Cynerio

North Lincolnshire and Goole NHS Foundation Trust Reduce IoT Risk and Achieve DSP Toolkit Compliance with Cynerio

NHS
Northern Lincolnshire and Goole
NHS Foundation Trust

Organization: North Lincolnshire and Goole NHS Foundation Trust (NLG)
Founded: 2001
Bed Count: 750
Notable: Annually care for over 135,000 emergency room patients

The Challenge

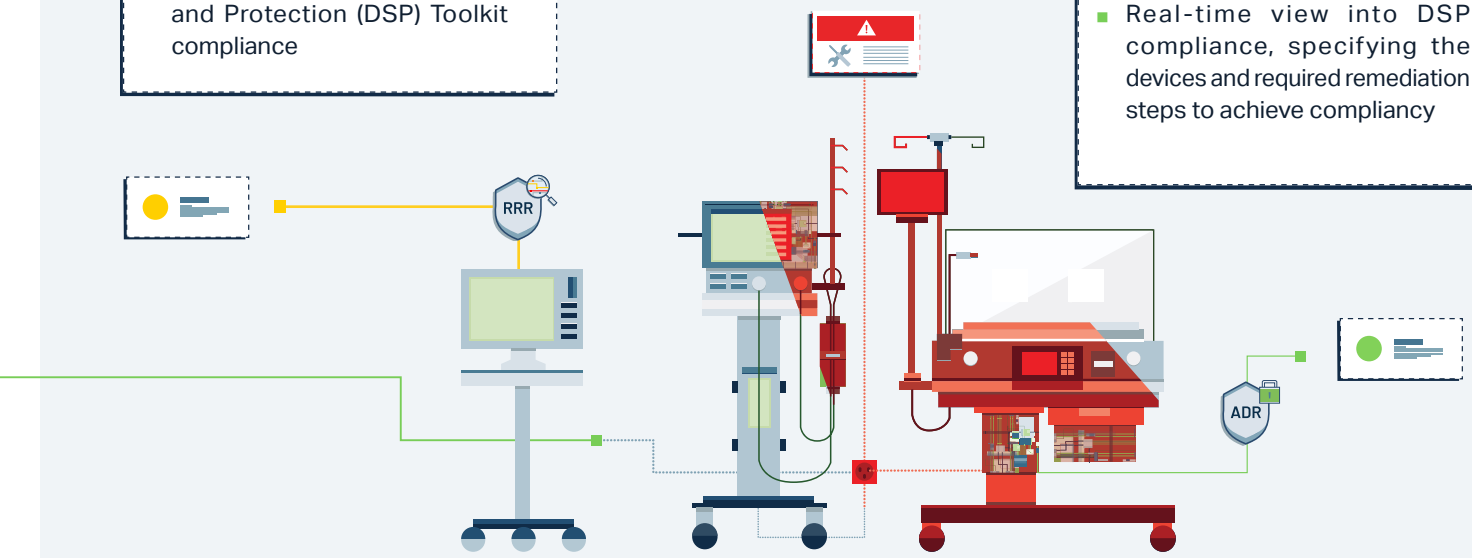
- Lack of visibility into hyperconnected IoT and IoMT environments
- IoT and IoMT out of the scope of existing IT security solutions
- Need to incorporate IoT devices within overall Data Security and Protection (DSP) Toolkit compliance

The Cynerio Solution

- **Rapid Risk Reduction (RRR)**
- **Attack Detection & Response (ADR)**

Business Impact

- Able to prioritise risk by criticality and automate mitigation at scale
- Quick identification and remediation of the vulnerabilities that enable attacks, allowing for safe micro of IoT and IoMT devices to healthcare workflows
- Real-time view into DSP compliance, specifying the devices and required remediation steps to achieve compliancy

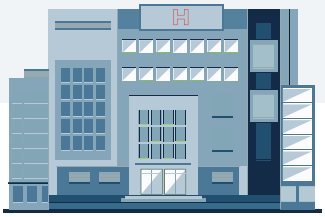


About North Lincolnshire and Goole NHS Foundation Trust

Northern Lincolnshire and Goole NHS Foundation Trust (NLaG) has hospitals in Grimsby, Scunthorpe and Goole, and provides services to a population of more than 450,000 people across North and North East Lincolnshire, East Riding of Yorkshire, East, and West Lindsey.

Every year, NLaG hospitals attend to more than 135,000 people in their emergency departments, whilst also delivering more than 4,500 babies, carrying out around 30,000 operations, and employing 6,800 staff members.

Currently, NLaG is investing over £130 million to transform the emergency departments at Grimsby and Scunthorpe as well as double its MRI and CT scanner capacity for North East Lincolnshire.

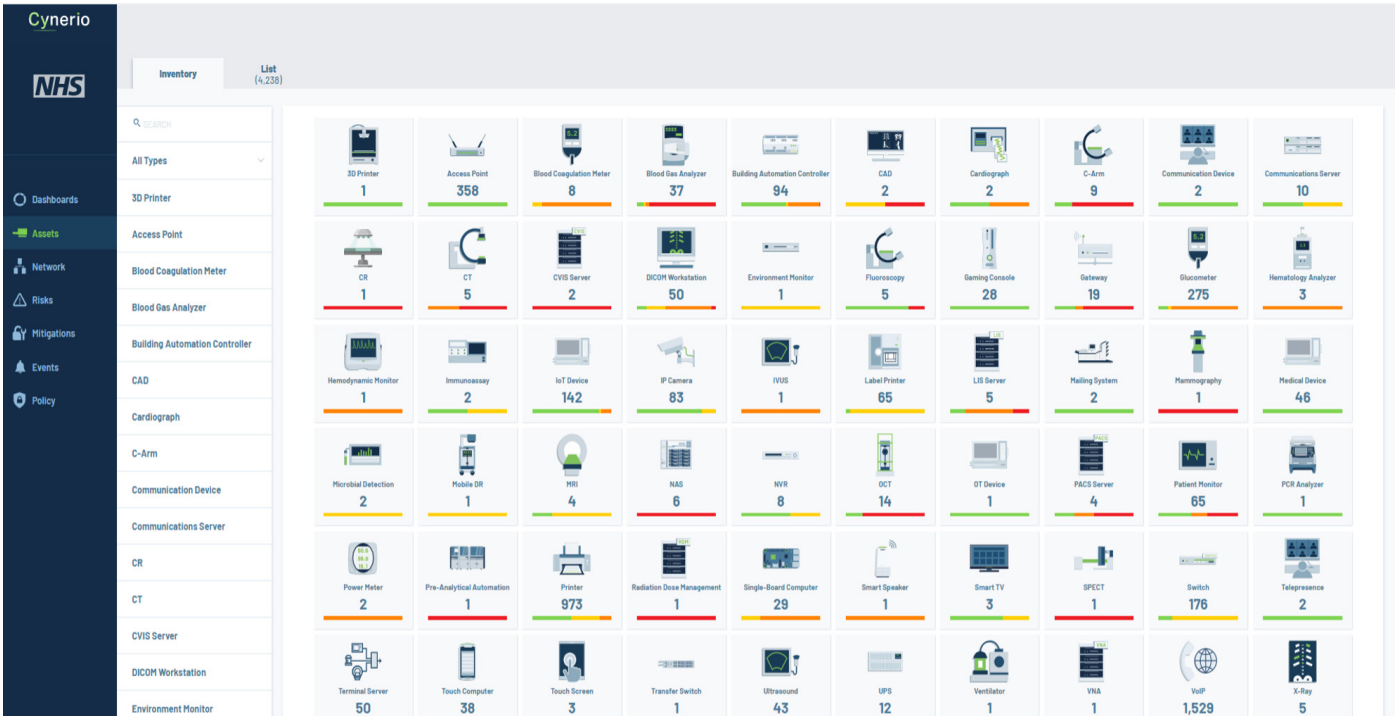


The Cynerio Solution – Proactive Healthcare IoT Risk Reduction and Remediation

NLaG recognised the inherent risks to patient safety and its operational capability as a result of its IoT and medical devices. The trust undertook an analysis, and after evaluating various technologies, **concluded Cynerio's dedicated healthcare Zero Trust and visibility solution was the best fit.**

Cynerio's Healthcare IoT cybersecurity platform automates end-to-end and continuous asset discovery and secures every connected medical, IoT and OT system without any software, agents or network scanning, prioritising devices delivering patient safety and confidentiality and without hospital service disruptions. The solution covers every threat vector with proactive and pre-emptive attack prevention tools, automated risk reduction, threat mitigation, and step-by-step remediation programs built on the NIST Zero Trust framework **to provide Rapid Risk Reduction (RRR) within healthcare IoT.**

Image: Get a bird's-eye view of all healthcare IoT and its potential risk in the Cynerio portal.



'Cynerio provides us with an unprecedented level of detail and understanding of our otherwise relatively unknown estate of IoT and medical devices, profiling risks that we would have otherwise not known about and their potential impact on our hospitals', says Tonya Fredrickson, IT Security Manager for NLaG. 'Prioritising and automating the mitigation steps to secure our environment—Cynerio is doing all the heavy lifting.'

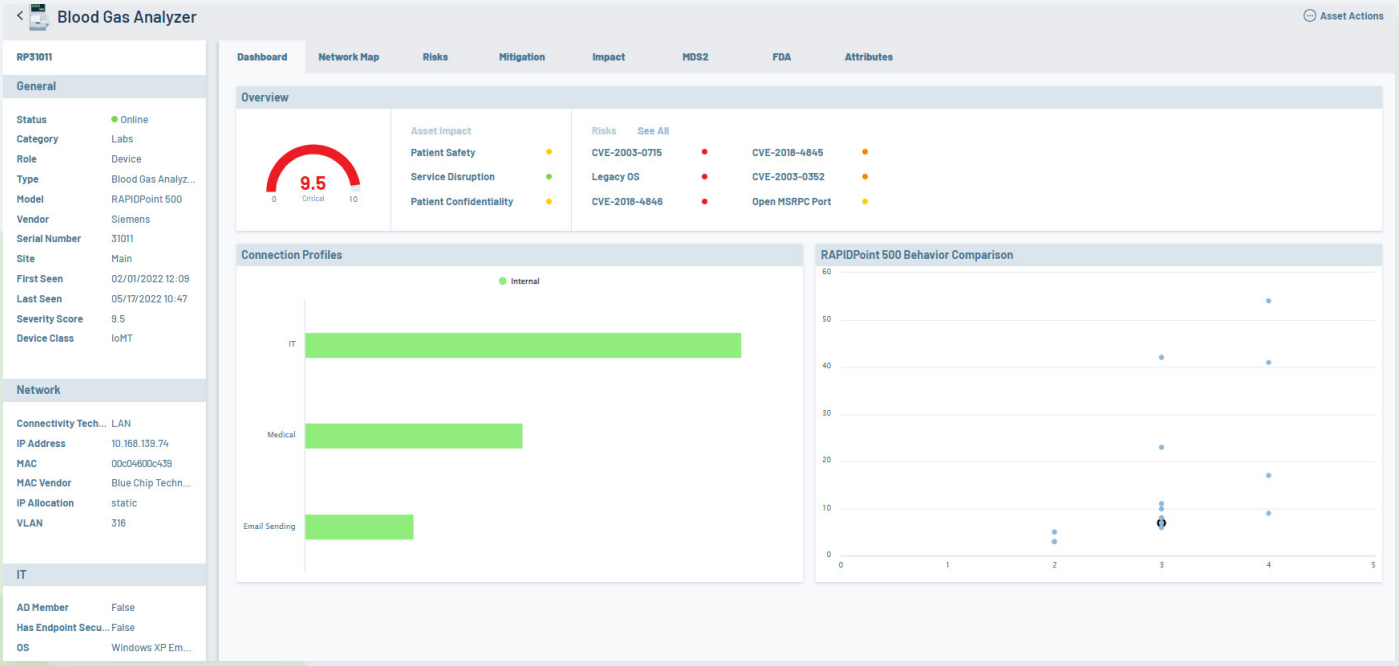


Image: IoT and IoMT devices are prioritised for remediation based on the potential risks to patient safety, data confidentiality, and service availability.

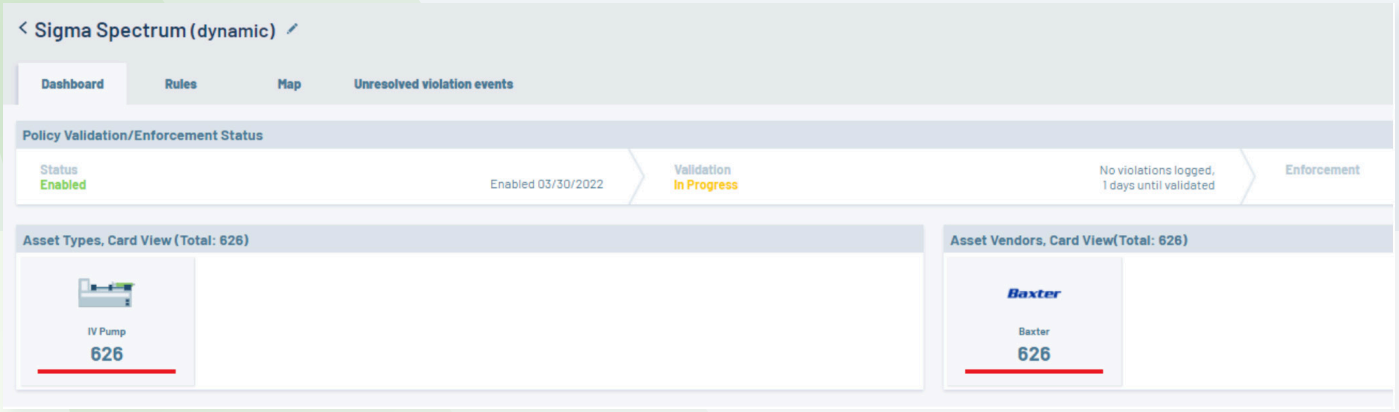
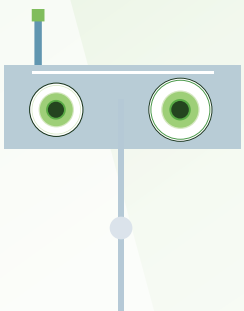


Image: Drill down on specific device types and vendors to determine the appropriate segmentation policies that won't disrupt patient care.

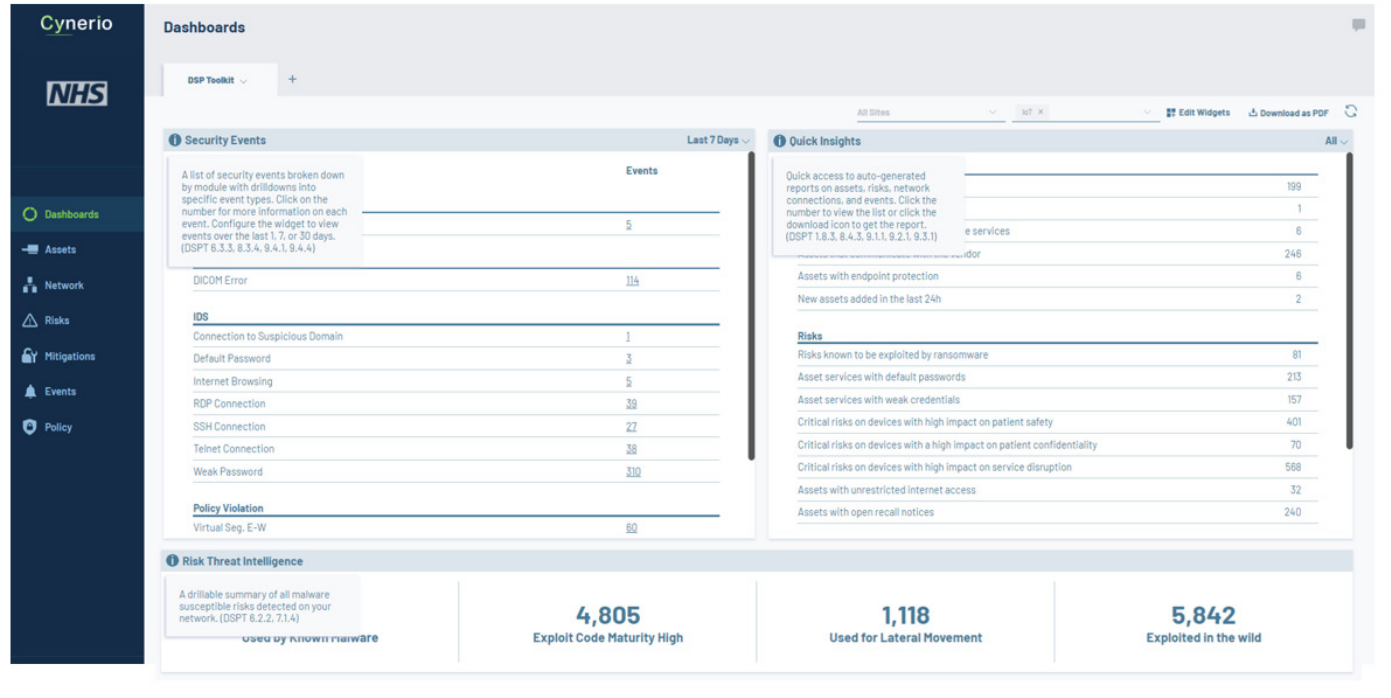


Clinically intelligent monitoring and threat detection identifies and profiles all connected medical, IoT, and OT devices on the network. **The platform's healthcare-specific AI helps pinpoint and identify anomalous connections.** To ensure quick and safe threat remediation, Cynerio's threat mitigation modelling automatically creates operationally safe mitigation plans with custom security policies healthcare teams can test, validate, and edit within its virtual segmentation validation sandbox before the solution enforces them on the network.

DSP Compliancy

IoT and IoMT are typically the most vulnerable devices on any hospital network, and security tools such as network scanners are not able to provide the required visibility or real-time behavioural analysis. As a result, these types of devices are often not factored into an organisation's DSP submission.

Image: The Cynerio platform gives hospitals the visibility to bring their healthcare IoT into DSP Toolkit compliance.



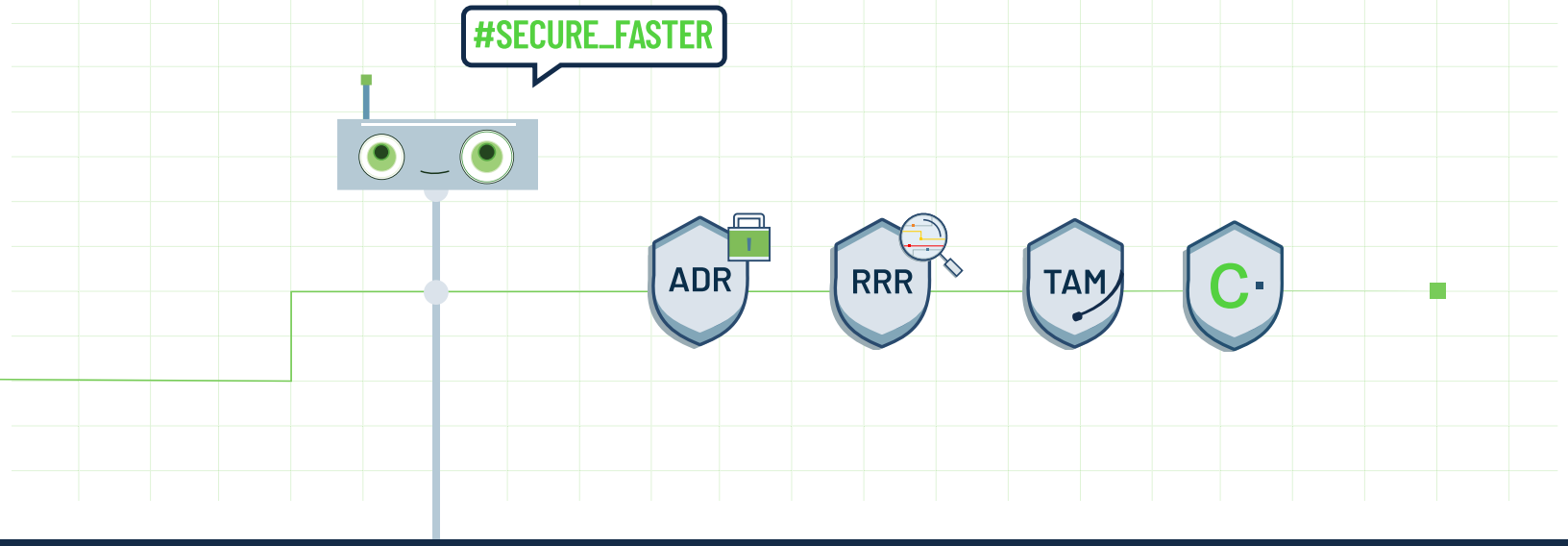
Utilising Cynerio's dedicated DSP dashboard, the team at NLaG not only understand its level of compliancy for over 30 evidence items, but the necessary remediation steps to achieve compliancy are also prioritised by criticality and impact on patient safety. Compliancy can further be achieved by utilising Cynerio's Zero Trust policy creation engine to dynamically enforce Zero Trust policies and other mitigation tactics where relevant.

'The Cynerio solution takes vast quantities of our data and distils it into prioritised multi-departmental actions that are manageable for our teams. We aren't presented with a dashboard of equally weighted overwhelming emergencies; instead, our vulnerabilities are curated and prioritised so we know exactly where to start', says Steven Mattern, Associate Director of IMT.

Image: The Cynerio platform shows where hospitals can make the most impactful changes to their IoT risk posture

The Benefits of the Cynerio Platform

- Go beyond inventory - Find and remediate the most critical healthcare IoT risks in under 30 days
- Confidently micro-segment connected devices with no impact on patient outcomes or functionality
- Automated, actionable, and plain-English mitigation plans that prevent the widest variety of threats
- Use device data to prioritise remediation based on potential critical risk to patients
- Identify and respond to ransomware and other attacks so they don't affect IoT and medical devices
- Get the visibility to integrate IoT, OT and connected medical devices within your IT security tools
- Ensure IoT security alignment between BioMed, security, network, facilities, and executive teams
- Stay up to date with IoT security compliance for HIPAA, NHS DSPT, and other international healthcare regulations



Cynerio

About Cynerio

Cynerio is the one-stop-shop Healthcare IoT security platform. With solutions that cater to healthcare's every IT need – from Enterprise IoT to OT and IoMT – we promote cross-organisational alignment and give hospitals the control, foresight, and adaptability they require to stay cyber-secure in a constantly evolving threatscape. We give healthcare organisations the power to stay compliant and proactively manage every connection on their own terms with powerful asset management, threat detection, and mitigation tools so that they can focus on healthcare's top priority: delivering quality patient care. For more information visit www.cynerio.com, or follow Cynerio on Facebook, Twitter, and LinkedIn.