CASE STUDY

FortiDeceptor Delivers Breach Protection for Critical Healthcare Services

In the sparse desert mountains of the Southwest U.S., the landscape is breathtaking—but the widely dispersed population creates a challenging environment for medical providers. Patients do not have many healthcare choices. That makes it crucial for healthcare facilities to provide uninterrupted service.

"There is a big weight on the shoulders of the IT team to provide an infrastructure that is stable and reliable," explains the CIO for one such healthcare organization. "Because of our rural setting, patients cannot just go down the street to a different hospital."

Adding to the challenge, IT staffing is lean at the regional hospital system. The team responsible for cybersecurity must also support the company's entire infrastructure of IT systems, including its electronic medical record (EMR) solutions and Internet-of-Things (IoT) medical devices. "Yet we have the same attack surface as large medical groups with security teams who can focus exclusively on investigating and following up on security incidents," the CIO points out.

An Industry at Risk

For the CIO, ransomware is a major concern, although it is certainly not the only threat on his mind. "There is not a lot that I do not worry about in the cybersecurity space," he says. "Even a breach that did not result in any system failure or data loss would trigger HIPAA [Health Insurance Portability and Accountability Act] consequences. We would notify patients, perhaps offering to monitor their credit, and we would have to apologize to the community. To avoid that scenario, I spend a large portion of my time enhancing security for our patients and staff."

His concerns are amplified by the fact that healthcare is the number-one sector targeted by cyberattacks. Last year, a similar hospital in another community fell victim to an attack on its EMR software. "A botnet accessed their network and detonated a couple of weeks later," he reports. "It took their EMR system offline for a week. These threats are not just theoretical."

The healthcare organization's small IT team prioritizes security processes designed to identify and mitigate such threats. A key weapon in their cybersecurity arsenal is Fortinet's proactive threat detection solution, FortiDeceptor.

Tightening Healthcare Defenses

The company first started working with Fortinet several years ago, when it began implementing FortiGate Next-Generation Firewalls (NGFWs). "The FortiGate firewalls are phenomenal products," according to the CIO. Fortinet's presence in the organization's infrastructure grew from there. By the time the IT team was considering FortiDeceptor, the company was using FortiSwitch secure access switches and FortiAP access points, FortiSandbox for advanced threat protection, FortiMail to protect communications, and FortiAuthenticator for user authentication, with FortiManager and FortiAnalyzer to manage the environment.

"Our deception decoys are confusingly similar to our actual services so that remote actors try their campaigns there. By exposing FortiDeceptor to threats that might otherwise be hitting our critical systems, we gain a true picture of what our externally accessible servers go through daily."

– CIO, Regional Hospital System

Details

Customer: Regional Hospital System

Industry: Healthcare

Location: Rural Southwest United States

Business Impact

- Prevention of brute-force external attacks through sophisticated detection and immediate response
- Blocking of lateral movement within the network
- Minimal time to deployment; FortiDeceptor was operational within 30 minutes
- Minimal ongoing management

Deception solutions only detect threats; they have no innate ability to respond directly to attacks. Thus, their effectiveness depends on tight integration with response and mitigation technologies. That made FortiDeceptor an obvious frontrunner for the healthcare provider. Still, the IT team considered several options. They ran demos of multiple products, says the CIO, "but none of the others were in the ballpark of what FortiDeceptor was able to offer us. We selected FortiDeceptor because of its security efficacy, ease of use, price, and the level of service we expect from Fortinet."

Deployment was seamless. "We got the device, set up a virtual meeting with the proof-of-concept team, and were rolling with FortiDeceptor within 30 minutes," he reports. "It was amazingly simple to get off the ground. Ongoing maintenance and management are streamlined as well. We apply routine updates and patches, but FortiDeceptor requires very little day-to-day care and feeding."

Deception Breeds Protection

The IT team used FortiDeceptor to build a fake environment that looks, from the outside, like different elements of the corporate network. They leveraged the tool's IT simulations to imitate core components of their technology environment, and they used its IoT capabilities to simulate medical equipment. A prebuilt medical decoy streamlined deployment.

"One of our main use cases for FortiDeceptor is to hang it out on the DMZ [demilitarized zone] side, to allow it to get hammered in the same way our real services would," says the CIO. "Our deception decoys are designed to be confusingly similar to our actual services so that remote actors try their campaigns there. By exposing FortiDeceptor to threats that might otherwise be hitting our critical systems, we gain a true picture of what our externally accessible servers go through daily."

The team also deployed FortiDeceptor on internal virtual local-area networks (VLANs) that house sensitive information, such as management data or medical devices. The security team now receives an alert when malware or another threat attempts to move laterally through the network. "Those kinds of attacks are harder to catch," the CIO says, but FortiDeceptor has proven its ability to do so. "We have used FortiDeceptor to detect both external attacks and internal hack attempts, including bad actors who have breached one of our network segments."

When a decoy detects a threat, FortiDeceptor automatically quarantines the potential malware, and information about the attack is disseminated throughout the Fortinet Security Fabric. The company's firewalls receive an alert to block any similar threat that may appear, whether it comes from outside the organization or attempts east-west traverse through the network.

"Having that Fabric integration—where FortiDeceptor is natively integrated with our FortiGate firewalls and can communicate that a threat needs to be blocked—has dramatically changed our security footprint," the CIO says. "The immediate response throughout the Security Fabric is extremely powerful. And we had that functionality on day one; no scripting is required. FortiDeceptor took minimal configuration and had extremely fast return on investment for identifying these potential threats and allowing us to automate our responses."

Products and Solutions

- FortiDeceptor
- FortiSOAR
- FortiGate Next-Generation Firewall
- FortiSwitch
- FortiAP
- FortiSandbox
- FortiMail
- FortiCall
- FortiVoice
- FortiAuthenticator
- FortiManager
- FortiAnalyzer

Services

- FortiCare Professional Services

"Having FortiDeceptor natively integrated with our FortiGate firewalls has dramatically changed our security footprint. And we had that functionality on day one; no scripting is required."

– CIO, Regional Hospital System

"For example," he adds, "in one case, our decoys detected that someone was trying to brute force their way into our network in the middle of the night. As soon as the threat was detected, our edge firewalls blocked the source IP, so that attacker was never able to get anywhere near our real servers."

New Heights of Threat Visibility

To ease the load that typically falls on the IT team, the healthcare company deployed the FortiSOAR security orchestration, automation, and response (SOAR) workbench. "The actual deployment of FortiSOAR was extremely easy," the CIO says. "I got the license, spun up the virtual machine, and it was ready to go in half an hour." However, using FortiSOAR effectively required some training.

The company engaged FortiCare Professional Services to help optimize the tool's configuration. "That was one of the wisest things we have done," the CIO adds. "FortiSOAR is user-friendly, but it is different from any technology we had used before, so it took us a while to understand what the workflows look like. FortiCare Professional Services coached us through setting up FortiSOAR, and their knowledge transfer to us was invaluable."

FortiSOAR ingests logs from countless network devices, as well as detection and data sources, using risk-driven alert prioritization to build a unified view. Furthermore, automated investigations provide a base-level determination of whether each anomaly represents a real threat.

Ongoing Consolidation to the Security Fabric Drives More Benefits

Security-driven networking continues to have momentum at the healthcare company. After the organization completed a multimillion-dollar project to construct new buildings, the CIO expanded on his positive experience with Fortinet, outfitting the buildings with hundreds of FortiSwitch and FortiAP devices at the LAN edge. Success in that deployment led to the decision to consolidate switching and wireless to Fortinet throughout the hospital. The same transition is also under way in the company's data centers. "The main driver for that has been the integration with the Fortinet platform, the support, and the product roadmap," reiterates the CIO.

The CIO describes some of the security features he likes from FortiAP and FortiSwitch products: "On the newer APs [access points], dedicated radios for vulnerability scanning have been a big seller for us. On the switching side, dynamic quarantines from a security perspective have been great. Identifying devices on switch ports in the user interface is also dramatically easier than it was in our previous environment. And then, the information all ties up to FortiAnalyzer, giving us a central repository to put together reports."

The healthcare organization is now continuing to transition to other Fortinet offerings as well, in many cases due to the Fortinet solutions' ease of use and performance. The IT team found FortiVoice Secure Unified Communications (UC) to be easy to configure. "Once you get introduced to this and see the ease of management compared with other popular call center solutions, you would look at this product and say, 'I cannot believe I wasted all my life doing these other configurations; this is unbelievable,'" says the CIO.

The company also added the FortiVoice UC solution's FortiCall calling plans. "We have had some really great outcomes with the FortiCall as our long-distance phone calling provider," the CIO says. "We saved dramatic amounts of money through the FortiVoice UC solution as opposed to our local telecom."

A Little Peace of Mind

With a prior firewall vendor, the healthcare company had to go through four different value-added resellers (VARs). "None of them agreed with what the others had done, so we were constantly having to redo our infrastructure, our configuration, and integration of the products. It was a nightmare," the CIO says.

That experience made him appreciate the tight integration and ease of management of the Fortinet solutions. "I have an I-heart-Fabric shirt on right now," he jokes, adding: "Using Fortinet solutions lifts a lot of weight off my team. Fortinet has proven its ability to support us as a healthcare organization. That has been especially critical during the pandemic. Logistical issues have put a lot of companies to the test over the past two years, but we have had great experiences with Fortinet."

Further, as the IT team had comments and suggestions about FortiDeceptor, Fortinet engineers worked with them directly to get resolution. “I have seen an extreme amount of growth in the product functionality since we deployed FortiDeceptor,” says the CIO. “They have an amazing development team that has been very responsive to our needs.”

Ultimately, the effectiveness of the healthcare organization’s security infrastructure flows directly from the company’s close relationship with Fortinet. “Having Fortinet as a partner gives me as much peace of mind as I can have in a cybersecurity world,” the CIO concludes. “That is close to zero, because there is always something to worry about as a security manager for a healthcare company. But at least I can now sleep through the night knowing our infrastructure will respond as soon as a threat emerges.”

December 12, 2022 5:07 PM

1882575-0-0-EN