# Case Study:
# Cylera empowering HDOs with its Healthcare IoT Security Solution.

## Customer Value Perspective:

As part of our vendor assessment on customer impact, we surveyed, verified, and obtained public use case details regarding a sampling of the companies' customers – large and mid-tier healthcare providers that were late and early-stage customers – to determine our findings.

Cylera focuses on providing Healthcare IOT asset intelligence and security with a business that spans healthcare networks and hospitals in the United States and the United Kingdom, as well as expansion in Northern Europe and the Middle East. The company serves large healthcare networks, such as St. Luke's University Health Network, and a variety of regional healthcare providers and hospitals. The company is well established in the UK, supporting several major NHS hospital systems. In addition, the company has been successfully building out its network of alliance, channel, and service provider partners.

Coming to Cylera's offering, the company offers a SaaS-based platform that is scalable and extensible, supporting medium hospitals with 150 or more beds as well as much larger networks that manage well over a dozen hospitals and more than 250 different facilities across multiple regions and even countries. The platform can readily discover, categorize, inventory, risk assess and monitor a large volume and diversity of healthcare IOT and connected medical devices for these customers. All customers surveyed anticipate continued growth in their IoT and IoMT assets and increased concern about managing attacks, as well as operational, privacy, and reputation risks. While there were a few unique use cases, the common challenges that were expressed by customers and fully satisfied by Cylera included:

- Improved security posture and the ability to mature security programs by eliminating IoMT inventory, vulnerability, and threat management operational and process gaps.
- Alignment to standards-based risk analysis of healthcare IoT devices to meet regulatory and operational compliance requirements (e.g., NIST, HIPPA, CCPA).
- In particular, the predominant compliance-driven initiatives across the NHS customers in support of the requirement of NHS's DSPT (Data Security and Protection Toolkit), which mandates asset and risk registry for connected medical devices.
- Enabling more accurate and up-to-date IoT/IoMT device microsegmentation in support of Zero Trust initiatives.
- Analytics that provided extensive usage of telemetry across sites and hospitals to ensure patient care availability, as well as to make informed budget decisions and cost-effective deployment.

"Cylera has provided us a means to fully know what we have, in-depth, and how to manage those devices and the risks according to our business priorities and revenue goals. The analytics provided can drive changed related to where IoMT assets are located, how they are scheduled, and how they are access to optimize their revenue potential."

Given early generation IOT security solution adoption, all surveyed Cylera customers shared that they conducted proof-of-value (POV)/comparative tests pitting Cylera against other top leaders in the 2023 Connected Medical Device Security SPARK Matrix™ – where Cylera consistently proved comparatively superior:

- A greater number of healthcare IOT assets discovered, classified, and vulnerabilities found: One customer cited "at least 15% more right out of the box, while the competing vendors had to come back weeks later with custom updates to support a new class of devices."

- Faster and easier deployment with one customer who expressed, "Within the first few hours we found our IoT, IoMT, and OT devices discovered, profiled, cataloged, and registered."

- More accurate risk profiling and scoring: Multiple customers expressed the outcome of better-prioritized actions that vastly reduced the remediation workload of their IT, security, and biomedical team members, who are in limited quantity in healthcare organizations. Customers also expressed significantly "less alert fatigue than other vendors."

- A higher degree of granular device details, including tracking of vulnerability, risk, utilization, and location – providing value to not only security but procurement and allocation processes as well. One customer cited "more informed data to improve business decisions in purchasing efficiency and revenues from underutilized devices."

- Advanced platform capabilities, including the use of ML, for more accurate identification, risk scoring, and behavior monitoring.

"… unmatched depth of visibility… results were eye-opening…. real-world operational factors and guidance are included in comprehensive risk profile generation."

## Analyst Opinion:

Cylera ranked in the top three of technology leaders (overall highest ranked) in Customer Impact and in the top four overall in the 2023 SPARK Matrix™ for Connected Medical Device Security Solution Providers. Surveyed Cylera customers gave excellent ratings for Cylera with regards to ease of use and deployment, demonstrating scalability and interoperability, as well as delivering an overall optimum purchase/customer experience. The common reasons for selection include comprehensive functionality, strong references, service/support capabilities, and the extent of ecosystem partnerships. Customers also consistently expressed the advantage of the value of Cylera's building relationships based on business outcomes and the overall responsiveness of the company's customer success staff.

Healthcare delivery leaders should consider Cylera on their Connected Medical Device Security (CMDS) solution shortlist. With a strong focus on the healthcare sector, Cylera stands to continue to build upon its market success -- taking advantage of competitor renewal cycles, new channel partnerships, regional market growth, and market consolidation.