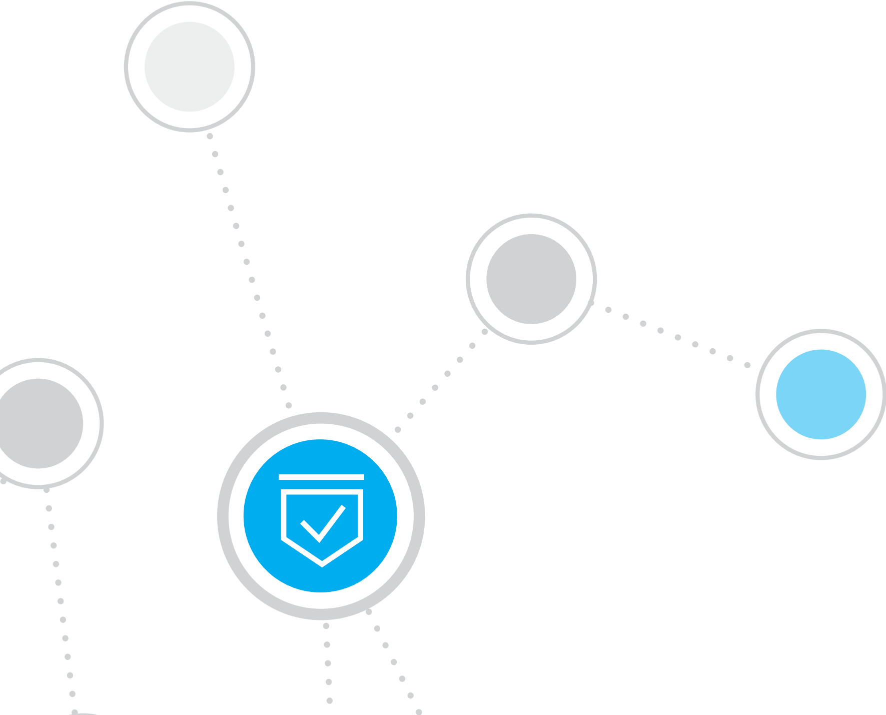
FORESCOUT

White Paper

Continuous Compliance with 800-171



Examples of CUI data include, but are not limited to:

- Support/Human Resources: This generally refers to personally identifiable information (PII). Examples include health records, legal documents, social security data, credit card information, and other personal information that isn't publicly available.
- Financial: Anything that could be used to adversely affect the U.S. economy, such as billing and inventories, bank transactions, account information and any data that could be targeted to compromise our economy.
- IT security: Data that might affect the availability, confidentiality or integrity of information systems and any vulnerabilities they may have.
- Law enforcement: Court records, information relating to the production of controlled substances, and the identities of certain whistleblowers, informants or victims of certain crimes.
- Patents: This includes patent applications, technical drawings of the inventions themselves, and secrecy orders pertaining to the products.
- Proprietary Business Information: Blueprints, specifications, shop drawings, etc.

CUI Complexity:

- 23 Categories
- 82 Subcategories
- 315 Unique Control ciatations
- 106 Unique Santion Citations

The Case for Protecting Data as a Critical Aspect of National Security

Data remains one of the top factors motivating hackers across the globe to land and expand their control over our production environments. With the advent of the dark web and other avenues, offensive cyber technologies are becoming commodities that are available to those with the desire to do harm, whether state-sponsored bad actor or lone wolf. It is no secret that our adversaries are getting smarter and faster every day and this was certainly supported in 2017 with the following big data breaches:

- **February:** U.S. Air Force suffered a data breach that exposed classified information.[1]
- **June:** More than 200 million voter records were exposed after a GOP data firm misconfigured Amazon's cloud storage service.[2]
- **September:** United States Army Intelligence and Security Command (INSCOM) suffered a data breach in which classified information could be freely downloaded from a web link.[3]

In these examples and in many others, attackers used known vulnerabilities and conventional attacks to gain access to these systems, often preying on systems that were not patched or managed by their existing Defense-in-Depth (DiD) solution. The underlying reason is that traditional DiD solutions do a poor job of tracking and managing IT inventory as assets connect and disconnect from production networks.

In response to the numerous breaches over the years, the Department of Defense (DOD) issued DFARS 252.204-7012 mandating that defense contractors and sub-contractors adhere to basic security protections identified in NIST Special Publication 800-171.[4] Its purpose is to protect Controlled Unclassified Information (CUI) and went live on 1/1/2018. Ramifications to non-compliant organizations include loss of current contracts and exclusion from future contracts until controls and a plan of action to remediate any gaps are in place. The NIST 800-171 Compliance Framework helps ensure that agencies, their contractors and associated organizations handling CUI maintain protective controls around the systems that transmit, store and handle CUI data.

The challenge in securing CUI

Identifying, securing and managing systems that contain or transmit CUI data can be a daunting task. The CUI standard is organized in layers of categories, sub-categories and citations identifying which data types must be protected as mandated by DFARS. However, in today's on-demand world, data moves too fast for traditional defense solutions. This is because most solutions today only provide "point-in-time" snapshots of their environment rather than continuous monitoring and analysis.

Imagine a security guard whose eyes remain closed all day except for 60-second intervals every 15 minutes in order to "scan" the area. If the guard happens to see something anomalous in the few minutes that their eyes are open, they can take care of the situation; however, if their eyes were closed, they would miss the event. Of course, one could hire more guards in hopes that collecting and collating scans would provide a more complete picture but that would hardly be effective or efficient. And yet most traditional DiD solutions view their world by taking intermittent snapshots on a scheduled basis to develop a level of situational awareness.

As with the guard example, many organizations try to coordinate their disparate discovery solutions to view what's connected, hoping the deltas between each scan will develop a complete picture. This condition is a major cause of blindspots on the network, which leaves hosts unmanaged, non-compliant, unsecured and prone to compromise. The news isn't all bad for DiD solutions, which still provide many foundational components to help organizations protect CUI data as it moves through and is stored on the networks and consumed on the endpoints; but, as with the security guard, they too need a boost in their efficiency and effectiveness.

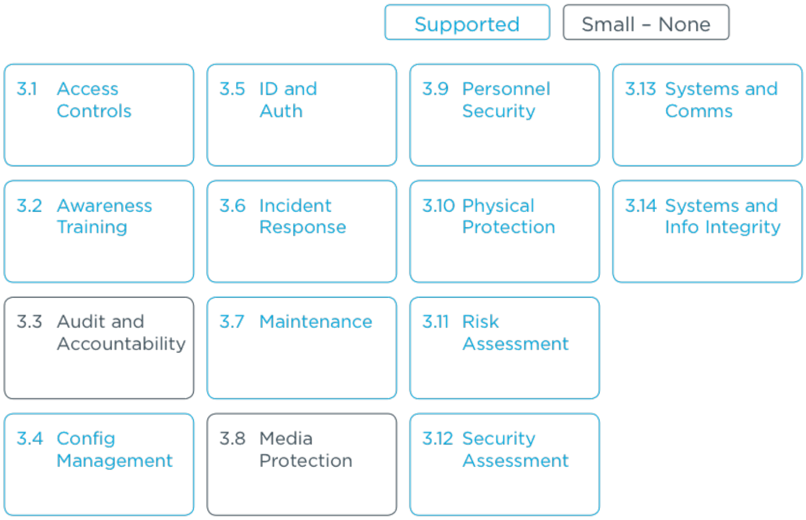


Diagram 1: *ForeScout support of 800-171 family of controls.*

Addressing 800-171 with ForeScout Continuous Compliance

The ForeScout platform provides support for approximately 87% of NIST 800-171 technical controls.[5] (See diagram 1.)

Table 1 shows the value ForeScout can deliver to existing DiD solutions to address the 800-171 controls. This is just a sample.[5]

Continuous Compliance – The Architecture

The cornerstone of continuous compliance is continuous visibility. The Continuous Diagnostics and Mitigation (CDM) program established by Congress is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

Control Family	Control(s)	Control Summary	ForeScout Solution
3.1 Access Control	AC-17(1)	Automate the monitoring and control of remote access sessions to ensure device and activity compliance while also detecting potential cyberattacks.	ForeScout has the ability to monitor and control remote access including VPN, WLC and MDM integrations. Consider a new employee connecting to the network with missing patches: • ForeScout assesses the newly connected device and detects that there are missing patches. • ForeScout proactively opens a ticket with the service desk, alerting them of the issue. • ForeScout sends a request to the patch management solution to update the device. • ForeScout verifies the connection is compliant and closes the incident automatically, helping to ensure remote connections are compliant and secure at all times.

Control Family	Control(s)	Control Summary	ForeScout Solution
3.4 Configuration Management	CM-7, CM-7(1, 4, 5)	Ensure system configuration is set to "least functionality," requiring periodic review, including software whitelisting/ blacklisting.	ForeScout collects and shares its asset intelligence with configuration management solutions, helping to ensure any gaps are filled. ForeScout also reads configuration data from configuration management solutions to compare against the running configuration of that endpoint in the field. Any deltas between the two can be immediately addressed by alerting the service desk via a ticket or alert, or resolving simple configuration issues automatically (for example, by installing a missing third-party agent). ForeScout can also assist with software whitelisting and blacklisting solutions, thus providing valuable asset information to third-party solutions while augmenting their functionality through our automated control actions (quarantine, software scanning and removal, third-party agent hygiene, etc.)
3.4 Configuration Management	CM-2	Requires the organization to develop, document, and maintain under Configuration Control a current baseline configuration of the information system.	With our ability to collect up to 700 attributes on assets, ForeScout can share comprehensive data and update the configuration management system in real time. ForeScout can be leveraged to identify pre- and post-connect changes on the device with bidirectional support, ensuring against unapproved asset changes. When real-time visibility is a reality, configuration management systems become actionable, allowing organizations to automate compliance with their asset configuration baseline. The ForeScout platform can assist in aspects of managing an information system baseline including: • Develop – identify connected systems and current patch levels • Document – share asset intelligence with third-party solutions (for example, CMDB/ITAM) • Maintain – direct automated responses to system configurations that fall out of compliance ForeScout can augment patch and vulnerability management solutions by sharing its complete asset visibility and situational awareness to help ensure baseline configurations are maintained at all times.
3.6 Incident Response	IR-4	Requires the organization to implement an incident-handling capability that includes preparation, detection and analysis, containment, eradication and recovery.	The ForeScout platform can be leveraged via policy to alert for changes on devices and/or anomalous behavior and provide data to your SIEM, event manager, or ticketing system in real time. Our flexible approach to integration allows for many ways to proactively notify personnel when incidents occur. The benefit of using ForeScout is that you can automate responses usually done by multiple teams based off of precise policies configured to requirements.
3.11 Risk Assessment	RA-5, RA-5(5)	Requires the organization to regularly scan their environment for vulnerabilities. Additional provisions are also required for systems with privileged access, prohibiting against data leakage.	ForeScout provides strong integrations with vulnerability management solutions, enabling them to react in real time when needed. This is accomplished by continuously monitoring the configuration of a ForeScout-monitored environment and alerting scanners immediately when an issue arises. This includes invoking scans for newly connected devices or connected devices that fall out of compliance. The benefit to an organization is that their risk posture is always maintained, as opposed to being on a schedule.

Table 1: *ForeScout value for select controls.*

Federal contractors and subcontractors subject to 800-171 may implement the guidelines of CDM within their own networks by conducting ongoing assessments and remediation throughout an asset's connection lifecycle. Here is an example of how this works:

ForeScout delivers continuous compliance management in two phases (see diagram 1):

Phase 1: Our platform shares endpoint intelligence with existing security and IT management solutions. This provides near-term value that greatly helps organizations move from a reactive to a proactive posture with cyber-incident management.

Phase 2: ForeScout SmartConnect™ provides pre- and post-connect assessment and protection for connected devices. The SmartConnect solution adheres to the principle of protecting the "connection lifecycle" (connect, work, disconnect) of endpoints. Its pre-connect approach uses dynamic ACLs or VLANs to help ensure that connecting devices are compliant. SmartConnect then performs post-connection policy checks designed to help ensure that the connected device remains compliant for the entire time of connection. Additionally, the SmartConnect solution can be extended to non-traditional devices (for example, sensors, cameras, bodywear), which often are the on-ramps to traditional computing environments.

Continuous Compliance – The Process

ForeScout agentlessly detects devices as they connect to the network, automates simple and repeatable tasks and infuses those elements into existing IT security and management services. As a result, it can illuminate blind spots and improve process workflow automation. ForeScout elevates your security strategy above traditional point-in-time security models (visibility through snapshots) to a Continuous Compliance Management program, providing ongoing assessment and remediation for the endpoint's connection lifecycle.

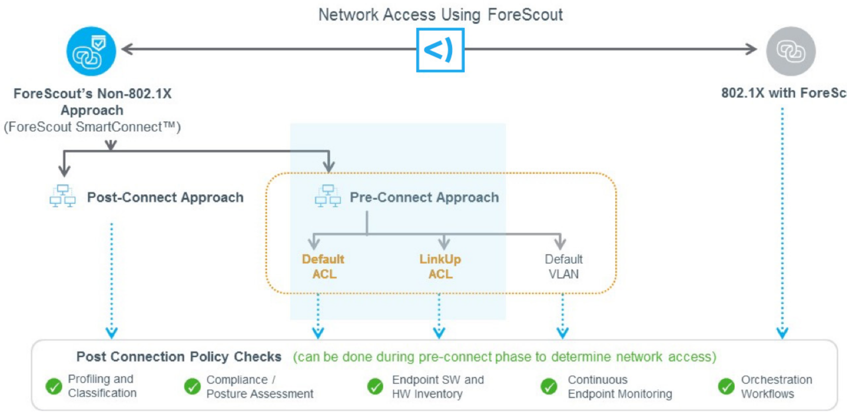

Network Access Using ForeScout
ForeScout's Non-802.1X Approach (ForeScout SmartConnect™)
802.1X with ForeScout
Post-Connect Approach
Pre-Connect Approach
Default ACL
LinkUp ACL
Default VLAN
Post Connection Policy Checks
(can be done during pre-connect phase to determine network access)
Profiling and Classification
Compliance / Posture Assessment
Endpoint SW and HW Inventory
Continuous Endpoint Monitoring
Orchestration Workflows

Diagram 2: *Protecting network access.*

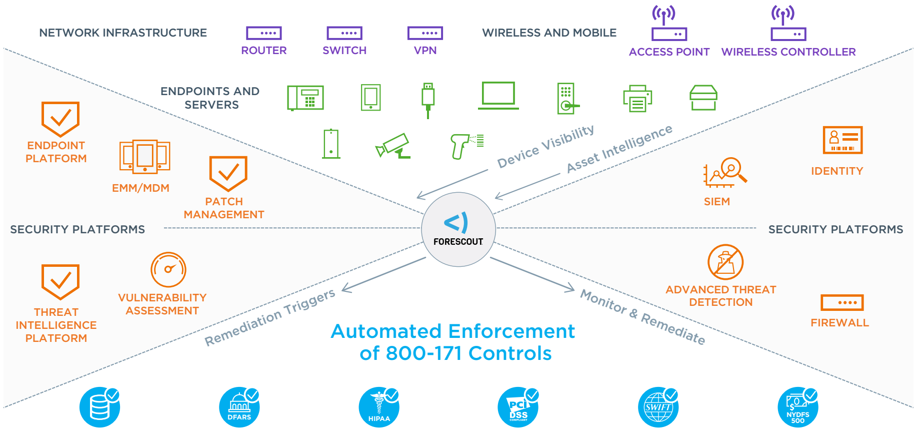


Diagram 3: *Transforming existing DiD solutions to continuous compliance management solution.* (This graphic will be updated to reflect a more dynamic approach to Orchestration)

ForeScout continuously inspects endpoints during the connection lifecycle. According to IDC, ForeScout can help an organization see approximately 25 percent more devices than previously known.[6]

Learn More

[Accelerate and Maintain NIST Compliance Solution Brief](#)

[Network Access Control Solution Brief](#)

ForeScout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional endpoints, IoT devices and operational technologies 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 December 31, 2017 more than 2,700 customers in over 80 countries improve their network security and compliance posture with ForeScout solutions. See devices. Control them. Orchestrate system-wide threat response. percent more devices than previously known.

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

[1] U.S. Air Force Breach: https://www.upguard.com/blog/us-airforce-suffers-massive-data-breach
[2] The Hacks that left us exposed in 2017: http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html
[3] Army data leak: https://www.upguard.com/breaches/cloud-leak-inscom
[4] DFARS 252.204 text: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm
[5] ForeScout addresses these controls fully or partially depending on architecture, applications and dependencies. Contact your ForeScout Sales team for a full list of 800-171 controls that ForeScout can support.
[6] IDC Business Value of ForeScout: https://www.forescout.com/idc-business-value/