BayCare Health System

CASE STUDY

Healthcare System Protects Medical Devices with Zingbox IoT Guardian

"Without Zingbox, we simply would not have known about these types of behaviors."

Ralph Oliva | Manager, Medical Device Integration and Security | *BayCare Health System*

INDUSTRY
Healthcare

ENVIRONMENT
More than 500 providers practicing in more than 160 locations, including 15 hospitals.

CHALLENGES
- Protect networked medical/IoT devices
- Compensate for traditional IT security solutions, which cannot be applied to connected medical devices
- No visibility into how devices are operating and communicating with outside world

ANSWER
Zingbox provides visibility into connected medical and IoT device communications through IoT Guardian.

RESULTS
- Maintains visibility into device operations and communications without any agents or clients on devices
- Enables discovery and identification of thousands of devices
- Categorizes threats and highlights those that are critical
- Monitors 33,000 medical and IoT devices currently

Customer Overview
BayCare is a leading not-for-profit healthcare system that connects individuals and families to a wide range of services at 15 hospitals and hundreds of other convenient locations throughout the Tampa Bay and West Central Florida regions. BayCare is also one of the largest private employers in the area, with an estimated $6.62 billion in annual impact on the region and the state.

BayCare's commitment to its patients is its highest priority. That means not only taking excellent care of its patients and investing in its communities, but also protecting patients' privacy and ensuring uninterrupted services. Unfortunately, cyberattacks on healthcare organizations have accelerated and are all too common, resulting in routine treatments being cancelled, surgeries being postponed, and, in some cases, hospital operations being significantly impacted due to attacks like ransomware.

While BayCare's security team takes its responsibility for protecting patient information very seriously, like all health-care companies, it was concerned about one particularly tough vulnerability to manage—its connected medical/IoT devices. Medical device manufacturers of all types create their products to perform specific medical tasks—like taking an MRI or administering a precise dose of medicine. These devices need to be networked to deliver relevant information. These connected devices are targets for threat actors, making them vulnerable to attacks. The challenge is that many medical devices often run on legacy operating systems, and the device manufacturers often do not apply the most recent security patches, even if one is available, due to the need for FDA validation and certification.

In order to guard against these vulnerabilities, BayCare took on several security initiatives. Working closely with the device manufacturers and the FDA, BayCare was able to install antivirus software on some of its devices. However, this approach proved not to be scalable, because the software often interfered with device operation. Other security tools, such as vulnerability assessment solutions, didn't yield any better results. Merely scanning connected medical devices with tools designed for IT assets often caused the medical devices to malfunction or be rendered inoperable.

"We all have the same problem. We all run million-dollar medical devices on legacy operating systems that unfortunately can't be patched," says Ralph Oliva, manager of medical device integration and security at BayCare.

BayCare knew something needed to be done to protect these devices and its patients. However, finding a solution that could provide the organization's security team with visibility into how its devices were communicating with the outside world proved difficult. Most of the solutions BayCare came across were designed for general-purpose IT devices, like laptops and servers, not for purpose-built medical equipment. When BayCare met with companies that claimed they could provide that visibility, they all wanted to install software on the medical devices themselves, which BayCare knew was a non-starter.

A New Approach for Protecting Medical Devices and IoT
BayCare knew it couldn't count solely on the medical device manufacturers to protect its critical equipment and its organization. Nonetheless, its security team had to find a way to provide that protection, and the BayCare team found a potential solution with Zingbox, a Palo Alto Networks company. Once engaged, Zingbox promised to give BayCare visibility into with whom, with what, and where their medical devices were communicating without having to install anything on the devices themselves. The BayCare team had never seen anything like it and quickly launched a proof of concept using Zingbox's IoT Guardian at one of its hospitals to determine the feasibility and effectiveness of this new technology.

"Within hours of deployment, we discovered and identified thousands of devices, including a few that gave us critical insight, allowing us to take action and implement preventive

measures," Oliva says. "We now receive alerts on various activities which were simply not visible before we partnered with Zingbox and implemented this solution."

Based on this success, the BayCare Information Security (IS) executive team approved the rollout of Zingbox IoT Guardian to all 15 of its hospitals—and quickly. After initially planning a three-month rollout, BayCare's IS vice president and CTO Scott Patterson challenged Oliva to see if the solution could be implemented any sooner. With Zingbox's help, Oliva's team rolled out IoT Guardian to all BayCare's hospitals in just three weeks.

Better Insight Leads to Better Protection

BayCare now uses IoT Guardian to monitor all medical and IoT devices. After deployment, BayCare received numerous alerts on how the medical devices were behaving. Additionally, BayCare now has insight on medical device usage and the ability to capture that data for utilization analytics reporting. "Without Zingbox, we simply would not have known about these types of behaviors," Oliva says.

Today, if one of BayCare's devices is acting outside of its normal behavior, Oliva and his team get a notification by text and email as well as on their dashboard. Additionally, these same alerts are actively monitored 24/7 year-round at the BayCare Security & Network Operation Center. IoT Guardian also categorizes threats and highlights those that are critical so BayCare knows to address them right away. BayCare now uses IoT Guardian to monitor 33,000 devices.

The Solution for an Industry-Wide Problem

BayCare isn't alone. Vulnerable medical devices are a problem for nearly every healthcare organization—organizations that are subject to an increasing number of attacks because they hold valuable data.

"This isn't a BayCare problem. It's an industry problem," Oliva says. Zingbox IoT Guardian is a security solution for medical devices and IoT that fills a much-needed security vulnerability gap.