CASE STUDY

Portuguese Energy Supplier Streamlines Operations with the Fortinet Security Fabric Platform and SOCaaS

Founded in 1930, Cooperativa Eléctrica do Vale D'Este is a nonprofit, limited liability cooperative society dedicated to the distribution and trade of low-voltage electricity across the municipalities of Famalicão and Barcelos in northern Portugal.

Covering an area of 6,000 hectares, CEVE serves 14 rural parishes, providing a diverse range of services to both businesses and consumers.

CEVE embarked on an ambitious modernization program with significant investment in new digital technologies and infrastructure, expanding the provision of "smart grid" services throughout the region to enhance the quality of these services and improve the efficiency of their operations.

This digital transformation, which provides CEVE with new tools to enhance and streamline its network operation and management, has also created new challenges, especially regarding cybersecurity. In 2023, this led to the creation of a dedicated cybersecurity unit and the appointment of Joel Queirós as CISO.

New Challenges, New Opportunities

In addition to the demands of digital transformation, the European energy sector has recently faced new regulatory reforms and a rapid increase in demand for renewable energy. At the same time, military conflict in Eastern Europe has disrupted supply, increasing price volatility and forcing providers to diversify their energy sources. Rapid advances in artificial intelligence (AI) have created new challenges, including accelerating the volume and sophistication of cyberattacks targeting operational technology (OT) environments like CEVE's.

For CEVE's newly appointed CISO, Joel Queirós, and his relatively small team of networking and security specialists, the priority was establishing broad, centralized visibility and control of the network and its security.

"As the size and complexity of our network and systems grew, performance had dropped, and overall visibility and control had been reduced as administration split between multiple independent systems, each with its own management console," explains Queirós. "This made it harder to detect and identify potential issues such as cyberattacks, which threatened business continuity and hindered compliance with new regulations such as NIS2."

The company's main data center had multiple redundancy levels and was replicated at a private cloud provider in Porto. However, with only limited space and access control and no fire suppression system, it urgently needed renovation, presenting Queirós with a unique opportunity to refresh the network and security infrastructure simultaneously.

CEVE
COOPERATIVA ELÉCTRICA DO VALE D'ESTE

"Although the other solutions had broadly similar features and functionality, only Fortinet offered the deep integration and ease of management we needed. Not only did the FortiSwitch high-performance LAN switch and FortiAP wireless access points come under the same management umbrella as the FortiGate network firewalls, but our existing endpoints and endpoint management system [FortiClient EMS] and cloud email security [FortiMail] also became part of the same unified security architecture, the Fortinet Security Fabric."

Joel Queirós,
IT Manager/CISO

Details

Customer: Cooperativa Eléctrica do Vale D'Este (CEVE)

Industry: Power and Utilities

Location: Portugal

Partner: Divultec

The Need for Consolidation and Convergence

To maximize the efficiency and effectiveness of his team, Joel Queirós knew they would need a converged networking and security solution with a single centralized management console as well as a high degree of intelligent automation that would enable them to offload various labor-intensive tasks such as log management and compliance reporting. This could also eliminate the need to manually replicate rules and correlate events across multiple devices, allowing for a more straightforward unified security posture to significantly accelerate threat detection and response.

With these goals in mind, CEVE evaluated three potential vendors, including Fortinet.

The Advantage of the Fortinet Security Fabric Approach

“Although the other solutions had broadly similar features and functionality,” recalls Queirós, “only Fortinet offered the deep integration and ease of management we needed. Not only did the FortiSwitch high-performance LAN switch and FortiAP wireless access points come under the same management umbrella as the FortiGate network firewalls, but our existing endpoints and endpoint management system [FortiClient EMS] and cloud email security [FortiMail] also became part of the same unified security architecture, the Fortinet Security Fabric.”

The new data center security architecture consists of two firewall clusters, each comprising two FortiGate Next-Generation Firewalls (NGFWs) configured in high availability (HA) mode. One cluster provides next-generation perimeter security, while the other segments the internal network into around 10 separate VLANs. This segmentation increases security and performance by isolating CEVE’s traffic into separate broadcast domains and preventing the lateral spread of cyberattacks that might breach perimeter security.

“We previously had some basic internal network segmentation,” adds Queirós, “ but the FortiGate network firewalls give us much more control. For example, we can now limit access on an individual user basis and very quickly apply that to multiple switches and APs.”

The data center’s servers and endpoints are connected through a combination of FortiSwitch Ethernet switches and FortiAP wireless access points, which are all managed as logical extensions of the FortiGate NGFWs. Endpoints are further protected through a combination of FortiClient and FortiEDR endpoint detection and response.

In addition to providing tracking, awareness, compliance enforcement, and reporting for CEVE’s endpoints, FortiClient also provides key telemetry to the Fortinet Security Fabric. CEVE also deployed FortiAnalyzer, Fortinet’s unified data lake and automation platform for visibility, control, and SOC automation to provide the necessary network analytics across the network. This helps identify threats and mitigate risks before breaches can occur.

“In the past, filtering logs, correlating events, and creating the necessary reports was a major drain on our resources,” recalls Queirós. “Now, with the help of FortiAnalyzer playbooks, many such tasks are automated, saving a huge amount of time.”

Business Impact

- Increased overall visibility and control of the entire networking and security infrastructure
- Simplified operations and NIS2 compliance through convergence, automation, and managed services
- Strengthened overall security posture and accelerated detection and response capabilities
- Enhanced customer experience and trust through increased network security, performance, and resilience

Solutions

- FortiGate Next-Generation Firewall
- FortiSwitch
- FortiAP
- FortiAnalyzer
- FortiEDR
- FortiMail
- FortiClient
- FortiAuthenticator
- FortiToken

Services

- FortiGuard SOC-as-a-Service
- FortiGuard Managed Detection and Response Service

To enhance VPN and remote server access security, CEVE deployed FortiAuthenticator, Fortinet's identity and access management solution, alongside FortiToken Mobile, its two-factor authentication (2FA) solution. This integration provided CEVE with a centralized, scalable enterprise solution that strengthens user access security by enforcing robust 2FA, effectively safeguarding critical resources against credential-based attacks.

Adding 24×7 Security Event Monitoring, Detection, and Remediation Advice

With its new Fortinet security architecture, CEVE had better visibility and control of the network than ever before. However, with only a small team, providing the 24×7 security operations coverage required of a critical infrastructure services provider would still be a challenge.

Rather than expand the team, Queirós opted for FortiGuard Security Operations Center-as-a-Service (SOCaaS) combined with FortiGuard Managed Detection and Response (MDR) Service, which provides 24×7 continuous alert monitoring and incident management.

SOCaaS investigates threats identified by FortiEDR or other sources in collaboration with the incident response team and, where deeper endpoint incident analysis is required, with the MDR team. During the investigation process, the SOCaaS team will assist the MDR team and the customer in providing any additional information, such as reports and logs.

With both fully customizable and out-of-the-box reporting as well as 24×7 access to the cybersecurity experts and resources of FortiGuard Labs, these FortiGuard managed services provide CEVE with the peace of mind that no matter how great the challenge, they will have the SOC resources required to respond quickly and efficiently, limiting their exposure to risk and ensuring compliance with the necessary regulations.

Looking Ahead

Freed from many of their former manual, labor-intensive administration tasks, Queirós and the team are now focused on optimizing and streamlining existing security operations. They are also starting to evaluate how best to support and secure the migration of key applications and services to the cloud.

"Replacing the entire network and security infrastructure for an operational data center such as ours without disrupting critical services is not a trivial task," comments Queirós, "but with the help of Fortinet and our local partner, we completed the whole project in about three months and without a single incident. This has given us great confidence in our relationship with Fortinet and the technology, vision, and expertise they bring to the table."

"We previously had some basic internal network segmentation, but the FortiGate network firewalls give us much more control. For example, we can now limit access on an individual user basis and very quickly apply that to multiple switches and APs."

Joel Queirós,
IT Manager/CISO

"In the past, filtering logs, correlating events, and creating the necessary reports was a major drain on our resources. Now, with the help of FortiAnalyzer playbooks, many such tasks are automated, saving a huge amount of time."

Joel Queirós,
IT Manager/CISO

"Replacing the entire network and security infrastructure for an operational data center such as ours without disrupting critical services is not a trivial task, but with the help of Fortinet and our local partner, we completed the whole deployment in three months without a single incident. This has given us great confidence in our relationship with Fortinet and the technology, vision, and expertise they bring to the table."

Joel Queirós,
IT Manager/CISO