University Hospital Southampton NHS Foundation Trust

University Hospital Southampton (UHS) NHS Foundation Trust provides services to some 1.9 million people living in Southampton and South Hampshire, plus specialist services such as neurosciences, cardiac services and children's intensive care to more than 3.7 million people in Central Southern England and the Channel Islands.

UHS is also a major centre for teaching and research in association with the University of Southampton and the Medical Research Council - UHS employs over 11,500 staff and became a Foundation Trust in October 2011.

UHS promotes the use of technology as a key enabler in delivering better patient care; either through their own award-winning informatic systems or through their procurement of leading edge IT solutions. They are recognised as one of twelve GDE (Global Digital Exemplar) NHS Trusts - NHS organisations are awarded this status for their IT thought leadership and adoption of effective technology.

The Challenge

NHS organisations are classed as 'hyper connected'; they have a high number of devices attached to their computer network, of which a significant percentage are IoT (Internet of Things) and medical devices which are targeted, and easily exploited, by cyber criminals to hold an organisation to ransom or steal valuable data, often containing patient information.

The Informatics department at UHS realised they faced an issue confronting many organisations - both within and outside of the healthcare community - whereby it is difficult to gain full visibility as to exactly what is connected to their network, the associated risk and how to mitigate the 'east-to-west' lateral movement threat from cyber exploitation.

The Solution

The team at Southampton embarked on finding a solution that addressed this challenge, and subsequently reviewed various NAC and other security solutions before settling on the Ordr Systems Control Engine (SCE).

Medical Devices

Medical devices are critical to patient care, but not always designed with security in mind.
They must be secured.

IoT Devices

IoT devices such as smart displays, fax machines, and printers can be compromised and become an attack vector.

Facilities Systems

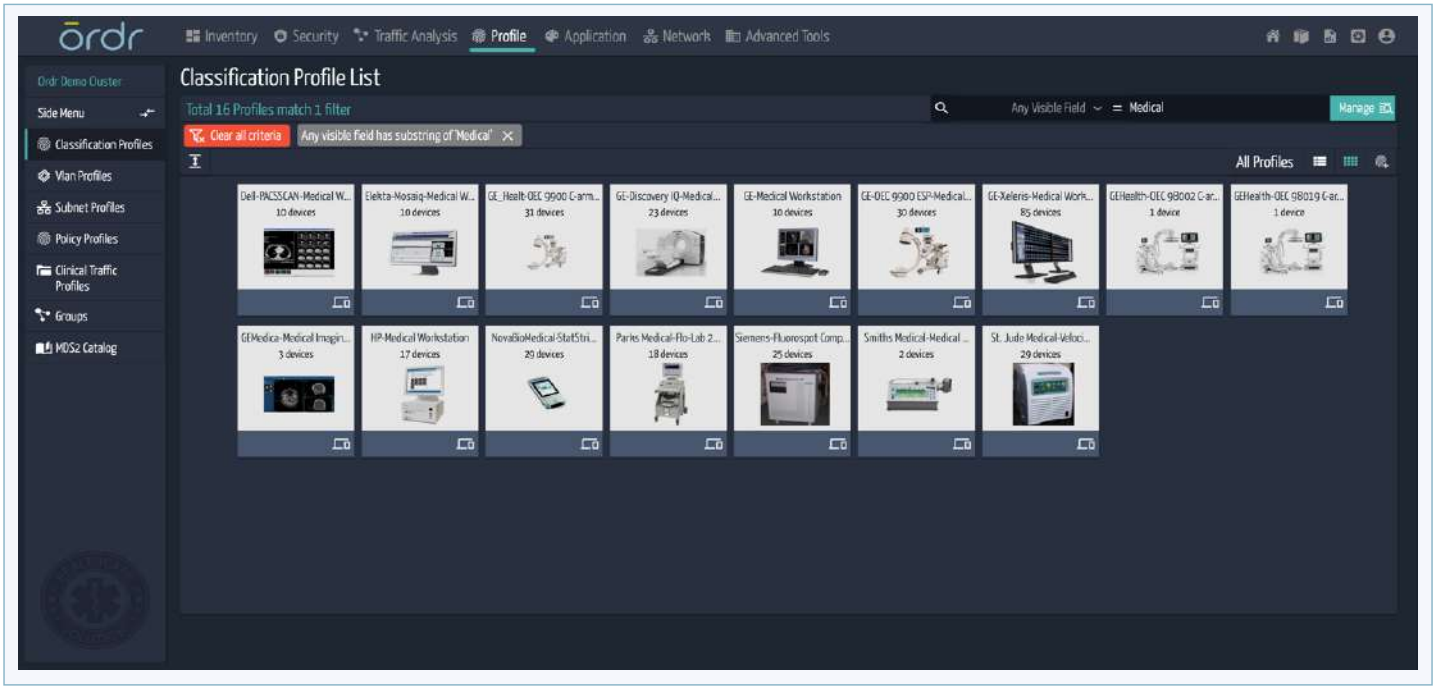
HVAC systems, elevator controls, and cameras are part of healthcareoperations and must be protected.

'We liked the simplicity of the Ordr solution coupled with its forensic level of insight. It's very intuitive and quick to install even on a network of this size, and instantly started to catalogue and risk profile every single device on our network; says Darran Lebas, the Network & IT Security Manager, 'the way it automatically classifies and then baselines the communications of all our devices is very impressive.'

UHS has deployed Ordr Systems Control Engine, with a number of small sensors connected in strategic locations feeding data back to Ordr SCE which displays all the information they require in a simple, elegant dashboard.

Using AI to dynamically profile all devices at massive scale to detect vulnerabilities, exploits, weak passwords or even medical device recalls across both wired and wireless networks, integrating with various threat feeds, including the NHS Cyber Alert (formerly CareCERT) Ordr offers UHS an unprecedented level of detail that dynamically, and in real-time, updates with each new device or event to detect rogue or anomalous behaviour instantaneously.

Once it is known what is connected and what risks each represents, Ordr SCE utilises segmentation security policies to ensure devices have the access they need while limiting exposure. By enforcing these policies on the hospital's own networking and security infrastructure, UHS is able to eliminate risks, isolate and remediate breaches, protect their entire enterprise and help to achieve Data Security and Protection (DSP) compliance.



Device Utilisation

Ordr SCE gathers real-time inventory information without touching the endpoints in a fully automated way. The SCE sees the device the moment it becomes active on the network, records operational activity, and records the time it goes offline.

Device information is gathered from type/model/modality/serial number to software information and:

- Automatically categorises devices for ease of management.
- Records devices that are connected vs in use, for how long and their activities.
- Shows real utilisation based on number of images and studies; not just time on-line.

This information is sent in real-time into the UHS asset management system to help clinical engineering staff optimise the operational efficiency of their expensive equipment so they can make data-driven decisions on capital planning and avoidance.

The Trust sees the deployment of the Ordr platform as being key in their quest to ensure the ongoing cybersecurity of their infrastructure and a vital part of the security arsenal.

'By delivering real-time device inventory, monitoring east-to-west communications and providing invaluable utilisation data, Ordr is proving to be a valuable asset to the Trust and is a critical component of our cybersecurity strategy' says Adrian Byrne, IT Director for the Trust.'

Benefits: Ordr is your single source of "truth" for device inventory, utilisation and security

Delivers the most comprehensive detection of risks and threats for all connected devices including unmanaged, IoT and IoMT devices.

Identifies devices with weak ciphers and certificates.

Identifies Manufacturer , NHS Cyber Alert and FDA recalls that impact devices in your network.

Identifies anomalous and suspicious communications to unauthorized networks and malicious sites.

Proactively remediates threats by segmenting devices to only allow "sanctioned communications".

About Ordr

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. For more information, visit www.ordr.net and follow Ordr on Twitter and LinkedIn.

About Ordr

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. For more information, visit **www.ordr.net** and follow Ordr on **Twitter** and **LinkedIn**.