Forescout Medical Device Security Delivers Security and Control of Thousands of Connected Devices

30%
attack surface reduction

50%
reduction of potential new and unknown threats

100s
of hours saved in their inventory mapping labor

About Assuta Medical

- Largest private hospital network in Israel
- Operates nine 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 one million patients annualy
- Holds JCI quality accreditation with excellence
- Service standards are ranked as top tier by the ministry of health

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. To do that it would need technology that easily identified medical devices so that these additional policies could be applied.

The hospital was seeking an automated 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 see both the device configuration (such as open ports, segmentation and default password usage) as well as vulnerabilities related to the version of operating system.

Solution

Forescout Medical Device Security was deployed across all nine hospitals, providing visibility and a vulnerability assessment for each device.

This technology was chosen for its ability to identify and assess all connected medical devices throughout the entire hospital network through continuous, real-time discovery and in-depth visibility. It achieves this via in-depth network inspection based on Layer7 medical protocol expertise and artificial intelligence.

"Forescout Medical Device Security 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 cyberattacks 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, Assuta Medical Center*

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 Forescout Medical Device Security'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 has coverage on all of their connected devices across dozens of different vendors, including those for life support and imaging.

Proactive Alerts

IT staff are now alerted about issues such as a medical device connecting into the wrong VLAN, the use of problematic network connection credentials and unusual communications to the internet. Through its AI capabilities, the system even identifies baseline deviations 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. Ongoing risk assessments recognize risky communication protocols, which generate alerts throughout the hospital network.

Countless Hours Saved

IT teams have reported hundreds of hours saved in inventory mapping labor alone. Improved risk prioritization based on more accurate assessments has cut in half the number of 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.

FORESCOUT®

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com