CASE STUDY

Fortinet Protects Widely Dispersed OT Equipment for Railroad Service Provider

Collaboration is crucial in railroad transit. One company's trains may run on tracks owned by another organization. "If company A's train, for example, needs to run on company B's track, it will cross over into company B's territory to do so," explains Jesse Fritz, network architect for Herzog Technologies, Inc. "Back-end management systems make this possible, handling messaging, signaling, and communication with the other company's railroad crossings and signals. These systems provide insights and control for the railroads."

Communication is key even for trains traveling their tracks. Crossing signals and track-switching mechanisms need to align with the engineers' expectations. Plus, railroads use an array of operational technology (OT) systems to monitor the performance of engines and other equipment. Keeping such data flowing is a key component of HTI's business. Trains moving down the tracks connect to base radio sites via radio frequency, and the base radio sites connect to the HTI corporate network.

Herzog, HTI's parent company, is the only organization in the world to build, operate, and maintain every aspect of railroad transportation. Over the past 50 years, Herzog has developed numerous innovations in railroad construction. The company owns railways and many trains. It also operates trains owned by other companies. Herzog performs maintenance on train equipment and rail lines, both its own and clients'.

The HTI division specializes in providing communication and technology services to support all of Herzog's various activities. "We are responsible for operating, managing, and maintaining the technology networks that support the railroad traffic," Fritz explains.

Security Is Mission-Critical in OT Environments

HTI develops custom railroad software, collects and manages GIS data, and monitors wayside signals and communications. It hosts train messaging, safety, and dispatch systems, both for other Herzog divisions and for external clients. In some cases, HTI integrates information from different organizations then sends the combined data back to the client systems. Across all these activities, security is top of mind.

"Through our own trains and the services we provide clients, we are responsible for moving 38 million people every year," Fritz says. "It would be devastating on multiple levels if any threat were able to impact, control, or manipulate trains, and it is HTI's responsibility to make sure that does not happen."

OT is Fritz's biggest security concern. The systems HTI hosts reside in two data centers, but the company also manages technologies spread through client dispatch centers and trackside base radio sites across the United States.

HERZOG

"Once we put in those first FortiGate firewalls, the move toward Fortinet grew rapidly. Everybody loved the visibility and that they did not have to dig into logs on the command line to get it. We got granular control quickly. Our executives were immediately impressed."

Jesse Fritz
Network Architect
Herzog Technologies, Inc.

Details

Customer: Herzog Technologies, Inc. (HTI)

Industry: Transportation

Location: Fort Worth, Texas

Business Impact

- Enhanced security and granular network control at a low cost
- Improved reliability of wide area network (WAN) connections
- 50% less staff required to manage widely dispersed network

Historically, Fritz explains, railroads built closed networks; there was no way for an outside attacker to hack into OT systems. But times have changed. "You cannot have a 100% closed network in which you remotely manage and maintain all that equipment," he says.

"Once you start centrally managing the equipment at railroad crossings and waystations, you have to extend security from the data center all the way into the field," he continues. "Our attack surface includes devices in shacks throughout the U.S. rail system, and it is my responsibility to protect those devices from threats." In addition, HTI needs to make information about clients' trains, tracks, and other assets available to those clients in real time. "The safe travel of both freight trains and tens of millions of passengers depends on the efficacy of our network security," Fritz adds.

Fortinet Sparks a Transformation

When Fritz joined the company four years ago, HTI's data centers were running security hardware that was approaching its end of life. The company's legacy virtual private network (VPN) solution was particularly unreliable. "I encouraged management to consider replacing the old security systems with Fortinet solutions," Fritz says. "Fortinet provides everything we need from a feature-set perspective. VPN was the gateway for us to see how Fortinet would perform in our environment."

HTI executives agreed to deploy a pair of FortiGate Next-Generation Firewalls (NGFWs) with FortiClient endpoint protection on internal systems that need to connect via VPN. For clients that access HTI-hosted systems via VPN, Fritz published railroad-specific VPN pages and then locked down access so that users could see only the specific applications they needed.

"Once we put in those first FortiGate firewalls, the move toward Fortinet grew rapidly," Fritz says. "Everybody loved the visibility they got into the VPN and that they did not have to dig into logs on the command line to get it. We got granular control quickly. Our executives were immediately impressed."

HTI worked with Fortinet strategic partner Liquid Networx to begin rolling out FortiGate NGFWs and FortiSwitch secure Ethernet switches throughout the HTI data centers. The FortiGuard Unified Threat Protection Bundle enhances the NGFWs' protections. The bundle includes intrusion prevention service, web security, content security, and data loss prevention functionality.

In some cases, HTI has been shifting client systems into its data center, so they benefit from this enhanced security. "We are moving whole railroads from other platforms to our data centers, so they will be behind the FortiGates," Fritz says. With the support of Liquid Networx, HTI has also been installing FortiGate NGFWs in clients' dispatch centers. This gives the dispatch centers a huge boost in security, as many previously had no security equipment outside their router. Throughout the HTI network, "The FortiGates act as security checkpoints that help us identify and block threats from reaching our equipment," he adds.

When HTI began managing FortiGate NGFWs in several network locations, Fritz activated Fortinet Secure SD-WAN. The software-defined wide area network (SD-WAN) solution has improved the reliability of HTI's network connections at a much lower cost than the company's legacy MPLS circuits. "Our railroad clients had been incurring outages with the MPLS circuits," Fritz says. "Their management teams were asking us to add more circuits. Because Fortinet Secure SD-WAN is included

Business Impact (cont.)

- 5x faster onboarding for new engineers saves on overhead cost
- Reduction in log analysis from hours to minutes

Solutions

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

Services

- FortiGuard Unified Threat Protection Bundle

"Our new network and security architecture is saving our clients money. More importantly, they have far better security on their network. Working with Fortinet and Liquid Networx gives Herzog Technologies a competitive advantage."

Jesse Fritz
Network Architect
Herzog Technologies, Inc.

with the FortiGate firewalls, we told clients we would replace their legacy security equipment with FortiGates and FortiSwitches and use Fortinet Secure SD-WAN for connectivity. The cost would be much lower even though we would be building redundancy and using technologies that are far easier to learn and manage."

Expanding the Reach of Security

Now that larger HTI locations are completing their transition to Fortinet, Fritz is eyeing the base radio sites spread across the country. With the help of Liquid Networx, HTI created a Fortinet Security Fabric platform template for those locations: A pair of desktop-model FortiGate NGFWs use Fortinet Secure SD-WAN to create IPsec tunnels into the appropriate dispatch center via an internet connection with a 5G/LTE cellular backup. FortiExtender supports the backup connection. Trains radio the sites with crucial information, and the sites pass that information on—very reliably, due to the redundancy—to HTI-hosted systems in the dispatch centers.

As an example of this approach in action, Fritz points to a specific railroad partner, a commuter railroad that relies on Fortinet solutions, end to end, for both networking and security. "Liquid Networx built us a template for the railroad," Fritz says. "I had a design in my head. They drew it up on paper, we worked together on a few changes, and they put together the configurations for us. They helped us roll out one test site, then we did the other 15 sites by ourselves, with a great degree of success."

Now, Fritz adds, "The whole railroad runs exclusively on Fortinet. Their dispatch centers in the field have pairs of FortiGates, as well as FortiSwitches and FortiExtenders. All their sites have the same models, and they all connect to the HTI network using Fortinet Secure SD-WAN. Each site has an internet connection and a dual-carrier cell, which are accessible to both FortiGates. So, each site has four tunnels to either of our data centers, and the SD-WAN manages that traffic."

He reports, "Without the help of Liquid Networx, the project would have required me to take on a month's prep work, which I just did not have time to do. Liquid Networx has the expertise to jump in when needed. That makes it possible for HTI to operate with a staff of three networking and security professionals, myself included."

Maintaining Staff Size and Saving Time

The FortiManager centralized management and FortiAnalyzer centralized logging and analytics solutions simplify security administration, reducing the time Fritz's team must dedicate to the task. FortiManager enables the centrally located staff to manage HTI's widely dispersed NGFWs in a streamlined and intuitive way.

"Although HTI is growing, we will not need another engineer for a while," Fritz says. "If we were on a different platform or had a mix and match of best-of-breed products, we would have to grow our engineering staff substantially. We can do as much, or more, with 50% less staff than if we were stuck with one of Fortinet's competitors."

Better yet, "I do not have to break the bank trying to find a bunch of highly specialized experts who have sat through yearlong classes to learn a competitor's solution," Fritz says. "I just have to find younger engineers who are hungry to learn, and they can get trained on Fortinet five times faster than on other security solutions. Learning Fortinet is faster, better, and easier."

HTI has set up administrative domains (ADOMs) in FortiManager to give clients access to their systems. "If a railroad has an internal engineer who understands security and networking, or if they use a different provider for some service, we can give them access to view or even co-manage systems we host. The ADOM enables us to control that access: We can give an individual granular access to specific resources without giving them access to everything. Or we can make their access read-only."

FortiAnalyzer enables Fritz and his team to understand what happens anytime quickly HTI experiences an issue. The consolidated interface of FortiAnalyzer offers a unified, real-time view of data across the Fortinet Security Fabric and other integrated systems, all from a singular dashboard. "If someone does something in the network that ends up stopping trains, I get a call asking, 'Who was in these systems at this time?'" he says. "In the past, it took me a couple of hours to parse through logs and figure out what was really going on with the systems in question. Now, with FortiAnalyzer, it takes me five minutes to answer those questions. That is a nearly 100% time savings."

Historically, Fritz says, visibility into security events was a pain point for HTI. Today, he says, "We can see all the IPs the FortiGates have blocked and where they are coming from. Our security is greatly improved, and we have happy executives—all the way up to our CEO. They get information fast, and they see that we are being very responsible with how we are spending money."

HTI is starting to roll out FortiAP access points, which Fritz describes as “a no-brainer for our office environments.” He adds, “The legacy wireless network cost just as much but was far less flexible. It also was an independent system from a different vendor, which meant more to manage. Having FortiAPs means everything we have to manage is on one platform.”

Next, the company is looking at implementing zero-trust network access. “I know the direction I want to go, and we are working with Liquid Networx to set that in motion,” Fritz says. “They will put together some use cases for us and present them to our executive team so that we can determine how to move forward.”

Ultimately, Fritz concludes, HTI’s relationship with Fortinet comes down to better service for the company’s railroad clients. “Our new network and security architecture is saving our clients’ money,” he says. “More important, they have far better security and granular control of all the traffic on their network. Working with Fortinet and Liquid Networx gives Herzog Technologies a competitive advantage.”

October 7, 2024 11:51 PM / 2912603-0-0-EN