Case Study

FORESCOUT

Liverpool John Moores University

British University Encourages Innovation and Boosts Security with Secure, Segmented Network Access

HOURS
to achieve enterprise visibility

$4M
projected 3-year savings in IT cost reductions

MINUTES
to quarantine noncompliant devices

LIVERPOOL JOHN MOORES UNIVERSITY

Industry
Education

Environment
21,000 wired and wireless devices—including 6,000+ IoT devices—across three campuses, 25 buildings; 3,500 employees and 22,000 students.

Challenge

- Encourage innovation while improving security
- Secure network access with very limited resources
- Prevent malware infections from BYOD systems
- Segment devices to restrict access to authorized areas or functions only

Security Solution

- Forescout platform

Overview

Liverpool John Moores University (LJMU), a public research university in Liverpool, England, struggled with how to provide an open, bring-your-own-device (BYOD) IT environment that promotes innovation yet does not compromise security—and do so with very limited resources. The university's existing network access control (NAC) solution helped to some degree but it didn't provide the level of granularity that LJMU needed to allow all types of devices, including thousands of IoT devices, onto the network with confidence. By replacing its NAC product with the Forescout platform, the university gained real-time visibility of all IP-connected endpoints and the highly granular, role-based access it needed to secure devices across its multiple wired and wireless networks. It is also reaping significant operational and business value.

Business Challenge

"Researchers are used to buying their own IT equipment and plugging it into their lab. To support innovation, we need to provide the right level of access to such devices without compromising other university systems…With only two people managing network connectivity for 22,000 students and 3,500 staff, it's critical that we have the right tools."
— John Cannon, Network Manager, Liverpool John Moores University

As at other public research universities, professors and students at Liverpool John Moores University have come to expect and highly value a "permissive" IT environment. In addition to its 4,500 corporate Windows PCs, the university has over 6,000 non-managed endpoints, including a broad spectrum of IoT devices — everything from CCTV equipment, cookers, point of sale devices, printers, HVAC systems, robots and web cameras to a CPR mannequin—all of which pose a cyber risk.

Use Cases

- Device visibility
- Network access control
- Network segmentation
- Device compliance

Results

- Rapid time to value—enterprise visibility within hours
- High degree of confidence regarding what is connected to the network
- Granular enough control to allow researchers to use their own devices and foster innovation
- Ability to limit lateral movement to reduce attack surface
- Dynamic segmentation automatically connects devices to appropriate VLANs
- More efficient, improved device compliance and ability to quarantine noncompliant devices within minutes
- Significant ROI—$4M+ three-year savings—from risk mitigation, business productivity and IT infrastructure cost reductions

> "Such accurate, real-time visibility gives me a high degree of confidence that we know exactly what's connected to the network. That's really foundational for effective IT security."
>
> — John Cannon, Network Manager, Liverpool John Moores University

According to LJMU Network Manager John Cannon, MAC spoofing and rogue devices were of specific concern. LJMU's existing NAC product did not prevent an authorized computer in one department's lab from being moved to another area and accessing sensitive information that it should not have access to. It was also easy for a malicious actor to spoof a printer, or for an HVAC contractor to open a door into one of the university's private networks, whether inadvertently or maliciously. Limited resources compound these IT security challenges.

Why Forescout?

"Top of the Line" NAC Solution with Easiest, Fastest Deployment

To solve these network access problems, LJMU decided to search for a new solution. After evaluating several leading NAC products, the network team chose the Forescout device visibility and control platform.

"We liked that the Forescout platform was vendor-neutral and not 802.1X-focused, so we wouldn't need to worry about being locked into one vendor in a future network hardware refresh," notes John Cannon, LJMU network manager. "The agentless Forescout solution was also by far the easiest to deploy. Within hours of plugging in the appliance for the Proof of Value, we had incredible visibility. The highly granular role-based access capabilities also impressed us. We saw the Forescout platform as top of the line; it had everything we wanted."

Business Impact

Accurate, Real-Time Visibility Across the "Wild West"

"We already knew we had a 'wild west' scenario—a little bit of everything—connected to our network, but with the Forescout platform, it's now all visible," explains Cannon. "The dashboard reporting tools make it easy for me to see everything and to answer questions in minutes, such as how many Windows XP devices we have, who uses them, what apps are on them, version and configuration information, and more. Such accurate, real-time visibility gives me a high degree of confidence that we know exactly what's connected to the network. That's really foundational for effective IT security."

Highly Granular Control Provides Confidence to Allow Network Access

Highly granular control was equally important for LJMU. "Thanks to the Forescout platform's granular classification and control capabilities and context awareness, we can connect an extremely broad range of devices to our network; we can trust that their access to the network is confined to the purpose for which they were purchased," notes Cannon. "For example, a building management system should only be able to report back to the BMS server. With Forescout, every type of device can have its own policy specifying what it is allowed to do."

"For example, Forescout has allowed us to set up and enforce controls so that the network-attached storage device the biomolecular science lab purchased can only be used within that lab," adds Cannon. "It can't be used somewhere else where it could be exfiltrating data."

Dynamic Network Segmentation Adds Extra Protection

To restrict device access to LJMU's wired and wireless networks, Cannon relies heavily on the Forescout platform's ability to dynamically assign VLANs. "I use dynamic VLAN assignment to make sure that printers stay on the printer VLAN,

> "The Forescout platform has become my go-to tool for network visibility, and its impact extends well beyond NAC. It's been a tremendous help for networking and security operations and has definitely improved our security posture and reduced risk."
>
> — John Cannon, Network Manager, Liverpool John Moores University

e-point of sale devices stay on the EPOS VLAN, and so on," explains Cannon. "If a device tries to connect to the wrong VLAN, it won't work. We also make extensive use of Dynamic Access Control Lists (DACLs), applied at switch level, to control what devices can communicate with."

After proving the dynamic ACL capabilities in a test environment, Cannon deployed them site by site or VLAN by VLAN with help from a Forescout support engineer. "Before implementing segmentation, we would test its impact to see what would be quarantined when we went live, so we could proactively contact users of those systems ahead of time and ask them, 'Why are you using that Windows 7 PC?'", explains Cannon. "Doing so allowed us to reduce and predict help desk ticket volume."

Easier Device Hygiene and Compliance and BYOD Monitoring

With comprehensive, real-time visibility across endpoints, it is now much easier for LJMU network staff to keep tabs on device cyber hygiene and assign to special VLANs devices that have vulnerabilities and cannot be patched, such as audiovisual devices and other IoT equipment."

The LJMU network team uses the Forescout platform to perform real-time security posture assessments, checking on the operating system and antivirus agents including version and configuration information. (In the future, the team plans to monitor for application version compliance as well.) The team also relies on the Forescout solution to help monitor the build process as it configures and adds approximately 1,000 new PCs to the network each year. "A lot of testing and validation goes into these PCs; Forescout provides different levels of control throughout the process."

In addition to monitoring and controlling staff devices, the Forescout platform monitors student BYOD devices to provide accountability and traceability. When students log in on their own devices, they are automatically steered towards a network that provides Internet access only.

Measuring Business Value

Switching to the Forescout platform from its previous NAC solution has helped LJMU network staff reduce some of the complexity of managing network access. "The user-friendly interface of the Forescout platform makes us more efficient, and, once set up, the solution requires very little day-to-day intervention," says Cannon. "Anything that helps simplify security management helps us a lot."

"Hard metrics are difficult, but I do know the Forescout platform has become my go-to tool for network visibility, and that its impact extends well beyond NAC," notes Cannon. "It's been a tremendous help for networking and security operations and has definitely improved our security posture and reduced risk."

In an attempt to quantify the economic value of using the Forescout platform, IDC completed an extensive business value analysis from numerous interviews of Forescout customers. Cannon used the ROI tool developed from this methodology to calculate the monetary benefits for LJMU. The tool showed $145,600 first-year savings and $4 million three-year savings primarily from risk mitigation, business productivity gains and IT infrastructure cost reductions.

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