



BEACON HEALTH SYSTEM

VTM, SIEM, DLP, Connected Medical Device & IoT Security Program

The Need

In recent years, Beacon Health System was created from its roots as two small community hospitals coming together into a thriving regional medical center with more than 800 beds and 7,000 associates. To support its expanded footprint, the northern Indiana Health System needed a partner to strengthen its overarching cybersecurity program.

Under the leadership of Mark Warlick, Chief Information Officer and Brian Abel, Director of Information Security and Project Management, Beacon and Fortified Health Security took a baseline of its security controls. At the time, the health system's latest score from the NIST 800-53 risk analysis was in the lower quartile for health organizations of a similar size.

The organization had moderate system development with Data Loss Prevention (DLP), and had deployed a Security Information & Event Management (SIEM) solution on limited systems. In addition, like most healthcare organizations today, there was zero SIEM visibility into their medical device inventory, as well as the risks that are associated with those connected devices.

Complicating matters during the formation of Beacon was the requirement to consolidate policy and implementation of a more unified and centralized cybersecurity program. Beacon's talented IT security staff was already stretched thin, and needed support to address these and a range of other cybersecurity issues. They called on Fortified to work within Beacon's budget parameters, to leverage existing investments in security solutions, and to elevate the hospital system's overall security posture.

The Solution

Working alongside Beacon's team of security professionals, Fortified began by implementing an industry leading Data Loss Prevention solution to gain visibility into what data was moving about as well as leaving the organization, and to develop new technical policies for safely transmitting sensitive data. The DLP solution was in place, operational, and effectively configured within 60 days of purchasing the product.

The Organization

Beacon Health System is northern Indiana's most trusted partner and guide to creating and maintaining health and well-being. Its awardwinning partners — Elkhart General Hospital, Memorial Hospital of South Bend, Beacon Children's Hospital, and Beacon Medical Group — are powered by more than 7,000 associates providing the best care possible to people of all ages.

As the regional leader in childbirth, mental health, cancer, pediatrics, trauma, heart and vascular care, stroke, surgery, weight loss services and community health programs, Beacon Health System helps the region achieve the highest quality of life.

Size

853 Beds

Location

Indiana

Website

www.beaconhealthsystem.org

Client since 2017

Employed Fortified services

Vulnerability Threat Management (VTM)

Security Information & Event Management (SIEM)

Data Loss Prevention

Connected Medical Device & IoT Security Program

Security Risk Assessment



Next, Fortified deployed its Vulnerability Threat Management (VTM) solution for monthly internal and external scanning. This would be an instrumental component to prioritize Beacon's patch management efforts. In an attempt to harden the organization's network, Beacon invested in next generation firewalls, which added full VTM IDS/IPS functionality. Additionally, through the partnership with Fortified, Beacon migrated the hospital's older and underutilized tool for SIEM monitoring into a new, fully managed solution that provides more robust and proactive threat monitoring capabilities.

Together, the Fortified VTM and SIEM solution quickly gave Beacon critical visibility into all its cybersecurity solutions working in tandem and in real time. Previously, an intrusion detection event and a system event alert occurring simultaneously would have been difficult to determine because the data was not being correlated. Fortified's integrated solution and managed service enables Beacon to determine an actual vs. perceived threat to the organization, and to respond accordingly. Today, threats like these are visible via a consolidated single pane of glass dashboard.

In addition to maturing their compliance-driven security initiatives, Fortified helped Beacon move to the forefront of new cybersecurity protection efforts aimed directly at clinical infrastructure and patient protection. Threat monitoring is now enabled on the health system's smart IV pumps and patient vital checking devices via Fortified's Connected Medical Device & IoT Security program. If the solution sees a device with activity that is unusual to the specific profile of that device, real time alerts are sent to the Beacon incident response team. This solution is also integrated into the Fortified single pane of glass dashboard.

The Outcome

Beacon's NIST data security scoring has doubled since it began working with Fortified in the spring of 2017. It has moved from being in the 25th percentile for data security to the 50th percentile. The health system believes it is on track to move to the 70th percentile by April 2019 through its continued partnership with Fortified, thus moving the organization to the higher end of Health Systems nationwide.

For Abel, the ability for Fortified to provide transparency for the Beacon environment and its associated risks is a substantial win for the health system. They now have insight into the databases that maintain sensitive data such as patient information (PII, PHI), and have the ability to monitor internal, external, and previously unknown threats.

With the assistance of Fortified, the next phase in Beacon's program includes plans to classify and secure the hospital system's Intellectual Property, including Board of Directors meeting notes, strategic plans and other sensitive information.

In spite of the far-reaching nature of the security program restructuring, the impact on associates and patients was minimal and did very little to impede the valuable flow of data throughout the organization. The number of Help Desk tickets was low — even during the implementation phase. Fortified was responsive to Beacon's budget and process, and worked within the organization's quarterly goals to distribute the costs of the project in as flexible a manner as possible.

About Fortified Health Security

Fortified Health Security is healthcare's recognized leader in cybersecurity — protecting patient data and reducing risk throughout the Fortified healthcare ecosystem. As a managed security service provider, Fortified works alongside healthcare organizations to build tailored programs designed to leverage their prior security investments and current processes while implementing new solutions that reduce risk and increase their security posture over time. Fortified's high-touch engagements and customized recommendations provide ROI and result in actionable information to reduce the risk of cyber events. The company is 100% committed to creating a stronger healthcare landscape that benefits more clients, protects more patient data, and reduces more risk.



Never take good relationships for granted. It's amazing who will cover for you and get things done when you need it the most. Fortified never failed to surprise me. They said whatever you need, we'll take care of it. Not many of them do that.

Brian Abel | Director of Information Security and Project Management
Beacon Health System

