CASE STUDY

Franciscan Health Utilizes Fortinet Security Fabric Solutions to Immunize IoT Medical Devices Against Attack

Following the Roman Catholic tradition of caring for those in need, Franciscan Health is committed to providing high-quality and compassionate healthcare. The company runs 14 hospitals and more than 350 satellite locations, including physician practices, imaging centers, urgent care centers, and other facilities across Indiana and Illinois.

In monitoring patient health and providing appropriate medical services, Franciscan Health's 29,000 employees rely on a wide array of medical equipment. However, these machines increase the corporate network's vulnerability to cyberattack.

"We have a significant attack surface, as all healthcare companies do," explains Chuck Christian, Vice President of Technology and CTO. "We have about 96,000 endpoints connected to our corporate network, including clinical engineering systems, IoT [Internet-of-Things] gear, and medical equipment. That does not include the separate guest network that we maintain for patients and visitors. It is crucial for my team to block unauthorized access to the corporate network—and to know immediately if someone gets past our edge security."

An Eye on IoT

Three years ago, Franciscan Health deployed the Ordr connected device security solution for asset inventory and to better track its disparate devices. Ordr is a Fortinet Fabric-Ready Partner whose Ordr Systems Control Engine (SCE) solution discovers and classifies every connected device, including IoT and other unmanaged devices throughout a network, then profiles each device's behavior and risks. Through the Fabric-Ready Partnership, Ordr and Fortinet collaborate to develop validated, end-to-end security solutions.

When Franciscan Health first deployed Ordr SCE, "it was eye-opening to see how many devices connect to our network," Christian says. "The data visualization in Ordr gives us a huge amount of information. We have visibility into the risk profile of every piece of equipment." This is important, he adds, because some devices could be leveraged as an attack vector into the corporate network: "The healthcare industry is very good about squeezing the last bit of juice out of any equipment. We have systems that are 15 years old, whose embedded operating systems have not been upgraded in that time, due to manufacturer requirements."

This new visibility into risk led Franciscan Health to begin deploying FortiGate Next-Generation Firewalls (NGFWs). The close engineering relationship between Fortinet and Ordr means that the FortiGate NGFWs integrate tightly with Ordr's asset management solution via open application programming interfaces (APIs). Christian's

Franciscan HEALTH

"The bad actors keep getting smarter, and we need to be as smart as they are. We need to make sure the business partners we have chosen will work with us to support our security goals. We get that with Fortinet and Ordr."

– Chuck Christian, Vice President of Technology and CTO, Franciscan Health

Details

Customer: Franciscan Health
Fortinet Fabric Ready Partner: Ordr
Industry: Healthcare
Headquarters: Mishawaka, IN

Business Impact

- Near-real-time visibility into emerging threats and attacks improves efficacy of security environment
- Time savings for IT staff

ordr

team has configured the solutions so that Ordr notifies the firewalls if it notices a specific situation or event.

"When we put in medical equipment, especially devices that we cannot manage or patch, they go behind the FortiGate firewalls," Christian says. "We are still in conversation about how the firewalls should act on those notifications—whether they should cut off a device's access to the network or alert a human who can determine whether it is a true threat or a false positive."

Wrapping the Network in the Fortinet Security Fabric

Since first starting to deploy FortiGate NGFWs, Franciscan Health has expanded its investments in solutions that integrate into the Fortinet Security Fabric. Christian's team implemented FortiManager to streamline deployment of new firewalls and leveraged threat intelligence from FortiGuard Labs.

"The ability to centrally manage our security environment through the FortiManager system is really helpful," Christian says. "When the Log4j vulnerability came to light, FortiGuard Labs provided us with information about the threat signatures. We put that information into the FortiManager solution, which sent it out to the NGFWs; they were then able to watch for the threat. We were prepared in case a Log4j attack got into the building.

"Fortinet enabled us to be proactive rather than reactive," he says. "I prefer to avoid spilling the glass of milk, instead of having to clean it up after the fact."

Products and Solutions

- FortiGate Next-Generation Firewall
- FortiManager
- FortiNAC

"Integration between FortiNAC and FortiManager enables us to ensure that configurations follow individual devices throughout our network, rather than staying fixed to a specific port."

– Chuck Christian, Vice President of Technology and CTO, Franciscan Health

Next, the team started segmenting their internal network, building dynamic rules within the FortiGate NGFWs to protect specific healthcare devices. "Our goal is to use east, west, north, and south segmentation," Christian says. "The Fortinet solutions use the information from Ordr to understand what behaviors are normal, and they alert us when a device behaves abnormally. For example, if we have a CT scanner that usually talks only to the EMR [electronic medical record] system, and all of a sudden it starts trying to connect to a foreign IP address that we have geoblocked, then the FortiGate firewalls tell us that something has gone wrong."

The microsegmentation reflects an organizational emphasis on leveraging the benefits of technology integrations. "We have a new strategy that revolves around the Fortinet Security Fabric," Christian says. "Rather than just connecting everything and running traffic, our networking strategy involves leveraging the hardware to turn the network into more of a security tool."

To that end, Christian's team recently launched a network access control (NAC) initiative. "The combination of microsegmentation and NAC policies means no equipment will be able to access anything of value to the organization unless it is supposed to," he says.

Dynamic, Integrated, and Secure NAC

The need for a NAC was clear, and the FortiNAC solution was the obvious choice. "As we begin to move toward zero-trust networking, we need to prevent devices from connecting to our network if we do not explicitly want to allow them," Christian explains. "I tasked my team with finding the best NAC. We talked to Gartner analysts, then did a deep dive into the FortiNAC solution. We found that it played well with the equipment we already had in place, so it made sense." His team is currently rolling out the FortiNAC product throughout the Franciscan Health organization.

"There are a lot of different choices we can make in terms of response in case an unknown device tries to plug into the Franciscan Health network," Christian says. "If we are completely unaware of the equipment, we can just deny it access. Or we can shunt it off to another network that has access only to the internet, or we can display a splash screen."

Ordr is already passing data on to the FortiNAC system via API for device visibility. Eventually, Ordr will also feed the FortiGate firewalls "proofed" rule suggestions. This intelligence sharing throughout the Fortinet Security Fabric will support

microsegmentation at Franciscan Health by enabling network access policies to be applied at a more granular level. Anytime a new device connects to the network—whether it is an MRI machine, a video surveillance camera, or any of the hundreds of other devices that might connect—it will receive a network profile. Then, every access-policy change that affects the subset of devices defined by that profile will be pushed out to the new device as well.

At the same time, the FortiNAC-FortiManager combination substantially improves the efficiency of network security. "In our legacy environment, if something happens—say, a port goes bad—and we need to move a device to another port, then one of the network engineers have has to go into the configuration of the switch and move those configurations to a new port. Integration between FortiNAC and FortiManager will enable us to ensure that configurations follow individual devices throughout our network, rather than staying fixed to a specific port."

Playing Chicken with Prospective Attackers

Having Fortinet solutions that are receiving information from a data source as strong as Ordr enables Christian "to future-proof our network security," he says. "I am very impressed with some of the forward-thinking actions Fortinet is taking to improve intelligence around threat management.

"Our goal is to make our network impenetrable," he continues. "The bad actors keep getting smarter, and we need to be as smart as they are. We need to continue to learn, and we need to make sure the business partners we have chosen will work with us to support our security goals. We get that with Ordr and Fortinet. Together, these solution providers help us to potentially stay ahead of bad actors, which will be very important into the future, because I am greatly concerned that the next generation of shape-shifting threats will be able to evade a lot of security systems."

Christian concludes with an analogy: "My father always told me, 'You are going to have 12 problems racing down the road at you. Most of them will veer off into the ditch. Your job is to figure out which one or two will actually run you over if you do not react to them.' The Fortinet Security Fabric solutions and Ordr help us discern and understand which types of threats we need to address."

January 26, 2023 9:02 PM

1927954-0-0-EN