

CASE STUDY

Brazilian Plastic Products Manufacturer Improves Safety and Availability Through IT/OT Security Integration

Fortlev is Brazil's leading manufacturer of water tanks and polyethylene tanks for water storage, as well as a leading manufacturer of PVC pipes and fittings. Founded in the state of Espírito Santo in 1989, the company is the country's leader in water storage solutions.

With a diversified portfolio, today Fortlev also offers accessories that help in the installation of reservoirs, tiles, and electrical accessories. The company has eight factories operating 24 hours a day, 7 days a week, with more than 1,700 employees.

Transforming To Meet Business Needs

Fortlev began using Fortinet products in 2015. At that time, the company was looking for a network security solution to support its nationwide operations, and the results derived from Fortinet FortiGate Next-Generation Firewalls (NGFWs) were optimal.

After a significant growth in its operations in recent years, Fortlev wanted to take advantage of Fortinet's capabilities to migrate and integrate the security platform for both its information technology (IT) and operational technology (OT) networks. The company intended to create a comprehensive environment with high availability, optimal performance, and security.

"We needed to redesign our network with a strong focus on availability and security, besides looking for the latest technology to support our operation," says Felipe Pinto Gomes, infrastructure and security coordinator at Fortlev. "We realized that Fortinet solutions met our needs."

With the advice and support of Brasiline, Fortinet's local partner, Fortlev performed an alignment and planning process aiming for a seamless and secure IT/OT integration. Its priorities were clear: focus on security, follow market trends, and be sure that it could react quickly in case of any network problem.

Availability and Security for a Converged Network Infrastructure

Availability and security were crucial for Fortlev's modernization, considering its OT security needs for the eight factories across Brazil. Its factories needed a cutting-edge technology to guarantee that all machines, sensors, and equipment related to its operation could be up and running 24/7.

"We wanted to extend all existing security capabilities we had in our IT environment to the industrial automation platform to have greater control and keep the OT environment free from threats", mentions Pinto Gomes. In response, the company deployed the Fortinet Security Fabric platform in all its factories, based on FortiGate Network Firewalls.

**FORTLEV**

"Today, with Fortinet, we have centralized management that allows us to configure and manage the IT/OT infrastructure from one place. This also means a more homogeneous environment when it comes to deploying updates and rules, which means a more transparent experience for users."

- Felipe Pinto Gomes, Infrastructure and Security Coordinator, Fortlev

Details

Customer: Fortlev

Industry: Manufacturing

Location: Brazil

Business Impact

- High availability for converged IT and OT networks
- 99% network availability to support operations in eight factories

The company has two networks that operate separately within the firewalls: one for the IT area and another that integrates the OT environment, which is directly related to its operations. With the Fortinet Security Fabric solution, Fortlev gained complete control of network traffic. The information coming from the outside is processed according to the rules established in the security platform to avoid any breach. In this way, it is possible for the company to provide greater security measures in the most critical areas of its business. “This helps us to have greater control and keep the infrastructure free of threats, with defined policies that allow us to see, understand, and validate everything that accesses the network,” adds Pinto Gomes.

Furthermore, the NFGWs enabled the deployment of the FortiGate Secure SD-WAN solution in Fortlev’s factories—previously connected via multiprotocol label switching (MPLS) and virtual private network (VPN) links. If one of the internet links fails, the system automatically switches in sub-second to another of the three available links. Thus, the company has reached its target of maintaining over 99% network availability, providing quality service to servers, Wi-Fi networks, and more than 750 computers connected from the eight factories throughout the country.

With the FortiGate Secure SD-WAN networking and security solution, Fortlev can now properly load balance the communication links. Today, the company has not experienced any incidents lasting more than five minutes for almost a year. “We can react in a short time and, if there are failures, have the system up and running very quickly. This level of automation has totally changed the user experience—we have had considerable benefits,” says Pinto Gomes.

Fortlev also added another complementary solution within the Fortinet Security Fabric. With FortiAnalyzer, the company constantly monitors the network and is aware of risks and threats that may affect IT/OT network performance. This solution also improves the monitoring and reporting of security threats, increasing the company’s capacity to process and analyze possible attacks. “In addition to visibility and security, we were looking for a system that was much more automated and offered intelligence to mitigate threats,” Pinto Gomes points out.

Furthermore, the pandemic caused a portion of Fortlev’s workforce to operate remotely—a movement that presented additional challenges in security and stability. FortiClient Enterprise Management Server (EMS) synergized perfectly with Fortlev’s goals, due to its inclusion of Zero Trust Network Access (ZTNA) features. This provided great flexibility to reliably deploy and manage FortiClient endpoint security policies on remote employee devices.

“Today, with Fortinet, we have centralized management that allows us to configure and manage the IT/OT infrastructure from one place,” Pinto Gomes states. “Fortinet allows me to have greater visibility and fewer rules. Ultimately, this also means a more homogeneous environment when it comes to deploying updates and rules, which means a more transparent experience for users.”

Business Impact (contd.)

- Centralized visibility and control enabling unified policies and rules management
- Proactive network monitoring to prevent threats and attacks

Solutions

- FortiGate Network Firewall
- FortiGate Secure SD-WAN
- FortiClient
- FortiAnalyzer

“We needed to redesign our network with a strong focus on availability and security, besides looking for the latest technology to support our operation. We realized that Fortinet solutions met our needs.”

- Felipe Pinto Gomes, Infrastructure and Security Coordinator, Fortlev