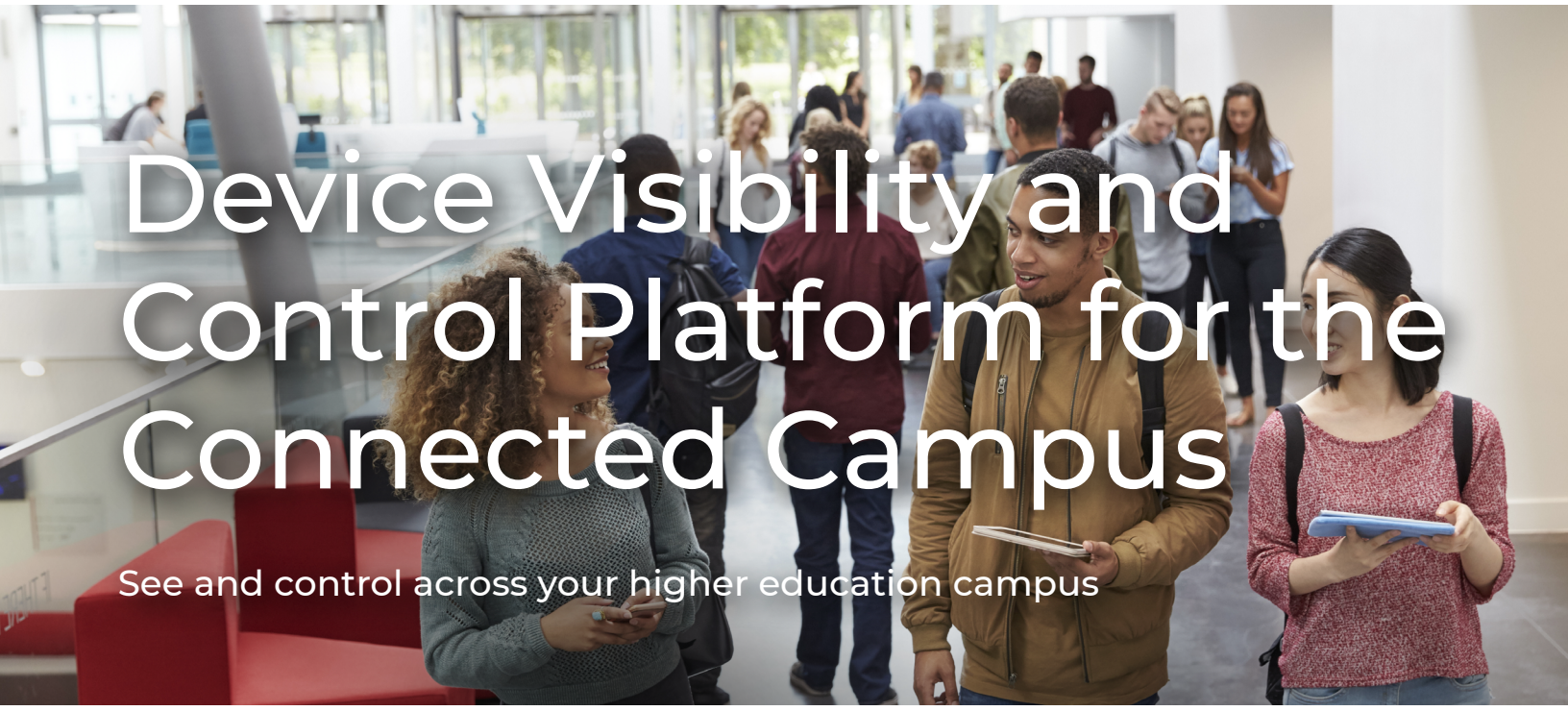
FORESCOUT



Device Visibility and Control Platform for the Connected Campus

See and control across your higher education campus

> "The visibility that the Forescout platform has given us into our network and security has been a game-changer."
>
> **–Troy Thomason, CIO and Assistant Vice President of Information Technology, Rollins College**

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. That includes everything from students' laptops and smartphones to IoT and OT devices, systems within campus police departments and athletic facilities, and much more. Today's campuses are giant repositories of personal and financial data—and sometimes even 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 when it comes to balancing risk against the needs of students, faculty, staff and the institution as a whole.

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 NIST 800-171 access control
- Preserving investment in infrastructure and tools

Information security remains a high priority for institutions of higher learning. For the fourth straight year it ranks number one on the EDUCAUSE Review's Top 10 IT Issues.[1] Nearly three-quarters of cybersecurity incidents in education are motivated by the possibility of financial gain, and one in five attacks on educational institutions are motivated by espionage, often targeting sensitive research, according to Verizon's 2018 Data Breach Investigations Report.[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, noncompliance 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.

The Forescout Solution

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. It serves as the common thread that binds security infrastructure together and unifies security management.

Here's how:

Absolute Device Visibility: Agentless discovery and classification in real time plus continuous posture assessment equals accurate situational awareness.

- **Discover** every physical and virtual device across campus, data center, cloud and industrial environments
- **Classify** diverse IT, IoT and OT/ICS devices in real time using passive-only profiling techniques that don't disrupt critical business processes, affect system uptime or introduce operational risk
- **Assess** and continuously monitor compliance of all devices without requiring agents or active interrogation

Automated Control: Use accurate situational awareness to automate policy-based controls and orchestrate actions.

- **Conform** with policies, industry mandates and best practices such as network segmentation
- **Restrict**, block or quarantine noncompliant or compromised devices
- **Automate** endpoint, network and third-party control actions to boost productivity, eliminate security management silos and accelerate incident response

Use Cases

The Forescout visibility and control 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:

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 ITSM tools such as ServiceNow® to boost operational productivity.

Incident Response: The Forescout platform can reduce the risk of business disruption from security incidents or breaches through automated response actions that also reduce related costs. According to Ken Compres, Senior Network Security and Integration Engineer/CSO, Hillsborough Community College, "With Forescout, our need to reimage infected computers dropped from 20 to 25 per month to just 1.5. When you consider staff resources and user downtime, that's a 240- to 300-hour productivity gain each month."

Network Segmentation: The Forescout platform can assess and segment devices on the fly using real-time device context. Administrative personnel, accounting departments and faculty 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 noncompliant 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.

*Notes

1. https://er.educause.edu/articles/2019/1/top-10-it-issues-2019-the-student-genome-project#issue1
2. https://www.verizon.com/about/news/ransomware-still-top-cybersecurity-threat-warns-verizon-2018-data-breach-investigations-report

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

© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 06_19