CASE STUDY

Network Reliability Enhances Patient Health: How Fortinet Secures a Critical Access Hospital

Critical access hospitals provide essential medical care to rural communities across the United States. The "critical access" status is available only to facilities farther than a 35-mile drive from any other hospital (15 miles in areas with only secondary roads) and with 25 or fewer acute-care beds.

One such facility, Mount Desert Island Hospital in Bar Harbor, Maine, serves about 150 islands off that state's coast. "A lot of the islands are sparsely populated, and we are the primary health system providing care for those residents," explains Tom Mockus, director of IT. "The population we serve year-round is about 15,000. What is challenging is that the local population balloons during tourist season. Last summer, our area had about 4 million visitors. That means our hospital's patient traffic swings wildly from season to season."

Another challenge is that auto traffic—and communications of every form—create single points of failure in medical emergencies. "If we were unable to provide care for patients, they could not easily get to another hospital, especially during a summer day," says Tony Manzo, IT Manager. "The hundreds or thousands of people trying to get onto or off the island could prevent an ambulance from moving quickly."

As the only acute-care provider on Mount Desert Island, the hospital must ensure its systems run 24×7. That is why it has prioritized cybersecurity. "The threat landscape is changing," says Will Houston, network security manager. Like any healthcare facility, Mount Desert Island Hospital stores sensitive patient data. But, adds Houston, "We are seeing threat actors shift their focus from ransomware to really trying to create business disruptions and shut down aspects of our hospital. It would be catastrophic if we had to divert patients. Even if they weren't in critical condition, they might not get into another emergency department for several hours. In our case, cybersecurity is a matter of life and death."

A High Level of Protection with Greater Reliability

A decade ago, the hospital used firewalls from another name-brand vendor to protect crucial information. As those devices approached end of life, Mockus and his team considered whether to upgrade their legacy hardware or head in a new direction. They evaluated several options, including FortiGate Next-Generation Firewalls (NGFWs).

"We liked that Fortinet had a mesh security framework—the Fortinet Security Fabric," Mockus says. "Even though we were starting with just the firewalls, we knew that if they worked we could add more solutions into the Fabric. We were very interested in using this approach to simplify management of our overall security infrastructure."

Mount Desert Island Hospital

"Because the entire Fortinet Security Fabric is under a single pane of glass, we can log in to one place to see everything. If one solution finds a threat, it is a very quick pivot to block it in policy. This is crucial to protecting our systems."

Will Houston
Network Security Manager,
Mount Desert Island Hospital

Details

Customer: Mount Desert Island Hospital

Industry: Healthcare

Headquarters: Harbor, Maine

Business Impact

- Better protection for applications and data, as Fortinet Security Fabric solutions coordinate threat detection and response
- Faster updates to security policy, as needed, due to better visibility into security events networkwide

He adds that when Mount Desert Island Hospital pulled the trigger on the FortiGate NGFW deployment, "A lot of people did not understand why we would move away from what was, at the time, the industry standard. Still, we took a chance and went with Fortinet, and that is one of the best decisions we ever made."

SD-WAN for Redundant, Resilient Connectivity

Ever since, Mount Desert Island Hospital has operated a hub-and-spoke network for the hospital campus, its seven external clinics, and its retirement village. Fortinet Secure SD-WAN connects the locations, backhauling all traffic to the hospital data center, where FortiGate NGFWs secure the network edge. FortiExtender devices provide a backup communications channel that kicks in if the hospital's primary ISP fails.

"We use Fortinet Secure SD-WAN to traffic shape," Houston says. "We have put redundant AT&T FirstNet and Verizon 5G/LTE SIM cards in the FortiExtenders to provide priority communications channels for our emergency medical services. That gives us a backup path for connectivity."

"A second ISP is not the right option for redundancy because we are on an island with one set of telephone lines coming in," Manzo explains. "Accidents happen all summer long, and it is just a matter of time before a vehicle takes out a telephone pole, causing the whole island to lose internet connectivity. The FortiExtenders give us a truly alternative internet link."

Before deploying the devices, Mockus tested them at a personal camp property. "It is in the middle of nowhere and does not even connect to the power grid," Houston reports. "He wanted network connectivity, so we piloted a FortiExtender with an LTE card. It worked great—he was able to disturb us when he was supposed to be on vacation." In fact, the pilot went so well that now every facility in the Mount Desert Island Hospital network has a FortiExtender for off-island connectivity.

A Tightly Woven Fortinet Security Fabric

Each of the hospital's facilities also utilizes FortiAP access points, as do employees working from home. The FortiAuthenticator user authentication tool coordinates with the FortiNAC network access control solution to confirm users' and devices' identities before allowing them onto the network.

Mount Desert Island Hospital is currently in the process of adding FortiSwitch secure Ethernet switches to the mix. Once the rollout is complete, each location will have direct internet connectivity. "The Fortinet SD-Branch infrastructure will enable us to control all the devices through one policy," Manzo says. "That means ease of management and, frankly, lower costs."

"We will be able to drill down to a specific port with FortiNAC," Houston says. "The intelligence we derive from that combination of solutions will reduce the amount of time our techs spend on activities like changing port access every time someone needs to move an office."

Transitioning to Fortinet switches will also improve security for Mount Desert Island Hospital by enabling more granular control and ensuring that the organization's security solutions communicate about perceived threats. "With FortiSwitch, we will be able to apply firewall policies right down to the user-access switches," Manzo says. "We will bring firewall policies closer to our end users." Adds Mockus: "And the mesh security features mean our Fortinet solutions talk to one another. If one detects an issue, all can respond."

Business Impact (cont.)

- Reduced staff time managing security through centralized security policy management
- Smooth transition to FortiVoice results in only five minutes total of phone system downtime
- Dramatic improvement in system reliability reduces staff time spent troubleshooting
- FortiOS consistency across products streamlines staff training and enables team members to fill in for one another

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiExtender
- FortiAP
- FortiAuthenticator
- FortiNAC
- FortiSwitch
- FortiDeceptor
- FortiAnalyzer
- FortiManager
- FortiVoice

Services

- FortiGuard AI-Powered Unified Threat Protection Bundle

The healthcare system uses the FortiDeceptor deception and isolation platform as an additional means of detecting threats to the network. “Within the past 30 days, FortiDeceptor has identified more than 500 different IP addresses that need to be blocklisted, and the Fortinet Security Fabric has blocked them across our entire network,” Houston says. “Being proactive in the modern world is key. We are using Fortinet products to build a massive wall with the goal of preventing bad actors from getting in.”

Faster Threat Response with Single-Pane-of-Glass Visibility

The Fortinet Security Fabric approach also greatly reduces the time staff must spend managing the Mount Desert Island Hospital infrastructure. The organization uses FortiAnalyzer and FortiManager management solutions to keep an eye on both policies and security events.

“We use FortiManager to make sure any changes to our security policies are approved and universal,” Houston says. “Our SOC [security operations center] has the capability to go in and look at any policies that could be creating problems. And if we need to change policies in response to a threat actor or for any other reason, we change it once, and it immediately spreads across our entire network, including to any teleworkers.

“We use FortiAnalyzer to identify indicators of compromise,” he continues. “We pull reports often and receive alerts on anomalies in our environment. Because the entire Fortinet Security Fabric is under a single pane of glass, we can log in to one place to see everything versus 15 different locations. If one solution finds a threat, it is a very quick pivot to block it in policy. This is crucial to protecting our systems: When a threat enters our network, we do not have much time to act.”

Houston describes a situation last year that could have been devastating for the health system. “FortiAnalyzer revealed an indication of compromise,” he says. “We identified the threat and put an end to it. But if we had not been able to identify the threat, or if we did not have all those tools in place, the situation would have been significantly worse. Having integrated Fortinet Security Fabric solutions that enable deep dives into data most likely saved our organization from having a bad day turn much worse.”

FortiVoice: A Rock-Solid Phone System

Two years ago, Mount Desert Island Hospital added the FortiVoice unified communications system to its infrastructure. “We had an aging IP phone system,” Manzo says. “In evaluating whether to upgrade it or go with something different, we looked at several solutions. We were intrigued by FortiVoice because of the cost of hardware and ongoing support.”

Moving to the FortiVoice platform felt like a leap akin to the hospital’s first foray into FortiGate NGFWs. “We could not find any other healthcare organizations using FortiVoice at the time, so it was a bit of an unknown,” Manzo continues. “But we were so comfortable with our other Fortinet products that we decided to go forward. That turned out to be a great decision.”

Mockus and his team worked directly with Fortinet to roll out FortiVoice. “We bought a block of service hours, planning for a weeklong implementation,” Manzo says. “Our in-house telecom engineer had no previous Fortinet experience and no previous PBX [private branch exchange] experience. But FortiVoice is so intuitive that, by day three, he was practically an expert in it.”

“We are no longer chasing bugs in the code on the switches or configuration changes that risk taking down the hospital like we did in the past. Plus, our reliance on support from our security provider has decreased a hundredfold. That has been eye-opening.”

Tony Manzo
IT Manager, Mount Desert Island Hospital

“As we transitioned to FortiVoice, we all wondered why nothing was going wrong. We were moving away from a 30-year-old system, so we expected big outages, but moving to FortiVoice was a non-event. Our total downtime was about five minutes.”

Tom Mockus
Director of IT, Mount Desert Island Hospital

In fact, Mockus says, the team was shocked by the rollout: "As we transitioned to FortiVoice, we all wondered why nothing was going wrong," he says. "A hospital cannot be without its phones for any length of time, so a phone conversion is terrifying. We were moving away from a 30-year-old system, so we expected big outages, but moving to FortiVoice was a non-event. Everything went as planned; the transition was totally smooth. Our total downtime was about five minutes."

"The other thing that was amazing," Houston adds, "is that FortiVoice enabled us to move away from an archaic paging system, as well. Fortinet has the simplest, best, most concise paging solution I have seen, and it is built into FortiVoice."

Ever since the transition, Manzo says, "The system has been rock-solid. We could not be happier with FortiVoice."

Fortinet Fosters Trust and Partnership

Across all the hospital's Fortinet solutions, reliability is saving the IT team a significant amount of time. "We are no longer chasing bugs in the code on the switches or configuration changes that risk taking down the hospital like we did in the past," Manzo says. "Plus, our reliance on support from our security provider has decreased a hundredfold. That has been eye-opening."

The Fortinet Security Fabric accelerates training of new security staff and enables team members to fill in for peers in different roles. "Once you get into the FortiOS GUI [graphical user interface], the solutions are pretty much the same," Houston says.

And if Mount Desert Island Hospital does encounter an issue, "Our support team makes us feel very comfortable," Manzo says. "Anytime we have an issue or a question, we reach out to them and get an immediate response."

> *"FortiAnalyzer revealed an indication of compromise. We identified the threat and put an end to it. Having integrated Fortinet Security Fabric solutions that enable deep dives into data most likely saved our organization from having a bad day turn much worse."*
>
> **Will Houston**
> Network Security Manager,
> Mount Desert Island Hospital

Mount Desert Island Hospital is now moving toward the FortiClient EMS endpoint management and security system. "EMS and ZTNA [zero-trust network access] architecture are our next stop," Houston says. "We are starting to use FortiAuthenticator to set permissions for certain users or user groups based on an existing policy rather than creating a separate policy. And by moving to FortiClient EMS, we will be able to deploy full-fledged ZTNA."

"I trust our contacts at Fortinet," Mockus concludes. "I cannot say that about every vendor I have worked with. But with Fortinet, I do not feel our representatives are just trying to sell us a product. Sometimes, they tell us the product we are considering is not right for us or that we need a smaller size. Fortinet is a partner to our organization, not just another vendor. That is the biggest differentiator that sets Fortinet far apart from the competition."