FORTINET

CASE STUDY

Spanish Renewable Energy Company Sets New Industry Benchmark for Secure OT/IT Convergence in the Cloud

Founded 20 years ago as a wind and solar energy developer, Capital Energy has built a presence along the entire renewable energy generation value chain from development, where the company has a consolidated position, to construction, production, storage, operation, and supply. Capital Energy has started moving into adjacent businesses from the company's solid base in renewables, building key competitive advantages. These advantages include producing green hydrogen and its derivatives, promoting and operating sustainable data centers, and deploying telecommunications capabilities associated with its electricity footprint.

With 16 offices and wind and solar projects in more than 1,000 municipal districts across Spain and Portugal, Capital Energy's goal is to bring value to all stakeholders all along its ecosystem and business lines.

Adapting to Change through Digital Innovation

With increasing global acceptance of the climate crisis, new EU regulations, and the effects of recent international conflict, European energy markets are undergoing massive change.

Realizing early on that the key to adapting to such change lay in digital innovation, Capital Energy appointed Víctor Gimeno Granda as Chief Sustainability and Digital Officer and tasked him with building an agile, world-class infrastructure capable of supporting the company's ambitious goals for sustainable growth.

One of Granda's and the team's key challenges was finding a solution for managing the inherent complexity of Capital Energy's expanding, diverse, and distributed IT and OT environments. Not only did these comprise a wide variety of cabled and wireless equipment from many different manufacturers, but they also needed to be accessed by multiple third-party organizations such as maintenance and construction contractors.

Following the digitalization sustainability joint management approach, cybersecurity is a key part of Capital Energy's risk management model. More specifically, using next-generation firewalls (NGFWs) allows the company to minimize environmental, social, and governance (ESG) risks, such as operational interruptions; loss of confidential information, customer, employee, and other stakeholders' trust; and even environmental damages.

Another key factor was the company's ongoing commitment to innovation, which spawns a continually evolving roadmap of new projects, all with their specific demands on the infrastructure.

capital energy

"It was clear from the start that we would need a highly scalable, secure, and well-integrated network infrastructure with broad visibility and control. And the only way to sustainably achieve the scaling and flexibility required to support our ongoing innovation was to move to an increasingly cloud-based architecture through our strategic partnership with Google Cloud Platform and secured with Fortinet Security Fabric solutions."

Víctor Gimeno Granda
Chief Sustainability and Digital Officer
Capital Energy

Details

Customer: Capital Energy

Industry: Power and Utilities

Location: Spain

Number of Secure SD-WAN Locations: 16

"It was clear from the start that we would need a highly scalable, secure, and well-integrated network infrastructure with broad visibility and control," explains Granda. "And the only way to sustainably achieve the scaling and flexibility required to support our ongoing innovation was to move to an increasingly cloud-based architecture through our strategic partnership with Google Cloud Platform and secured with Fortinet Security Fabric solutions."

Secure and Resilient Interconnection of all Sites

The first priority was to fully secure all data to and from Capital Energy's large and distributed network of remote sites in the most efficient and reliable way, considering that an increasing volume of this data would be destined for the cloud.

To achieve this, Granda and the team opted for a software-defined wide area network (SD-WAN) architecture, in which relatively inexpensive broadband access at each site provides secure, private WAN access and local internet breakout for its evolving cloud-based services.

After thoroughly evaluating available options, Capital Energy chose the Fortinet SD-Branch solution. The integrated SD-WAN functionality of FortiGate Next-Generation Firewalls (NGFWs) provides WAN connectivity to Madrid and other offices while extending cybersecurity throughout the network access layer at the WAN edge.

FortiSwitch and FortiAP act as logical extensions to the FortiGate, providing connectivity for all Capital Energy's industrial control systems (ICS), including Industrial Internet of Things (IIoT), and other devices, such as remote terminal units (RTU), and programmable logic controllers (PLC) whether wired or wireless, with consistent access security policies.

In addition to its integrated SD-WAN functionality, the FortiGate NGFW can identify and police most of the common ICS/SCADA protocols to define zones and conduits following OT security best practices.

This is done through configuring 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.

"A key advantage of the Fortinet solution is its level of integration," explains Israel Devesa, CIO and CTO at Capital Energy. "Not only does it have all the capabilities we need, but they all work together seamlessly, something that is essential for building a manageable, converged infrastructure."

For increased endpoint protection and to consolidate remote access for staff and third-party contractors through a single cloud-based hub, Capital Energy selected FortiClient for its integrated support for zero-trust network access and two-factor authentication via FortiToken.

To extend the scalability and range of user identification methods beyond the inherent capabilities of FortiGate, FortiAuthenticator was added, running as a virtual machine (VM) in the cloud.

Internal segmentation of cloud entities, such as the various data lakes (repositories for business intelligence and compliance data) and new service deployment platforms was accomplished with additional FortiGate VMs.

Business Impact

- Defined new industry benchmark for secure OT/IT convergence in the cloud
- Increased access security through a cloud-based access hub for third-party contractors
- Enhanced OT data acquisition security through secure SD-WAN architecture
- Increased visibility and simplified administration with the Fortinet Security Fabric architecture

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiAP
- FortiClient
- FortiAuthenticator
- FortiToken
- FortiManager
- FortiAnalyzer
- FortiSIEM

"A key advantage of the Fortinet solution is its level of integration. Not only does it have all the capabilities we need, but they all work together seamlessly, something that is essential for building a manageable, converged infrastructure."

Israel Devesa
CIO and CTO
Capital Energy

To enhance visibility and control for both cloud and physical assets and to help streamline SD-Branch deployment to remote sites—many of which are not monitored—FortiManager with zero-touch deployment was also used.

The success of Capital Energy's large-scale hybrid deployment is due to the single console of FortiManager to unify all firewall deployments, setting consistent security policies for on-premises, virtual, and FortiGates in Google Cloud Platform for a hybrid mesh firewall deployment.

Using application-centric SD-WAN business policies, Capital Energy can now fine-tune traffic steering decisions based on performance service level agreement (SLA) targets for each WAN provider.

Overall event monitoring, analysis, and reporting for the resulting infrastructure was further enhanced by adding the FortiSIEM security information and event management solution and FortiAnalyzer.

Industry 4.0 and Securing the Migration to Cloud-Based SCADA

Increasing business agility through digital acceleration initiatives is essential for any business facing rapid market change, and Capital Energy is no exception.

One of the ways Fortinet helps with the increased complexity and security challenges created by such change is through the Fortinet Security Fabric cybersecurity platform. The Fortinet Security Fabric covers the expanding digital attack surface of modern cloud and hybrid networks, enabling self-healing security and automated protection for all users, devices, data, and applications.

One example of Capital Energy's digital innovation, essential to delivering a constant, dependable energy supply from the fluctuating output of wind and solar, is the development of intelligent battery energy storage systems (BESS) that can make safe and efficient use of second-life batteries (used automotive batteries, which, although no longer suitable to power vehicles, still have a residual capacity of around 70–80%).

"Innovation, such as using second-life batteries in BESS, is key to meeting our sustainability goals," explains Granda. "But running the complex, AI-driven software algorithms to enable it calls for a new generation of IT/OT convergence in the cloud. Fortinet and Google Cloud help us achieve these goals."

To turn such projects into reality, Capital Energy is in the process of migrating key elements of the company's supervisory control and data acquisition (SCADA) systems to Google Cloud, effectively separating the data acquisition part of SCADA, which remains mostly physical, from the supervisory control part, which becomes virtualized.

Capital Energy's transition to an increasingly cloud-based architecture has many potential benefits, such as increased scalability, greater operational efficiency, and reduced cost. Still, it also changes the cybersecurity risk profile in novel ways. While replacing legacy terminals with web-based consoles, for example, removes some of the security concerns associated with maintenance and patching, the potential attack surface of the overall ICS has expanded, exposing the environment to new threats. By correlating threat information across the entire infrastructure, the Fortinet Security Fabric platform helps Capital Energy identify all such threats more quickly and automatically launch the most effective response.

As with all Fortinet solution deployments, external threat intelligence is provided by FortiGuard Labs, which collates and processes the data from millions of sensors and hundreds of global partners. Leveraging machine learning and other artificial intelligence, FortiGuard Labs identifies and characterizes known and previously unencountered threats. FortiGuard AI-Powered Security Services are also natively integrated into the Fortinet Security Fabric.

"In many ways, we are charting new territory here at Capital Energy. It was very important for us to work with a solutions provider with whom we could face these new and unique challenges together," adds Granda. "Our partnership with Fortinet, therefore, goes far beyond our use of their products. We share a common vision, which gives us confidence that the solutions we deploy today will continue (or evolve) to meet our needs tomorrow."

September 26, 2023 7:46 AM

2371902-0-0-EN