CASE STUDY

SOUTHAMPTON UNIVERSITY HOSPITAL NHS TRUST

# Scaling Segmentation with Forensic-Level Intelligence

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.

## Challenges

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.

Copyright © 2025 ORDR Inc.

# Solutions

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 ORDR AI Protect for Segmentation.

### 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 healthcare - operations and must be protected.

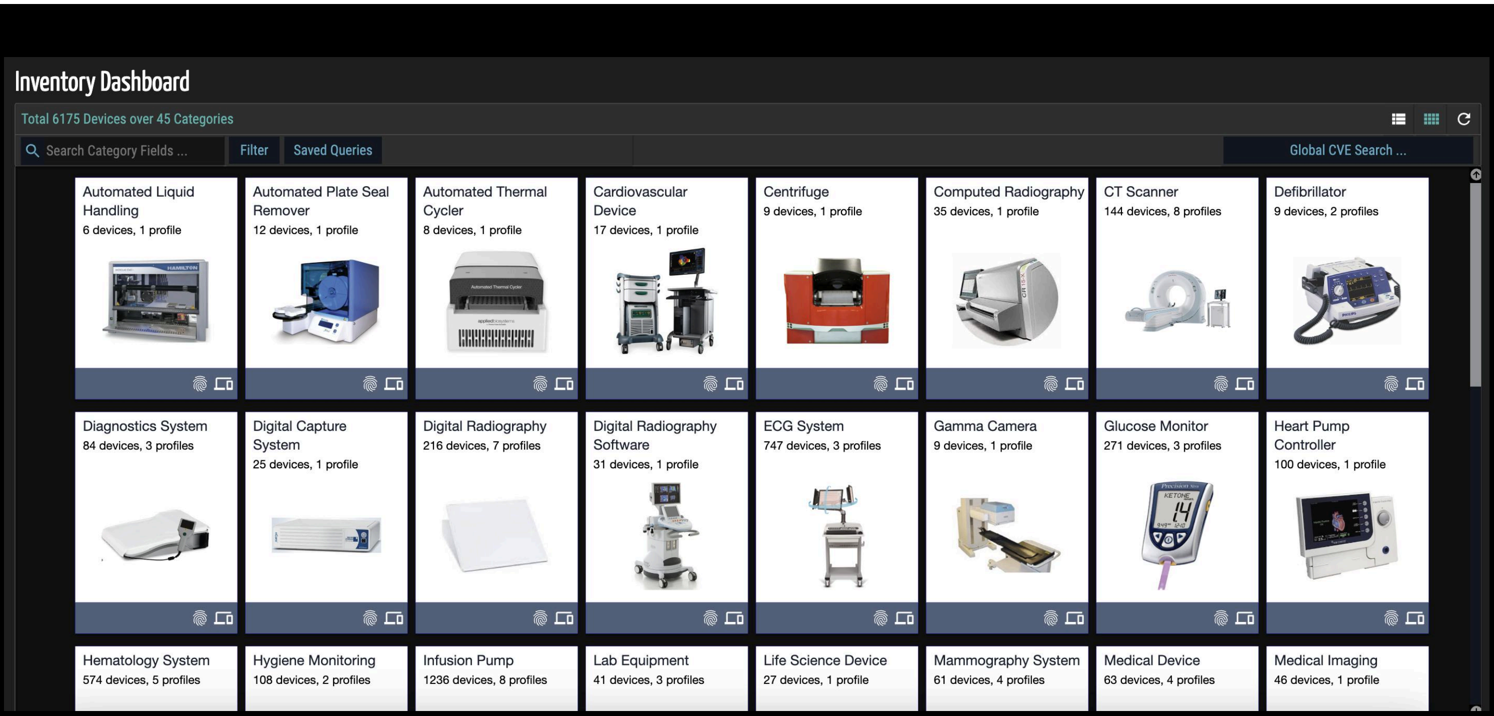
> *We liked the simplicity of the ORDR solution coupled with its forensic-level insight. It's very intuitive and quick to install—even on a network of this size—and it instantly started cataloging and risk profiling every single device on our network. The way it automatically classifies and baselines the communications of all our devices is very impressive,"*
>
> **Darran Lebas**
>
> *Network & IT Security Manager at Southampton University Hospital NHS Trust*

UHS has deployed the ORDR AI Protect platform, with a number of small sensors connected in strategic locations feeding data back to ORDR 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 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.

Copyright © 2025 ORDR Inc.



Inventory Dashboard

Total 6175 Devices over 45 Categories

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Automated Liquid Handling<br>6 devices, 1 profile | Automated Plate Seal Remover<br>12 devices, 1 profile | Automated Thermal Cycler<br>8 devices, 1 profile | Cardiovascular Device<br>17 devices, 1 profile | Centrifuge<br>9 devices, 1 profile | Computed Radiography<br>35 devices, 1 profile | CT Scanner<br>144 devices, 8 profiles | Defibrillator<br>9 devices, 2 profiles |
| Diagnostics System<br>84 devices, 3 profiles | Digital Capture System<br>25 devices, 1 profile | Digital Radiography<br>216 devices, 7 profiles | Digital Radiography Software<br>31 devices, 1 profile | ECG System<br>747 devices, 3 profiles | Gamma Camera<br>9 devices, 1 profile | Glucose Monitor<br>271 devices, 3 profiles | Heart Pump Controller<br>100 devices, 1 profile |
| Hematology System<br>574 devices, 5 profiles | Hygiene Monitoring<br>108 devices, 2 profiles | Infusion Pump<br>1236 devices, 8 profiles | Lab Equipment<br>41 devices, 3 profiles | Life Science Device<br>27 devices, 1 profile | Mammography System<br>61 devices, 4 profiles | Medical Device<br>63 devices, 4 profiles | Medical Imaging<br>46 devices, 1 profile |

## Device Utilisation

ORDR gathers real-time inventory information without touching the endpoints in a fully automated way. The ORDR platform 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.

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.

Copyright © 2025 ORDR Inc.

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

Threat Prevention

**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".

> *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,”*
>
> **Adrian Byrne**
>
> *Former long-time CIO for the Trust*

Copyright © 2025 ORDR Inc.

## About Us

ORDR is the leader in AI-powered asset risk and exposure management, trusted by top organizations across healthcare, pharmaceuticals, manufacturing, and financial services. With insights from over 100 million asset types, ORDR's platform empowers security teams to identify their biggest risks and take swift, effective action. From maintaining security hygiene to real-time threat detection and protection using microsegmentation, ORDR makes action not just possible but automated and simple — bringing ORDR to chaos.

ORDR is backed by top investors including Wing Venture Capital, Ten Eleven Ventures, Battery Ventures, Mayo Clinic Ventures, and Kaiser Permanente Ventures. For more information, visit www.ordr.net and follow ORDR on X and LinkedIn.

*For more information, visit* **ordr.net**

*Follow Ordr on*

Ready to bring ORDR to your chaos?

REQUEST A DEMO

Copyright © 2025 ORDR Inc.