aireye

Hadassah Hospital enforces its wireless security policy using AirEye

Hadassah
University
Hospital
Founded by Hadassah, the Women's Zionist Organization of America

About Hadassah University Medical Center:

Hadassah's 850 physicians 1,940 nurses, 1,020 paramedical and support staff work on two medical center hospital campuses in Israel with more than 1,000 beds, 31 operating rooms, and nine specially oriented intensive care units, all managed with the combined skills of thousands of health care professionals.

Every year, Hadassah provides nearly one million people with hospital services.

Industry:	Challenge:	Solution:	Added values:
Healthcare	Enforcing Hadassah’s wireless network security policy	Network Airspace Control and Protection (NACP)	• Deploys easily and seamlessly • Increases its cyberdefense against ransomware • Eliminates gaps in network segmentation • Prevents unauthorized peer to peer connections (e.g. Wi-Fi Direct)

The Challenge

Enforcing Hadassah's wireless network security policy

Zafrir Argov, CIO at Hadassah University Medical Center, has been following the exponential increase in cyber-attacks across the medical industry.

"Healthcare, a target once considered taboo by hackers, last year became the number one target for ransomware attacks.

Hadassah is no different than other global hospitals when it comes to cyberattacks."

Responsible for the IT and security of all technological aspects at the hospital means that Argov oversees a myriad of assets in the organizational environment - from corporate networks to medical devices and applications, and even the wireless connections of random visitors such as patients, food suppliers and contractors. "In terms of cyber security, our team is not necessarily looking for more visibility. What we need to know is what an attacker can leverage, what is the current gap, and how to fix it automatically," Argov says.

For this, Argov and his team develop stringent security policies across different layers and implement in-house and vendor-provided controls for enforcement.

For instance, they knew that there were wireless networks generated by the medical devices themselves, but they wanted to ensure that Hadassah's providers were in fact placing the necessary security controls.

Argov's team focused the hospital's wireless security policy around the medical and corporate wireless networks, taking into account also wireless-capable devices in the campus that were not owned - and by nature, not controlled - by Hadassah. All the hospital's corporate and medical networks are secure with all the necessary requirements - certificates, encryptions, DLP solutions, turning off peer to peer networks, and more. Hadassah's devices communicate only on their own monitored and secured networks, while all other non-controlled devices communicate only on other open networks.

The problem was that the team was not able to fully enforce this policy. For instance, they knew that there were wireless networks generated by the medical devices themselves, but they wanted to ensure that Hadassah's providers were in fact placing the necessary security controls.

In another scenario, they were concerned that corporate machines, such as printers that were already connected to Hadassah's corporate wired network, also had their wireless capabilities deliberately turned on.

This happened when a doctor turned on Wi-Fi Direct and when the team asked him why, the doctor said he was preparing for a patient consultation and that's what he would do at home. The team's conclusion was that no matter how much security awareness training they put in place, the user will always find the workaround to get their job done. "The only way we could find out these wireless policy violations was by manually walking around the campus looking for wireless signals, say, broadcasted from medical devices or even the hospital's printers. An infeasible solution, to say the least", he noted.

"[Ransomware] is one of our worst-case scenarios. The medical devices are life-critical - they're not desktops or servers that I can roll back to their latest backup. We can't just turn one of the devices off. The impact of this could be as serious as creating a medical center with an incredibly knowledgeable staff but with the technology of the '50s,"

The Solution

Network Airspace Control and Protection (NACP)

Enforcing the wireless policy was critical. Argov was very much concerned that these Wireless Receptors - those wirelessly-connected devices that connect also to the hospital's wired network - can act as entry points to attackers. Once ransomware takes control of such a Wireless Receptor, it can also propagate within the hospital's network. "That is one of our worst-case scenarios. The medical devices are life-critical - they're not desktops or servers that I can roll back to their latest backup. We can't just turn one of the devices off. The impact of this could be as serious as creating a medical center with an incredibly knowledgeable staff but with the technology of the '50s," he stressed. is the current gap, and how to fix it automatically," Argov says.

For this, Argov and his team develop stringent security policies across different layers and implement in-house and vendor-provided controls for enforcement.

The risk was insurmountable when it came to a campus with so many visitors and their uncontrolled digital devices. "This makes the issue so acute. Even if we can somehow try and workaround the issue of Wireless Receptors, we have no visibility or control over the visitors' devices. Is there a compromised visitor device with a hacker sitting thousands of miles away trying now to wirelessly connect to one of Hadassah's X-Ray machines? Are visitors wirelessly connecting to X-Ray machines in search for strong signals and now causing a regulatory issue? How about a visitor's wireless device that created a new network, say by generating a hotspot - how do we ensure that one of Hadassah's devices is not connecting to it? Network logs do not show this fully and satisfactorily. These are just a few scenarios that demonstrate to us that it is possible to bypass the wireless security policy".

[They] realized that the only solution that can effectively enforce the wireless security policy and prevent this wirelessly-led abuse of the hospital's assets was a Network Airspace and Control (NACP). No other solution they had, or looked at, was able to provide, or overlap, with the type of protection they were looking for.

After researching, Argov and his team realized that the only solution that can effectively enforce the wireless security policy and prevent this wirelessly-led abuse of the hospital's assets was a Network Airspace and Control (NACP). No other solution they had, or looked at, was able to provide, or overlap, with the type of protection they were looking for.

Argov made it clear that the NACP solution they would choose would have to be "effortless". He would not allow rolling out a solution that required human resources - not during the height of the COVID-19 pandemic where human resources were so scarce.

The team tested AirEye's NACP solution and was pleased with the breadth of the solution. AirEye proved that it monitors all wireless activity in the campus airspace, all of Hadassah's corporate and medical devices as well as uncontrolled visitor's wireless devices.

"AirEye acts as a dome over our medical campus, allowing us to work as usual albeit all the wireless connections in our airspace. We assume we have open connections, but are assured that in the area where the system is installed, the chances that someone will connect to the network is low. If there's a medical device generating a new network - AirEye prevents any communication to it beyond its intended purpose. When AirEye detects a malicious or unauthorized association such as a printer with Wi-Fi Direct turned on, it blocks any connections to it."

"AirEye acts as a dome over our medical campus, allowing us to work as usual albeit all the wireless connections in our airspace. We assume we have open connections, but are assured that in the area where the system is installed, the chances that someone will connect to the network is low. If there's a medical device generating a new network - AirEye prevents any communication to it beyond its intended purpose. When AirEye detects a malicious or unauthorized association such as a printer with Wi-Fi Direct turned on, it blocks any connections to it."

The Results

Enforcement of Hadassah's wireless security policy

Five months after initial deployment, Argov and his team are still implementing the findings AirEye uncovered. "We were aware that we had visitor devices in my network, but not to the extent discovered. What we weren't aware of was the quantity of large medical uncontrolled devices in the airspace across Hadassah's two medical campuses".

Most of all, AirEye uncovered new open networks that were generated by Hadassah's medical devices such as the X-Ray devices, MRI machines, ultrasound devices, blood pressure devices, ventilators, defibrillators, and others. While these devices were connected to the corporate network to send back the patient data, they had also created their own Wi-Fi network to receive communications from patient sensors. Furthermore, Argov found through AirEye that these new wireless networks were in fact being abused, whereas visitor devices - not the device sensors - were connecting to them.

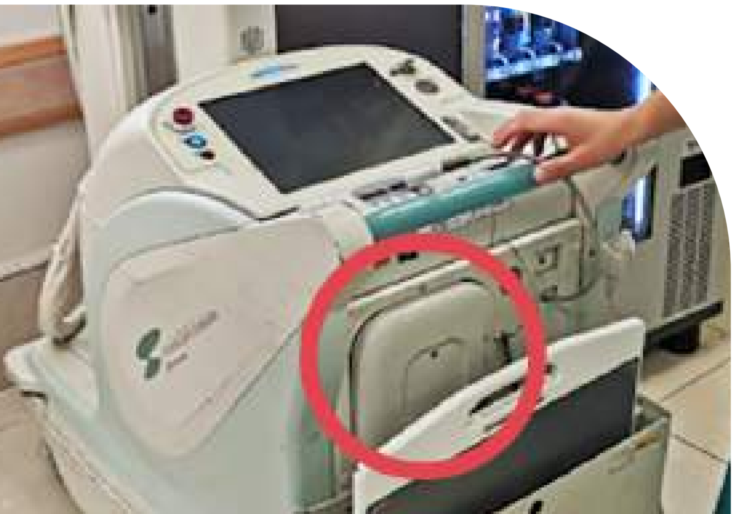
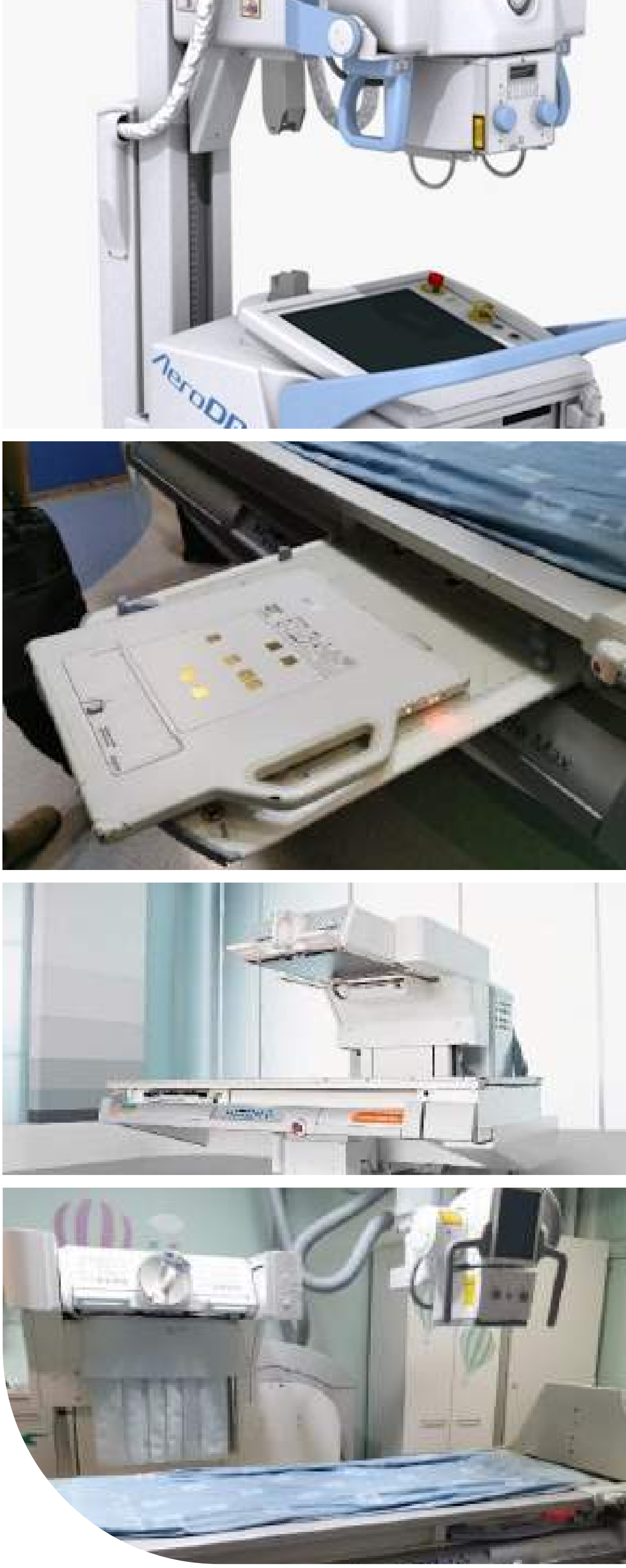


Figure 1: A wireless portable X-Ray machine. The X-Ray machine acts as an open Access Point (as indicated by the little rectangle), whereas patient data is recorded by the plates (large rectangle) and sent back to the device over Wi-Fi.



Figures 2-4: Various wireless medical devices that create open wireless connections while also connecting to the hospital's wired network.

The team were also pleased that they could eliminate gaps in their network segmentation strategy. “We make sure to segment the hospitals’ networks - we have several sub-networks where we classify and categorize which devices can use which network. Wireless capabilities challenge these segmentations since, say an MRI technician might look for a stronger signal coming from a different wireless network. Since a lot of these devices, by their design, require a manual first connection, it’s pretty trivial to do,” he explained.

Figures 5-8: Wireless blood pressure, PET-CT, ultrasound and X-Ray devices which require a manual connection to the corporate network upon initial setup or on each usage.

There were even business units that had their own purchasing power, with the mandate of purchasing projects from start to finish, and had created networks of their own. “That’s usually common in hospitals when we try to speed up operations. We’re responsible though for security and so with AirEye, we were able to regain control and protect our network airspace without impeding healthcare”.

Additionally, on a daily basis AirEye uncovered various printers with their peer to peer capability, Wi-Fi Direct, turned on. “This is a pop-the-weasel game. We keep finding new ones, turn them off, to only find new ones come up again. There is no way we could manually and continuously see when they’re switched on, and certainly be rest assured that no one is connecting to them.”

Figure 9: The healthcare division purchased a new Access Point (as indicated by the red rectangle) for a stronger wireless signal.

“At end of day, AirEye allows the team to control our airspace.” Argov concludes. “I want to make sure that there are no unauthorized connections to Hadassah’s devices, and authorized devices do not connect to unauthorized or unmonitored networks - from specific segmented networks to Guest and simply ad-hoc ones generated by visitors. Before the AirEye rollout this was just a policy on paper.
Today, it’s a policy that we can actually enforce.”

About AirEye

Enforcement of Hadassah’s wireless security policy

AirEye is the leader in Network Airspace Control and Protection (NACP).

Its AirEye Dome platform enforces the HDO's wireless security policy and prevents attacks that leverage the Antennae for Hire that are broadcasting in the HDO's network airspace.

AirEye’s SaaS solution monitors all wireless communications broadcasting in the HDO's airspace in real-time, prevents violations of corporate wireless security policy and blocks attacks automatically.