CASE STUDY

Green Energy Provider Converges OT and IT Security through Platform Approach

Rising in 2016 from the merger of South Tyrol's two largest energy companies, SEL and AEW, Alperia has grown to become a major driving force for change, raising awareness and engaging collaborators in the areas of environmental sustainability and the mitigation of climate change through clean, renewable energy.

Through a combination of targeted community investments and technological innovation programs, Alperia is actively working to reduce environmental impact, not just for the company itself, but for the whole region.

Operating 34 hydroelectric power stations, seven district heating plants, an electricity grid spanning 9,200 Km, and 1,000 electric vehicle charging points, Alperia serves over 370,000 customers and aims to be fully carbon neutral by 2024.

Ensuring Safe, Reliable, and Continuous Energy Services

To ensure safe, reliable, and continuous critical services, Alperia securely collects and processes operational technology (OT) data from multiple types of industrial control system (ICS) and Internet-of-Things (IoT) devices located in 200 sites across the southern Alps.

This OT network uses a combination of proprietary fiber-optic cabling and secure VPN (for sites beyond the reach of fiber-optics), which had previously been managed by multiple external service providers.

To increase the overall security, control, and visibility of its critical services and to simplify the regulatory compliance process, Alperia decided to bring its entire management infrastructure in-house.

Step 1: A Secure, Unified OT Infrastructure

Alperia's first step was to ensure secure segmentation of OT traffic based on criteria such as location, device type, and the ICS/SCADA protocols in use. This was in accordance with the ICS security best practice of defining distinct zones, boundaries, and conduits.

Alperia needed a resilient, ruggedized solution with powerful, centralized management, to ensure secure connectivity across this large and diverse network, especially for unmanned sites operating under potentially harsh environmental conditions.

Furthermore, as a multi-utility services provider operating within the EU, Alperia required comprehensive reporting and analytics to help ensure compliance with industry regulations.

After evaluating several potential solutions, Alperia chose, with the support of the partner KONVERTO, FortiGate Rugged Next-Generation Firewalls (NGFWs) for

alperia

"The FortiGate has advanced multi-level protection and specific ICS/SCADA-aware functionality and provides all the security, resilience, and performance we needed. And for some of our hydroelectric plants, the compact FortiGate Rugged with its support for redundant power supplies (including 110V supply) and its ability to withstand atmospheric contaminant, made it one of only very few products able to operate reliably in that environment."

Sandro Moretti
Head of Networking and Infrastructure
Alperia

Details

Customer: Alperia

Industry: Power and Utilities

Location: South Tyrol, Italy

Partner: KONVERTO

the OT segmentation, with FortiManager and FortiAnalyzer providing centralized management, logging, analytics, and reporting.

"The FortiGate has advanced multi-level protection and specific ICS/SCADA-aware functionality and provides all the security, resilience, and performance we needed," explains Sandro Moretti, Head of Networking and Infrastructure at Alperia. "For some of our hydroelectric plants, the compact FortiGate Rugged supports our redundant power supplies (including 110V supply), and it has the ability to withstand atmospheric contaminants, making it one of only very few products actually able to operate reliably in that environment."

The FortiGate can identify and secure most of the common ICS/SCADA protocols through deep packet inspection (DPI) of the network traffic. Leveraging the FortiGate Rugged intrusion prevention system (IPS), matching malicious signatures for OT malware or applications are blocked and the network protected. Additionally, FortiGuard Labs threat intelligence support of Fortinet devices ensures real-time security through continually updated signatures.

Industrial network security is enabled through the configuration of security policies in which multiple services, such as IPS, AV, and application control, can be mapped to each protocol.

In parallel with this specific protocol support, additional vulnerability protection is provided for applications and devices from the major ICS manufacturers, through a complementary set of signatures and incorporated into the Rugged FortiGate through integrations as part of the broad OT Tech Alliance program.

"The FortiGate is well suited to our needs," comments Stefano Lodola, Senior Security Specialist for Alperia. "And with FortiManager zero-touch deployment, we were able to create configuration templates that let us deploy to remote sites without having to send out security specialists each time. This made the whole process much faster and less prone to error."

Step 2: Integration of Cloud and Hybrid Services

Following the success of the OT network deployment, Alperia began a process of accelerated digital transformation, deploying new cloud services through AWS, and starting to integrate the IT and OT environments into a single converged infrastructure.

The obvious cost efficiency and usability benefits of cloud and IT/OT convergence had to be weighed against potential increases in exposure to cyberattacks.

One of the ways that Fortinet solutions address the security challenges is through the Fortinet Security Fabric, a consolidated cybersecurity platform. The Fortinet Security Fabric covers the expanding digital attack surface of hybrid and converged OT/IT networks, enabling adaptive, self-healing security and automated protection for all users, devices, data, and applications.

"Unifying deployment and management across OT, IT, and cloud environments through the Fortinet Hybrid Mesh Firewall approach," explains Moretti, "and by signing a three-year enterprise agreement with Fortinet, we now have unlimited access to the full range of functionality. This simplifies the ongoing administration of our expanding Fortinet infrastructure and reduces our operating costs."

To handle the increased throughput and resilience required at the main branch offices, the FortiGate NGFWs were deployed in a high-availability cluster configuration.

Business Impact

- Enhanced security through secure zoning of the OT network
- Increased overall visibility and simplified administration through a hybrid mesh firewall approach
- Reduced operating expenses while improving the security, reliability, and efficiency of the network

Solutions

- FortiGate Next-Generation Firewall
- FortiManager
- FortiAnalyzer

"The FortiGate is well suited to our needs," comments Stefano Lodola, Senior Security Specialist for Alperia. "And with FortiManager zero-touch deployment, we were able to create configuration templates that let us deploy to remote sites without having to send out security specialists each time. This made the whole process much faster and less prone to error."

Stefano Lodola
Senior Security Specialist
Alperia

“Consolidating management and audit trails across all environments, including cloud, has been critical to our overall security,” adds Lodola, “especially since, in addition to our own staff, we are improving secure OT access to multiple third-party contractors. Without the integration between FortiOS, FortiManager, and FortiAnalyzer, this would be very hard to do in a secure way.”

Next Steps

Moretti and the team are now focusing on developing and protecting new cloud services, such as a web portal for consolidating and simplifying external support of programmable logic controllers (PLCs) and other industrial equipment.

To help secure such services from the full range of potential cyberattacks, the team has started evaluating additional solutions such as Fortinet’s web application firewall FortiWeb, and FortiSandbox.

The threat intelligence is provided by FortiGuard Labs, which collates and processes the data from millions of sensors and hundreds of global partners worldwide. Leveraging machine learning and artificial intelligence (AI), FortiGuard Labs can identify and characterize known and previously unknown threats.

FortiGuard Security Services also natively integrates with the Fortinet Security Fabric, ensuring that as the threat landscape changes, the technologies deployed in the Alperia network are continuously and automatically updated.

“As we expand our use of Fortinet products, the true value of the Fortinet Security Fabric is becoming ever more apparent,” adds Moretti. “Each individual solution does its job well, but when they come together, you end up with something even more powerful and intelligent than the sum of its parts.”

August 23, 2023 3:51 AM

123456-0-0-EN