and different actions are taken based on the outcome of the policy assessment. The four workflow phases in a C2C framework are 1) Discovery and Classification, 2) Authentication and Authorization, 3) Pre-Connect Compliance Policy, and 4) Post-Connect Compliance Policy.

Phase 1: Discovery and Classification

Effective discovery and classification requires multiple methods of both active and passive techniques. Relying on only a few of these discovery methods can leave gaps in visibility. Complete visibility requires discovery and classification via network device interrogation such as polling ARP tables, receiving SNMP traps, monitoring 802.1X RADIUS and DHCP requests, ingesting SPAN and/or NetFlow data, targeted NMAP scans, credentialed login (SNMP, SSH or Active Directory), leveraging an optional agent and more. Having both active and passive discovery and classification methods gains a complete picture of devices connected to the network, including what they are, where they are connected (switch, switchport, VLAN, WAP, WLAN, vSwitch, etc.), what ports are open on devices, software installed on managed endpoints and more.

Phase 2: Authentication and Authorization Policy (Control Network Access)

Although the DoD Security Technical Implementation Guide (STIG) for network access control currently standardizes on 802.1X for authenticating devices connecting to DoD networks, authentication and authorization under the C2C framework can be accomplished with or without 802.1X. Traditional IT devices can be easily authenticated and authorized using multiple methods, including 802.1X with an installed supplicant or agent, applying pre-connect access control lists and releasing devices upon successful device certificate-based authentication, or logging into devices via Windows services with valid domain credentials.

In many cases, non-traditional OT, PIT and IoT devices cannot support 802.1X supplicants and therefore should be authenticated using something more than a list of approved MAC addresses, which is the minimally secure and easily spoof-able security offered by MAC Authentication Bypass (MAB). For example, a printer connecting to the network should authenticate both by using MAB and a pre-configured SNMPv3 credential prior to assignment to the print VLAN. This mitigates risk of an unauthorized device spoofing an authorized MAC address and circumventing access controls.

ForeScout recommends C2C implementations in the DoD include the following Authentication and Authorization Policy checks:

- **Device Authentication Check** – Depending on whether a traditional IT or non-traditional OT/PIT/IoT device, device authentication may be performed using a variety of methods. The ForeScout platform delivers all of these authentication and authorization methods, whether 802.1X-based or not.
- **Cross-Domain Violation Check** – Devices belonging to a network at a higher classification should not be able to authenticate and connect at a lower classification, which could lead to the leaking of classified information. In addition to instantly quarantining an offending device upon connection, ForeScout can perform immediate alerting actions and provide forensic evidence to investigating administrators, including the machine host name, the logged-in user and where the device is physically attempting to connect to the network.
- **Spoofed Device Check** – For devices that authenticate to the network using MAB, a recommended supplemental check can verify the device presents itself and acts as expected for its class of device. For example, the ForeScout platform can validate that a printer on the MAB is correctly classified as a printer (as opposed to a Linux box spoofing an authorized printer MAC address) prior to assigning it to the printer VLAN.

Phase 3: Pre-Connect Compliance Policy (Compliance on Connection)

Once a device is authenticated and authorized to connect to the enterprise network, but prior to being granted full access to network services (i.e., "pre-connect"), the C2C framework assesses security compliance against critical security controls. Because a thorough inspection of EVERY security control and configuration setting on the device can be time-consuming and unnecessarily delay a user's access to the network, the pre-connect assessment is focused ONLY on the most critical security controls—situations where non-compliance poses too great a risk if the device is allowed on the network.

ForeScout recommends C2C implementations in the DoD include, at a minimum, the following pre-connect compliance policy checks:

- **Host-Based Security System (HBSS) Framework Agent Health Check** – The ForeScout platform validates that the HBSS Framework agent is installed and running. If found uninstalled or stopped, the ForeScout platform automates the remediation actions to install or start the agent. This results in the elimination of HBSS management gaps and an increase in security across all HBSS-protected devices.
- **Assured Compliance Assessment Solution (ACAS) Scheduled Scan Check** – The ForeScout platform validates that the ACAS solution has performed a vulnerability scan of the device within the timeframe required of DoD or local security policy. If the device's last scan is found to be outside of the required timeframe, the ForeScout platform automatically triggers ACAS to launch a vulnerability scan on the potentially non-compliant device. This results in a current and complete assessment of all devices on the network, including transient devices and those that are typically offline during scheduled scans.
- **ACAS Scan Results Check** – The ForeScout platform validates that the current ACAS vulnerability scan results for a device do not include any high-risk or combined-risk vulnerabilities. While the local command may set the threshold for identifying which high-risk or combined-risk vulnerabilities preclude device connection, the ForeScout platform automates the access control, alert, and/or remediation actions depending on the specific

vulnerability scan results. Devices posing the highest levels of risk are thus prevented from connecting to the enterprise network until the risk has been mitigated.

- **Software Patch Management Agent Health Check** – The ForeScout platform validates that the command's software patch management agent (for example, Microsoft SCCM, Tanium Patch and IBM BigFix) is installed and running. If found uninstalled or stopped, the ForeScout platform automates the remediation actions to install or restart the software patch management agent. Because of the ForeScout platform's redundant device manageability processes, it is uniquely able to remediate an endpoint with a failed software patch management agent to provide additional assurance that endpoints can be updated by the patching solution so that known vulnerabilities are thoroughly mitigated.

When pre-connect compliance policy checks determine that a device is non-compliant, the ForeScout platform directs the device to a limited-access network segment using VLAN assignment and/or access control lists (ACLs) and/or virtual firewall (vFW), where the device can be remediated without introducing risk to the enterprise network. Once remediated and reassessed as compliant, the ForeScout platform provides full access to network resources based on the authorizations granted to the user and/or device. Furthermore, the ForeScout platform continuously monitors the device against these checks, automatically taking the proper control and remediation actions if the device falls out of compliance while connected to the enterprise network.

Phase 4: Post-Connect Compliance Policy (Ongoing Compliance Enforcement)

After the C2C framework assesses a device's critical security controls as compliant, the device is deemed to be within an acceptable level of risk to connect to the enterprise network and is granted access to the network based on the authorizations of the user and/or device. At this point (i.e., post-connect), additional security controls are checked for compliance and remediated if found non-compliant.

ForeScout recommends C2C implementations in the DoD include the following post-connect compliance policy checks:

- **HBSS Supporting Agent Health and Status Check** – The ForeScout platform validates that all mandated HBSS agents (for example, Host Intrusion Prevention System, Policy Auditor, Asset Baseline Module, Rogue System Detection, Device Control Module and Asset Publishing Service) are installed and running.
- **Data at Rest (DAR) Agent Health and Encryption Status Check** – The ForeScout platform validates that the DAR agent is installed and running, and that the hard disk is encrypted.
- **Antivirus and Antimalware Agent Health and Scan Status Check** – The ForeScout platform validates that the command's AV/antimalware agent is installed and running, the definition files are up to date, and a scan has been performed within the policy timeframe.
- **Software and Patch Compliance Check** – The ForeScout platform validates that the device's software is patched and up to date, and that there are no new software packages or advertisements available for installation on the software patch management server.

- **Prohibited Software Check** – The ForeScout platform validates that prohibited software is not installed or running. Examples of prohibited software could include peer-to-peer, instant messaging and other categories of software deemed too risky to allow on network-connected devices.
- **External Device Check** – The ForeScout platform identifies external devices and peripherals connected to devices on the network, including devices connected to USB ports, such as mobile devices, hard-disk drives, flash drives, etc. The platform validates that only approved devices are connected and disables non-compliant external devices.
- **STIG/SCAP Compliance Check** – The ForeScout platform validates the configuration of Windows workstations and servers against applicable configuration baselines, SCAP standards and STIGs, including the validation of application settings. Low-scoring systems are easily identified with full reports of failures reported to the appropriate administrator for remediation and resolution.
- **Other Security Agent Health and Status Checks** – As most endpoint security controls rely on agents, the ForeScout platform validates that these required security agents are installed, running and up to date. Examples may include agents required for application whitelisting, data loss prevention, host firewall, 802.1X supplicants and smartcard middleware as well as agents required for advanced persistent threat/advanced threat detection and other security capabilities.
- **OT/PIT/IoT Network Behavior Check** – The ForeScout platform validates that a non-traditional OT, PIT or IoT device communicates only with authorized management servers, alerting and taking control actions if changes to the device fingerprint, network behavior, or client/server session traffic are detected.

Automate NetOps and Cybersecurity Functions: The ForeScout platform automatically remediates devices found non-compliant against pre-connect compliance policy checks and/or post-connect compliance policy checks while they attempt to connect or they are already connected to the enterprise network. Furthermore, the platform continuously monitors against these checks, automatically taking appropriate remediation actions if the device falls out of compliance while connected to the enterprise network.

Value of a Comply-to-Connect Implementation

Current DoD customers using the ForeScout platform share many examples of how implementing C2C has secured their networks and provided increased value, including:

- Raising Command Cyber Readiness Inspection (CCRI) scores well into the 90-100 percent range for unclassified and classified network inspections while decreasing inspection preparation workload
- Satisfying requirements of the 2017 National Defense Authorization Act, which requires the DoD develop “a comply-to-connect policy that requires systems to automatically comply with the configurations of the networks of the Department as a condition of connecting to such networks.”

Acronym Glossary

DHCP (Dynamic Host Configuration Protocol)

MAC (Media Access Control)

Nmap (Network Mapper)

RADIUS (Remote Authentication Dial-in User Service)

SNMP (Simple Network Management Protocol)

SPAN (Switch Port Analyzer)

SSH (Secure Shell)

VLAN (Virtual Local Area Network)

VPN (Virtual Private Network)

VoIP (Voice over Internet Protocol)

vSwitch (Virtual Switch)

WAP (Wireless Application Protocol)

WLAN (Wide Area Local Area Network)

- Also satisfying requirements of the 2017 National Defense Authorization Act, which requires the DoD to have controls around software licenses on endpoints and prohibits purchasing new software in excess of $5M until such controls are in place
- Filling the gap in current security capabilities created by non-802.1X-capable devices
- Reducing manpower requirements for software and patch management by 75 percent, enabling realignment of personnel to proactive analytics, forensics, and active cyber defense tasks

The ForeScout platform offers the critical capabilities to enable DoD's C2C program to meet industry best practices and implement leading Infrastructure Security Frameworks:

- Comprehensive network-based visibility, discovery and classification of devices connecting to the network
- Redundant manageability and control of devices
- Orchestration with mandated security solutions such as HBSS and ACAS as well as fielded network management solutions
- Continuous monitoring and automated remediation of devices following initial connection to the network

The ForeScout platform is the core foundation in any C2C framework, delivering authentication and authorization, pre-connect, and post-connect compliance policy assessment and remediation for traditional IT, non-traditional OT, PIT and IoT devices on the network.

Learn more at
www.ForeScout.com

ForeScout

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

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

About ForeScout

ForeScout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. As of June 30, 2017 more than 2,500 customers in over 70 countries improve their network security and compliance posture with ForeScout solutions. See devices. Control them. Orchestrate system-wide response. Learn how at www.forescout.com.