FORTINET

CASE STUDY

Broad Fortinet Security Fabric Implementation Secures Electricity Provider’s Critical Infrastructure

As key suppliers in the nation’s energy infrastructure, regional electricity providers are in the crosshairs of many prospective cyberattacks. If one of these businesses fell victim to an attack, millions of people might lose power, with potentially life-threatening consequences for some affected customers. One major electric power station in the Midwestern United States experiences these pressures daily.

“We are a coal-fired power plant,” explains the organization’s IT manager. The company is focused on providing cleaner energy, yet “We are attacked every day by environmental groups. We also face threats from people outside the country who want to take down the power grid. One of my key goals as the leader of the IT department is to prepare our technology infrastructure to withstand those attacks.”

Ten years ago, the power company’s lean IT team was struggling to meet this mandate. They wanted to deploy a security architecture that would simultaneously enhance the company’s security posture and improve the efficiency of management.

That is when the power station began rolling out FortiGate Next-Generation Firewalls (NGFWs) to protect the perimeter of its IT network. The NGFWs leverage the FortiGuard AI-Powered Security Services Unified Threat Protection (UTP) Bundle, and the company has found its intrusion prevention system (IPS) and intrusion detection system (IDS) functionality particularly important in strengthening edge security. Another FortiGate NGFW serves as a termination point for remote users’ SSL VPN connections.

The NGFWs provide basic network segmentation, separating client systems from servers and isolating the VPN segment from everything else. The company’s OT devices run on their own distinct network.

Rapid Expansion of the Fortinet Footprint

For a decade, the firewalls have provided great security, thwarting threats day in and day out. After several years, the power company began transitioning its IT and OT networks to FortiSwitch secure Ethernet switches as well. In the IT environment, the tight integration between the FortiSwitches and the FortiGate NGFWs simplifies management of both devices. On the OT network, the FortiSwitches provide connectivity for the programmable logic controllers (PLCs) and other OT devices core to keeping power flowing to the company’s customers.

Ruggedized FortiSwitches have proven particularly beneficial in the harsh environment of the company’s underground coal mine. Miles and miles of Ethernet cables run through the tunnels, with FortiSwitches providing miners connectivity to the outside world. With a host of monitors, cameras, and voice communication systems, reliable connection is key, but wireless is unreliable underground. Using

“By simplifying network and security management through tightly integrated solutions, Fortinet enables the power station’s seven-person IT department to operate, support, and secure a critical-infrastructure network.”

IT manager,
Major Electric Power Station

Details

Customer: Major Electric Power Station

Industry: Power and Utilities

Location: Midwestern United States

Business Impact

- Reduced time to investigate and remediate from 18-20 hours to less than 5 minutes
- Reduced the burden on security teams by up to 99%
- High-level security alerts at any time of day or night
- Streamlined data loss prevention

Ruggedized FortiSwitches, the power company ensures reliable connectivity in harsh environmental conditions. These switches are designed to withstand extreme temperatures, dust, and moisture, making them ideal for maintaining seamless communication and operational efficiency in the mines.

Within the past few years, the power company has further extended its Fortinet infrastructure. It began using FortiExtender 5G/LTE wireless devices to provide connectivity in pop-up locations—for example, when it is constructing new facilities. FortiEDR endpoint detection and response offers additional protection to endpoints throughout the organization, and the FortiNAC network access control solution locks down user permissions . FortiAuthenticator and FortiToken provide user authentication. FortiSandbox isolates and tests any suspicious network traffic, and FortiDeceptor serves as a series of honeypots, designed to attract any malicious actors who make it through the perimeter defenses of the OT network.

The power station has not experienced a single successful attack since deploying its Fortinet infrastructure.

Visibility through Analysis

As his team deployed increasing numbers of Fortinet solutions, the IT manager wanted a centralized location to view the information those solutions were collecting. "I wanted to see who was logging in to the VPN," he says. "How long were they there? What type of data, and how much data, were they pulling? I wanted to know what types of websites our users were going to."

To answer these and many more questions, the power station deployed FortiAnalyzer, which pulls log data from all the company's Fortinet solutions. Now the IT manager receives a dozen reports each week giving an overview of everything going on with the network. The reports highlight any issues his team needs to investigate. For example, they were once alerted to an attempted brute force attack on their environment, which enabled them to respond very quickly. Accessing the data within FortiAnalyzer saved them a great deal of time they would otherwise have spent digging through log files in individual security solutions to discover the attack.

"We use FortiAnalyzer to see things like what ports are in use and what different users are doing," the IT manager says. "We can see everything down to what a particular user is clicking on or even what keywords they typed into Google searches. So, if a network blip happened at 2 o'clock yesterday from a particular source IP, we can use FortiAnalyzer to dig into the cause. This kind of search is easy because FortiAnalyzer enables us to filter out so many different factors. We could get there with the FortiGate log files, but it would take a long, long time."

In fact, he adds, the data from FortiAnalyzer is so helpful in investigations of network activity that the company's controls team requested an appliance of their own. "They wanted their own FortiAnalyzer, and now they use it to answer their controls questions," the IT manager says. "They used to call me every single morning to ask about the causes of certain network activities, and now they hardly ever reach out to me anymore. That lets me focus more on my day-to-day work."

Soon after deploying FortiAnalyzer, the team decided to roll out the FortiSIEM security information and event management solution to gain even more detailed information about security events. FortiSIEM consolidates data from a wide range of systems from a variety of different vendors.

Business Impact (cont.)

- Daily time savings for IT manager, as controls group utilizes their own FortiAnalyzer appliance
- 10–20 hours per week saved across IT team by eliminating manual log file reviews
- Hundreds of thousands of dollars a year in spending avoided, as enterprise SOC capabilities are available without doubling IT staff

Solutions

- FortiGate Next-Generation Firewall
- FortiSwitch
- FortiExtender
- FortiEDR
- FortiNAC
- FortiAuthenticator
- FortiToken
- FortiSandbox
- FortiDeceptor
- FortiAnalyzer
- FortiSIEM
- FortiManager

Services

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

"We put data into FortiSIEM from all our switches, all our domain controllers, all our firewalls, every system on our network that can help us log an event," the IT manager explains. "It holds 90 days of data, and if we ever want to go back and look at who or what attacked us, and from where, we can go into those SIEM logs and find out."

He adds that FortiSIEM has been particularly helpful in detecting unusual movements of corporate data. "Sometimes, people will start pulling data from SharePoint or will upload a lot of their personal files and folders," the IT manager says. "When an individual's data transfers exceed a certain volume, the SIEM sends me an alert. I can contact the person and ask what they are doing. A couple of times, this has enabled me to prevent employees who are leaving the company from stealing some pretty significant documents on their way out."

Enterprise-Quality Security for Hundreds of Thousands of Dollars Less

The IT manager leveraged Fortinet's FortiGuard SOC-as-a-Service (SOCaaS) as a final security backstop. Fortinet security operations center (SOC) analysts monitor the power company's FortiGate logs and alerts and investigate threats with notifications to the IT manager about anything he should know. From breaches and compromises to suspicious traffic hitting the firewalls, the SOCaaS notifies the IT manager and recommends actions he can take to remedy the situation.

> *"The logs collected by FortiAnalyzer are also reviewed by the FortiGuard SOC-as-a-Service ; we have 137 million logs that have been reviewed by the Fortinet SOC team. The alerting we get across all these platforms makes me comfortable that our networks are not getting compromised."*
>
> IT manager,
> Major Electric Power Station

The SOCaaS dashboard is easy to understand, and the power company's IT manager sees this as a crucial step in making sure he is immediately aware of any true threats his network faces. Better yet, for low-level issues, he can read the alerts in a report the next day without being awakened in the middle of the night.

"The logs represented by FortiAnalyzer are also reviewed by the SOC-as-a-Service; we have 137 million logs that have been reviewed by the SOC in the cloud," the IT manager says. "The alerting we get across the Fortinet Security Fabric makes me comfortable that our networks are not getting compromised."

He adds, "Implementing the Fortinet products lets me sleep at night. We have all the protection we would get from a full SOC department. But we can reach that same end goal without doubling the size of our staff."

All told, the IT team is saving 10 to 20 hours a week that they previously spent on log analysis, and they are avoiding spending the hundreds of thousands of dollars a year that would otherwise be necessary for the enterprise-level protection they have achieved through the Fortinet Security Fabric. Not only do they have time for more big projects to support the company's growth, but they can easily pass on knowledge of the security infrastructure to new staff as needed.

Sold on the Fortinet Security Fabric

To that end, the power station recently deployed FortiManager, which further increases efficiency for the IT team. Rather than updating each firewall individually, they can make a policy change once and then distribute it to all their FortiGate NGFWs through FortiManager.

"I will continue to add Fortinet solutions to my environment because of how well they play together, how efficient they can be centrally managed, and how safe they have made our networks," the IT manager says. And if he has a concern about the security infrastructure, he can turn to a single vendor rather than five or six, which streamlines resolution of any issues. By simplifying network and security management through FortiManager, Fortinet enables the power station's seven-person IT department to operate, support, and secure a critical-infrastructure network.

"The difference between our network security before Fortinet and our security now is night and day," the IT manager concludes. "I have a diagram on my wall of the Fortinet Security Fabric, and I have marked the solutions that we have." Anytime Fortinet comes out with a new product, "I plan on implementing it if it would help our business in any way."

FORTINET

www.fortinet.com