Zingbox

CASE STUDY

INDUSTRY

Healthcare

ENVIRONMENT

588-bed hospital serving a nine-county service area, with approx. 5,000 medical devices in operation.

CHALLENGE

- Calibrate number of devices in operation
- Establish baseline for normal device behaviors and enforce security
- Implement a solution without interfering with regulatory guidelines

SOLUTION

- Discovery and categorization of all medical devices in use
- Intelligence about device behaviors
- In-depth real-time dashboard
- Fully implemented solution without any modification to devices

Hospital Gains Seamless Security–and Peace of Mind–with Zingbox IoT Guardian

The Limits of Spreadsheet Security

For many healthcare facilities that procure medical devices at a rapid rate, tracking and securing each device can be an expensive and consuming undertaking. Such challenges were top of mind for security managers at a 588-bed hospital when they first approached Zingbox. Coordination between clinical and security teams was breaking down as each department had different answers for exactly how many devices had come online. The hospital's visibility problem had grown so complex that the security teams resorted to managing a spreadsheet that listed every device entering the system. While this provided them with some amount of inventory capability, this was a highly manual, time-intensive process that still didn't offer them enough details to determine if all the connected medical devices were behaving normally. This left them powerless to enforce security on these devices.

However, even though their spreadsheet didn't meet their needs for a real-time inventory of medical devices, it was the least intrusive option that the hospital security managers could find. They contacted several vendors in search of a better solution, but too many required modifying medical devices in ways that could leave the hospital liable if the devices malfunctioned. Many vendors also required that they shut down their network for a given period of time during installation, which would have proven costly and disruptive to patient care. Still other vendors had security products that weren't specifically engineered to protect IoT devices.

A Precise, Non-Intrusive Security Snapshot

With Zingbox's IoT Guardian, the hospital found the precise, holistic, and non-intrusive solution they needed. IoT Guardian provided details of all devices, categorized each device and established its baseline for normal behavior. It gave the hospital a definitive hub of information that streamlined communication between teams, providing clear answers for anyone in any department, at any time of day. And all these features were implemented with no network disruption and without any modification to device hardware or software.

The hospital's engagement with Zingbox began with a Proof Of Concept (POC) and quality review of their network that was kicked off in few days, which is far below average for the industry. A week into the POC, Zingbox had completed full implementation of the solution, creating an accurate inventory of close to 5,000 devices in the hospital's network, discovering and categorizing over 95 percent of medical devices. The hospital's previous security tools only detected and identified about 5 percent. At the conclusion of the POC, Zingbox discovered 17 connected medical devices that were vulnerable to the latest cyber threats.

> "The Zingbox solution discovered over 95 percent of medical devices compared to current tools that could only detect about 5 percent."

This categorization process is a key reason why IoT Guardian could so effectively discover, discern, and defend the hospital against security risks. By leveraging machine learning and three-tier profiling techniques that go beyond identifying each device's manufacturer and model number, IoT Guardian baselined acceptable behaviors and from it, created the unique "personality" of each device. This enabled the hospital to identify not only the kind of device — for example, an x-ray machine — and whether it was online, but also the typical days and times it was used, who used it, and many other details unique to this device's utilization in this particular hospital. As the hospital's director of internet services and telecommunications says, "The intelligence and accuracy of elaborate device personalities allowed us to turn Zingbox into a tool that regulates medical device behaviors."

A Partnership That Empowers the Customer

Zingbox's mission is to empower the customer with products that provide automatic peace of mind and the ability to take decisive action. At the hospital where IoT Guardian was implemented, the IT teams could assess risk on an ongoing basis with a simple glance at a dashboard, no matter how many medical devices were being added to the system every day. Because the product proved to be so easy and effective, the hospital now uses it to secure not just medical devices but also surveillance cameras, HVAC systems, and other IoT devices.

And when widespread security issues strike systems around the world, the hospital is protected by 24/7 monitoring and alert services. For example, when the WannaCry ransomware attack disrupted more than 230,000 computers worldwide in May 2017, Zingbox proactively contacted the hospital to assure them that they were monitoring any possible risks to their infrastructure. While many healthcare systems' operations were disrupted after the attack, the hospital didn't suffer any losses.

But even though IoT Guardian provides seamless security behind the scenes, Zingbox also provides front-and-center customer service for the hospital. Once a month, a dedicated customer success manager meets with the hospital's IT team to discuss product updates and their long-term aspirations.

In healthcare, protecting patients is an industry-wide responsibility. By implementing today's most state-of-the-art IoT security platform and building lasting partnerships with every customer, Zingbox enables healthcare systems to integrate technology into their care experiences without compromising their patients' safety. With this strong security foundation, providers can more effectively heal their patients through technological innovations that advance care.

About Zingbox

Zingbox IoT Guardian is an Internet of Things security solution that provides visibility into and protection for enterprise IoT assets against cyber and insider threats. A non-intrusive, agent-less, signature-less solution, IoT Guardian uses machine learning for asset discovery, risk assessment, baselining the normal behavior of devices, and discovery of threats. Zingbox was founded by Silicon Valley IT industry leaders and experts in networking, big data, IoT and security.