CASE STUDY

Financial Institution Turns to Fortinet to Build Trust in Network Security, Reliability, and Performance

Outstanding customer service can be dangerous. "That sounds strange," acknowledges David Kennedy, "but my experience at Trustmark indicates it is true. For 20 years, our company has consistently received top ratings for service. Our employees are focused on doing the absolute best they can for our customers. I worry, though, that sometimes they are too kind. Going out of their way to be helpful might make it easier for bad actors to manipulate them."

As the executive vice president and CIO of Trustmark, Kennedy is responsible for cybersecurity across an assortment of financial services offerings. Trustmark provides personal and business banking through more than 180 branches in six states. It also has large mortgage servicing and insurance divisions, as well as equipment leasing and commercial real estate businesses.

In total, the company has approximately 3,000 employees in over 200 locations. For Kennedy's cybersecurity team, leveraging the right technology is key to mitigating the risks that may follow from employees' innate helpfulness. "We are continuously working to boost users' understanding of potential cybersecurity pitfalls," Kennedy says. "We also have to overbuild our security systems."

The Fortinet Conversion: A Slam Dunk

A few years ago, when Kennedy left the oil and gas industry to join Trustmark, the firm's overbuilding approach resulted in a security architecture that was difficult to manage. "The Trustmark team bought a lot of networking and security products from different vendors but did not fully integrate them," Kennedy says. "So they had a tangled web of solutions to manage, which created the risk of gaps in coverage."

Kennedy, by contrast, had been using Fortinet solutions for years and appreciated that the Fortinet Security Fabric tightly integrates solutions throughout the networking and security architecture. When he joined Trustmark, he was tasked with building an infrastructure that would be sustainable for the long term.

"With the legacy vendor, we had situations where one solution in the architecture might throw out false information to another," he says. "For example, the management tool might say endpoint protection had been updated, even though nothing had happened on the actual client endpoints. That vendor added functionality by acquiring and rebranding products without properly rolling them into the ecosystem. Every time we bought a new product, we had to add staff to specialize in that product. It became very apparent that both security threats and our attack surface were going to continue growing. We needed to invest in technologies that would enable us to manage 10 more, 100 more, or even 1,000 sites without exponentially scaling up our security team."

Trustmark

"In the long run, it is more economical for us to transition to Fortinet solutions than to continue with our legacy vendor. Demonstrating the business case took a little time, but it is always a slam dunk when better technology costs less."

David Kennedy
Executive Vice President and CIO
Trustmark

Details

Customer: Trustmark

Industry: Financial Services

Headquarters: Jackson, Mississippi

Fortinet-Secured Endpoints: 200+

Business Impact

- More secure network with better visibility
- Dramatically improved reliability and network performance

The legacy vendor was quite entrenched in Trustmark's IT culture, but Kennedy gave FortiGate Next-Generation Firewalls (NGFWs) to a couple of his engineers to play with at home. "They asked, 'What about training?' and I said, 'You are not going to need a lot of training,'" he reports. "After a very short time, when we would have meetings about building a new branch or turning up a new site, the first question would be whether we should use Fortinet."

Kennedy adds that a lot of the culture shift was driven by the promise of the Fortinet Security Fabric. "Products that are Fortinet Security Fabric–enabled close the gaps and make my team's jobs easier," he says. "It is one thing to sit in a room and have a salesperson with a PowerPoint presentation tell you that a product is easy to use or integrates well. It is another thing to experience it yourself. Once our number of Fortinet products started to reach a critical mass, the culture flipped. Now, the guys who were very committed to our legacy vendor are asking me whether we can test FortiSwitch enterprise switches. A few years ago, they would have considered that to be heresy.

"Overall, in the long run," he adds, "it is more economical for us to transition to Fortinet solutions than to continue with our legacy vendor. Demonstrating the business case to the team took a little time, but it is always a slam dunk when better technology costs less."

The Fortinet Transition: Both Lucky and Smart

In 2019, Trustmark began rolling out FortiGate NGFWs to serve as headends for its virtual private network (VPN), with the FortiClient solution providing VPN connectivity on endpoints. The emergence of COVID-19 made this transition seem prescient, as the installed FortiGates provided the VPN capacity to cover all the newly remote employees. All they only needed to deploy FortiClient on the endpoints, a simple operation with the FortiClient EMS system.

"I would rather be lucky than smart, and our timing was very lucky," Kennedy says. "We had started down the road to Fortinet VPN when COVID hit. The pandemic unlocked the funding for us to roll out FortiClient to every endpoint in the company. The decisions were made, and our design was ready to go, so COVID accelerated deployment."

The solution worked well, and the FortiGate NGFWs proved their value. Trustmark soon began replacing legacy firewalls with FortiGate NGFWs as they reached end of life. The firm also rolled out Fortinet Secure SD-WAN, which comes with the FortiGate NGFWs, for software-defined wide area network connectivity between locations. Now, each Trustmark branch and office has a 60 Mbps Ethernet connection to the internet and a 20 Mbps VPN connection back to headquarters, with a 5G cellular connection enabled by a FortiExtender device as a backup.

"The FortiGate firewalls decide how to route traffic based on what the traffic is," Kennedy says. "The VPN links are far more expensive than the internet links, but they are crucial for guaranteeing quality in our Voice over IP [VoIP] and mainframe connectivity."

The FortiGuard Enterprise Protection Bundle protects the firewalls with web filtering, application filtering, intrusion prevention system (IPS), and intrusion detection system (IDS) capabilities. It also includes specialized operational technology (OT) and Internet-of-Things (IoT) protections, including a continuously updated list of signatures for threats to industrial equipment. "Each location has IP-enabled environmental control systems, IP-enabled access systems, and a video security system," Kennedy explains. "We leverage the OT signatures in the Enterprise Protection Bundle to protect those attack surfaces."

Business Impact (cont.)

- Elimination of need to add staff with every new product
- Overall reduction in cost of networking and security technologies

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiNAC
- FortiClient
- FortiAuthenticator
- FortiManager
- FortiAnalyzer
- FortiExtender

Services

- FortiGuard Enterprise Protection Bundle

"FortiNAC automation gives my staff more time for innovation, for thinking critically about how we want to engineer our networks versus just ensuring we have connectivity. FortiNAC, in concert with the FortiGates and Fortinet Secure SD-WAN, is a very elegant solution."

"We have 290 IT vendors in our vendor management system, and Fortinet is one of two that we see as a true partner. We look forward to working with Fortinet for years to come."

David Kennedy
Executive Vice President and CIO
Trustmark

FortiNAC and FortiGate Solutions Keep Devices Segmented and Secure

Trustmark also uses the FortiGate NGFWs for internal segmentation of each location's local area network. The firm always wanted to isolate sensitive equipment such as ATMs and alarm systems from other network resources, but "That was difficult with our legacy vendor," Kennedy says. "By contrast, when we install a FortiGate firewall, we can create and maintain that segmentation relatively easily."

Trustmark deployed the FortiNAC network access control solution to ensure that each device connecting to its network is placed in the right segment. Kennedy's team considered several NAC options, but an in-depth, six-month proof of concept (POC) sold them on FortiNAC.

"The team was OK with our legacy NAC until they understood what the FortiNAC solution has to offer," Kennedy says. "During the POC, they were amazed by how much of the work FortiNAC can automate. That automation gives my staff more time for innovation, for thinking critically about how we want to engineer our networks versus just ensuring we have connectivity. FortiNAC, in concert with the FortiGates and Fortinet Secure SD-WAN, is a very elegant solution."

Now, Kennedy's team is profiling each type of device that might connect to the Trustmark network and determining how security tools should treat it. Each branch's ATM has its own network segment, as do various OT security devices. Kennedy estimates that most Trustmark locations have around seven virtual local area network (VLAN) segments. When FortiNAC discovers a new device on the network, it assigns it a VLAN.

"Because we are geographically dispersed and do not have security personnel in every location, people in branches sometimes move equipment on their own," Kennedy explains. "If they think a device would look better in another part of the space, they might find an open Ethernet port over there and plug it in. With our Fortinet architecture, my team no longer worries about that kind of situation. We know that each device will be treated appropriately based on what it is."

For example, he continues, "A third party handles all transactions for our cash-advance machines. Traffic from those machines needs to go directly to the third party so that we do not have to worry about PCI [Payment Card Industry] compliance on those transactions. It is critical for the cash-advance machines to be on the correct VLAN, and with our Fortinet infrastructure, that is not a concern. Anytime a cash-advance machine is added or moved within a branch, the FortiGate firewall works with the FortiNAC solution to automatically allocate it to the right VLAN."

Efficient Management of a Dispersed WAN

Using the FortiManager management platform, Kennedy's team has streamlined rollout of new security infrastructure components. This is important, as the firm frequently opens new locations.

"A lot of our branches are several decades old, and we are in a process of consolidation," Kennedy explains. "We might open a new, big branch in a vibrant part of town and close two smaller branches. The result is usually about the same square footage, but it is more efficient to operate." The firm also runs multiple financial literacy locations and provides mobile ATMs for events such as festivals. All in all, Kennedy says, "We have branches coming on and off the network all the time, in different locations and with different security requirements, and we use FortiGate firewalls to secure them. It is absolutely critical to have an efficient rollout process."

That is where FortiManager comes in. "From an architecture design standpoint, FortiManager is a very elegant tool for deploying FortiGate firewalls," Kennedy says. "In our legacy environment, we used a third-party management tool. Getting visibility down to a granular level was cumbersome, and every task required manual intervention. With FortiManager, we have created very specific profiles, which we apply to gear depending on what its ultimate destination is. That eliminates mistakes and enables the team to get new firewalls out the door very quickly."

Meanwhile, the FortiAnalyzer, a central analytics and automation platform, converts raw network data into actionable insights to fine-tune security posture, identify potential vulnerabilities, and ensure ongoing compliance with regulatory standards. FortiAnalyzer provides Trustmark's managed security service provider with deep insights into the firm's security environment. That has triggered conversations with Fortinet about available security operations center products. Kennedy expects to evaluate FortiDeceptor soon.

Big Benefits across Security, Reliability, and Performance

The consolidated Fortinet solutions have greatly improved security throughout the bank's network. "Previously, when all traffic was backhauled to headquarters over the VPN, my team's visibility into the network and security events was limited," Kennedy says. "Now, with FortiGate firewalls on-premises at each location, we can run application security, IDS, IPS, and other security functions locally. We also have much greater visibility, which enables us to head off security issues a lot earlier in the attack chain."

In addition, the improvement in visibility has reduced the resources Trustmark must expend on network management and security. "We no longer have to dispatch technicians every time someone in a branch moves a device to a new port because the port either is not live or is on the wrong VLAN," Kennedy says. "Moving to the Fortinet architecture has made a demonstrable difference in the number of service tickets we receive."

Moving to Fortinet has also improved the performance and reliability of the Trustmark network. In the legacy environment, "We had significant issues around latency, jitter, and connectivity," Kennedy reports. "From a user experience standpoint, the shift to Fortinet has made a big difference.

"We have a lot of locations in small towns, and we frequently experience landline failures," he continues. "With our legacy infrastructure, the conglomerate of products would eventually affect a failover, but it took time. That often caused issues because our mainframe is finicky about any loss of activity. With Fortinet, we have not had an outage in months. Some of our associates have commented, 'I guess our telecom provider fixed the problems.' That is not true; the frequency of outages has not changed. But nobody notices outages because of how the FortiGates handle failover."

Looking toward a Future with Fortinet

Kennedy's team is now considering replacing its legacy networking gear with FortiSwitch switches and FortiAP access points in each location. Zero trust and zero-trust network access are also on their radar. "FortiClient is part of our standard image on every endpoint," Kennedy says. "Even on devices that will probably never need VPN capabilities, we install FortiClient because it is the first building block of the pyramid in our move to zero trust. That transition will probably take us a couple of years, and Fortinet is the easy piece of that puzzle."

Whatever the future holds for the Trustmark network, Fortinet is likely to play a key role. "We really appreciate that we understand Fortinet's long-term product roadmap," Kennedy says. "A lot of the investments we make require a commitment of three or five years with the products. Working with a company that operates at the convergence of networking and security is very helpful from a strategic planning standpoint."

Plus, he adds, "My team feels we are part of a partnership with Fortinet rather than just another customer. There have been plenty of times when Fortinet has scratched our back as much as we have scratched theirs. Not just in purchasing and deployment, but there are times they have taken our feedback and made modifications to products as a result. We have 290 IT vendors in our vendor management system, and Fortinet is one of two that we see as a true partner. We look forward to working with Fortinet for years to come."

January 10, 2024 2:04 AM

2513101-0-0-EN