FORTINET

CASE STUDY

How One company Efficiently Secures over 1,500 Venues by Standardizing on the Fortinet Security Fabric

When corporate or government entities need support in food service, retail operations, cleaning, or facility maintenance, they turn to a leading service provider. “We are engaged in all walks of life,” says the director of field infrastructure services. “We provide diversified services to hospitals, K-12 schools and colleges, corporate campuses, and manufacturing sites. We serve the corrections industry, and we provide concessions in many sports arenas and national parks across the United States.”

The company operates equipment, including point-of-sale (POS) systems, in around 1,500 customer locations. It also relies on applications hosted in the Microsoft Azure and Amazon Web Services clouds or in its data centers. Either way, the director says, “We generally bring the network solution to our clients.” Protecting this network is business-critical for the facilities management provider.

“Security is a huge concern for us,” he explains. “We are responsible for protecting people’s identities and personal information such as credit card data. Our success or failure in security reflects not only on us but on our clients as well. But, because we are operating equipment within client locations, securing the network can be complicated. In some cases, we collaborate with clients on networking, but we always request that they at least let us install our own firewall so that we can control the security of our POS systems and any IoT devices we have in place.”

FortiGates Are Key to Building a Centralized and Secure Infrastructure

In 2017, as its networking and security technologies approached end of life, the company re-evaluated how it handled network security. At the time, most customer locations had networking staff on-site. But, IT leaders envisioned a solution in which the company’s many locations could be managed centrally. After completing their due diligence, they selected FortiGate Next-Generation Firewalls (NGFWs) supported by the FortiManager centralized management platform and the FortiAnalyzer analytics platform.

“Fortinet offered us a way to bring all our security capabilities together and create a more centralized and secure infrastructure,” the director says. “We adopted a new security policy that follows zero-trust principles, and Fortinet enabled us to carry out that vision. Nothing that we had in place previously would have allowed us to come close to the level of security we have now.”

Today, the company places one or more FortiGates at the network perimeter in most locations it manages. Many of these FortiGates are supported by the FortiGuard AI-Powered Security Services Unified Threat Protection Bundle. “We do not license those services across the board, but we provide them when our clients need them,” he says. “IPS [intrusion prevention system] is the service clients ask about most often.”

“By transitioning to Fortinet, we have centralized everything with a team that is much, much smaller. I used to be based at one of our national parks, with a staff of six to support two parks. Now I have a staff of eight supporting firewalls and switches across 1,500 locations.”

Director of Field Infrastructure Services

Details

Industry: Hospitality

Number of Secure SD-WAN Locations: 1,500

Business Impact

- Massive cost savings
- Greatly enhanced security vs. legacy environment
- Flexibility to connect networking and security devices to any client environment

The company creates virtual LANs (VLANs) to segment its POS systems from other network traffic. “We follow PCI [Payment Card Industry] best practices for payment data,” he explains. “The FortiGate firewalls let us put individual point-of-sale vendors on their own network segments, so we can provide very restrictive rules for each vendor. We do the same thing for IoT and digital-sign vendors.”

The team uses FortiManager to oversee this vast landscape of dispersed firewalls from corporate headquarters. “We do all our work in FortiManager,” he says. “It is very rare for my team to log in to a firewall itself. We use policies and access control lists extensively, maintaining them in FortiManager. Fortinet solutions enable us to apply shared policies across hundreds of firewalls, across all our lines of business. This ability to centrally manage our firewalls and push out policies from the central office is the single most valuable aspect of the FortiGates for us.”

Meanwhile, FortiAnalyzer brings all of the company’s traffic and event data onto a single device. “For problems that span multiple firewalls or communications between our hosts, we have consolidated information,” he says. “Being able to see traffic end to end in one place makes troubleshooting easy. And then we can log in to the firewalls from FortiManager to solve the problem.”

One more key feature of the FortiGates: “Fortinet solutions are very adaptable without a lot of effort,” he says. “The flexibility of the FortiGate configuration lets us interface with our client networks, which may include all sorts of different network technologies. No matter what systems a client uses, we know that we can adapt our Fortinet interfaces to connect to them in a way that suits both our needs and our clients’ needs. Fortinet solutions really shine through in that regard.”

FortiAPs, FortiSwitches, and Fortinet Secure SD-WAN Further Streamline Networking

The company also leverages Fortinet Secure SD-WAN, using the technology in several ways. One, the director explains, is to aggregate bandwidth in some far-flung places. “For example, in some national parks, we cannot get as much bandwidth as we would like,” he says. “By their nature, these clients are located in places where the fastest connection might be a T1 or DSL line. We might add some kind of cell or satellite service as well, then use Fortinet Secure SD-WAN to stitch together enough bandwidth to provide our most important applications with the connectivity they need.”

Another use case: “Fortinet Secure SD-WAN also helps us build network resiliency. We will pair a strong circuit with a lesser connection. Then, if our main circuit fails, our point-of-sale systems will still have some connectivity.”

A year after deploying the FortiGates, FortiManager, and FortiAnalyzer, the company standardized on FortiAP access points. “We use FortiAPs because we can centrally manage them,” he explains. “Their integration with the FortiGates means we can follow the same network practices and policies on the access points as on the firewalls. We feel we are doing a very good job of managing security across our wireless access, which is always higher risk than the wired networks.”

Business Impact (contin.)

- Competitive advantage created through stringent security standards and system interoperability with client sites
- Secure SD-WAN bandwidth aggregation
- Improved network reliability
- Accelerated deployment of new networking and security hardware

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiManager
- FortiAnalyzer
- FortiAP
- FortiSwitch

Services

- FortiGuard AI-Powered Security Services Unified Threat Protection (UTP) Bundle
- Fortinet Enterprise Agreement

“When we are working with prospects, we explain how our Fortinet solution meets their security standards… and that our flexible configuration can interface with their solutions. In these ways, using Fortinet solutions provides our company with a competitive advantage.”

Director of Field Infrastructure Services

More recently, the company standardized on FortiSwitch secure Ethernet switches as well. “We have been deploying only FortiSwitches over the past few months, and that has transformed our deployments,” he says. “Previously, each switch held its own configuration. With FortiSwitch, we can plug a switch in and have it instantly picked up by the firewall and loaded with our standard configuration. That has greatly accelerated our deployment of systems in the field and improved our ability to get resources into the correct VLAN.”

“The move to FortiSwitch has also alleviated the need to have skilled technical people installing all our equipment in the field,” he adds. “Once the FortiGate and FortiSwitch are in place, an engineer sitting in headquarters can go into the FortiGate and manage the devices. That means we can now do most of our work remotely, which is crucial for my team of eight network engineers.”

“Where the Fortinet solutions really shine is in locations where we have operations spread across a dozen buildings. Bringing in firewalls that we can seamlessly manage as a group of devices saves us a great deal of money that we could have spent building a large network.”

Director of Field Infrastructure Services

Improved Security, Cost Savings, and a Competitive Advantage

In fact, the director says, the company would need a much larger staff if its network were built on a different solution set. “Fortinet solutions have such a well-developed GUI [graphical user interface] that there is always an efficient path to accomplish what we need to on our devices,” he reports. “The fact that we do not have to maintain individual policies for each firewall saves us countless hours of work. And being able to access all our equipment without going into multiple interfaces is a great time saver.”

“Before the Fortinet solutions, every one of our lines of business had its own staff handling networking and security,” he continues. “By transitioning to Fortinet, we have centralized everything with a team that is much, much smaller.” As an example, he adds, “I used to be based at one of our national parks, with a staff of six to support two parks. Now, I have a staff of eight supporting firewalls and switches across 1,500 locations. The park where I once worked has a single networking team member who is there only part of the year.”

The effectiveness of security has also improved across the company locations, according to the director. One reason is the FortiGates network segmentation and consistent policy management. Another is the enhanced visibility the team has into security events.

“Knock on wood, we have not had any incidents directed at us,” he says. “However, we are working in client locations where there are aspects of security we do not control, and we frequently find ourselves side by side with security incidents. Anytime that happens, we use the local FortiGate to shut down access to the company’s corporate network while still accessing our on-site equipment through FortiManager and FortiAnalyzer.”

The ability to turn on advanced protections when needed makes the company a more desirable service provider for some prospective clients. “When we are working with prospects, we explain how our Fortinet solution meets their security standards,” he says. “We proudly describe our standards and explain that our flexible configuration can interface with their solutions. In these ways, using Fortinet solutions provides us with a competitive advantage.”

The Fortinet Security Fabric has proven reliable, even for Voice over Internet Protocol systems located in remote national parks. “The bandwidth aggregation with Fortinet Secure SD-WAN enables us to provide resilient services; we frequently prevent outages,” he says. “If some rusty T1 line goes down in a remote location, the site likely will not even know the difference.”

The icing on the cake is that the Fortinet infrastructure is also saving money. In addition to its lean networking staff, the company was able to eliminate the managed service provider that previously provided SD-WAN services and reduce the number of devices its network requires. “Where the Fortinet solutions really shine is in locations where we have operations spread across a dozen buildings,” he says. “Bringing in firewalls that we can seamlessly manage as a group of devices means we can avoid building an unnecessarily large network, which saves us a great deal of money.”

The company has further reduced costs by signing a Fortinet Enterprise Agreement. "The fact that we can easily bring devices into and out of the Enterprise Agreement saves us a lot of money," he says. "Given the number of devices we manage, we are regularly replacing older devices with newer ones. Having the Enterprise Agreement in place means we can remove an end-of-life device and replace it with a new device within the same FortiCare contract. That has resulted in big savings for us."

Next, the company is looking at adding FortiNAC network access control to the mix. "Since we started deploying FortiGates, we have had a very natural progression into additional technologies," he says. "We are always interested in further developing our security best practices because we know that a secure environment develops over time. As we have gained experience with the FortiGates and FortiManager and optimized our use of those solutions, we see that FortiNAC could take our security platform to the next level by dynamically restricting network access and using profiles to assign our endpoint devices to VLANs."

> *"As Fortinet grows, our security practices grow as well. Whenever we identify a need or what we may deem a place to improve, there always seems to be a Fortinet solution that will fill that gap."*
>
> **Director of Field Infrastructure Services**

"As Fortinet grows, our security practices grow as well," he concludes. "Whenever we identify a need or what we may deem a place to improve, there always seems to be a Fortinet solution that will fill that gap."