CASE STUDY

Zero-Trust Security from Fortinet Enables IT/OT Convergence for Chinese Automotive Manufacturer

Around the world, manufacturers are benefiting from unprecedented operational efficiencies from the convergence of information technology (IT) and operational technology (OT). However, as organizations become increasingly connected, the expanding network edge has also led to a significant increase in cyberattacks on mission-critical infrastructure. This is of considerable concern to manufacturers, as many of the industrial control systems (ICS) in place today have not been designed with security as top of mind. As digital innovation in manufacturing gathers pace, OT security has become a top priority.

The Complexities of Securing OT in the Automotive Industry

OT security presents a particular set of challenges for companies in China's fast-growing automotive sector. Vehicle manufacturing plants are among the most heavily automated in any sector, with large-scale deployments of robots, and automated operations covering everything from welding and painting to assembly.

With the forces of Industry 4.0 driving change in the sector, automotive plants are becoming increasingly connected. Robots, control systems, and smart sensors, for example, are being tied together in a single smart system to drive output and productivity gains. At the enterprise layer, businesses are bringing Enterprise Resource Planning (ERP) and Manufacturing Execution System (MES) capabilities together to further optimize production. However, doing so increases the complexity of the network and exposes the OT network, which has traditionally been air gapped, to cyberattacks.

Exacerbating this risk is the fact that operations staff have not required in-depth knowledge or skill sets in cybersecurity. Even in an air-gapped environment, it therefore remains common to see staff or equipment vendors using external flash drives or laptops to upload contents to a controller during maintenance, leaving systems open to attacks.

Preparing OT for External Threats

It is in this context that a major China-based automotive manufacturer set about unifying its operations across its value chain with the aim of optimizing productivity and efficiency. With a widely dispersed set of production plants, offices, R&D facilities, and marketing hubs across China and other countries, the company faced a significant security challenge.

The manufacturer realized that it needed to upgrade its security infrastructure to ensure the security of its converged environment. It had used industrial firewalls to protect the network at the level of Internet Protocol (IP) and Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) port filtering. However, some of its industrial controllers are supported by legacy operating systems such as Windows XP and 7 as well as outdated firmware. These lack the necessary security features for proper zoning and protection, required to defend against advanced cyber threats.

With its IT/OT convergence ramping up, the manufacturer needed to urgently upgrade its OT security. This meant ensuring that the OT network, which once had only to be protected against industrial control threats, also had to be ready to deal with threat types common to enterprise networks.

Details

Customer: Automotive Manufacturer

Industry: SCADA/Manufacturing

Location: China

Business Impact

- Robust zoning and segmentation to stop malware spreading across networks, enabling the convergence of OT and IT
- Zero-trust security framework that enables safe manufacturing innovation comprised of increasing automation
- Monitoring of the full OT/IT network and assets, enabling anomaly detection at deeper OT layers

Solutions

- FortiGate Next-Generation Firewall
- FortiManager
- FortiSwitch
- FortiAnalyzer

The OT network also needed to be secured so it could not be used as an access point to the wider enterprise network, particularly when it comes to the operations platform used to integrate industrial communication protocols. The platform was custom-built before security became such an important consideration. The manufacturer therefore needed to ensure proper network zoning and segmentation to segregate physical assets and functional areas. Otherwise, once one device or production line became infected, the threat could potentially spread across the entire global network.

Collaborating on the Right Security Posture

In addition to its technology challenge, the company also needed to ensure that its operations staff had the skills and knowledge to help protect the organization. With ransomware attacks on OT networks increasing worldwide, this was a key priority.

Fortunately, the manufacturer's enterprise IT team was highly skilled and was able to collaborate with their colleagues in OT to ensure best practices were embedded early in the transformation, and to provide advice on the best systems to invest in. The company previously deployed a range of Fortinet solutions in the enterprise network, and due to their good experience of the technology, the IT security team was quick to recommend them to their OT team members.

In 2020, the company's OT leadership arranged a benchmark test of Fortinet's security solutions against market alternatives to identify which provided the best cost-to-performance ratio. Tests included firewall application identification and virus attack detection. In a test that used a virus sample provided by a third party, Fortinet's detection rate was above 80% out of the box and reached 95% when optimized. The detection rate for competing products, on the other hand, was just 20%. This huge capability gap meant that Fortinet was chosen as the manufacturer's preferred security partner.

Securing the Production Network with Fortinet

Today, the automotive manufacturer protects its production network with FortiGate Next-Generation Firewalls (NGFWs), FortiSwitch, FortiManager, and FortiAnalyzer. Fortinet's solution enables microsegmentation and traffic control detection, strengthening the company's ability to identify and control unknown threats, while also enhancing its incident response to ensure the timely reporting of security breaches. This raises the OT security benchmark, thereby enabling the digital innovations so crucial in the automotive manufacturing industry.

Through microsegmentation, the automotive manufacturer is embracing a zero-trust security framework. Leveraging the FortiGate NGFWs, the company has accomplished horizontal isolation at the top layer of its production network and across multiple plants. Meanwhile, its vertical segmentation isolates the IT/OT network boundary within the plant. In this architecture, even if an industrial control system (ICS) or application system is infected by malware, the threat can be quickly contained at the device or application level, preventing it from spreading across the network.

The company's new OT security infrastructure provides a clear demarcation of the whole network across its office locations, ICS, mobile devices, and servers. In addition, Fortinet's support of a wide range of industrial communication protocols allows for the monitoring of the full OT/IT network and assets through active inquiry and passive traffic functions, enabling anomaly detection at deeper OT layers for a stronger security posture.

April 6, 2022 3:48 AM
1542816-0-0-EN