BayCare

CASE STUDY

BayCare's Prescription for Protecting Healthcare IoT

BayCare Health System, a leading not-for-profit Florida healthcare provider, uses Palo Alto Networks IoT Security to secure all its traditionally unprotected Internet of Things and Internet of Medical Things (IoT and IoMT) devices easily, efficiently, and effectively.

paloalto NETWORKS

IN BRIEF

Customer

BayCare Health System

Industry

Healthcare

Country

United States of America

Products and Services

Medical care

Organization Size

25,600 employees, with 500 providers in 160 locations, including 15 hospitals

Challenge

BayCare was searching for a solution that could protect its traditionally unsecured IoT and IoMT devices from attack as well as increase visibility and security for the entire system.

Requirements

- Discover and identify thousands of unknown devices
- Monitor 33,000 medical and IoT devices
- Maintain visibility and communication without any agents or clients
- Categorize threats and elevate critical ones

Solution

Thanks to Palo Alto Networks IoT Security, BayCare was able to dramatically increase visibility into connected medical and IoT device communications and secure these previously unsecured devices.

IoT Security Ensures a Healthier Security Posture

BayCare Health System is a major not-for-profit healthcare provider serving patients across the Tampa Bay and West Central Florida regions. As one of the largest private employers in the area, BayCare not only delivers outstanding medical care to its patients and the community but also provides an estimated $6.62 billion in annual impact on the state economy. Protecting BayCare from attacks helps bolster both the physical and financial health of the region.

BayCare's security team understands that in healthcare, downtime simply isn't an option. To provide consistent, excellent care, they must secure patient information and maintain patient privacy while also protecting the entire organization from cyberattacks, ransomware, and system interruptions. This requires them to secure a growing number of networked medical devices typically running on unpatchable legacy systems.

Challenge

SECURING TRADITIONALLY UNSECURED MEDICAL IOT DEVICES CALLS FOR A NEW APPROACH

Specialized medical devices often run on older or outdated operating systems, and they usually go unpatched due to the need for FDA validation and certification. In fact, according to Unit 42 research, 83% of medical imaging devices ran on unsupported operating systems in 2019—a 56% increase from 2018. Legacy antivirus and other traditional security solutions often interfere with these devices, potentially disrupting patient care. Furthermore, the machines are networked together to deliver relevant information to providers across the BayCare system, compounding the risk to the organization.

Ralph Oliva, BayCare's manager of medical device integration and security, knew these medical devices needed to be protected and that he and his team needed visibility into how the machines were communicating with the outside world. He also knew BayCare wasn't alone in needing to protect unsecured medical devices—it was a problem that had plagued medical systems for years. When talking about their challenges protecting their growing array of medical devices, he shared, "This isn't a BayCare problem. It's an industry problem."

Requirements

Like so many modern healthcare providers, BayCare needed a security solution that could identify and protect all its unsecured devices, no matter what they were, where they were, or what operating system they used. Oliva and his team were looking for a state-of-the-art system that was:

- Agentless and passive
- Device manufacturer- and operating system-agnostic
- Able to monitor all of the organization's medical and IoT devices

> "We all have the same problem. We all run million-dollar medical devices on legacy operating systems that unfortunately can't be patched."
>
> **— Ralph Oliva, Manager of Medical Device Integration and Security**

Solution

PALO ALTO NETWORKS IOT SECURITY SPEEDS UP PREVENTION

BayCare identified Zingbox IoT Guardian—now Palo Alto Networks IoT Security—as a security solution that looked to offer exactly what they needed. The team quickly set up a proof of concept (POC) at one of their hospitals to determine the effectiveness of the 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 implemented this solution."

Based on this success, BayCare's information security executive team quickly approved the rollout of the solution to all 15 of its hospitals. Based on the success of the POC, BayCare's information security VP and chief technology officer Scott Patterson challenged Oliva to see if his team could implement the solution across the system even more quickly than the planned three-month rollout. Oliva and his team had it up and running in all BayCare's hospitals in just three weeks.

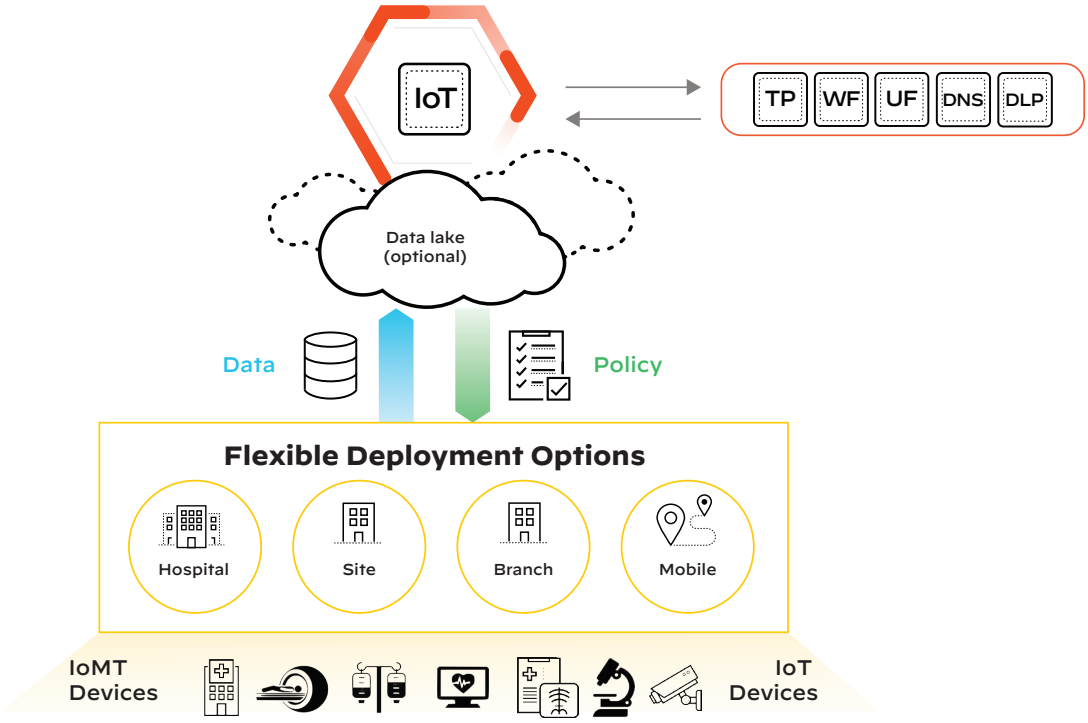

Figure 1: The healthcare industry's most comprehensive IoT security solution, delivered effortlessly as a single platform

Benefits

BETTER INSIGHT AND VISIBILITY LEAD TO BETTER PROTECTION

BayCare now uses Palo Alto Networks IoT Security to monitor all IoT and IoMT devices across its environment. 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. IoT Security has fundamentally changed BayCare's security posture. "Without it, we simply would not have known about these types of behaviors," Oliva says.

Table 1: Goals and Outcomes of IoT Security for BayCare

Goals	Outcomes
• Increase overall visibility • Use an agentless, passive, and device-agnostic solution • Monitor all of BayCare's medical and IoT devices • Secure tens of thousands of IoT and IoMT devices as well as legacy systems • Increase overall security	• Implemented in just three weeks • Discovered and identified thousands of unknown devices within hours of deployment • Now monitoring 33,000+ medical and IoT devices • Improved insight on device behavior and usage, resulting in better protection • Gained visibility into actionable threats • Now delivering fast, effective threat response via high-severity text alerts and categorization of threats

CONSTANT MONITORING ENABLES QUICKER, MORE TARGETED RESPONSES

Today, if one of BayCare's devices starts acting outside of its normal behavior, Oliva and his team get notified by text and email as well as on their dashboard and can respond immediately. The BayCare Security & Network Operation Center also actively monitors these same alerts 24/7. To combat alert fatigue and noise, IoT Security categorizes the threats it uncovers and highlights critical ones so the team knows to address them right away. BayCare now uses IoT Security to monitor more than 33,000 devices.

BayCare isn't just a healthcare provider. It also employs more than 25,000 Floridians and adds more than $6.5 billion annually to the local economy.

A Cure for an Industry-Wide Problem

Vulnerable medical devices have troubled the entire healthcare sector for too long. With the valuable patient data they hold, healthcare organizations have been subject to an increasing number of attacks.

BayCare used to struggle to secure the ever-growing number of medical and IoT devices across its network. Happily for Ralph Oliva and his security team, Palo Alto Networks IoT Security has finally filled this dangerous vulnerability gap.

Visit us online to find out more about how IoT Security can help you improve visibility, protect your medical and IoT devices, and strengthen your overall security posture. You can also start a free trial and see the benefits of IoT Security in your own environment.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com