CyberMDX

CASE STUDY

CyberMDX Brings Device-Centric Insights Across 60+ Models to Englewood Health

Challenge

Englewood Health, one of the leading hospitals in New Jersey, recognized the need for a security and visibility management platform for the clinical assets used throughout the organization. They were lacking insight into the number of deployed devices, both managed and unmanaged, challenged with the existing manual and error-prone process for device inventory. The biomedical and clinical teams also wanted a solution that provided real-time visibility into the network that would enable them to prioritize remediation and receive alerts when a device was at risk. Englewood Health was looking for one platform that could be used by multiple departments: Clinical Engineering, Security, and IT.

Solution

The CyberMDX Healthcare Security Suite was chosen as the exclusive solution for providing Englewood Health with a comprehensive platform to identify, categorize, and secure all connected medical devices. The agentless deployment was completed within a few hours, bringing visibility to the clinical network and shedding light on the hospital's blind spots. Based on its superior integration with multi-vendor platforms, future plans include integrating the solution with a network access control (NAC) solution.

The CyberMDX solution enables hospitals to identify, access, detect, and defend against potential cyber-attacks with continuous discovery of IoT and medical devices, comprehensive risk assessment, and AI-based containment and response. It's enterprise-grade, with support of SSO, MFA, and RBAC.

Summary

Englewood Health is one of New Jersey's leading hospitals and healthcare networks. Composed of Englewood Hospital, the Englewood Health Physician Network, and the Englewood Health Foundation, the health system delivers nationally recognized care in a community setting to residents of northern New Jersey and beyond. The organization is continually expanding services and enhancing access through the Englewood Health Physician Network. This coordinated network of office-based and hospital-based providers, connected through a single electronic health record, offers primary care and specialty services at more than 75 locations in six counties.

Additionally, the solution detects and evaluates potential threats with comprehensive vulnerability and threat detection. It provides real-time threat analysis and operational status using an agentless deployment model, without requiring client software on any medical device in your network.

Results

Englewood Health was able to realize benefits from the solution immediately, including:

- Full discovery and profile of medical devices in the network; 99% of the medical assets were identified and profiled automatically (vendor, model, OS mac, serial number); with more than 60 different medical device models, including previously unknown connected devices.
- A risk profile was diagnosed for each connected asset, with an associated security insight and recommendation for each one. More than 50 vulnerable devices and credential flaws were found.
- Granular visibility to current network segmentation, including analysis of medical devices and non-medical devices in each segment, connectivity between VLANs, and breakdown of devices by type and vendor
- Threat detection - Anomaly and malicious activity detection with customized alerting.
- Comprehensive visibility platform and dashboard for clinical network and medical device security, supporting both the biomedical and IT security teams. In the past, these departments operated separately with little collaboration between them. With the CyberMDX solution, they now work together to ensure the security of the network and the safety of their patients.
- Seamless integration: Quick, agentless Integration with Symantec for log review/monitoring.

> *"CyberMDX's solution automatically identified all connected medical devices on our network including model numbers and MAC addresses, showed us what they are connecting to, and helped us prioritize by providing a risk level for each device.*
>
> **Vince Rosati,**
> **Director of Biomedical Engineering**

99% of medical assets identified

More than 50 high risk devices identified

Customized reports for IT and IS teams