CASE STUDY

Fortinet Brings Superior Security to Industrial-Scale Poultry Producer

An industrial-scale poultry operation produces a significant amount of top-quality chicken each week. Its processing facilities meet high standards for safety and quality, as demonstrated by regular audits and industry awards.

Headquarted in North Carolina, the poultry producer has four processing plants across two states; each plant is supported by an on-site hatchery, feed mill, and other production facilities. The corporate network is crucial in keeping all these facilities running smoothly. Operational technology (OT) equipment plays a key role in poultry processing, while IT systems provide necessary communications, quality control, and back-office functions.

A cyberattack that affected any of these areas might potentially lead to business issues that could undermine the company's image as a leader in quality assurance. An unexpected OT outage could even create safety concerns for staff on the production line. Three years ago, the company became acutely aware of the risk and embraced the Fortinet Security Fabric for its networking and security infrastructure.

Turning to Fortinet after a Security Scare

The initial trigger for this pivot was an incident that started one night in December. "At around 3 a.m., a database administrator doing some work noticed that certain files were being encrypted," explains the company's network security administrator. "It was a ransomware attack in progress. We took everything offline and began working with a third-party security firm to recover."

One of that firm's first recommendations was that the company install a more robust endpoint detection and response (EDR) solution. In particular, the firm described how FortiEDR could improve the poultry provider's security posture. The company was quickly convinced, and its IT team began rolling out FortiEDR to all 800 company endpoints, with the Fortinet support team helping them deploy and optimize the solution.

The IT team was immediately pleased with the improvement in endpoint security. "FortiEDR provides much better visibility into what is happening on our network than what we had with our legacy endpoint security," the company spokesperson says. "You can easily see exactly what FortiEDR is doing, and it began alerting us to vulnerabilities that were not visible in our prior environment. We began talking about other changes we needed to make."

At the time, the company's networking and security infrastructure consisted of a mix of products from several vendors. Its director of IT, saw an opportunity to simultaneously improve security throughout the company's network and efficiency for the IT team. "The thing we liked most was the Fortinet Security Fabric," he says.

"Working with an assortment of providers makes everything more complicated. The idea of building a security posture with a single provider whose products tightly integrate was very appealing. We quickly made the decision to standardize on Fortinet solutions wherever possible."

Director of IT

Details

Industry: Food Production

Business Impact

- Significantly improved security posture
- Better visibility into network and security
- Workload for central IT team reduced by about 60 hours per month
- 20–30 hours saved per month on management time
- Faster changes to local networks

"It is not just that the firewalls integrate with the switches, but all the other solutions do as well, including FortiGuard SOC-as-a-Service."

"Working with an assortment of providers makes everything more complicated," he continues. "We saw a lot of security gaps we wanted to fill, and the idea of building a security posture with a single provider whose products tightly integrate was very appealing. The Fortinet partner we were working with explained where Fortinet could take us, and I cannot emphasize enough how impressed we were. We quickly made the decision to standardize on Fortinet solutions wherever possible."

A Fully Fortinet Shop

The company began migrating to FortiGate Next-Generation Firewalls (NGFWs) and FortiAP wireless access points. Each of the company's five primary locations now has a high-availability pair of FortiGate NGFWs, and all its other buildings have a single FortiGate. The firewalls are equipped with the FortiGuard AI-Powered Security Services Enterprise Protection Bundle. Having the bundle's intrusion prevention system capabilities, security rating for posture management, and Internet-of-Things visibility license gives the company confidence that external threats will not be able to access its network.

The FortiGate NGFWs fully separate the company's OT network from its IT systems. "Our OT devices cannot communicate with the outside world unless we proactively build them a direct path to do so. For example, as a one-off because the manufacturer requests it," the company spokesperson reports. "In addition, within our IT network, we use VLANs [virtual LANs] to prevent traffic from moving laterally. This protects our systems should an attacker get past our perimeter security."

Benefits of the Fortinet solutions became apparent early in the rollout. "As soon as we saw the FortiGates in action, we were excited about the ease of management," he says. "Our legacy firewalls relied on a CLI [command-line interface], and staff in our plants lacked the expertise to manage their local firewalls. But with the Fortinet GUI [graphical user interface], they can do a lot of the firewall maintenance and management themselves."

The team was similarly impressed with the FortiAPs, some of which are designed for use outdoors. "Staff pressure-wash our production facilities every day, so the access points have to withstand a lot of water," he says. "Plus, some of our APs are located in freezers to provide wireless network access when staff are doing inventories there. Those APs have to withstand very cold temperatures."

The team appreciate the access points' performance in these harsh environments and their range in every condition. "The FortiAPs have better coverage than our legacy wireless devices, which means each one can cover a larger area," he says. "We do not need as many devices as we had previously, so we are saving money and reducing management time by about 20 to 30 hours per month."

Solutions

- FortiEDR
- FortiGate Next-Generation Firewall
- FortiAP
- FortiSwitch
- Fortinet Secure SD-WAN
- FortiClient Endpoint Management Server
- FortiSIEM
- FortiManager Cloud
- FortiAnalyzer Cloud

Services

- FortiGuard AI-Powered Security Services Enterprise Protection Bundle
- FortiGuard SOC-as-a-Service

"We are definitely better covered than we were before we moved to Fortinet. Having security experts monitoring our network 24×7 gives us confidence that we are well-protected during those off hours in the middle of the night and on weekends."

Network Security Administrator,

As contracts with other providers ended, the company migrated to FortiSwitch secure Ethernet switches and Fortinet Secure SD-WAN. "We changed our network to have two different communications providers coming in," the spokesperson explains. "Each site can connect directly to the internet, rather than being backhauled to our data centers."

The company also installed FortiClient Endpoint Management Server (EMS) to provide remote users with secure access and Fortinet security controls. "Our goal is to become a Fortinet shop for all our networking environment," he says.

Security and Efficiency, with 24×7 Threat Scanning

The team engaged FortiGuard SOCaaS to monitor and detect security events on their network 24×7. FortiGuard SOCaaS provides continuous security event monitoring and threat detection by leveraging advanced AI, ML, and the expertise of Fortinet analysts who analyze alerts from Fortinet solutions to pinpoint critical incidents demanding immediate attention.

Recently, the team also transitioned their FortiEDR deployment to a managed service provided by Fortinet partner Thrive. Thrive leverages the FortiSIEM security information and event management solution to collect and analyze the company's endpoint security data as part of this agreement. "We still control the EDR, but Thrive performs ongoing scanning of network vulnerabilities and security events, and they will react to events when necessary," he explains.

The SOCaaS and managed EDR services build the team's confidence that Fortinet security experts will catch threats immediately if the company ever faces another attack after business hours, on weekends, or holidays. "We are definitely better covered than we were before we moved to Fortinet," he says. "Our plants operate 24 hours a day, while our IT team generally works standard office hours. Having security experts monitoring our network 24×7 gives us confidence that we are well-protected during those off hours in the middle of the night and on weekends."

Meanwhile, the internal IT team uses FortiManager Cloud and FortiAnalyzer Cloud to provision, monitor, and secure the FortiGate NGFWs, FortiSwitches, and FortiAPs companywide. The centralized team can make a policy change once and have it replicated to devices in every location.

"Network administration is centrally managed out of Troutman through the cloud-based management tools," he says. "FortiManager Cloud and FortiAnalzyer Cloud enable us to very quickly look at anything we need to see."

Fortinet's Ease of Use Makes IT Staff More Productive

This visibility is a key benefit of the company's Fortinet infrastructure. "The fact that the solutions are easy to use and all intertwined around the firewall makes all the difference in the world," he says. "To me, the key benefits are that the Fortinet solutions can be centrally managed. FortiManager Cloud and FortiAnalyzer Cloud have a great GUI that is simple to use, and everything is tightly integrated throughout the Security Fabric."

The spokesperson concurs: "Having the firewalls, switches, and access points from the same solution provider enables them to talk natively, so they all know exactly what is going on at any point in time. That makes our network more secure," he says. "And the Fortinet solutions are much more intuitive to use than our legacy systems. Because we have a graphical representation of our security posture, we can quickly see what is happening and respond if necessary."

Time savings in activities such as establishing new VLANs, configuring switches and access points, and tracing physical connectivity—made possible through the Fortinet Security Fabric's improvements to network visibility—reduce the team's workload by about 60 hours per month. "Before, we had to spend a lot of time chasing wires and running things down," he says. "Ninety percent of what our IT team does is troubleshoot network- and connectivity-related issues. And so the switches and access points have made us much more efficient."

At the same time, the Fortinet solutions' ease of use has enabled its director of IT to spread the networking and security workload throughout the IT team. Because the solutions' GUIs do not require specialized expertise, any IT staff member can perform firewall, switch, or AP management tasks. "IT administrators in the different locations are now responsible for managing their own equipment," he says. "We have given them more permissions, so they no longer have to call the host office and wait for changes to be completed."

As a result, tasks such as turning on a port for a new security camera can happen in a few minutes rather than taking a few days. "IT staff within our production plants can work faster, troubleshoot better, and get things running smoothly and fixed quicker," he emphasizes. "The entire team loves that."

"Technology is moving so fast today, and securing the corporate network is such a critical issue that it is very important for the infrastructure to be easy to use," he concludes. "Security teams need a graphical user interface to solutions that are tightly integrated and centrally managed. That is what we are getting with Fortinet."

October 2, 2024 3:26 AM / 2831761-0-0-EN