ANN & ROBERT H. LURIE CHILDREN'S HOSPITAL OF CHICAGO

World-Class Pediatric Hospital Efficiently Secures Network Access With the Great Bay Network Intelligence Platform™

At a Glance

- Top Pediatric Hospital in Region
- 12,000 Network Endpoints
- Twelve Locations

Patient safety is the number one concern at Ann & Robert H. Lurie Children's Hospital of Chicago and being able to quickly detect and secure unknown and unmanaged devices on the hospital's network is critical. A breach could severely jeopardize patient safety and care, sensitive data, the hospital's reputation and more. This is why the Great Bay Network Intelligence Platform™ was chosen as a critical component in the network design for the hospital's $900 million, 24-story building.

By automatically identifying, profiling and authenticating the IoT and medical devices on the network, the Great Bay Network Intelligence Platform™ eliminated the need to devote IT resources to these manual and time-consuming tasks. The platform simplifies device onboarding workflows, expedites network troubleshooting and helps ensure regulatory compliance.

Securing State-of-the-Art Healthcare Delivery

Lurie Children's is the region's top provider of pediatric care. In its 223-bed, inpatient facility, maintaining patient safety and the care continuum is the hospital's primary driver behind maintaining a secure network. Intrusions and unauthorized activity could jeopardize life-saving applications and instruments. Hundreds of thousands of confidential records could be violated, resulting in harsh fines, loss of confidence, business disruptions

and/or legal proceedings. To avoid these consequences, Lurie Children's wanted to implement total 802.1X security for its wired network.

This level of security is further complicated by the esoteric nature of medical devices. As Manager of IT Network and Security Infrastructure, Chris Dozois explains, "Every [medical device] vendor is unique, making it a tricky job to secure those devices." IoT and medical devices can include anything from RFID exciters to bedside monitors and printers, faxes, security cameras, infusion pumps, video, voice, facility automation and even patient entertainment equipment, none of which typically hold a supplicant for which to administer traditional security software. The IT team at Lurie Children's Hospital had 7,600 IoT and medical devices that had to be manually

Critical Needs

- Maintain the patient safety and care continuum via a secure, wired 802.1x network
- Achieve continuous device identification, validation, network authentication and onboarding workflows
- Automate network asset inventory—in real time
- Expedite network troubleshooting
- Meet compliance regulations
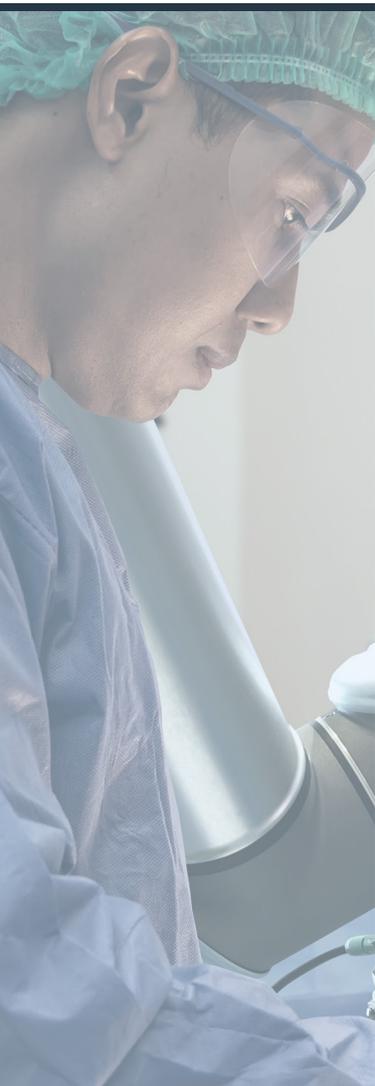
Summary of Benefits:

7,600 IoT and medical devices discovered, profiled, monitored and secured

Achieved savings of 2 full-time equivalents (FTEs) due to automated endpoint profiling and asset inventory

Increased operational efficiency by automating device onboarding workflows

Met compliance regulations with 802.1X network security requirements

inventoried, profiled and authenticated to the network. In addition, they were tasked with manually white-listing the MAC address for each device.

The Solution: Unmatched Endpoint Visibility and Real-time Validation

Fortunately Lurie Children's Hospital found a robust solution in the Great Bay Network Intelligence Platform™. The platform automatically identified, profiled and authenticated 100 percent of the hospital's IoT and medical devices. "We were basically dealing with just a list of thousands upon thousands of MAC addresses. There was no good way to track, audit and manage it," Dozois said. "Really, to have 802.1X enabled on the wired network just simply wouldn't be possible without this tool."

As new IoT and medical devices are added to the network, the platform automatically detects and identifies the device and validates its profile and credentials before enabling network access. The platform also tracks and records all device activities and movements across the network, which can be critical in speeding response timelines during a security event.

The Results: Security Plus Impressive Savings

The hospital has achieved quantifiable security and operational benefits since its deployment of the Great Bay Network Intelligence Platform™. Maintaining an automated, up-to-date asset inventory, as well as having continuous device identification, validation and network authentication workflows has enabled the hospital to reassign two full-time equivalents (FTEs) to other projects. In addition, the IT team feels confident knowing

> " We wouldn't be able to have an 802.1X secured environment without this tool.
>
> **Chris Dozois**,
> Manager of IT Network and Security Infrastructure

they can quickly locate a device and take action when a potential event arises. Lastly, the hospital has been able to significantly strengthen its adherence to compliance regulations by maintaining a real-time asset inventory and by having full visibility into all IoT and medical devices on the network.

In short, Dozois has no reservation in recommending the tool. He concludes, "We've been happy to have conversations and reference calls about the Great Bay Network Intelligence Platform™. It's definitely a quality product."

Great Bay Software is an IoT security and operational efficiency leader providing comprehensive visibility and control over endpoints on the network so organizations can secure data, preserve customer trust and protect revenue. By delivering real-time insight into device identity, location and behavior, Great Bay helps organizations identify and respond to potential threats and improve operational efficiency, all while supporting millions of connected devices.