CASE STUDY

NHS Trust Providing Services for 350,000 Patients

Streamlined DSPT Compliance and Medical Device Security

Better device visibility, proactive cyber defence, and improved operations

Background

University Hospitals of Morecambe Bay (UHMB) NHS Foundation Trust is a 678-bed group of community sites and three hospitals in Barrow-in-Furness, Kendal, and Lancaster in North West England. Like many hospitals attempting to modernize its operations, it was mid-way through an extensive digital transformation of its medical and systems records. Under the NHS's DSPT (Data Security and Protection Toolkit) requirements, the Trust was also required to build and maintain an accurate asset and risk registry of all connected medical devices across multiple networks and sites, and in light of rising cybersecurity threats.

Following the deployment of the Cylera platform, an agentless medical and healthcare IoT device (IoMT) cybersecurity and intelligence platform, UHMB was able to quickly gain a real-time and comprehensive risk-scored inventory of all connected devices. As a result, persistent vulnerabilities were uncovered, some of which were previously undiscovered zero-day risks, which were brought to the attention of device manufacturers. Cylera was able to then drastically improve the security and compliance of a vital NHS Trust and the safety of its data and patients.

DSPT is an online self-assessment tool for organisations to use to measure performance against the National Data Guardian's 10 data security standards. Any organisation with access to NHS patient data and systems is required to comply with the toolkit for assurance that good data security practices are being met and personal information is being handled correctly.

NHS University Hospitals of Morecambe Bay NHS Foundation Trust

"Before Cylera, we thought we knew what we didn't know. The Cylera platform has provided a means to identify and assess what we have, and at a depth that gives us the ability to meet our regulatory requirements, manage the priorities and workflow around risk, and help our vendors to assist us achieve a stronger security posture,"

Head of IT, University Hospitals of Morecambe Bay NHS Foundation Trust.

The Challenges

- **Complexity:** UHMB needed to manage the security of numerous devices distributed across multiple locations and inter-related networks but lacked visibility into all the network traffic and a complete asset inventory while maintaining business continuity and patient care. A system that provided a single, simplified, and holistic view of all devices, networks, and vulnerabilities across multiple locations via interlinked networks was needed.
- **DSPT Requirements:** UHMB needed to adhere to a new DSPT 2022-23 requirement to create and maintain an accurate medical device register for all connected devices at healthcare facilities. Previously at UHMB, not all devices and assets were known or identified on the network, and the data available on devices was inconsistent across the multiple sites.
- **Managing Vulnerabilities and "True Risk":** With many priorities and limited staffing, UHMB had to gain visibility of existing devices' scored vulnerabilities and security gaps. The UHMB IT team also needed to be able to respond promptly to threats and urgent NHS DSPT Cyber Alerts.

Solution and Benefits

As a specialist in IoMT cybersecurity and intelligence, the Cylera platform automates the process of managing and securing entire connected device landscapes through a progression of asset identification, real-time risk analysis and visibility, profiling, and improved medical device management.

The Cylera platform has been installed at one main location so far, with the management console centrally managed by the UHMB IT team. With 18 sensors monitoring network traffic and devices across multiple sites, more than 22,000 medical and IoT devices have been found, with plans to add more. Within the first few hours, connected IoT, IoMT, IT, and OT devices were discovered, profiled, and cataloged for UHMB's medical register. These devices were also scanned using Cylera's patented Network Device Emulation Engine™ technology and scored based on risk for vulnerabilities, all while maintaining zero-touch and without disrupting devices and patient care.

Here are a few of the operational outcomes and benefits at UHMB:

Accurate Registry of Connected Medical Devices

UHMB's team has been given a comprehensive, real-time, device registry with continuously updated details for all connected IoT and IoMT devices and guidance for risk and remediation thanks to Cylera's asset discovery, characterization, and categorization process. This uses passive, patented, Adaptive Datatype Analysis™ to interpret device communications and discover all connected assets with unmatched depth visibility.

DSPT Regulations Management

UHMB complies with DSPT regulations using Cylera's built-in NHS Cyber Alerts Dashboard that keeps Trusts up to date on key Cyber Alerts which have been issued, with built-in mechanisms to help manage the workflow associated with receiving, managing, resolving and reporting on these issues.

Business Impact

Cylera's Platform automatically creates and maintains the registry of connected medical devices within the Trust to streamline the process of locating a device, which leads to improved efficiency and workload, as well as effective maintenance, personnel, and patient scheduling. The registry also provides valuable insights for making informed business decisions such as purchase vs. rent when managing the availability of consumable inventory of key patient equipment (e.g., infusion pumps). It also assists in managing vendor and third-party issues at scale like being able to detect when ePHI (Electronic Protected Health Information) is present in devices for compliance risk and DSPT requirements.

"True Risk" Analysis with Zero Touch

Using Cylera's patented Network Device Emulation Engine™, UHMB was able to deeply analyze all device behavior at the packet level for security threats, such as malware, unknown devices, equipment failures, or other anomalies - all without disrupting UHMB's patient care or physically touching devices. These risks are then priority ranked and the system administrator is alerted.

Upon scanning, two main vulnerabilities were found, which may allow remote attackers unauthorised access to some network connected devices. As a result of Cylera identifying these vulnerabilities, the IT team applied the necessary patches from the applicable vendors. However, Cylera's Platform still noted vulnerabilities and a higher-than-expected risk score on one device type. Initially, the device vendor was unresponsive to requests for assistance and challenged the findings - causing additional concern for the IT team. The technical details highlighted by the Cylera Platform were therefore critical in demonstrating the risk to the vendor, which was able to provide the necessary patches to resolve the identified risks.

> "Before Cylera, we thought we knew what we didn't know. Cylera's Platform has provided a means to fully identify and assess what we have, and at a depth that gives us the ability to meet our regulatory requirements, manage the priorities and workflow around risk, and help our vendors to assist us achieve a stronger security posture."
>
> Head of IT, University Hospitals of Morecambe Bay
> NHS Foundation Trust

Conclusion

Using patented techniques, Cylera's Platform helps customers find, identify, and manage their assets to protect what matters most - patient care, safety, privacy, and business continuity. Cylera makes it easier to monitor devices, manage workflows, and utilise built-in risk-based remediation guidance. For UHMB sites, Cylera was able to gather deeper information that assisted in compliance to DSPT requirements and National Data Guardian's security standards providing reliable information used to apply the needed pressure on a large third-party vendor to respond and support their security findings.