CASE STUDY

Healthcare Facility

MANAGED SECURITY &
SECURE MANAGED WIFI

Challenges

Poor WiFi coverage and concerns for the security of their increasing number of IoT devices.

Their current firewall was aging and reaching end-of-life and end of support.

Shortage of IT staff to oversee the expanding IT infrastructure and technology needs.

Lack of capital budget needed to overhaul the equipment to update their network infrastructure.

Telesystem
IT's About Trust

About the Customer

Our customer is a non-profit Critical Access Healthcare Facility in Missouri. The facility offers a wide range of medical services including emergency care, outpatient services, radiology, bone mineral density (DEXA) scans, as well as Pulmonary and Oncology treatments.

As the facility increasingly relied on IoT-enabled medical devices, they encountered issues with poor WiFi coverage and the critical need to ensure the security of these devices.

Unsatisfied with the solution their previous provider recommended, the customer sought out a service provider with the expertise to oversee the entire network solution while also providing a comprehensive Cybersecurity Roadmap.

Telesystem's Solution

With device security and performance in mind, Telesystem utilized advanced design tools and heat-mapping applications to develop a robust and scalable network solution to overhaul their existing WiFi network and secure their growing IoT devices stack. The deployment included high availability Fortigate 200F firewalls as well as Meraki Switches and advanced Access Points to resolve their issues with poor WiFi coverage, secure the network infrastructure, and update their aging firewall. This step significantly improved the connectivity and reliability of the facility's network, providing a solid foundation for their IT infrastructure and continued connectivity for their medical devices throughout the facility.

To further support the customer's cybersecurity concerns, Telesystem provided comprehensive cybersecurity consulting services which included conducting a thorough risk assessment to identify areas of vulnerability and provide a roadmap for enhancing their cybersecurity posture. To address security gaps which were uncovered in the assessment, Telesystem provided 217 #HackersSuck bundle seats for their employees which includes comprehensive security awareness training, advanced email protection, and endpoint protection. This comprehensive approach was to effectively mitigate the customer's security concerns and provide a solid framework for ongoing cybersecurity management.

The Results

Recognizing the critical necessity of a reliable and secure WiFi network to support IoT-enabled medical devices for employees and patients, Telesystem designed a network solution that not only efficiently met the customers' requirements but also alleviated the strain on their limited IT staff.

Telesystem’s Managed Security and Managed WiFi solutions helped turn the hospital’s equipment expenditures into an operating expense rather than capital, while the 24x7x365 monitoring and maintenance of the entire stack ultimately frees their team from the burden of maintaining the components, patches and updates.

In addition to safeguarding business and patients' personal information from cyber threats, Telesystem's solution fulfilled the customers connectivity, support, and security needs, while also allowing for future scalability and additional functionality down the road. This ensured that the business remains operational and adaptable to evolving technology, supported by a provider capable of meeting their evolving needs and keeping them up to date with the latest technology and security developments to support their medical devices both now and in the future.