CyberMDX
A FORESCOUT COMPANY

CASE STUDY

University of Michigan Health-West Secures 100+ Connected Device Types Across 26 Locations

UNIVERSITY OF MICHIGAN HEALTH-WEST
MICHIGAN MEDICINE

Summary

University of Michigan Health-West is an integrated healthcare system offering expert, award-winning care that's accessible and convenient, with a personal touch. It includes more than 26 locations across Wyoming and Michigan including hospitals, heart and vascular services, physician offices, a cancer center and more.

Challenge

"University of Michigan Health-West was looking for a solution that provided in-depth visibility and real-time discovery mapping of all connected medical and IoT devices. This was the first, yet critical step as we rolled out a comprehensive healthcare IoT security strategy with CyberMDX," said Miguel Hernandez, Security Analyst at University of Michigan Health-West.

As University of Michigan Health-West continues to move to a more digital, connected, and interoperable infrastructure, they needed a solution that was able to:

- Maintain a real-time, automatic connected device inventory –
  - What are all of the connected devices (medical devices, IoT, IT and OT)?
  - Where are all of the connected assets?
  - Which type of risk is associated with each device?
- Agentless protection of unmanaged devices that remained unprotected by AV/EDR solutions
- Detect threats in real time (i.e. east-west traffic)
- Automatically track medical device recalls
- Gain insight into device utilization metrics

Solution

The CyberMDX Healthcare Security Suite was exactly the solution University of Michigan Health-West needed to identify, categorize and secure all connected medical and IoT devices. Deployment was quick and

> *We joined forces with CyberMDX to help ensure patient safety and improved care with 360-degree visibility and security into all of our connected technologies.*

Miguel Hernandez
Security Analyst
University of Michigan Health-West

University of Michigan Health-West was able to gain visibility and insight into the connected devices on their network. The centralized installation required only two sensors, and the cloud-based web console allowed for highly distributed facility coverage.

Now, University of Michigan Health-West was able to get full discovery and profiles of all the connected (managed and unmanaged) devices in their network, whether medical devices, IoT, workstations, mobile and more. Each connected asset had a risk profile created, and any malicious activity detected provides customized alerts to the security team.

The University of Michigan Health-West team took advantage of CyberMDX's comprehensive dashboards and reports for clinical network and medical device security, helping the information technology (IT) and security teams to share information and collaborate more than they had in the past.

Results

The solution provided different importance to different teams at University of Michigan Health-West. The real value was in everyone being able to access a single source of truth but seeing it in a way that was specifically relevant to their role.

Team	Value Defined
Executive team and Board	• Device utilization analytics • Optimize incident response • Business value dashboards
IT Networking / Security teams	• Device risk management • Active vulnerability scanning optimization • Real time asset discovery • Updated CMDB • Network segmentation planning • Threat detection
BioMed/ Clinical Technicians	• Recall notifications • Streamlined patch management • MDS2 validation • Device location • Device data flow • Manage vulnerabilities and recalls

Quick & efficient deployment covering dozens of distributed sites

More than 115 different types of devices identified and classified

Customized reports for IT, Biomed, Compliance and Executives

Highlighted security issues related to ePHI, patient safety, and Internet exposure

APR22