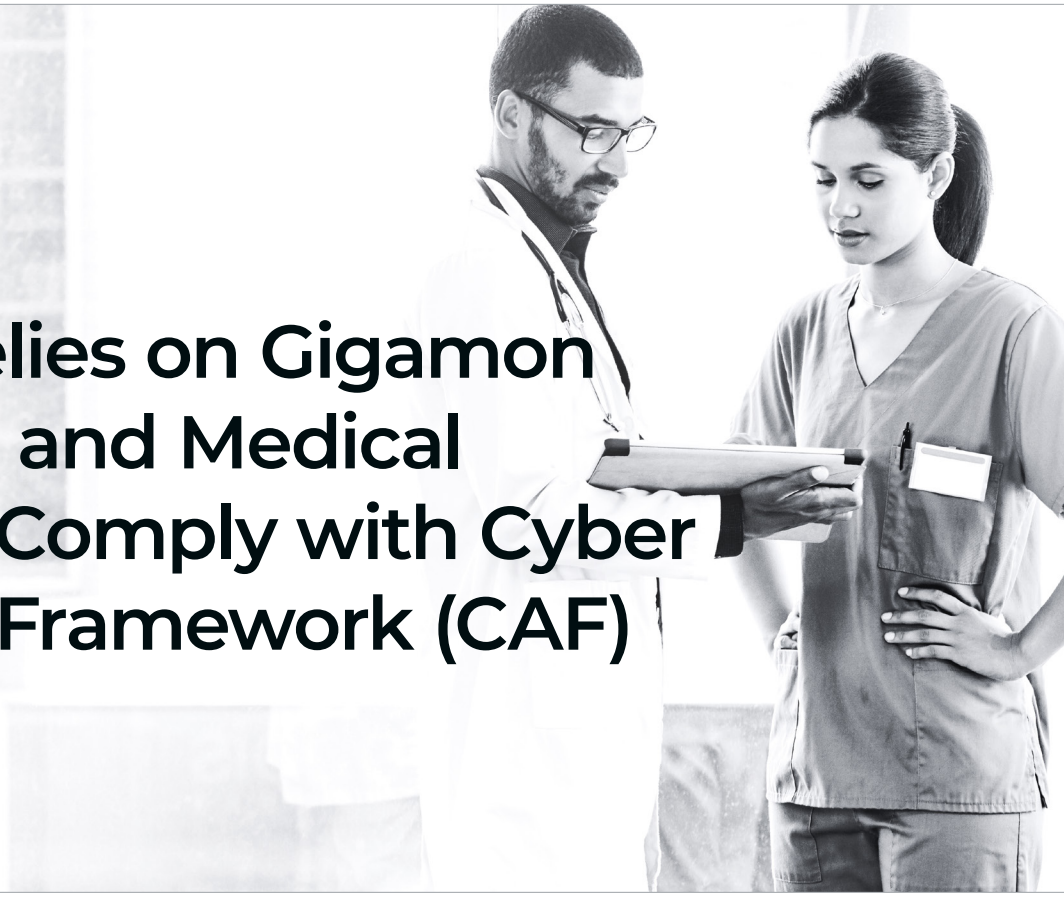
Case Study

NHS Trust Relies on Gigamon to Secure IoT and Medical Devices and Comply with Cyber Assessment Framework (CAF)



A huge benefit we have experienced from our Gigamon deployment is being able to provide assurance of compliance to the government and our stakeholders. We can feel confident that we are proactively reducing cyber risk by improving asset visibility and ensuring alignment with the CAF-DSPT.

SHANE MARTIN
Network Manager at York and Scarborough Teaching Hospitals

Challenges

- Elevating cybersecurity posture
- Gaining comprehensive visibility across the entire estate
- Capturing and assessing internet of things (IoT) security for medical equipment and other devices in order to get a true picture of the organization's risk profile
- Complying with the Cyber Assessment Framework (CAF) standard put forth by the U.K. government's National Cyber Security Centre (NCSC)

Customer Benefits

- Streamlined compliance with CAF framework
- Strengthened protection of sensitive patient data
- Identified and gained a deeper understanding of devices on the network
- Prioritized focus based on the data received from the Gigamon solution

Solution

- GigaVUE-FM fabric manager
- GigaVUE® HC Series

About Customer

York and Scarborough Teaching Hospitals NHS Foundation Trust is a not-for-profit acute community healthcare provider delivering a wide range of services for 800,000 people in the York, U.K. area covering 3,400 square miles. The hospitals have a total workforce of 10,000 who work across five main hospitals and several community sites. It is primarily funded by the government.

Platform Manager Paul Chappell supervises Rob Birchall, Platform Cyber Analyst, whose responsibility it is to ensure the hospitals are in compliance with Cyber Assessment Framework (CAF) standards put forth by the U.K. government's National Cyber Security Centre (NCSC). Network Manager Shane Martin is responsible for LAN, VLAN, and telephony security across the estate.

Business Challenge

The Trust was aiming to boost its security posture and increase visibility into its hybrid cloud environment. Its environment consists of approximately of 8,500 PCs, 500 servers, 2,000 mobile phones, 500 network switches, and 1,000 Wi-Fi access points located across all sites providing access to shared digital services. The wide area network (WAN) connects about 50 sites and 4,000 mobile and home workers to the HSCN NHS network, hospital-based systems, and the internet. The organization also has a whole host of network-connected IoT equipment and devices such as CCTVs, nurse call systems, door access controls, lighting, internet protocol television (IPTV) systems, and building management systems (BMS).

The organization's primary requirement was to get a better handle on the security of its IoT devices. It needed a solution compatible with its software-defined networks (SD-WANs) and have the ability to extrapolate and encapsulate traffic to feed into its other security tools.

In its search for the right solution, the security and network team evaluated two other vendors prior to engaging Gigamon. They quickly discovered that solutions from competing vendors were not compatible with the hospital's technology infrastructure and security stack. One vendor lacked the ability to SPAN to the side area sensor. The other vendor's equipment was limited by the number of SPANs that could be terminated.

"We had over 150 wiring closets that were causing issues when trying to SPAN across the environment. It would require multiple VLANs. The number of SPAN sessions that could be terminated on the core switches was lower than the amount that would be generated, so we needed a way to consolidate them and bring the data flows into the core," explained Martin.

In addition to improving visibility, another top priority was compliance with the U.K. government's NCSC CAF, which requires healthcare organizations to demonstrate a comprehensive understanding of its IoT estate.

Resolution

The hospital deployed GigaVUE-HC1 and GigaVUE-FM fabric manager to identify IoT devices on the network. Core to Cloud, the healthcare organization's trusted cybersecurity managed services partner, was instrumental in advising and supporting the solution design and implementation.

GigaVUE-FM now provides teams with single-pane-of-glass visibility into the hospital's network-connected IoT devices and feeds enriched traffic data into Cylera and other tools like Forescout and Armis, providing value as part of a broader ecosystem.

"Now I am able to see what devices we have and where and analyze the risk they pose. Thanks to Gigamon, we can also better manage multiple SPANs — something we were unable to do using our core infrastructure," explained Martin. "For example, with Gigamon, there's an unlimited number of SPANs that can be terminated. This helps us pinpoint bottlenecks and improve overall network performance."

An interesting insight was discovering that some IoT devices, such as pathology analyzers, were connected to the network through other IoT devices. "We actually have two IoT devices to enable that connectivity," shared Martin.

Benefit

The Gigamon deployment at York and Scarborough Teaching Hospital has provided a wealth of data that lays the foundation for the hospital's next steps. "We can actually start putting definition around the information and start implementing security controls within the network," Martin said. "Our long-term goal is to limit the amount of traffic being generated in a VLAN to that particular type of device and traffic, essentially segregating it from the main corporate infrastructure and data flow."

Gigamon integrations have also enabled the Trust to get the most from its security tools. "Gigamon has helped our team gain insights from the security tools so we can surface what needs to be done next and quickly remediate issues," said Chappell. Additionally, Gigamon has made it easier for the organization to map to the U.K. compliance framework and easily show evidence of compliance.

"A huge benefit we've experienced from our Gigamon deployment is being able to provide assurance of compliance to the government and our stakeholders. We can feel confident that we are proactively reducing cyber risk by improving asset visibility and ensuring alignment with the CAF-DSPT," said Martin. "We have visibility into previously unknown devices on the network that can take action where needed. This makes my life easier, and it means I'm not taking as much home with me."

Birchall summarized the business value of the deployment by saying: "Our Gigamon deployment is a step forward in our journey toward cyber maturity. It's not just about visibility—it's about building confidence with our stakeholders that we're actively managing risk and aligning with the CAF. The insights we've gained are helping us prioritize investments and demonstrate measurable progress toward a more resilient infrastructure."

He pointed out that the organization's Gigamon implementation has established a template for other NHS hospitals to follow.

About Core to Cloud

We specialise in cutting through the noise to deliver real, actionable insight and solutions that protect your business – without overcomplicating it. From critical visibility gaps to fast-moving threats, we work with you to design, implement, and manage cybersecurity strategies that are both robust and realistic.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

06.25_01