Case Study

FORESCOUT

Northern Health and Social Care Trust

Northern Trust Selects Forescout for Real-time Network Visibility and Control of Endpoints including Embedded Systems and Medical Devices

HOURS
is all it took to witness the power of the Forescout platform

CUSTOM
security policies using the Forescout platform

FASTER
incident response than ever before

Northern Health and Social Care Trust

Industry
Healthcare

Environment
15,000 endpoints spread across 150+ sites

Challenge
- Limited visibility and control of the ever-growing numbers of networkconnected devices that are neither Trust-owned nor managed

Security Solution
- Forescout platform

Overview

The Northern Health and Social Care Trust (Northern Trust) is one of five health Trusts in Northern Ireland that became operational on April 1st 2007. It provides a broad range of health and social care services across ten local council areas and includes two large acute hospitals and six non-acute hospitals. The Northern Trust provides services for a population of approximately 460,000, the largest demographic area of any Trust in Northern Ireland, and has approximately 12,000 employees. It has a rural geography, with 150+ sites connected using a range of network infrastructure technologies — from superfast broadband to high capacity short haul data circuits with a capacity of typically 100 Mbps or higher. Northern Trust's network serves approximately 15,000 endpoints.

Business Challenge

For some time, the Trust had been concerned about the limited visibility and control it had over the ever-increasing numbers of endpoints that are neither Trust-owned nor managed connecting to its network — such as medical, clinical engineering and BMS (Building Management Systems) devices. This presented a risk in terms of ICT network security and governance, as an ICT security incident could have the potential to directly impact the delivery of health and social care services to patients and clients. Northern Trust required a solution to address these issues.

Why Forescout?

During Northern Health and Social Care Trust's in-depth research into the most appropriate solution, it found the Forescout Platorm to be the only one without a dependency on additional equipment or specific software version requirements.

Use Cases

- Device visibility
- Device compliance
- Network access control
- Incident response

Results

- Comprehensive, real-time visibility of the network, including endpoints, that are neither Trust-owned nor managed, e.g. medical, clinical engineering and BMS (Building Management Systems) devices
- Real-time visibility of ~15,000 endpoints and proactive remediation to keep rogue users, devices and applications at bay
- Secure and continuous network connectivity, helping Northern Trust to deliver uninterrupted critical health and social care services
- Increased ICT security and governance controls via simple policy configuration
- Easier and faster compliance reporting, e.g. Information Governance and ISO 27001, reducing manual overhead
- More rapid internal threat identification and remediation

"We found other solutions that we considered, which compared to Forescout were quite expensive, plus they wouldn't give us the complete coverage that we needed," said Pat Black, ICT Network & Security Manager at Northern Health and Social Care Trust.

Black and his team were particularly impressed with the agentless aspect of the Forescout platform. The ability to have device visibility, security scan/profile, and to be able to run a risk assessment of everything connected to the Trust's network, without having to install anything on to the individual devices was seen as a significant benefit.

With a scope of work completed, and professional services provided by Foursys, Northern Trust arranged for Forescout's Proof of Concept (PoC) solution to be set up within Antrim Hospital, its largest acute hospital.

> "With the help of Foursys, the Forescout platform was easy to deploy, didn't need a lot of associated hardware to run, even for an organisation of our size and ticked all the boxes with regards to assessment, policy enforcement and compliance."
>
> — Pat Black, ICT Network & Security Manager, Northern Health and Social Care Trust

Business Impact

Real-Time Visibility of Managed and Unmanaged Device Types

Pat Black commented, "Within a matter of hours of the appliance being installed, we began to witness the power of the Forescout platform. The network infrastructure environment that we work within has a significant number of connected devices that are neither Trust-owned nor managed. If a device presents a security or governance risk, a decision needs to be made quickly on how to effectively manage that risk, particularly if it is a compromised medical device. Forescout has allowed us to reduce the risk associated with these non-Trust owned and unmanaged devices, and enabled us to respond to incidents and alerts more quickly than we had ever been able to do in the past."

Policy Creation and Enforcement

Northern Trust has created a range of custom security policies using the Forescout platform. Black explained, "You can leverage Forescout's solution to manage devices in many different ways. For instance, we have a number of staff who need VPN access over 3G from their corporate laptops. Endpoint protection could not block the 3G SIM when connected to the corporate network and presented a vulnerability/security risk. We easily configured a policy in the Forescout platform to block the 3G SIM whilst on the corporate network and it worked brilliantly. We wouldn't have expected this capability prior to the Proof of Concept."

Uninterrupted Delivery of Critical Health and Social Care Services

Black commented, "The approach we've been taking is to manage restrictions on connectivity such that they are at an absolute minimum, whilst maintaining

appropriate levels of security and governance. In the health sector connectivity and indeed security for medical devices, in particular, is essential in terms of uninterrupted delivery of critical health and social care services. With Forescout, we can achieve this safe in the knowledge we have visibility and, all importantly, control over most types of network connected devices."

Easier and Faster Compliance Reporting

Prior to deploying the Forescout platform, producing compliance reporting against ICT Security, ICT Governance, Information Governance, ISO 27001 and other policies and standards was time consuming for Northern Trust, as well as difficult to execute accurately. Forescout, combined with Foursys' professional services, gave a simple solution to a complex problem.

Looking Forward

Pat Black concluded, "The Internet of Things is upon us, and there is an almost exponential growth in the number of network connected devices, so this is why we arrived at the Forescout solution. With the help of Foursys, the Forescout platform was easy to deploy, didn't need a lot of associated hardware to run, even for an organisation of our size, and ticked all the boxes with regards to assessment, policy enforcement and compliance. The Forescout platform is acknowledged as an integral part of our network infrastructure and security toolset, and there is more to come, as we continue to develop our knowledge, skills and experience of using it.

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