CASE STUDY

Provincial Health Services Authority and Fraser Health Authority Boost Cybersecurity Processes and Compliance with Claroty xDome

Overview

Prominent Canadian health systems, the Provincial Health Services Authority and Fraser Health Authority, have been flagship customers of Claroty for over three years. Over this time period, they have worked diligently to strengthen their cybersecurity posture across their wide network of medical devices and IT infrastructure. The health system spans 127 clinical sites, including urgent care centers, with nearly 300 sites integrated under its operations. They have a robust IT infrastructure, deploying 11 collection servers across multiple locations. The security team owns the platform, with clinical engineering and security teams working in close collaboration to ensure the protection of patient data and other assets.

Challenge

The organizations faced several challenges that spurred their decision to invest in an automated asset discovery solution for their IoMT, IoT, and OT devices within clinical and non-clinical workflows. The biggest pain points across both IT security and clinical engineering teams were:

Provincial Health Services Authority

PHSA is a publicly funded health service provider that provides specialized health care services to communities across British Columbia, on the territories of many distinct First Nations. PHSA has a unique role in BC's health authority system: to ensure that B.C. residents have access to a coordinated provincial network of high-quality specialized health-care services, working in partnership with the province's health authorities and health-care professionals to improve access to evidence-informed practice closer to where people live and to effectively promote health, manage chronic conditions and reduce the burden of illness.

fraserhealth

Fraser Health is the largest regional health authority in British Columbia, and it is the heart of health care for over two million people in 20 diverse communities from Burnaby to Boston Bar on the traditional, ancestral and unceded lands of the Coast Salish and Nlaka'pamux Nations, and is home to 32 First Nations within the Fraser Salish region. Their hospital and community-based services are delivered by a team of 48,000+ staff, medical staff, and volunteers dedicated to serving their patients, families, and communities.

- Manual Data Collection Processes: Since this HDO was not using a comprehensive discovery tool, all records were tracked and maintained manually, leading to inefficiencies and potential security risks. This put the HDO at risk for frequent data discrepancies, particularly in identifying and tracking medical devices across sites.
- Vulnerabilities and Risk: A government audit pointed out blind spots in some areas of existing cybersecurity processes and controls, especially regarding medical device tracking and network segmentation.
- Audit Response: The team responsible for managing medical devices needed to leverage the data from devices to assess the vulnerability and risk level of the medical devices and secure the network security posture.

The PHSA teams felt that the next step was to implement a solution that could speed up some of these challenges, improve security postures, and relieve some current operational deficits.

Solution

By partnering with **Claroty** and implementing its purpose-built healthcare solution, **Claroty xDome for Healthcare**, PHSA and FHA were able to quickly fill the immediate gaps in device discovery, tracking, and risk management. Key highlights of leveraging the solution include:

A Robust, Accurate Data Foundation: Claroty xDome facilitated the identification of key device attributes such as MAC addresses and IPs, which were critical in tracking and locating infusion pumps and other devices that were previously missed. It also resolved discrepancies with devices marked as retired in the CMMS, or that had been incorrectly relocated across sites. Communication mapping directly in the platform helped to visualize device interactions to understand the behavior of devices on the network at a deeper level. This newly added data would then be extremely valuable to drive stronger incident response efforts.

Transparency into Risk and Cybersecurity Deficits: The system was able to assess vulnerabilities and exposures, particularly around devices that contain Personal Identifiable Information (PII) and Protected Health Information (PHI). xDome helped identify misconfigured systems, some of which may not have been properly networked and residing on corporate VLANs. It helped uncover gaps in network segmentation and revealed devices sitting on unsegmented or insecure VLANs.

Audit Compliance: With the help of Claroty, the health systems successfully prepared for their government audits. For a new building at the Children's Hospital in Vancouver specifically, 28 recommendations were made for improving cybersecurity, all of which were approved by governance. The recommendations ranged from simple actions like changing default passwords to more complex tasks like managing vulnerabilities and establishing patch management processes. This increased regulatory compliance while boosting overall cybersecurity effectiveness for the health system.

Network Visibility and Protection: PHSA also embarked on a network segmentation project to better manage its vast network of medical and corporate devices. Initially, they identified the communication flow of devices and implemented initial segmentation measures to mitigate risks. As the system expanded, they incorporated Forescout and Fortigate to enable microsegmentation, providing greater control over device interactions. Their long-term goal is to enable tighter microsegmentation across all devices as they continue to integrate across their network infrastructure.

Outcomes

By implementing Claroty xDome, leveraging core solutions such as Exposure Management, Threat Detection, and Network Protection efforts, PHSA and FHA witnessed vast improvements in their cybersecurity efforts and operational requirements.

Automated device discovery immediately enabled enhanced device visibility across their networks. With over 70,000 managed workstations, the health systems improved visibility into devices and how they communicate across their corporate networks to provide an accurate, up-to-date view across their entire infrastructure.

Provincial Health Services Authority, Fraser Health, and their entities were able to vastly improve meeting auditing requirements. The results showcased vast improvements in their cybersecurity frameworks, particularly around the management of medical devices and vulnerabilities. The new processes and procedures being augmented by Claroty xDome were able to address audit findings and establish a much stronger governance framework overall.

In addition to meeting auditing requirements, risk mitigation was much stronger through the implementation of more proactive security measures for identifying vulnerabilities and assessing risks. This resulted in efficiency gains, along with the integration of alerting, dashboarding, and reporting into existing workflows and environments.

Because Claroty xDome is built on the AWS platform, it leverages AWS's inherent scalability and security features, such as encrypted connections between on-premise networks and AWS, immediate access to new features and threat definitions, and automated updates. These features ensure a comprehensive and adaptive cybersecurity posture that aligns with modern demands for flexibility and scalability in security solutions.

PHSA and FHA have completed their deployment to the 127 sites and continue expanding their use of Claroty xDome to improve security postures, incident response, and network security. As their security workflows expand, the security team is also exploring ways to drive and prove greater ROI (Return on Investment) through the sophisticated security capabilities offered by Claroty xDome. With the continued support of Claroty xDome, the health systems are well-positioned to meet future audit and security demands and achieve long-term operational efficiencies and risk mitigations moving forward.