CASE STUDY

HOW A CYBERATTACK ACCELERATED HVHS TO IoT SECURITY MATURITY

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, the College of Healthcare Information Management Executives recognized HVHS as one of the 'Most Digitally Wired' health systems. After a disruptive NotPetya cyberattack in 2017, HVHS recognized a need for detailed clinical device data as a part of their cybersecurity infrastructure modernization strategy.

After selecting Medigate, which is hosted on Amazon Web Services (AWS), HVHS leadership recognized the value of accurate clinical device details. Armed with comprehensive knowledge of connected assets across all three hospital facilities, they found that HVHS could eliminate several outdated security and asset management routines. Additional integrations to Endpoint Detection/Response (EDR), Vulnerability Management (VM), Network Access Control (NAC), and Firewalls dramatically improved their overall security posture.

Uniquely Connected. For Life.℠
HERITAGE VALLEY HEALTH SYSTEM

Company:
Heritage Valley Health System

Location:
Beaver, PA

Number of Beds:
392

Number of Hospitals:
3

Website:
heritagevalley.org

Challenges

- Device data were incomplete, siloed, and largely outdated, with no validation mechanisms in place.
- VM tools could not distinguish medical and non-medical assets.
- Inefficient troubleshooting, as stakeholders lacked a common data set about the asset in question.

Solution

After a thorough evaluation, Heritage Valley Health System selected Medigate as their Healthcare IoT security partner. They deployed Medigate's Core Visibility, Insights, and Anomaly Detection platform and enabled the Clinical Cyber Hygiene, Network Policy Management, and Clinical Device Efficiency modules.

- Medigate enabled notification of known CVE's and recalls.
- Integration with VM tools enabled clinical context information for endpoint scanning.
- NAC integration allowed for dynamic device segmentation policies.
- Up-to-date asset inventories allowed for data-driven device procurement.

Results

After a negative cyberattack experience, HVHS mounted an effective response, and their security ecosystem is now considered market-leading. Today, CISO-led security decisions are enablers of value-based care.

- Vulnerability identification and real-time alerts initiate remediation workflows.
- EDR and VM platforms enrich asset data and further refine device risk scoring.
- Knowledge of device attributes, security posture, and network status improve overall productivity.
- Asset utilization data improves supplier negotiations, maintenance, and capital planning processes.

"Not only did Medigate accurately identify more devices than 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

And with Claroty Medigate being hosted on AWS, Heritage Valley Health System also leverages AWS Services providing the inherent scalability of AWS, encrypted connections between on-premise networks and AWS, along with the ease of integration into the AWS landscape.