FORESCOUT

Comply to Connect

Implement controlling countermeasures to safeguard your information systems

The ForeScout platform 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. This device visibility and control solution:

- 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

Overview

Comply-to-Connect (C2C) is a comprehensive cybersecurity framework of tools and technologies designed to increase cybersecurity efficiency across The Department of Defense's (DoD) current and emerging operational environments. The desired effect enables ongoing insight into the state of local operating compliance with DoD CIO security policies and U.S. Cyber Command operational security orders. C2C emphasizes the use of synchronized orchestration to reduce labor-intensive cybersecurity efforts and increase operational cybersecurity efficiency. C2C augments the effectiveness of the Department's Information Security Continuous Monitoring program by reporting on the state of asset security compliance as a condition of remaining connected to the network. Security risk positions derived from the visualized state of non-compliance will inform the decisions made by those communities of interest responsible for information, network, mission and departmental risk management.

Critical Characteristics of a C2C Framework

An effective C2C framework requires the following four characteristics:

- **Comprehensive Network-Based Visibility, Discovery and Classification of Devices** – Accurate visibility requires a combination of network integration and advanced active and passive analytical techniques to identify the growing numbers and types of connected devices (see visibility sidebar on page two). Other approaches leave visibility gaps.
- **Redundant Manageability and Control of Devices** – Comprehensive device control requires simultaneous agentless and agent-based endpoint inspection and control.
- **Orchestration with Mandated Security and Network Management Solutions** – Compliance with DoD security policy requires out-of-the-box, bi-directional integration with DoD-mandated security tools.
- **Continuous Monitoring and Automated Remediation** – Compliance must be continuously monitored and maintained for devices that were deemed compliant when they initially connected to the network.

Comply-to-Connect Phases

The security of a C2C framework is delivered by a workflow of four 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:

- **Phase 1: Discover and Classify** – Complete visibility to discover/classify/locate connecting devices.
- **Phase 2: Authentication and Authorization** – Control network access at the access layer, with or without 802.1X.
- **Phase 3: Pre-Connect Compliance** – At connection, control access based on compliance with security policies.
- **Phase 4: Post-Connect Compliance** – Continuously monitor each device, control access/maintain compliance.

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.

Compliance Policy Examples

Pre-connect compliance assessment addresses only the most critical security controls, while post-connect compliance assessment includes the remaining security controls. The following are examples of common DoD compliance policies and their corresponding automated remediation actions:

- **Host-Based Security System (HBSS) Agent Health Check** – Are they installed/running? If not, auto-remediate.
- **Assured Compliance Assessment Solution (ACAS) Scan Check** – Completed as part of routine scans? If not, trigger scan.
- **ACAS Scan Results Check** – Are there high-priority outstanding vulnerabilities that have not been remediated? If so, auto-trigger notification/remediation.
- **Software and Patch Compliance Check** – Are patches up to date? If not, trigger agent check-in.
- **External Device Check** – Are any unauthorized external devices plugged into the device? If so, disable device.
- **STIG/SCAP Compliance Check** – Is device properly configured against DISA STIGs?
- **OT/PIT/IoT Network Behavior Check** – Are there any anomalous protocols or communication requests?

Impact

Current DoD units share examples of cybersecurity success after implementing C2C, including:

- **Raises Command Cyber Readiness Inspection (CCRI) Scores** – Well above 90 percent and with reduced manpower.
- **Satisfies FY17 NDAA Mandates** – Delivers Comply-to-Connect, software license control, SCADA/ICS control.
- **Fills Gaps in Securing Non-802.1X-Capable Devices** – Sees OT/PIT/IoT devices, controls device spoofing attempts.
- **Reduces manpower** – Software and patch management requirements cut by as much as 75 percent.

Summary

The ForeScout platform offers comprehensive capabilities for DoD's C2C security framework: network-based discovery and classification of devices, redundant manageability and control of devices, orchestration with mandated security solutions such as HBSS and ACAS, and continuous monitoring of connected devices. The ForeScout platform can form the core of any C2C framework, delivering authentication and authorization, pre-connect and post-connect compliance policy assessment, and remediation for traditional IT and non-traditional OT/PIT/IoT devices on the network.

Learn more at
www.ForeScout.com

FORESCOUT

ForeScout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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

Acronym Glossary

DHCP (Dynamic Host Configuration Protocol)
HTTP (Hypertext Transfer Protocol)
IoT (Internet of Things)
ICS (Industrial Control System)
LDAP (Lightweight Directory Access Protocol)
MAC (Media Access Control)
NDAA (National Defense Authorization Act)
NetBIOS (Network Basic Input/Output System)
Nmap (Network Mapper)
OT (Operational Technology)
PoE (Power over Ethernet)
PIT (Platform IT)
RADIUS (Remote Authentication Dial-in User Service)
SNMP (Simple Network Management Protocol)
SPAN (Switch Port Analyzer)
SCADA (Supervisory Control and Data Acquisition)
SCAP (Security Content Automation Protocol)
STIG (Security Technical Implementation Guide)
VLAN (Virtual Local Area Network)
VPN (Virtual Private Network)