Regional Health System Increases Network Visibility and Mitigates Cybersecurity Risk

By utilizing RedSeal's Fully Managed Services (FMS) security offering, this healthcare organization has improved its overall risk assessment and mitigation capabilities

A regional health system comprising hospital campuses, health centers, physician groups, rehabilitation centers and other outpatient care locations in eastern and northeastern Pennsylvania has long been recognized as a pioneer in healthcare. The health network's team of more than 20,000 clinicians care for hundreds of thousands of patients each year across its emergency departments, outpatient practices, and inpatient beds. The health system adopted a number of novel healthcare technology solutions to enhance patient care, including medical devices connected to the Internet of Medical Things (IoMT). With the addition of these new devices, executive leadership recognized the importance of enacting more comprehensive cybersecurity practices to increase visibility across its network environment. Doing so was necessary to better protect the health system from the growing number of costly cyberattacks plaguing the healthcare industry.[1]

Leading the charge to develop cybersecurity best practices that mitigate vulnerabilities and comply with institutional and federal policies and regulations is the health system's top cybersecurity expert. A longtime security professional with federal agency experience, he is extremely conscious of the risk that medical IoT devices confer to the entire enterprise.

"The fact of the matter is that medical devices are not designed to be hardened and secure against cyberattacks," he pointed out. "They are designed to bring about healthcare outcomes — to heal and help people. And the components you find in these devices are incredibly vulnerable to attack."

The care we provide to our communities is constantly and intentionally improving, aided by better, more efficient medical devices that are securely connected and accessed by our clinicians and practitioners. Those devices increase our attack surface, so securing them and maintaining authoritative visibility and situational awareness is a must."

The health system has as many as 150,000 devices on its network at any given time. Because of the risks involved, it sought an experienced and trusted vendor partner to strengthen the health network's overall security posture. In addition, the health system needed to implement tools that would give greater visibility into its network activity and enable it to effectively protect its network ecosystem.

"The care we provide to our communities is consistently rated as the best in the nation and is constantly and intentionally improving, aided by better, more efficient medical devices that are securely connected and accessed by our clinicians and practitioners," he explained. "Those devices increase our attack surface, so securing them and maintaining authoritative visibility and situational awareness is a must. It's our top priority."

Mitigating risk with MITRE ATT&CK protocols

As cyberattacks have become more sophisticated, healthcare organizations must adopt best practices to, as the health system's cybersecurity expert put it, "prepare the battle space." The health system relies on the MITRE ATT&CK (adversarial tactics, techniques, and common knowledge) framework, a comprehensive knowledge base that gives security personnel key insights into attacker behavior and techniques, to help it prevent potential attacks and keep patient information, payment information, and other key data secure.

"The MITRE ATT&CK framework is meant to be bolted on to any other risk management framework you may have, like the payment card industry data security standard (PCI DSS) or the Health Insurance Portability and Accountability Act (HIPAA)," he explained. "If you implement the security controls that organizations like HIPAA, the National Institute of Standards and Technology (NIST), the Payment Card Industry (PCI), and others suggest, you can reduce risk in a cost-effective manner. It's also designed to be more proactive than most security approaches. It looks for the hundreds of techniques and thousands of sub-techniques that threat actor groups currently use to attack networks—so you know what to expect and how to best respond to a threat."

While this approach helped the health system manage the overall risk posture of the hospital, it was still in need of tools that could provide visibility of its entire network, including its hundreds of thousands of medical IoT devices. The health system decided to implement a solution called Medigate, a network monitoring tool that visualizes every device connected to the network, its location, and its current security posture. It also engaged RedSeal to integrate for visibility of the Medigate implementation of MITRE ATT&CK framework, creating a crucial base layer for the security team to detect potential threats more easily.

"RedSeal enables us to speak authoritatively about what's on the network at any given time," said the health system's security leader. "It also shows us where threats may be positioned. Ninety-nine percent of the time, the techniques listed as potential threats are completely benign. It's expected activity. For example, one such technique is port knocking. We use port knocking within our organization to turn a switch on or to enable certain functions. But there is that 0.01 percent of cases where this technique is not being used by us. You want to be aware of those. We have the tools needed to see where these different techniques are happening, and then if they are part of that 0.01 percent, to give us the knowledge of what the threat entails so we can anticipate what their next steps would be and be more proactive about stopping them."

The value of managed services

Maintaining a strong cyber-risk management approach is an ongoing, iterative and dynamic process, said the health system's cybersecurity expert. Its RedSeal/Medigate integration has increased the health network's overall digital resilience and has reduced the amount of time it takes the cybersecurity team to troubleshoot and determine the root cause of potential threats.

"The RedSeal/Medigate integration is a critical and foundational component of our security posture that supports our common operating picture for cyber-situational awareness and threat hunting using the MITRE ATT&CK framework," he said. "The increasing accuracy of

Security should be at the front of everything. Involve security and risk management personnel early in any new initiatives, whether they are new merger and acquisition events or technology projects."

this model, and its visualizations of the network, greatly increases our overall cyber-visibility."

Leveraging RedSeal's Fully Managed Services (FMS) provides additional benefits to the health system's team, empowering the health network to turn its resources toward focusing on issues and deliverables vital to the health of its business—and, most importantly, its patients.

"RedSeal's professional services are top notch," said the cybersecurity professional. "They are part of our team. They understand our challenges, they understand our environment, and they understand what we need. They've really gone above and beyond in providing value to our organization. Their work brings value to the people who are responsible for the care and feeding of all our medical devices. And they bring value to the people who are responsible for risk reduction and getting the data and reports we need to comply with different regulating agencies."

Finding a way forward

Any experienced cybersecurity professional will tell you that it's not a question of *if*, but *when*, your network will be attacked. Visibility over the network is essential for preventing attacks before the costs prove too much to bear. When asked what advice he has for other healthcare organizations looking to prepare their own network battle space, the health system's cybersecurity expert answers with confidence.

"The threat is real. Security should be at the front of everything. Involve security and risk management personnel early in any new initiatives, whether they are new merger and acquisition events or technology projects," he said. "Invest in the human capital, tools and preparation required to get you the visibility and awareness you need. Then, identify which services can be outsourced or shifted to managed offerings—and, equally as important, which services cannot be—based on your existing security posture. There is going to be a significant investment involved because of all of the preparation that needs to happen. But the value returned from that investment is phenomenal, especially when you are working with the right partners."

Learn more about RedSeal here.

References

1. IBM. 2022. *Cost of a Data Breach Report 2022*. https://www.ibm.com/reports/data-breach.

REDSEAL

About RedSeal

RedSeal—a security solutions and professional services company—helps government agencies and Global 2000 companies see and secure their on-premise networks and cloud environments. The RedSeal award-winning security solution verifies that networks align with security best practices, validates network segmentation policies, and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk.