MEDIGATE

How a Cyberattack Drove HVHS to IoT Security Maturity

Case Study

Executive Summary

Heritage Valley Health System (HVHS) is an integrated delivery network providing health care for residents throughout Western Pennsylvania, Eastern Ohio and the panhandle of West Virginia. In addition to several national care quality awards, HVHS was recently recognized by the College of Healthcare Information Management Executives (CHIME) as one of the nation's "Most Digitally Wired" health systems.

Having experienced a disruptive *NotPetya* cyberattack in 2017, HVHS leadership took action to modernize its cybersecurity infrastructure. Recognizing the need for more comprehensive and detailed asset visibility, IoT cybersecurity vendors were competitively evaluated and Medigate was selected.

Notably, rapid recognition of the operational value of the delivered data quality drove Biomed and Clinical Engineering project engagement. Outdated security and asset management routines were identified and eliminated. Armed with a comprehensive connected asset knowledge base spanning all three hospital facilities, integrations to Endpoint Detection/Response and Vulnerability Management were executed. In addition, a Cisco ISE Network Access Control (NAC) initiative along with Check Point firewall deployments are now underway and ahead of schedule.

Uniquely Connected. For life.℠
HERITAGE VALLEY HEALTH SYSTEM

Company:
Heritage Valley Health System

Industry:
Healthcare

Bed Size:
700

Website:
www.heritagevalley.org

Challenges

Security, Biomed, Clinical Engineering and IT staff needed a way to effectively collaborate at all times -- not just during emergencies.

- No mechanisms for updating existing inventories were in place. The available data were incomplete, siloed and largely outdated.
- Vulnerability Management (VM) practices were a concern, as medical and non-medical assets could not be distinguished.
- Cross-functional troubleshooting was inefficient, as stakeholders had different views and understandings of the asset(s) in question.

Solution

A dynamic, risk-scored inventory of all connected assets was quickly delivered as a common, shareable foundation. Cross functional engagement was quickly achieved.

- Existing vulnerabilities across facilities were identified and real-time alerts were generated to initiate timely remediation.
- Medigate's integration to EDR and VM platforms enriched existing asset data and further refined risk scoring. Product recall management processes also saw instant improvements.
- Knowledge of device attributes, security posture and network status improved productivity; relevant cuts of the underlying data were orchestrated as workflow enhancements that were naturally adopted.

Results

HVHS's positive response to its negative cyberattack experience is noteworthy. Committed to infusing security best practices into cross-functional workflows, investments in risk reduction practice have accelerated its journey to operational maturity.

- HVHS security ecosystem is now considered market leading.
- CISO-led security decisions are viewed as enablers of value-based care.

The data orchestrated throughout HVHS's now integrated asset management and security ecosystem are continuing to deliver new efficiencies and insights. Resulting new asset utilization insights, for example, are now being analysed by Finance to improve capital planning.

> *"During our solution evaluation phase, we focused on the ability each vendor demonstrated in passively identifying our medical device connected asset inventory. Not only did Medigate accurately identify a multiple of the devices discovered by its competitors, but the level of device attribution they delivered made our decision to go with them easy. The results of our Proof-of-Value gave us confidence that our asset management and security objectives were realistically achievable."*

Robert Swaskoski,
Chief Information Security Officer
Heritage Valley Health System

MEDIGATE

Get in touch

Email: **contact@medigate.io**
Visit: **medigate.io**