CASE STUDY

Manufacturer Turns to Fortinet to Achieve Security Compliance in the Demanding Defense Sector

In today's digital-first world, all companies need to prioritize cybersecurity. However, some are under greater threat than others due to the nature of the work and the sensitive data they transact.

Because the manufacturing company sells to the government and its major prime contractors, as well as to prominent vehicle manufacturers in agriculture, construction, mining, locomotive, mass transportation, and the oil and gas industry, it is a tempting target for criminal hackers and nation-state-based threat actors alike.

Cybersecurity for Compliance

Given its elevated risk profile, this manufacturer is tasked with demonstrating high cybersecurity preparedness through client contracts and external compliance mandates. One of the cybersecurity engineers comments: "As a defense contractor, we have a lot of compliance to fit on top of standard security practices, including network segmentation and real-time logging, so this is a key priority for us."

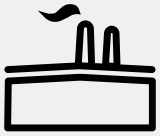
The company is working toward achieving Cybersecurity Maturity Model Certification (CMMC), which mandates regular cybersecurity assessments of contractors to the U.S. Department of Defense. To achieve compliance, the company must demonstrate alignment with the National Institute of Standards and Technology Cybersecurity Framework. The vice president of IT adds: "The CMMC is absolutely essential. Without it, we cannot do business with the defense market."

This manufacturer has, therefore, been engaged in a program to rebuild and enhance its networking and security systems across its three manufacturing locations.

Building on the Fortinet Security Fabric

As the company began planning its security overhaul, a trusted vendor recommended it look at Fortinet's product portfolio. Attracted to the ease of management and predicted time savings of using Fortinet products, the company deployed FortiSwitch Ethernet switches and FortiGate Next-Generation Firewalls (NGFWs). Along with hardware, the company added the FortiGuard AI-Powered Unified Threat Protection Bundle, which is used for deep packet inspection. Already deployed in all its manufacturing plants and soon to be rolled out in more facilities, this initial investment was just the start of a broader Fortinet Security Fabric solution.

Following the rise of remote working following the COVID-19 pandemic, the manufacturer subsequently enabled the VPN function of its FortiGate NGFWs. FortiClient Fabric Agents augmented this, allowing remote users to have device-level visibility, control, and zero-trust network access.



"With FortiSwitch, the configuration takes place automatically, and the entire process takes just 15 minutes for each switch. We can configure the entire switching network in a couple of hours, which frees up time to focus on performance and security rather than managing devices."

Vice President of IT

Details

Industry: Manufacturing

Business Impact

- Ability to comply with required defense-industry standards
- Significant reduction in time spent managing devices
- Enhanced network performance for a better employee experience
- Increased visibility of network and potential threats

The company's next step was to activate the Fortinet Secure SD-WAN functionality of its FortiGate NGFWs for use on its internal encrypted tunnels that connect its four manufacturing locations. One of the network engineers explains: "We mostly use the Fortinet Secure SD-WAN for monitoring purposes because tools provided by telecom companies do not always show the full picture." The company also relies on FortiAnalyzer for network monitoring, logging, and reporting. "FortiAnalyzer is our main storage solution for logs, so we can look at what is going on within the network and keep on top of bandwidth issues," he adds.

More recently, the company deployed the FortiSIEM security information and event management solution with user and entity behavior analytics (UEBA) to gather real-time logs and rapidly identify abnormal behavior, a key pillar of its compliance strategy.

Additionally, the company completed a high-availability deployment of FortiAuthenticator for resilient identity authentication services. "We have one FortiAuthenticator in our colocation facility and one at one of our factories. This provides much-needed redundancy so our people can keep on working if one of the sites fails," a spokesperson from the company explains.

Networking and Security Made Easy

One of the standout benefits of the Fortinet Security Fabric is that it has dramatically reduced the time the IT team spends managing devices. "Before Fortinet, we had to configure each switch consecutively, and it took around an hour for each to be done," says the vice president of IT. "With FortiSwitch, the configuration takes place automatically, and the entire process takes just 15 minutes for each switch. We can configure the entire switching network in a couple of hours, which frees up time to focus on performance and security rather than managing devices."

He adds: "I have worked with several competing switch solutions, and none come close to the ease of use we get with Fortinet. Especially when setting up switch ports or troubleshooting issues, Fortinet is exponentially easier than environments that rely on a command-line interface. Fortinet devices use a visual interface and are much more intuitive, which makes our job all the easier."

The company finds that this ease of use extends to all its Fortinet Security Fabric solutions via FortiOS, Fortinet's operating system. "Take the FortiClient solution as another example. It is very easy to make changes on a broad spectrum. So, if there is something wrong with the VPN connection, or if we need to block or unblock a web filter, we can apply the change to every user in a couple of clicks."

Solutions

- FortiGate Next-Generation Firewall
- FortiClient
- FortiAnalyzer
- FortiManager
- FortiAuthenticator
- FortiSIEM
- Fortinet Secure SD-WAN
- FortiSwitch

Services

- FortiGuard AI-Powered Unified Threat Protection Bundle

"We have tuned FortiSIEM so we can see exactly what we need to see and maintain a year's worth of pertinent logging data for compliance uses. The solution has enabled us to spot suspicious activity and potential attacks and resolve these cases rapidly."

Cybersecurity Engineer

This ease of management proved crucial in the early days of the pandemic when the company had to pivot to a remote-working model in just two weeks. Although the company had not used the VPN function of the FortiGate NGFWs until that time, it proved simple to set up the feature, and the firewalls had no problem coping with the volume of traffic that came with approximately 1,000 employees working from home.

Locking Down Security and Compliance

From a security perspective, Fortinet is proving invaluable in helping the company achieve its compliance goals. The FortiGate NGFWs play a key role in this respect, enabling the company to segment its locations and servers into separate virtual LANs. The approach enables the manufacturer to ensure that staff can only access appropriate IT resources at its various locations. "The FortiGate NGFWs allow us to be more locked down as an organization and control information flows across our infrastructure," the spokesperson adds.

With monitoring a key element of its compliance requirements, the company feeds data from its FortiGate NGFWs, FortiClient Fabric Agents, and FortiAnalyzer solution into the FortiSIEM and UEBA agent. “We have tuned FortiSIEM so we can see exactly what we need to see and maintain a year’s worth of pertinent logging data for compliance uses. The solution has enabled us to spot suspicious activity and potential attacks and resolve these cases rapidly.”

The UEBA agent is especially useful to the manufacturer, enabling precise logs on all devices. “If an attack ever hits us, the UEBA will help us piece together what happened, which is a key compliance requirement for us the spokesperson adds.

Increasing Network Performance and Integration

In addition to helping with compliance, Fortinet Security Fabric analytics capabilities help boost network performance. Mostly, this comes from using FortiAnalyzer to monitor for bandwidth issues. If users are experiencing issues with their systems, the IT team can quickly rule out the internet connection as the cause.

Overall, the company’s networking and security infrastructure benefits from the high levels of integration that comes with the Fortinet Security Fabric. The vice president of IT explains: “We have been growing our security posture for a while, and we have been impressed with the levels of compatibility and interoperability we have received. Other vendors promote interoperability, but Fortinet’s approach really stands out.”

Extending the Fortinet Security Fabric

Looking ahead, the company plans to continue to grow its relationship with Fortinet. “From a compliance perspective, we must achieve the Federal Information Processing Standards [FIPS]. Fortinet’s products come with a FIPS mode we consider implementing across the Security Fabric.”

The company also plans to deploy the FortiNAC network access control solution. This is also part of its compliance response, as it is mandated to be able to disable network ports if required. Finally, the company is considering using Fortinet in its OT environment and is currently reviewing use cases for the FortiGate NGFWs in this environment.

In conclusion, the spokesperson adds: “We have very specific and demanding networking and security requirements. Fortinet is the ideal partner to address these requirements, and we have increased our Security Fabric over the years as a result. We look forward to working with them in the future as we continue to build a best-practice compliance and security posture.”

April 26, 2024 12:21 AM
2674368-0-0-EN