Baptist Healthcare Case Study

BACKGROUND

Baptist Health is a full-spectrum health system made up of nine hospitals, 23,000 employees (in addition to more than 2,000 independent physicians), more than 400 points of care, and nearly 2,500 licensed beds.

The organization's employed provider network, Baptist Health Medical Group, has close to 1,500 providers, including more than 750 physicians and over 740 advanced practice clinicians.

Baptist Health is working to strengthen its cybersecurity posture and Zero Trust platform by adding more layers of defense and equipping itself with the relevant tools to protect against the next generation of attacks.

CHALLENGE

Baptist Health operates and relies on an extensive system of medical devices, IoTs, and traditional IT equipment, all of which need to be properly managed to ensure the efficacy of cybersecurity efforts; an asset inventory is, therefore, critical.

However, an accurate asset inventory is difficult to achieve; a lack of Layer 1 visibility means that "understanding what's in our facilities at any given time is a big challenge," says Michael Erickson, CISO of Baptist Health.

This is a significant risk as the new generation of attack tools is "getting more sophisticated and smaller." These tools hide within other assets – be it medical devices, IoTs, peripherals – and exploit the Layer 1 blind spot by spoofing legitimate devices.

"If you have an attack tool that's designed to actually look like, or simulate or impersonate something that's relatively benign, and it's in your environment and it's not doing anything, it's pretty difficult to know that it's there", says Michael.

Security solutions cannot differentiate between a legitimate HID, a MAC spoofing device or any other rogue device, thus allowing the latter to bypass security controls and initiate harmful attacks. With countless devices in use at Baptist Health, ranging from critical medical devices to everyday peripherals, there is cause for concern regarding their integrity. "When you think about the delivery of a piece of equipment, are we able to be sure that the equipment that was delivered is actually what was designed by the manufacturer?"

BAPTIST HEALTH

Industry: Healthcare

IT environment: 25,000 employees covering 4 states in Southeastern US with over 330K connected devices

HAC-1 SOLUTION

Visibility

Sepio's Hardware Access Control (HAC-1) solution deals with the root cause of the problem –asset visibility by using a new data source – Physical Layer – L1 data. HAC-1 provides complete visibility of all IT/OT/IoT hardware assets, whether they are managed or unmanaged. "[HAC-1] is helping us increase our visibility, including the network [and] helps us to monitor the existence of devices down to the peripheral level, including mice and keyboards and wireless devices." Michael states. The solution goes deeper than any other security tool by using various Layer 1 parameters to generate a digital fingerprint of every device and assign it a risk score.

Additionally, HAC-1 identifies anomalies in device fingerprints to detect suspicious activity that would otherwise go unaccounted for. "[Sepio is] able to understand if [a] device has anything embedded in it, or an extra chip set that may not be what it poses to be or what it's designed to do", says Michael.

The Layer 1 visibility provided by HAC-1 provides Baptist with "a much more robust dataset" that, in turn, enhances asset management. More than that, "it's really helping in terms of business decision support in ways we hadn't predicted. We're bringing a new set of information to our asset inventories and it's helping us better plan the lifecycle of assets. Also, we are gaining a better understanding of what devices we need," Michael adds about HAC-1.

Policy Enforcement

HAC-1 enables greater control over hardware assets through its policy enforcement feature - which capitalizes on the solution's ultimate asset visibility. The system administrator defines a set of rules for the system to enforce based on roles or device characteristics.

HAC-1 compares a device's digital fingerprint with the pre-defined rules, ensuring that only authorized devices are granted access, thus enabling a Zero Trust Hardware Access approach that Baptist uses as part of their overall Zero Trust platform. "Using Sepio's tool, we can add a layer of authentication at the device layer," states Michael.

> *HAC-1 is helping us increase our visibility, including the network, and helps us to monitor the existence of devices down to the peripheral level, including mice, keyboards and wireless devices.*
>
> **Michael Erickson | CISO**
> Baptist Health

Rogue Device Mitigation

Through its complete asset visibility and policy enforcement features, HAC-1 provides Rogue Device Mitigation. For Michael, preventing hardware-based attacks "is a critical component of Baptist Health's Zero Trust strategy" as "we've been seeing an increase in the number of low-cost and highly effective tools in that market that are designed to look like benign peripheral devices."

HAC-1 instantly detects any device that breaches the pre-defined policy or gets identified as malicious by the solution's internal threat intelligence database. The unauthorized device triggers an alert, and HAC-1 initiates an automated mitigation process, carried out by third-party tools, to block the device.

Smooth Deployment and Implementation

HAC-1's seamless integration with third-party tools makes it an important layer in Baptist Health's Zero Trust approach; while also putting such tools to better use by providing greater visibility, thus maximizing security investments.

HAC-1 requires no hardware resources and does not monitor any traffic or disrupt the networking infrastructure, allowing for speedy and smooth widespread deployment. Further, as an autonomous and self-contained solution, HAC-1 requires minimal human intervention, and the straightforward user interface can get managed by non-cybersecurity experts. Thanks to its low maintenance requirements, "[HAC-1] happened to be something that was very lightweight and something very simple to install. And we saw value from it very quickly, without adding staff", praises Michael.

We're bringing a new set of information to our asset inventories and it's helping us better plan the lifecycle of assets and better understand what devises we need so we're better at asset management.

Michael Erickson | CISO
Baptist Health

HAC-1 requires no additional hardware resources, no additional staff, doesn't monitor any traffic or disrupt networking infrastructure, and has low maintenance requirements. We saw value from it very quickly.

Michael Erickson | CISO
Baptist Health

HAC-1 - VISIBILITY & SECURITY OF HARDWARE ASSETS

Main Benefits

Complete Visibility of all Hardware Assets: With all devices and anomalies detected, enterprises benefit from a greater overall cybersecurity posture. Gaining full visibility of all hardware devices from endpoint peripherals to connected devices (IT/OT/IoT), Sepio uses unique physical layer hardware fingerprinting technology and data augmentation from endpoints and networks.

Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.

Rogue Device Mitigation (RDM): Threat mitigation upon discovery of rogue or threatening devices. Integrations with existing security platforms such as NACs and SOARs for mitigation and remediation enhancements.

System Architecture