CASE STUDY

SOUTH TEES HOSPITALS NHS FOUNDATION TRUST

Intro & Background

South Tees Hospitals NHS Foundation Trust is a leader in the healthcare industry, providing comprehensive care services to over 1.5 million people across the Tees Valley, North Yorkshire, and other parts of the United Kingdom. With a reputation for innovation in fields such as orthopaedics, cardiology, maternity care, and robot-assisted surgery, the trust is dedicated to using digital technologies to improve patient outcomes and experiences. However, as the use of cyber-physical systems (CPS) and other connected devices increased, Digital Director, Dr. Manni Imiavan, recognised the need to prioritise cybersecurity, especially for the trust's fleet of IoMT and other medical devices.

Dr. Imiavan, along with the Assistant Head of ICT, Mike Jackson, and his team had been proactively working to address cybersecurity risks long before the infamous WannaCry ransomware attack disrupted NHS operations globally in 2017. However, they knew they needed to do more to mitigate these risks and safeguard care delivery. This case study highlights how the South Tees team partnered with Claroty to enhance the security of medical devices, streamline compliance, improve efficiency, and safeguard care delivery across all six healthcare facilities managed by South Tees Hospitals NHS Foundation Trust.

The Goal

Dr. Imiavan and his team had long been laser-focused on building and optimising the IT security infrastructure and capabilities at each South Tees facility. However, with the increasing digitisation and innovation in the healthcare industry, they recognised the need to broaden his team's focus to include securing the growing number of IoMT and IoT devices, and other connected devices integral to patient care delivery.

To achieve this, the team set out to meet several key goals, which included:

- Strengthening the security of medical devices against cyber threats, particularly ransomware attacks.
- Extending existing IT security monitoring and network segmentation controls to cover medical devices.
- Proactively assessing, strengthening, and reporting on the overall cyber hygiene and risk posture for each South Tees facility.
- Fulfilling the compliance requirements of the UK's Data Security and Protection Toolkit (DSPT).

Customer Key Challenge(s)

The South Tees team faced challenges that are all too familiar to security teams in healthcare organisations. First and foremost, they lacked a centralised, up-to-date inventory of their growing number of connected devices. This made it difficult to monitor and secure their network effectively.

Secondly, they had limited visibility into device behaviours and communications, which made it hard to monitor device traffic, understand how devices communicate with each other and with the wider network, create (much less enforce) network security policies to safely and effectively segment devices, and identify potentially malicious activity.

Thirdly, they face the challenge of dealing with a broad array of care-critical medical devices that are "unpatchable" and, therefore, vulnerable to attack. Many of these devices are either too old to patch, use legacy systems for which security patches are no longer available, and/or cannot tolerate enough downtime to enable patching because they support patients whose health and safety require them to operate continuously.

Lastly, Mr Jackson's team has resource constraints and pressure to quickly demonstrate the ROI of his programme. They needed to find a solution that can be implemented quickly and efficiently, while also delivering tangible results to justify the investment.

Customer Solution with Claroty

To address these challenges, South Tees turned to Medigate by Claroty, a comprehensive medical device security platform. They implemented all modules in the platform -

Vulnerability & Risk Management	Network Protection	Threat Detection	Device & Lifecycle Management	Operational Intelligence
Healthcare enterprise device risk overview & vulnerability management orchestration	Implementation of Zero-Trust network policy orchestration	Contextualized identification, alerting, & response	Clinical device life cycle management to maximize utility & procurement decisions	Device profiles & utilization for efficiency optimization

To further enhance their security position and extend the value of their existing IT security investments, South Tees is integrating Fortinet's FortiNAC solution with Medigate. The integration with FortiNAC enriches the managed wired device data in Medigate providing switch and location information.

Results

With the Medigate platform in place and integrated with their new Fortinet solution, South Tees was able to improve their overall security position and gain greater visibility and control over their medical device inventory. They were able to automate network access control and reduce the risk of unauthorised devices connecting to their network. They also gained greater visibility into device behaviours and communications, which allowed them to detect and respond to potential threats quickly.

Perhaps most importantly, South Tees was able to demonstrate the return on investment (ROI) of their cybersecurity programme to key stakeholders. By improving their security position, they were able to reduce the risk of data breaches and other security incidents, which could have had a significant impact on patient safety and the organisation's reputation. Additionally, harnessing device utilisation data will allow South Tees to negotiate lower maintenance fees with device vendors — and, ultimately, prove additional ROI of the Medigate platform.

Conclusion

Healthcare organisations face unique challenges when it comes to securing and managing their growing number of connected medical devices. However, with the right solutions in place, it is possible to overcome these challenges and improve the overall security position. By partnering with Medigate by Claroty and Fortinet, South Tees was able to improve their medical device security and gain greater visibility and control over their inventory.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial, healthcare, and commercial environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide comprehensive controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the leading investment firms and industrial automation vendors, Claroty is deployed at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.