FÖRTINET.

Heavy Equipment Manufacturer Secures 100-Year Legacy With Global IT and OT Protection

Founded over a century ago as an independent manufacturer of farming equipment, Galucho has grown to become an internationally recognized brand in the development of efficient solutions not just for agriculture, but also in the sectors of transport equipment and the environment.

Still a privately held company, Galucho now has production facilities in Portugal, in Sintra, in Albergaria-a-Velha (Aveiro) and in partnership with local companies in Algeria. Building on its strong foundations of technological innovation, efficiency, and engineering excellence, Galucho has become a leading force in the worldwide market for efficient solutions in all three of its core business sectors.

Operational Efficiency Through Network Resilience and IT/OT Integration

Over the years, Galucho expanded its use of IT across every stage of the product lifecycle, from design and development to full-scale production. As it did so, the company realized that its IT infrastructure would need to be remodeled to support the evolving needs of the business.

With around 50% of its critical business applications and services migrating to the cloud and a growing need to integrate its operational technology (OT) environment with the IT network, Galucho needed a secure, resilient solution that could scale and adapt to its changing requirements without introducing even more complexity.

As a manufacturer of large, industrial-scale equipment, the network and its precious cargo of data and services needed to be instantly available across the entire operations base—a large production facility comprising both indoor and outdoor areas, exposed to a wide range of environmental conditions.

For performance and security reasons, the network also had to be logically divided into separate zones. This would keep administrative IT traffic separate from the various OT domains of the production units and their industrial control systems, while still allowing for overall visibility and control of the entire infrastructure.

Improved Visibility and Asset Control Through the Fortinet Security Fabric

"We had a legacy switching network with an outdated Wi-Fi overlay and an added security layer that was no longer adequate to protect our assets," explains Miguel Borges, IT Director for Galucho. "What we needed was something more stable and scalable, with security integrated at its core."

After a thorough evaluation of various competing solutions, Galucho chose Fortinet. "The Fortinet network firewalls, switches, and Wi-Fi access points performed really well and met all our technical requirements," Borges confirms. "But more importantly, they all work together under a common management and security umbrella, giving us complete visibility and control over the whole infrastructure."

At the core of Galucho's new secure networking solution is the FortiGate Next-Generation Firewall (NGFW). In addition to its robust and comprehensive range of advanced threat protection capabilities, FortiGate can identify thousands of traffic types, including many of the proprietary protocols used in OT environments. Furthermore, with its custom-designed security processor unit (SPU), the FortiGate NGFW can accomplish all of this additional security processing without compromising throughput or latency—even when traffic is SSL-encrypted.

GALUCHO

> *"We had a legacy switching network with an outdated Wi-Fi overlay and an added security layer that was no longer adequate to protect our assets. What we needed was something more stable and scalable, with security integrated at its core."*
>
> – Miguel Borges,
>   IT Director, Galucho

Details

Customer: Galucho

Industry: Manufacturing

Location: Portugal

Business Impact

- Better protection of manufacturing and customer data distributed across factories in several countries

- Secure wireless communication within production facilities and between production and management parts of the business

The "management and security umbrella" Borges referred to is made possible by a common security operating system—FortiOS—than underpins all Fortinet Security Fabric solutions. Recent enhancements to FortiOS enable Galucho's IT team to see all their OT network assets in FortiManager, arranged in topologies prescribed by the Purdue model (a reference architecture for security segmentation in ICS networks). In the same interface, IT staff can also monitor OT traffic flows and create new policies.

Enterprise Zone Secured With Fortinet LAN Edge Solution and More

On the enterprise (IT) side of the network, Galucho welcomed the Fortinet LAN Edge approach of integrating FortiSwitch Ethernet switches and FortiAP access points into the security architecture. This approach reduces complexity for the IT staff, enhances security throughout the network, and helps to contain operational costs.

The FortiSwitch and FortiAP solutions are available in a wide range of speeds, port densities, and form factors, including ruggedized versions that operate in environments with wider temperature variations. Galucho leveraged the variety of Fortinet LAN Edge offerings to provide secure, reliable access across all of its production facilities.

For enhanced endpoint protection—specifically for wireless access—Galucho deployed the FortiClient Fabric Agent, extending the Fortinet Security Fabric to the company's mobile client devices. This gives on-the-go and remote users more secure access to network resources, while providing the IT team with a unified view of endpoints for better tracking, compliance enforcement, and reporting.

Policy enforcement is also easier now because FortiSwitch and FortiAP, are administered as logical extensions of the FortiGate NGFW through the same management interface. So, when IT staff defines an access policy, FortiGate NGFWs across the organization automatically apply it to both wired and wireless access.

Moreover, the integration of FortiGate, FortiSwitch, FortiAP, and FortiManager within the Fortinet Security Fabric enables a cybersecurity mesh architecture that can greatly improve Galucho's security posture. With advanced automated threat mitigation, as well as proactive threat detection and correlation, the Fortinet Security Fabric shortens response time and reduces security risks.

To further protect its enterprise zone, Galucho deployed FortiMail, which shields email users from both volume-based and targeted attacks. FortiMail also helps Galucho prevent the loss of sensitive data and maintain compliance with regulations.

As with all Fortinet solution deployments, external threat intelligence is provided by FortiGuard Labs, which collates and processes the data from hundreds of thousands of sensors and over 200 global partners around the world. FortiGuard Labs leverages machine learning and other types of artificial intelligence (AI) to identify both known and previously unknown threats.

"The results beat our expectations," Borges says. "Not only did the new infrastructure fulfill its objectives in terms of better security, stability, and control, but it has also drastically reduced the time and resources spent managing it, which means we can now be more proactive in supporting the business."

Business Impact (contd.)

- Enhanced ability to monitor compliance with data privacy regulations

- Greater IT effectiveness and reduced burden on the staff through integrated network and security operations

Solutions

- FortiGate Next-Generation Firewall

- FortiSwitch

- FortiAP

- FortiMail

- FortiClient

- FortiManager

"The Fortinet network firewalls, switches, and Wi-Fi access points performed really well and met all our technical requirements. But more importantly, they all work together under a common management and security umbrella, giving us complete visibility and control over the whole infrastructure."

– Miguel Borges,
IT Director, Galucho

FEERTINET