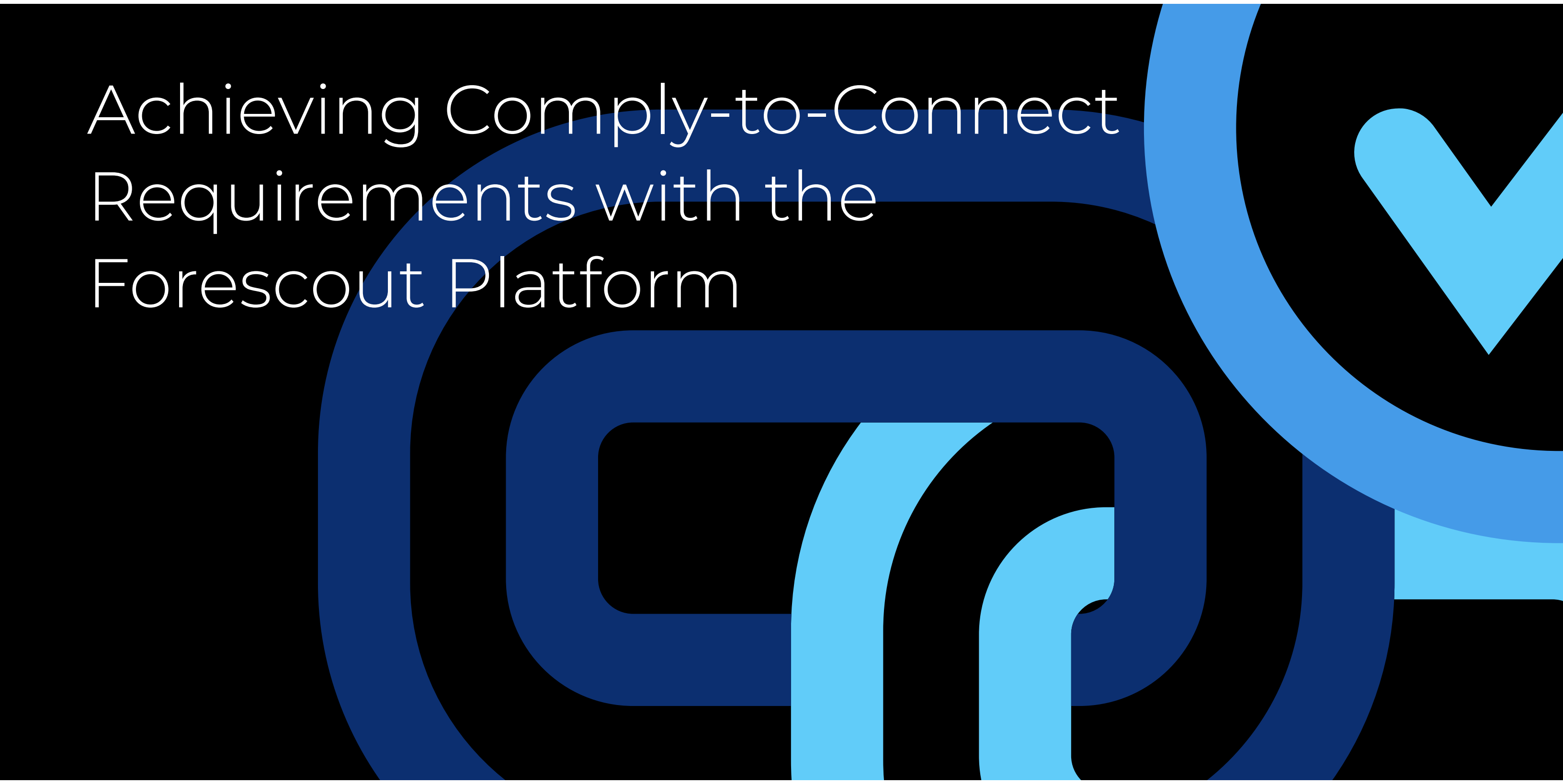
FORESCOUT

Active Defense for the Enterprise of Things™

Achieving Comply-to-Connect Requirements with the Forescout Platform



Executive Summary

The U.S. Department of Defense Comply-to-Connect (C2C) program specifies five critical steps to defend organizations from cyberattacks and mitigate risk. The Defense Information Systems Agency (DISA) C2C Program Management Office chose the Forescout platform as an essential component of a C2C defense because of its foundational role in achieving the requirements of these five steps and proven efficacy in U.S. military environments. The Forescout platform provides continuous discovery, classification and security compliance assessment of every network-connected thing – traditional as well as non-traditional devices. It also integrates with other cybersecurity tools, allowing automation of administrative, incident response-related and other workflows for greater efficiency and effectiveness. This whitepaper will help you understand why DISA chose the Forescout platform and how this device visibility and control solution can help you achieve C2C compliance in each step of the C2C framework.

= STEP 1

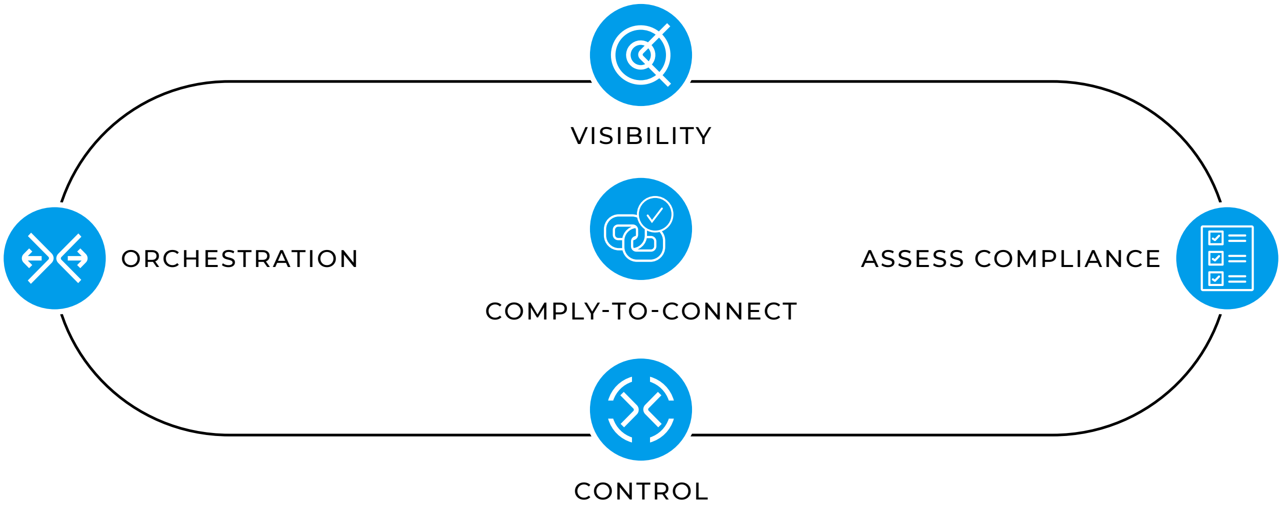
= STEP 2

= STEP 3

= STEP 4

= STEP 5

Comply-to-Connect Framework



Why Forescout?

Key aspects of the C2C Program include:

1. Continuous discovery, monitoring and reporting of traditional and non-traditional endpoints.
2. Security process transformation to include automating basic security functions and sharing information across cybersecurity and management tools to optimize security, reduce risk to the Department of Defense (DoD) mission and meet the goals of the DoD Digital Modernization Strategy.
3. Security product orchestration to include the use of policy-based control capabilities to increase the effectiveness of defensive cyber operations while reducing reliance on manual activities to perform routine administrative functions required to maximize security investments on DoD networked assets.

The Forescout platform provides proven, effective technology in C2C pathfinder environments and was chosen by the DISA C2C Program Management Office for delivering the required capabilities to meet enterprise C2C operations. The Forescout platform is the foundation for detecting, identifying and categorizing all assets on DoD networks, as well as the central point of integration with other DoD cybersecurity tools, providing automated administrative workflows and cyber incident response operations.

Preparation and Readiness

The Forescout solution provides the following benefits to organizations starting to implement C2C:

Infrastructure vendor-agnostic. The Forescout platform is compatible with most network hardware and works in heterogeneous environments, so you can meet C2C requirements and increase your network's overall security without being forced to upgrade or replace existing infrastructure.

802.1X-agnostic. The Forescout platform provides the widest range of options to meet authentication requirements – 802.1X as well as non-802.1X, policy-based methods.

Visibility across every connected thing. The Forescout platform's agentless approach enables the discovery of all endpoints connecting to the DODIN. As defined by U.S. Cyber Command, these include mobile devices, desktops and servers, networked user devices, network infrastructure, Internet of Things (IoT) devices and platform IT (PIT, also referred to as OT) devices. IoT and PIT/OT represent the fastest-growing risk area for daily operations. Left unaddressed, these "non-traditional" devices create a massive attack surface that adversaries can exploit to steal sensitive data or disrupt mission-readiness of the DoD. The C2C framework provides a common platform comprised of COTS (commercial off-the-shelf) technologies, with the Forescout solution at the core, that addresses connected device visibility challenges associated with these new network and mission realities.

Fast, flexible, non-disruptive deployment. The Forescout platform often delivers 100% visibility within days and policy-based access control and segmentation within weeks. Forescout also offers software-based appliances that can be loaded in virtual environments as well as a range of physical appliances, allowing you to tailor design implementation to meet operational needs and minimize physical footprint.

Backing of the C2C PMO. The Forescout platform is backed by the C2C Program Management Office (PMO), which provides software licenses, administrator training and engineering assistance. The PMO also issues an Authority to Operate (ATO) and security documentation, standard configurations, policy sets and other materials to assist teams implementing C2C. This PMO support generates significant cost savings for units or commands, helping them quickly operationalize their C2C solution.

Steps to Implementing C2C

Step 1: Discover, Identify and Categorize

Comprehensive discovery and classification of hardware connecting to an enterprise network are foundational to securing your network. Solutions relying on agents, sensors or network scans cannot provide complete visibility. Agents are bound to fail; sensors are difficult to fully deploy across all network segments, and rogue devices evade network scans to remain hidden. This is true of all networks – whether wired or wireless, physical or virtual, on-premises or cloud, information technology (IT) or operational technology (OT). That's why an agentless approach like Forescout's is needed.

C2C requires a comprehensive enumeration of devices connecting to the network. This discovery and classification must also include an understanding of where devices are connected (switch, switch port, VLAN, WAP, WLAN, vSwitch and so on) to the network. The Forescout platform uses a variety of methods to discover, classify and collect information about connecting endpoints. (See sidebar.) Data gleaned from these techniques is then used to classify traditional IT and non-traditional IoT/PIT/OT devices by operating system, manufacturer, device model and other parameters, allowing administrators to make intelligent, policy-based security decisions.

Effective identification and categorization require comprehensive visibility, and comprehensive visibility requires multiple active and passive techniques. Relying on only a few of these discovery methods can leave visibility gaps. You need to "see" all network-connected devices by conducting such activities as polling ARP tables, receiving SNMP traps, monitoring 802.1X RADIUS and DHCP requests, ingesting SPAN and/or NetFlow data, performing targeted NMAP scans, using credentialed logins (SNMP, SSH or Active Directory), leveraging an optional agent and more. In addition to data about each device, you need to know where the device is connected, what ports might be open, software installed on managed endpoints and more.

A single, converged platform is critical to delivering C2C to all DoD networks comprising the DODIN and for all endpoint categories defined by U.S. Cyber Command: workstations and servers, mobile devices, network user support devices, network infrastructure, IoT and PIT or OT devices. The legacy model of endpoint security, which focused only on the more easily managed Windows/Mac/Linux endpoints, no longer provides the security needed to protect the network. C2C solutions must mitigate the risk of any and every unauthorized or noncompliant endpoint connecting to the DODIN across every endpoint category.

By implementing the visibility functionality of the Forescout platform, you can fulfill all the requirements of C2C Step 1. The Forescout platform will be able to discover, identify and categorize every endpoint connected to your network. With this comprehensive, context-aware, real-time visibility as a foundation, administrators can then begin to move to implementing the next steps in the C2C framework, applying access controls and other security and efficiency measures.

Step 2: Interrogate

In this phase of C2C requirements, the Forescout platform delivers the capabilities necessary for you to gain a thorough security posture assessment of all connected endpoints. With a comprehensive inspection of each endpoint, security administrators can assess risk and prioritize remediation of the vulnerabilities and threats that are most critical.

With its easy-to-use console and customizable dashboard, the Forescout platform lets you create risk-driven policies to assess and monitor device compliance. You can assess compliance based on the condition of thousands of endpoint attributes. These checks can be performed before or after the endpoint fully connects to the production network. Examples of endpoint interrogations include:

COMPLETE VISIBILITY

A sampling of methods used by the Forescout platform for device discovery, identification and categorization

- Poll switches, VPN concentrators, access points and controllers
- Receive SNMP traps from switches and controllers
- Monitor 802.1X requests to a built-in or external RADIUS server
- Monitor DHCP requests to detect when a new host requests an IP address
- Monitor a network SPAN port to see network traffic such as HTTP traffic and banners
- Run Network Mapper (Nmap) scans
- Run device-specific scans using credentials
- Analyze Flow 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 for increased resiliency

- **Device Authentication.** Authenticates devices using a variety of methods depending on whether the device is a traditional IT or non-traditional IoT/OT/PIT device and whether the environment is based on 802.1X.

    - **802.1X Authentication**
      For 802.1X environments, a RADIUS Plugin broadens the scope of standard 802.1X authentication technology to include device profiling, endpoint compliance and access and remediation enforcement. The plugin enables the Forescout platform to provide authentication and authorization instructions to network devices, to integrate with user directory servers and to employ the Forescout platform 802.1X policies to detect, authenticate and control network endpoints and associated user activity. (The Forescout solution dynamically maintains the repository of MAC addresses of endpoints that do not have a functioning 802.1X supplicant by adding and removing devices via Forescout platform policies, checking and verifying devices for MAC spoofing and duplicate MAC address on the network.

    - **Non-802.1X, Policy-Based Authentication**
      For non-802.1X environments, the Forescout platform provides integration with more than 40 switch and wireless vendors using Simple Network Management Protocol (SNMP), Secure Shell (SSH)/Telnet and RADIUS to support existing heterogeneous networks. This architecture helps eliminate deployment, configuration and ongoing operational and cost challenges associated with 802.1x deployments and managing a MAC Address Repository (MAR.)

- **Endpoint Security Solution (ESS) Framework Agent Health:** Validates that the ESS framework agent is installed and running. For example, verifies that all mandated Host-Based Security System (HBSS) agents – Host Intrusion Prevention System, Policy Auditor, Asset Baseline Module, Rogue System Detection, Device Control Module and Asset Publishing Service – are installed and running.

- **ACAS Scan:** Validates that the Assured Compliance Assessment Solution (ACAS) solution has performed a vulnerability scan of the device within the timeframe required by DoD or local security policy.

> **C2C enables users to break down siloed tools that they had in the past and make them work more effectively and efficiently. This saves time and money while sustaining unprecedented levels of compliance across the enterprise.**

- **Software Patch Management Agent Health:** Validates that the patch management software agent – for example, Microsoft SCCM or Tanium Patch – is installed and running.
- **STIG/SCAP Compliance:** Examines the configuration of Windows workstations and servers against applicable configuration baselines, Security Connect Automation Protocol (SCAP) standards and Security Technical Implementation Guides (STIGs), including the validation of application settings.
- **Other Security Agent Health and Status:** Confirms that required security agents are installed, running and up to date. Examples may include agents required for application whitelisting, antivirus, antimalware, data loss prevention, host firewall, 802.1X supplicants, smartcard middleware and other security capabilities.
- **Software and Patch Compliance:** 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:** 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:** Identifies external devices and peripherals connected to devices on the network, including devices connected via USB ports, such as mobile devices, hard-disk drives and flash drives.

Standard and customized reports and alerts provide details for any devices that fail to meet compliance baselines or score poorly.

After the Forescout platform determines a device is compliant with critical pre-connect security controls, the device is deemed to have an acceptable level of risk to connect to the enterprise network and can be automatically granted access based on the user and/or device authorizations. At this point, additional post-connect security controls can be checked for compliance.

Compliance enforcement does not end after initial assessment and access. C2C requires that devices be continually checked for compliance to remain connected. If a device becomes noncompliant while connected, enforcement actions can promptly and automatically trigger remediation.

Step 3: Automate Remediation

The Forescout platform gives administrators the means to automatically remediate noncompliant devices against pre- or post-connect compliance policy checks. Based on the information gathered during C2C Step 2, the Forescout platform can automatically orchestrate remediation tasks such as:

- **Reinstall or Start ESS Agent:** If the ESS agent is found to be uninstalled or not functioning properly, automatically install or start the agent.
- **Run ACAS Scan:** If the device's last scan is found to be outside of the required timeframe, automatically trigger a new ACAS vulnerability scan on the potentially noncompliant device. (The scan can also kick off a real-time assessment of all devices on the network, including transient devices and devices that are typically offline during scheduled scans.)

- **Validate ACAS Scan Results:** Automatically validate that the current ACAS vulnerability scan results for a device do not include high-risk or combined-risk vulnerabilities outside the threshold dictated by the C2C PMO. Based on scan results, allow or block access, trigger an alert and/or generate remediation actions.
- **Install or Restart Patch Management Software:** If the patch management agent is found uninstalled or stopped, automatically install or restart the agent. (Because of the Forescout platform's redundant device manageability processes, it is uniquely able to remediate an endpoint even when the patch management agent has failed.)
- **Report or Remove Unauthorized Software:** Automatically, report or remove prohibited software from an endpoint, cleaning up devices that contain outdated software versions or devices to which users have installed risky or unnecessary applications.
- **Report or Block External Device:** Automatically report or block unauthorized devices, such as personal mobile devices, unauthorized speakers or gaming systems.

This is just a sampling of the security processes that can be automated using the Forescout platform. Any of the thousands of device attributes that the platform collects can be used to trigger an automated action. 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. The Forescout platform continuously monitors the device for compliance, automatically taking remediation actions if compliance is not maintained.

Aside: In a DoD environment, device compliance and remediation are tightly coupled with security solutions mandated by DoD and Service-specific policy, including Endpoint Security Solution (ESS), Host Based Security System (HBSS), Automated Compliance and Scanning (ACAS) and other Service capabilities. Remediation of noncompliant devices also demands integration with fielded software and patch management solutions. Thus C2C requires certified out-of-the-box integration with both mandated and fielded solutions that deliver security and network management services. Forescout extended modules for integration with third-party tools have received the necessary certifications.

Step 4: Authorize Connection

With the Forescout platform, administrators can implement high-level management directives concerning general user and device access levels as well as local network access controls. Building on the discovery, interrogation and remediation data provided in the previous three C2C steps, the Forescout platform provides the granular access controls that serve as the foundation for a Zero Trust environment and contribute to a defense-in-depth strategy. The utilization of rich contextual data about users and endpoints allows administrators to continuously validate policy compliance and address situations such as the following:

- **Cross-Domain Violations.** To reduce the risk of data exfiltration, devices belonging to a network with a higher classification level should not be authorized to connect to networks with a lower classification. In addition to instantly quarantining offending devices upon connection, the Forescout platform performs immediate alerting actions and provides forensic evidence to aid in investigation.

- **Spoofed Devices.** For devices that authenticate to the network using MAC Address Bypass (MAB), a supplemental check can verify that a device presents and behaves according to its classification. 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.
- **Unusual OT/PIT/IoT/ICS/SCADA Network Behavior.** The Forescout platform can validate that non-traditional OT, PIT, IoT, ICS, or SCADA devices communicate 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.
- **Health and Compliance Assessment:** The Forescout platform can continuously monitor the network, working to ensure that authenticated and authorized devices remain in compliance and can be trusted for continued access to network resources (as described in Steps 2 and 3).

These additional checks help administrators accurately determine the true trust-ability of the endpoint and user. While traditional methods of authentication such as 802.1X have been used in the past for authorization, in today's world, authentication does not equal authorization. The Forescout platform's ability to support device authentication on both traditional devices (via 802.1X) and non-traditional (via policy-based authentication) with compliance posturing (steps 1, 2, & 3) allows for an authorization matrix to be built to meet downward-directed and Authorizing Official (AO) specifications.

Step 5: Enforcement and Situational Awareness

Once the compliance level of the network has been raised to the acceptable risk level through C2C Steps 1 through 4, you can automatically and continuously enforce security policies across your piece of the DODIN. You can also extend the visibility gained from the Forescout platform to other tools in your environment to orchestrate workflows and accelerate response actions.

THE PROGRAM

C2C Program Office Responsibilities

- Core Solution Software Licenses – centrally procured and sustained
- Integration Module Licenses – centrally procured and sustained
- C2C System Administration Training – courses available globally
- Baseline Configuration Management – C2C policies and software version control

Services/Agencies/Centers Responsibilities

- Hardware Environment – acquisition and sustainment
- Implementation and Operations – uniformed or contractor support

With automatic policy enforcement enabled, the Forescout platform continuously monitors connecting and connected devices to ensure they remain in compliance with security policy. If a device is found noncompliant, the Forescout platform orchestrates remediation actions organically or through third-party integrations with other security tools on the network. These actions include, but are not limited to, the ability to automatically generate a trouble ticket, orchestrate a patch management solution to take action on a specific device, or restart failed endpoint processes. Automating these types of processes allows scarce cybersecurity resources to focus their efforts on real threats instead of spending time fixing basic hygiene conditions.

In addition, the Forescout platform becomes the single source of truth for real-time network endpoint connectivity and cybersecurity posture. Reports created using the customizable C2C dashboards available within the Forescout platform convey critical security status information at all levels of command for a shared understanding of every connected device across all component DODIN networks. Reports can also be created by configuring external data feeds or integrations to ensure real-time network compliance data is shared with other security tools; government command and control (C2); governance, risk management and compliance (GRC) and identity, credential and access management (ICAM).

In conclusion, when all five steps of the C2C framework are fully operational, continuous monitoring and reporting become the standard operations, reducing the need for spot inspections or audits since the cybersecurity posture of the DODIN is shared at all levels of command. The Forescout platform helps you fulfill the requirements of every phase of the Connect-to-Comply framework. By providing continuous adaptive protection based on real-time risk analysis, it actively protects your enterprise, your mission and users, assets and data while enabling decision-makers to assess cyber readiness for mission execution 24/7/365.

FORESCOUT CREDENTIALS

DoDIN APL (U.S. Department of Defense Information Network Approved Products List)

FIPS (Federal Information Processing Standards) 140-2

NIAP (National Information Assurance Partnership) Common Criteria Certification

US Marine Corps ATO (Authority to Operate)

US Navy ATO (Authority to Operate)

U.S. Army CoN (Certificate of Networthiness)

About Forescout

Forescout is the leader in Enterprise of Things security, offering a holistic platform that continuously identifies, segments and enforces compliance of every connected thing across any heterogeneous network. The Forescout platform is the most widely deployed, scalable, enterprise-class solution for agentless device visibility and control. It deploys quickly on your existing infrastructure – without requiring agents, upgrades or 802.1X authentication. Fortune 1000 companies and government organizations trust the Forescout platform to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity.

Visit forescout.com to learn how Forescout provides active defense for the Enterprise of Things.

Don't just see it.
Secure it.™

Contact us today to actively
defend your Enterprise of Things.

forescout.com/c2c/ c2c@forescout.com toll free 1-866-377-8771

FORESCOUT®
Active Defense for the Enterprise of Things™

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