# Visibility Platform for the Connected Campus

## See and control across your higher education campus

Today's institutions of higher learning are collaborative by nature and open by necessity. The connected campus is key to student success and the higher-education mission. However, device sprawl, the massive growth in BYOD and IoT devices, and the convergence of traditional IT and operational technology (OT) networks place new challenges on security teams, operational staff and budgetary resources.

In today's colleges and universities, IT security staff must be able to see devices as they connect to the campus network and ensure they are secure, regardless of their location in the classroom, lab, data center or cloud. The ForeScout platform identifies and secures these devices, without agents, and can help ensure that if they are connected, they are compliant and secure.

### The Challenge:

To minimize risk, you have to be able to see what is on your network. Today's campuses are smart cities with sports venues, retail centers and police forces. That includes everything from students' laptops and smartphones to IoT and OT devices, systems within campus police departments and athletic facilities, and much more. They are giant repositories of personal, financial, and often, protected medical data.

Students connect an average of four to six devices to the network, ranging from laptops to gaming systems. IoT devices in the form of security cameras, vending machines and security access systems present a unique and expanding challenge. And unknown or preauthorized visitors connecting pose additional challenges about the right approach to managing risk balanced against the needs of students, faculty, staff and the institution as a whole.

Information security remains a high priority for institutions of higher learning. For the third straight year it ranks number one on the Educause Review's Top 10 IT Issues.[1] As new devices connect to campus networks, the attack surface continues to evolve and expand. Breaches in the education sector jumped 103 percent in the first half of 2017 compared with the last half of 2016.[2] In addition, regulatory standards such as PCI DSS for retail devices, HIPAA for medical devices and data, and NIST 800-171 for environments supporting U.S. federal government security requirements continue to pose challenges for institutions. In fact, non-compliance or a significant data breach can result in the loss of federal research funding and student aid, as well as significantly damage the school's reputation.

**Organizational Challenges**

- Developing a risk-based security strategy that keeps pace with security threats and challenges
- Data management and governance: Protecting personal, financial and healthcare data
- Ensuring regulatory compliance with PCI DSS, HIPAA, NIST, DFARS and other mandates
- Securely accommodating visitors and students using multiple devices each day
- Student-centered institution: Advancing technology's role in defining the student experience on campus

**Technical Challenges**

- Automating endpoint discovery and classification for BYOD, IoT and OT devices
- Streamlining BYOD onboarding
- Classifying agentless IoT devices and laboratory equipment
- Dynamically segmenting devices based on real-time device insight
- Automating hardware and software inventory and reporting
- Reducing the need for system reimaging and downtime due to malware
- Discovering and profiling operational technologies without disrupting network access
- Successfully implementing 800-171 access control
- Preserving investment in infrastructure and tools

> **The Visibility that the ForeScout Platform has given us into our network and security has been a game-changer.”**
>
> — Troy Thomason, Director, Networks and Operations, Rollins College

## The ForeScout Solution

There is a platform to automate detection and control of devices connecting to your institution’s networks. ForeScout’s device visibility platform lets you see the diversity of the devices connecting and the risk they pose to your environment. Using the ForeScout platform enables a more comprehensive understanding of risk and the subsequent ability to control or deny access based on the threat a device poses to your institution.

Here’s How:

**See:** ForeScout is Transforming Security through Visibility™ in higher education by providing in-depth visibility using a combination of active and passive monitoring techniques to discover devices the instant they connect to the network—without requiring agents. The ForeScout platform classifies and assesses these devices and virtual instances, then continuously monitors them as they come and go from the network. For example, when students return from break and connect to the campus network, ForeScout can see if any new applications have been installed on their devices and determine if they present a threat to the institution.

**Control:** Once each device on the campus network is discovered and its purpose is understood, the ForeScout platform can enforce a broad range of host and network controls. You can restrict access of non-compliant devices or quarantine a device based on anomalous behavior and notify its owner of a security concern. If a student device, new lab equipment or a building security system accesses parts of the network it’s not allowed to, ForeScout can deny that access and can automatically execute a range of responses depending on the severity of the transgression. Minor violations might result in a warning message sent to the student or device owner. Faculty and staff who bring their own devices can be redirected to an automated onboarding portal.

Serious violations could result in actions such as blocking or quarantining the device, reinstallation of a security agent, re-starting of an agent (such as third-party antivirus or encryption software) or process, triggering the endpoint to retrieve an operating system patch, segmenting to a more secure VLAN, or performing other remediation actions.

**Orchestrate** ForeScout extends agentless visibility and control capabilities to leading network, security, mobility and IT management products via ForeScout Extended Modules. For example, integration between the ForeScout platform and an institution’s Enterprise Mobility Management (EMM) solution can ensure devices connecting to the network belong to students, if required. ForeScout can dynamically share endpoint device identity, configuration and security details with an institution’s other security and management systems. This bi-directional data exchange strengthens institutional intelligence and adds to the overall properties that can be applied to the rules engines of other tools, enhancing policies and actions.

## Use Cases:

The ForeScout device visibility platform discovers devices as they connect to the campus network, helping to ensure they are compliant with your institution’s policies and securing IT and OT networks as they converge. Here are a few common use cases:

> **“We were totally blind as to what systems and devices were live on the network. Today we know what’s on our network—including IoT devices. The ForeScout platform classifies the device and slips it onto the appropriate VLAN segment.”**
>
> — Ken Compres, Senior Network Security and Integration Engineer/CSO, Hillsborough Community College

**Asset Management:** It can be an arduous task to maintain an accurate, up-to-date hardware and software inventory, including current configurations and OS patching status of devices across a distributed campus environment. The ForeScout platform provides a real-time inventory and security assessment of devices as they come and go from your campus network to illuminate blind spots that periodic scanning tools miss. In addition, the platform shares rich contextual data with operations staff, help desk personnel and third-party ITAM tools such as ServiceNow®.

**Network Segmentation:** The ForeScout platform can assess and segment devices on the fly using real-time device context. Administrative personnel, accounting departments and instructors can be placed onto secure network segments that are invisible to even the most curious computer science graduate students. Student gaming consoles can be isolated to operate in their own specific VLAN segments, and students and visitors with non-compliant devices can be limited to Internet-only access. Likewise, IP-connected laboratory and research equipment can be placed in secure networking zones, and building access systems, HVAC systems, surveillance cameras and other IoT devices can safely operate and be continuously monitored within secure network segments where compromised devices are contained to limit potential damage or lateral movement within the network in the event of a cyberattack or other malicious activity.

**Regulatory Compliance:** The ForeScout platform provides real-time controls and automated reporting to support your efforts in demonstrating regulatory and policy compliance for PCI DSS, HIPAA, NIST, DFARS and other mandates. To support compliance initiatives, ForeScout can automatically identify devices and determine their compliance status, grant full access if the device is compliant and the person’s role justifies their access attempt, and allow or deny access based on device compliance posture and user authorization.

**Securing IT and OT Networks:** While industrial equipment needs to be secured, these devices are not uniformly ready for active interrogation or authentication by security solutions without risking disruption. The solution is to first establish the visibility of all devices on OT networks in a passive manner. Next, selectively enable OT, IT and IoT assets that can submit to active security interrogation techniques. By deploying the ForeScout platform, it is now possible for organizations to gain visibility and control of IP-based devices using passive discovery and monitoring techniques—without impacting performance of the OT network.

These use cases are just a few of the challenges ForeScout can help you address in efforts to bring about a more secure and efficient institution. The ForeScout platform can also extend visibility, control and orchestration across cloud environments, automate guest access enrollment and control, accelerate threat detection and response, and provide secure mobility of employee-owned devices.

## Learn more:

Campus Compliance Solution Brief

Hillsborough Community College Case Study

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] https://er.educause.edu/articles/2018/1/top-10-it-issues-2018-the-remaking-of-higher-education

[2] https://campustechnology.com/articles/2017/09/20/education-data-breaches-double-in-first-half-of-2017.aspx