FORESCOUT

Comply-to-Connect: The Basis for Cybersecurity

Introduction

The cybersecurity challenges facing federal government agencies are more complex than ever and demand comprehensive solutions capable of securing networks, devices and data. The explosion in the numbers and types of connected devices, coupled with the increased reliance on the data that is being exchanged, makes it imperative for Chief Information Security Officers (CISOs) to create trusted environments for their organizations.

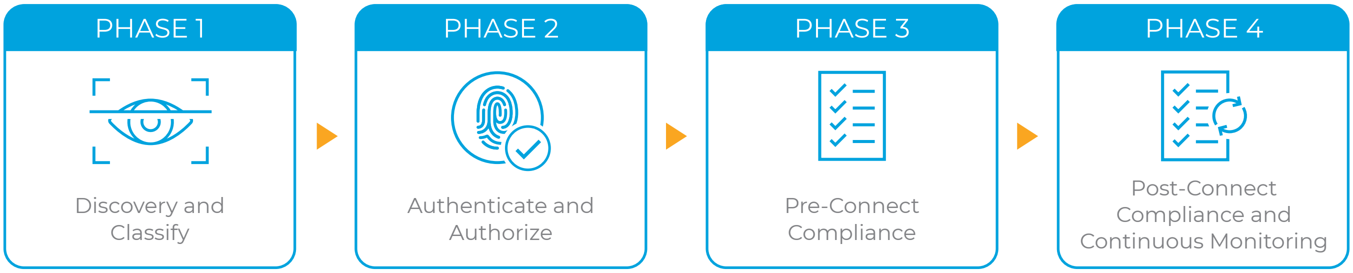
Comply-to-Connect, or C2C, is the Department of Defense's next major step forward in network security for all networks comprising the Department of Defense Information Network (DoDIN) and at both the non-classified and classified levels. C2C is a program that delivers capabilities to accomplish two primary goals:

1. First, C2C fills existing capability gaps in currently fielded enterprise security solutions through complete device identification, device and user authentication, and security compliance assessment.
2. Second, C2C automates routine security administrative functions, remediation of noncompliant devices and incident response through the integration of multiple management and security products and continuous monitoring.

Whereas other enterprise security solutions focus on a subset of DoDIN-connected devices, C2C applies to all categories of DoDIN-connected devices: workstations/servers, mobile devices, user peripherals, platform IT devices, IoT devices, and network infrastructure devices.

The Comply-to-Connect Process

Among DoD officials, device visibility is a recognized shortcoming in the agency's long-term network management and security strategies. C2C is rectifying this by providing tools that discover and categorize every connecting device, running them through inspection layers that assess devices and users against security policies, and authorizing connection only when compliant. C2C also orchestrates remediation actions taken against noncompliant devices to bring them into compliance and authorize their connection. It then continuously monitors all connected devices to ensure they remain compliant and secure.



PHASE 1
Discovery and Classify

PHASE 2
Authenticate and Authorize

PHASE 3
Pre-Connect Compliance

PHASE 4
Post-Connect Compliance and Continuous Monitoring

Phase 1

In phase 1 of C2C, every device is discovered as it connects to the network. More than 1,000 attributes are captured about connecting devices through two dozen passive and active methods of data collection. This contextual information, including who manufactured the device, which operating system it is running, what switch port it is connected to and numerous other host- and network-based attributes of the device, allows C2C tools to understand exactly what the device is as well as key information about its configuration. With this information, C2C aligns the device with similar devices for actions taken later in the process.

Phase 2

Once discovery and classification are complete, phase 2 of C2C uses multiple factors about the device to determine whether it is a known corporate or organization asset. C2C tools can be configured to authenticate devices using an 802.1X-based methodology if available, but can also use multi-point authentication on non-802.1X-compatible devices. C2C combines the use of MAC Authentication Bypass (MAB) lists with additional information to ensure MAB-based authentication is part of the security strategy, not a way around it. In phase 2, the C2C capabilities automatically establish whether a device can be authenticated and allowed to connect to the DoDIN.

Phase 3

Phase 3 of C2C is where C2C capabilities take cybersecurity beyond any DoD enterprise solution fielded to date. At this point, connecting devices are assessed against a series of pre-connect security policies to ensure they are compliant with the most critical ones before any network access is granted. In other words, C2C confirms that a device poses a low enough level of risk to connect to the DoDIN.

Authenticated devices may be out of compliance for many reasons, including that the endpoint security agents are not functioning properly, security agents are not communicating with their management server or their supporting data files are outdated or corrupt. Other common issues on a device include obsolete software patches and unauthorized software. Still, more problems that are routinely found include unchecked indications of compromise that may have been reported through another tool but are still on the endpoint because no action has been taken beyond simply creating yet another trouble ticket or alert for the understaffed security operations team to address.

Phase 4

Once a device and user pass all pre-connect compliance checks, phase 4 of C2C grants network access into the proper network segment for the device type/user and continuously monitors the device while connected to ensure it remains in compliance. Different device categories are grouped with like devices so that security policies don't have to be one-size-fits-all. For example, a security camera does not have to pass muster with the same security policies as a desktop computer, and the desktop PC has different security criteria than a mobile smartphone. C2C tools use the information collected earlier in the connection process to assign the device to the proper segment. This data-defined network segmentation enables flexibility in security policy enforcement while still providing administrators with a centralized management tool.

Forescout Device Discovery and Classification

Forescout combines the techniques below with an advanced device categorization taxonomy that classifies traditional and IoT/OT devices in heterogeneous network infrastructures.

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

C2C enables the following compliance checks:

- **Endpoint Security System Status Check** – Verifies that all mandated agents are installed, properly configured, running, and are communicating with the proper server.
- **Vulnerability Scan Status Check** – Verifies that the command's vulnerability assessment scan has been performed within the defined policy timeframe.
- **Data at Rest (DAR) Agent Health and Encryption Status Check** – Validates that the DAR agent is installed and running, and that the hard disk is encrypted.
- **Software and Patch Compliance Check** – Checks 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** – 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.

Beyond 100-percent device visibility and centralized access control, C2C also provides automated endpoint remediation. Far too often, endpoint issues are found and reported through agent-based tools but go unaddressed due to higher priorities in an administrator's ever-growing list of alerts and required actions. With C2C, information from other network security and management tools becomes actionable. C2C's orchestration engine automatically directs integrated tools to do what they do best. For instance, if a Windows-based laptop attempts to connect but has not had a vulnerability scan within policy timelines, the C2C platform will limit network access for the laptop and direct the network vulnerability scanner to perform the scan on this device. If it finds a vulnerability that should have been patched days ago, the platform will direct the patch management tool to take the necessary steps to bring the device into compliance. Once complete, the device can then be quickly scanned again to update device status and share that information with other tools in the security framework such as a SIEM or CMDB.

The Technology Behind C2C Capabilities

Discover – Forescout eyeSight uses over 20 passive and active monitoring techniques to discover managed and unmanaged devices connecting to heterogeneous network infrastructure.

- User devices (laptops, tablets and phones)
- Virtual and physical computers, storage and network devices
- IoT, IoMT, OT and IIoT devices

Classify – eyeSight auto-classifies traditional, IoT and OT devices using a multi-dimensional classification technology to identify device function, type, operating system (including version), vendor and model.

- 550+ operating systems and versions
- 5,500+ vendors and models
- 10,000+ device types

Assess – eyeSight continuously monitors the network and assesses the configuration, state and security of connected devices to determine their compliance posture and risk profile.

- 350+ healthcare OT device vendors
- 130+ IT/industrial OT protocols support
- 3,000+ models of IIoT and OT Devices
- 600+ networking vendors and models across 350+ OS versions

Control – Forescout eyeControl enforces and automates policy-based network and host controls through integrations with heterogeneous physical and virtual network infrastructure. Actions can be automated or administrator-initiated and gradually increased to minimize disruption while reducing the manual effort to enforce network access, improve device compliance, implement network segmentation and accelerate incident response.

Orchestrate – Forescout eyeExtend products share device context between the Forescout platform and other IT and security products to automate policy enforcement across disparate solutions and accelerate system-wide response to mitigate risks. Included in the C2C solution are eyeExtend modules that integrate with other DoD enterprise program solutions.

Summary

Comply-to-Connect is the DoD's comprehensive solution to address the current uncertainty when it comes to cyber readiness to meet mission challenges and to secure the DoDIN against adversarial cyber activity. As the initial enterprise rollout gets underway, the Department is looking at future baseline capabilities, including deeper knowledge and control of industrial control systems and other operational technology devices, as well as modeling and simulation of network segmentation to optimize security.

Forescout Bona Fides/References

- Unified Capabilities Approved Products List (UC-APL) Compliant
  https://aplits.disa.mil/processAPList.action
- National Information Assurance Partnership (NIAP) Compliant
  https://www.niap-ccevs.org/Product/index.cfm
- Enterprise Software Initiative (ESI) Blanket Purchase Agreement (BPA)
  https://www.esi.mil/
- Multiple Service Authority to Operate (ATO) Certifications
- Defense Information Systems Agency C2C Program Management Office (PMO)
  https://disa.mil/
- Forescout Technologies C2C Information Page
  https://www.forescout.com/c2c/

More Compliance Checks

- **External Device Check** – 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** – Examines 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.
- **OT/PIT/IoT Network Behavior Check** – 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.

About Forescout

Forescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, real-time discovery and classification of every IP-connected device, as well as continuous posture assessment. As of December 31, 2019, more than 3,700 customers in over 90 countries rely on Forescout's infrastructure-agnostic solution to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity. Learn how 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

Learn more at Forescout.com