Solution Brief

Strengthening Campus Security and Compliance with ForeScout

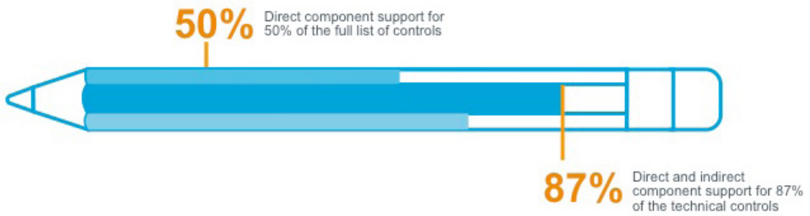
Preserve federal funding for research and financial aid with strong security measures

Higher Education institutions face a constant struggle to comply with regulations while fending off increasing numbers of attacks. And, of course, the stakes are high since non-compliance or a significant data breach can result in loss of valuable federal funding.

In July 2015, in a Dear Colleague Letter, Department of Education leadership reminded institutions of their obligations to protect student data accessed and used under Title IV of the Higher Education Act of 1965.[1] More recently, the Department of Education advised institutions to "ensure the appropriate long-term security of certain Federal information in the possession of institutions" by following the recommended requirement of NIST Special Publication 800-171. The Department further strongly encouraged institutions that fall short of NIST standards to "assess their current gaps and immediately...design and implement plans in order to close those gaps using NIST standards as a model."[2]

The Additional Challenge

For research universities there is additional pressure to comply with NIST 800-171. The Department of Defense (DoD), through the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204.7012, requires colleges or universities with government research contracts to protect the confidentiality of Controlled Unclassified Information (CUI), which may include financial information, genetic data, research data and other forms of unclassified information.[3] Non-compliance with 800-171 can result in losing valuable federal funding for research and potentially losing financial aid.



Business Challenges

- Changing regulatory compliance requirements
- Balancing the need to collaborate with mandates to protect data
- Improving overall network security
- Demonstrate and maintain DFARS compliance

Technical Challenges

- Keep targeted attacks from stealing CUI data or forcing network downtime
- Discover connected devices, including BYOD, and identify levels of compliance
- Prevent infected or non-compliant devices from spreading malware
- Measure effectiveness of security controls and demonstrate compliance with 800-171
- Orchestrate unified, automated device remediation and threat response capabilities

ForeScout addresses 87% of NIST 800-171 technical controls.[4]

One of the nation's top academic medical centers is the hub of a large university's patient care, health research, teaching and community outreach missions. The Center supports research and medical schools separate from the university.

The ForeScout platform provides the medical center with:

- Comprehensive monitoring and control over network connections and usage of devices ranging from smartphones and tablets to heart monitors, medical kiosks and ultrasound machines
- An unobtrusive inspection and granular, policy-based enforcement of all devices requesting access to, or currently accessing, network resources
- Help to realize greater IT resource savings through continuous monitoring, intelligence and informed response

The ForeScout platform simplifies 800-171 implementation and DFARS compliance efforts by automating and accelerating device discovery—helping to reduce overall risk and maintain and demonstrate ongoing compliance. The benefits can be improved IT operations through continual compliance management, reduced costs through automation and fewer audit findings, and ultimately, fewer breaches caused by unmanaged or unaccounted-for assets in your environment.

Using ForeScout and 800-171 to help bring simplified, continuous compliance to your campus

In December 2017, the Health Sciences Center of a Tier 2 University reported unauthorized access to folders containing Medicaid patient billing information. The breach involved access to a network server containing the data of over 279,000 individuals.[5]

NIST 800-171 establishes a well-defined structure for protecting the confidentiality of CUI by first providing *basic security requirements* that are fundamental to protecting confidential information and systems.[6] That same directive provides *derived security requirements,* which are a subset of the NIST 800-53 rev. 4. Non-federal organizations must also "describe in a system security plan, how the specified security requirements are met or how organizations plan to meet the requirements."

Simplifying Compliance

ForeScout helps to simplify your NIST 800-171 implementation and compliance management efforts by:

1. Helping to account for missing or hidden assets on your networks so they are accounted for.
2. Automatically and continually checking the endpoint compliance posture and taking action (for example, open a ticket, send an email alert, request a patch update, etc.) necessary to bring the device back into compliance.
3. Infusing ForeScout asset intelligence and task automation capabilities into your existing IT security and management solutions, improving their scope of coverage, and moving from task automation to process workflow automation.

Continuous Compliance

Continuous compliance with 800-171 starts with knowing the devices that connect to your campus networks, regardless of platform and type. This includes traditional systems such as servers that contain student registration data, learning management sytems and financial databases as well as non-traditional IoT devices. Segmenting and protecting sensitive systems and networks by enforcing effective access control policies is the next step. Finally, orchestrating across your existing security products to provide seamless and real-time response to potential threats to student and patient data provides the path to continuous compliance. The cycle is then repeated. Table 1 highlights the key controls behind automated and continuous compliance with 800-171 in three primary use cases for campus InfoSec personnel, and how the ForeScout platform supports these controls.

Use Case	NIST 800-171 Control	How ForeScout Helps
Configuration Management According to an ECAR, 2016 study, the volume and diversity of devices that connect to campus networks are increasing:[7]	NIST 800-171 3.4.1 and 3.4.2: Establish baseline configurations and inventories of systems	The ForeScout platform's policy-based workflow agentlessly monitors endpoints against approved baseline configuration elements. ForeScout can also report existing configurations and changes to the baseline configuration in real time. This provides immediate feedback to the organization of systems that are compliant to the baseline and any assets that need attention.
Media Access Campus network access control (NAC) solutions must manage the corporate- and employee-owned devices you know of as well as the increasing numbers of unauthorized, "under-the-radar" devices you don't know and peripheral devices that can be used to steal data.	NIST 800-171 3.8.2: Limit access to CUI on system media to authorized users.	You can leverage ForeScout to enforce digital access based off of policies inherent to the platform. ForeScout can see external/removable hard-disk drives, and flash drives and can either allow or deny access in real time.
Incident Response Campus Security Operations Centers must not only provide safeguards that ensure inappropriate access to campus networks is swiftly identified, but must remediate and report breaches within 72 hours.	DFARS ((7012-c (1)(ii)) NIST 800-171 3.6.1 and 3.6.2: Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery and user-response activities, and provides mapping to the relevant security controls that address incident-handling, monitoring and reporting techniques.	You can automate responses and notify personnel of breaches across multiple teams through ForeScout's ability to detect changes on devices and anomalous behavior in real time. This data is provided to your SIEM or integrated with your applications.

Table 1: *Use cases of how ForeScout addresses continous compliance with 800-171.*

See The ForeScout platform offers the unique ability to see devices the instant they connect to your network, without requiring software agents or **prior** knowledge of the devices. It sees devices other products may simply be unable to, such as smartphones, tablets, laptops and other corporate-owned and personal mobile devices as well as Internet of Things (IoT) devices. ForeScout's Device Cloud now includes 3+ million devices from more than 500 customers for crowd-sourced IoT device insight, and enables auto-classification of enterprise devices.

Control Unlike systems that tag violations and send alerts to IT and security staff, ForeScout enforces network access control, endpoint compliance, mobile device security and threat control, in one automated system. As a result, students, faculty, administrative staff, contractors and guests can access the appropriate campus network resources without compromising security. In addition, the ForeScout platform continuously monitors devices on your network and improves the effectiveness of your security policies so you can demonstrate compliance with 800-171 and the DFARS regulation.

Orchestrate ForeScout integrates with more than 70 network, security, mobility and IT management products* via ForeScout Base and Extended Modules. This ability to orchestrate information sharing and operation among myriad security tools allows you to:

- Share context and control intelligence across systems to enforce unified network security policies
- Reduce vulnerability windows by automating system-wide threat response
- Gain higher return on investment (ROI) from your existing security tools while saving time through workflow automation

Campus Network Access Control (NAC)

ForeScout offers comprehensive NAC capabilities based on real-time visibility of devices the instant they access the campus network (NIST 800-171 3.4.1 and 3.4.2). It continuously scans the network and monitors the activity of known, company-owned devices as well as unknown devices such as personally owned and rogue endpoints. And it lets you automate and enforce policy-based network access control, endpoint compliance and mobile device security. In fact, ForeScout provides an extensive range of automated controls that help preserve the user experience and help keep business operations running to the maximum extent possible.

Share Context and Automate Security Workflows

ForeScout Extended Modules for Next-Generation Firewalls (NGFWs) enable IT teams to orchestrate dynamic network segmentation and create context-aware security policies within next-generation firewalls based on continuous device monitoring and extensive endpoint insight from the platform. ForeScout's Extended Module for Splunk provides IoT classification and assessment context to SIEMs for incident correlation and prioritization. Combined solutions from ForeScout and Palo Alto Networks® or Check Point® Software are designed to detect advanced persistent threats (APTs) and indicators of compromise (IOCs). The Extended Modules feed user ID information into the NGFWs as well as exact classifications of actual devices for automated policy enforcement and threat response (NIST 800-171 3.6.1 and 3.6.2).

Successfully implementing 800-171 Access Control with ForeScout

With visibility into devices connected to the network, the ForeScout platform provides direct component support for over 50 of the 109 NIST 800-171 controls and supplemental support across over 90 controls.[4] 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—illuminating blind spots and improving process workflow automation. This functionality also helps comply with regulations such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and potentially many others that affect higher education institutions.

Learn More

Continuous Compliance White Paper

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.

*As of December 31, 2017
[1] Dear Colleague Letter: July 29, 2015: https://ifap.ed.gov/dpcletters/GEN1518.html
[2] Dear Colleague Letter: July 1, 2016: https://ifap.ed.gov/dpcletters/GEN1612.html
[3] DFARS 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting": https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012
[4] ForeScout addresses these controls fully or partially depending on architecture, applications and dependencies. For a complete list of controls supported by ForeScout, please contact your account team or visit www.forescout.com/products/counteract/control/.
[5] 'Hacking Incident' Impacts Nearly 280,000 Medicaid Patients: https://www.healthcareinfosecurity.com/hacking-incident-impacts-nearly-280000-medicaid-patients-a-10587
[6] NIST Special Publication 800-171 rev. 1: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
[7] ECAR Study of Undergraduate Students and Information Technology, 2016: https://library.educause.edu/-/media/files/library/2016/10/ers1605.pdf

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