Freeman Health System Selects Ordr For Multiple IoT Security Use Cases

Freeman Health Freeman Health is the largest medical network in Joplin, Newton County, Missouri, USA. Freeman operates two campuses in Joplin and a satellite hospital in Neosho, Missouri, along with other health services facilities. Freeman has earned dozens of individual awards for medical excellence and patient safety.

- **Founded in 1922**
- **Best Hospital in Southwest Missouri for (2019 U.S. News & World Report)**
- **5000 employees**
- **>350 physicians on staff**
- **Healthcare services representing more than 60 specialties**

Tucked in the southwest corner of Missouri, Joplin is a city best known for being a waypoint along historic Route 66. Freeman Health System is transforming that perception, bringing a reputation for medical excellence to Joplin.

Freeman Health has earned dozens of individual awards for medical excellence and patient safety, and was named Best Hospital in Southwest Missouri for 2019 by *U.S. News & World Report*.

As the largest medical network in southwest Missouri with 5,000 employees, including more than 350 physicians on staff, Freeman Health System provides healthcare services representing more than 60 specialties. The Freeman Health System network is anchored by the flagship, 339-bed teaching hospital, Freeman Hospital West, affiliated with Kansas City University of Medicine and Biosciences. Other Freeman Health locations include Freeman Hospital East, Freeman Neosho Hospital, Freeman Physician Group of Pittsburg (Kansas), the Ozark Center for comprehensive behavioral health services, two urgent care clinics, dozens of physician clinics, and a variety of specialty services facilities.

Freeman Health's IT enterprise is complex, extensive, and distributed across many locations. The organization makes extensive use of IP-connected devices—the Internet of Things (IoT) and Internet of Medical Things (IoMT)—to run its facilities and to care for patients. Skip Rollins, Freeman Health Systems' CIO, described the organization's IoT network as consisting of 17,000 devices, of which many are directly involved in patient monitoring. The remainder include facilities management equipment like HVAC, environmental controls, door locks, and security cameras, as well as administrative devices like IP phones, office systems, intercoms, mobile devices, and laptop computers.

Freeman Health needed a tool to discover and secure its entire IoT portfolio.

SECURITY TEAM CHALLENGES

Understand what devices are connected to the network

Keep track of device vulnerabilities and recalls to communicate to device owners

Understand how devices are communicating outside the enterprise

Identify anomalous and suspicious device communications

CIO CHALLENGES

Ensure all connected devices across the organization are secure

Support finance procurement decisions with device utilization details

Medical Center of Excellence Seeking To Secure Extensive IoT Portfolio

Ordr was introduced to Freeman Health by managed security services provider Talus Solutions, a member of the Ordr partner program. Talus specializes in helping address the unique security challenges facing health-care organizations, including the growing use of smart, connected medical devices. Freeman works closely with Talus, and is an aggressive adopter of IT and security technologies.

The Ordr Systems Control Engine is industry's most comprehensive platform for IoT, IoMT, and OT discovery, management, and security. Ordr can discover and classify every device in a network within a few hours of installation with granular context such as device type, manufacturer, serial number, operating system, location and more. Ordr can also identify devices with vulnerabilities, weak certificates, weak passwords, and active exploits.

"We worked with Talus to get the Ordr Systems Control Engine in for a proof-of-concept, and the things it showed us that were on our network, and the information it gave us about those devices was eye opening," Rollins said. "Before Ordr, we thought we knew what was deployed, but now we can see precise details like the device type, serial number, manufacturer, location and more."

One IoT Security Platform For Multiple Use Cases

After the proof-of-concept, Freeman deployed the Ordr Systems Control Engine (SCE), and now uses it to identify devices and their risk profile. Freeman also uses it for a variety of other use cases. Freeman's IT Security Manager Raun Williams also uses the Ordr platform to monitor for any security issues. As non-IT groups within the organization such as biomedical and facilities teams put devices into service, Raun ensures that these devices are secure.

"We need to know what's coming on the network, how they are behaving and communicate about vulnerabilities and risks to the different groups within the organization," Williams explained. "It's easy to manage Windows devices, but things like cameras and facility controls are difficult. From a security standpoint, everything's a vector."

The Ordr Systems Control Engine (SCE) integrates with threat intelligence feeds to stay up-to-date on known vulnerabilities, ICSA–ICS-CERT advisories, and FDA vulnerability and recall alerts. In addition, the Ordr Flow Genome maps each device's unique, customer-specific communications patterns, and profiles exactly how it should behave. Unlike users, IoT devices have specific and predictable communications patterns. For example, video cameras need to connect to a camera management

system; medical imaging devices need to communicate to a central PACS or DICOM server.

Raun can visualize any suspicious or malicious behaviors from devices and take appropriate action. Rollins said Ordr revealed previously unknown and concerning communications patterns by some devices that were "calling home to places all over the world, like Russia and China." But with those behaviors uncovered, Freeman was able to take mitigating action.

Device Utilization Insights Helps With Capital Spend

Another use case for CIO Skip Rollins is the use of Ordr Flow Genome's sophisticated analytics to support business decisions.

"My job as CIO has evolved so much. We're much more focused on the business aspect now than we are managing the technical side of operations. When our healthcare staff puts in a request for new devices, we have to help our finance teams make smart capital spend decisions. Ordr is a tool we lean on not only for visibility and security, but for device utilization insights. Now, we look at the need, and how the device is being used, and help finance with procurement decisions." Rollins explained.

Rollins cited a recent example of a requisition request for new EKG machines. Rollins saw that Freeman's existing EKG inventory were being utilized at 40 percent. "Working with our finance department, we were able to reallocate existing EKG devices rather than spend money to buy new equipment because we could see what we had, how it was being used, and make better business decisions," Rollins explained.

Ordr Word Of Mouth Spreading In CIO Community

As an early adopter of Ordr, Rollins is very happy with the product. "We are aggressive with our use of technology, and we rely on Ordr as both a security and business tool," Rollins said.

He's not the only one. "I've talked with CIOs all over the country and many use Ordr today. It's unusual for a tool to actually do what the vendor says it's going to do. Ordr actually does what the vendor says it will do and it does even more. That positive word of mouth about Ordr has spread rapidly among the CIO community," Rollins added.

For organizations that are struggling with wrangling the security and management challenges associated with the expansion of IoT and IoMT devices in their IT infrastructure, Ordr has proven its value for one of the healthcare industry's most voracious consumers of health technology.