CyberMDX
A FORESCOUT COMPANY

CASE STUDY

CyberMDX Delivers Security and Control of Thousands of Connected Devices

Challenge

Assuta Medical, the largest private hospital network in Israel, was manually conducting physical inventory of connected medical devices every year which would takes months to be completed. They also had a policy to segment all of their medical and clinical devices from the other non-medical devices, however the existing security and network technology tools in place could not automatically distinguish between general IT endpoints such as laptops, tablets smartphones and medical devices. The hospital needed a security assessment of each medical device, wanted to be alerted when a device was at risk and needed the ability to prioritize remediation above other non-critical systems. In order to do that it would need technology that easily identified medical devices so that these additional policies could be applied.

30%
Attack surface reduction

50%
Reduction of potential new and unknown threats

100s
Hours saved in their inventory mapping labor

The hospital was seeking an automated technology solution that would identify and provide a detailed inventory and classification of connected medical devices so that they would no longer have to manage this manually using spreadsheets. They also sought a solution that would provide a risk assessment for each device. They needed to look both the device configuration such as open ports, segmentation and default password usage as well as vulnerabilities related to the version of operating system.

Assuta
RAISING HEALTH STANDARDS

About Assuta Medical

- Largest private hospital network in Israel
- Operates 9 hospitals and medical centers
- Owned by Maccabi Healthcare, the second largest HMO in Israel
- Performs approximately 15% of surgeries in Israel
- Cares for the health of more than 1 million patients annualy
- Holds JCI quality accreditation with excellence
- Service standards are ranked as top tier by the ministry of health

Solution

The CyberMDX solution was deployed across all 9 hospitals, providing medical device visibility and a vulnerability assessment for each device.

The CyberMDX Healthcare Security Suite was chosen due to the solution's ability to identify and assess all connected medical devices throughout the entire hospital network through continuous real-time discovery and in-depth visibility. The solution achieves this via in-depth network inspection, based on Layer7 medical protocol expertise and artificial intelligence.

The solution provides comprehensive information about the medical devices connected to Assuta's network. It can identify appropriate metadata including manufacturer, model, serial numbers, MAC address(es), IP addresses, and operating systems, eliminating the need to capture this information manually, which was tedious and inaccurate.

Assuta was also impressed with CyberMDX's ability to provide a clear and concise risk assessment of each medical device, considering their known exposures, the attack potential, and operational criticality.

Results

Significantly Improved Visibility

Across all eight sites, the hospital was provided with coverage on all of their connected devices; different devices, provided by dozens of different vendors including those for life support and imaging.

Proactive Alerts

For incidents when a medical device connected into the wrong VLAN. The system also recognized and alerted to the usage of problematic network connection credentials. In addition, it detected and alerted IT on unusual communications to the internet. Lastly, AI capabilities identified deviations from set and defined baselines between the medical devices and the corporate network.

Reduced Attack Surface

By improving segmentation and eliminating vulnerabilities, IT saw at least 30% of the attack surface reduced. This automated another manual task and provided precise recommendations on relevant action items. Initial and ongoing risk assessment and abnormalities detection recognized risky communication protocols and alerts throughout the hospital network.

Countless Hours Saved

IT teams reported hundreds of hours saved just in their inventory mapping labor alone. They also improved the accuracy of their risk assessment prioritization and overall cut in half all potential new and unknown threats.

Actionable Insights

These insights included: default password usage recognition, closing of unnecessary and dangerous management ports, helping enforce smart micro-segmentation project, finding old OS and application with vulnerabilities that needed to be updated.

> *CyberMDX's solution is innovative and adapted to the environment of hospitals. The solution was selected and deployed in all eight Assuta hospitals and medical centers after we realized there was a growing threat between cyber threats and existing security solutions we had deployed. The unique technology enables us to control and manage the security of thousands of connected devices within the network, as well as prevent in advance cyber attacks from happening. The solution illuminated dark parts of the network, some of which are at high risk, which were unseen and unprotected before by any existing technology.*
>
> **Tamir Ronen**
> Chief Information Security Officer at Assuta Medical Center

APR22