



Connexus Energy Secures Scada, ICS, And IT Environments With A Single Integrated Solution

INDUSTRY

Utilities

HEADQUARTERS

Ramsey, Minnesota

COMPANY SIZE

201-500 employees



OVERVIEW

Based in Ramsey, Minnesota, Connexus Energy is Minnesota's largest electric cooperative, providing electricity and services to member residents and businesses.

OUR SOLUTION



CHALLENGE

Connexus Energy serves more than 130,000 members across seven counties north of Minneapolis. Energy companies have become significant targets for cyber attackers and malicious nation-states that aim to disrupt vital services. Utilities have relied on Supervisory Control and Data Acquisition (SCADA) and Industrial Control System (ICS) networks for decades to control and monitor devices and data across their distribution networks. As smart grids, smart devices, and Internet of Things (IoT) devices become widely adopted, traditional SCADA and ICS systems often lack the same level of security controls needed to defend against sophisticated cyber attackers who can exploit their vulnerabilities to create widespread damage.



The Quantum 1200R Rugged Appliance delivered ruggedization, comprehensive security, centralized visibility, and compliance best practices in one product. Its footprint is so small that it easily fit in every environment we needed to place it in.

Melissa Kjendle, Cybersecurity and Senior Infrastructure Analyst



“We have some corporate devices that connect to an external network, and we didn’t want them to introduce vulnerabilities to a network where there might also be servers,” says Arcopedico’s Information Technology Department Manager, Serafim Couto.

“Our SCADA system is our bread and butter,” said Jon Rono, Group Leader for Technology Services at Connexus Energy. “We wanted to make sure that it delivers power safely, securely, and without interruption in the face of increasingly malicious cyber attacks. We began looking for a better way to secure it and be alerted to any communication issues that might compromise service.”

Connexus Energy used many different security solutions from multiple vendors, such as Cisco, McAfee, and Palo Alto Networks. Each solution had specific management requirements, which consumed a lot of the team’s technical resources. Individual security team members responsible for cyber security, help desk, endpoint security, network security, and server security had to parse logs from different systems to identify issues and respond accurately.

“We wanted one management solution for all of our security needs,” said Rono. “We needed a single pane of glass that would work across all of our systems and streamline visibility.”

Finding a solution for protecting the SCADA system while delivering centralized visibility across the entire security environment was challenging. Secure gateways for the SCADA system have to operate in extreme physical conditions. They must fit within constrained spaces or locations that are difficult to access. Environments are harsh, with dust, sub-zero temperatures in Minnesota winters, and high heat and humidity in summer months. Many of Connexus Energy’s existing security solutions were not ruggedized at all or only partially ruggedized. Simply keeping everything operating—and trying to make them work together—was consuming a lot of time without delivering the desired results.

“



Bringing security and management under Check Point changed our focus from reacting to becoming proactive. I don’t have to use resources to do all of the work that Check Point does automatically for us. One solution did it all and delivered higher value.

Melissa Kjendle, Cybersecurity and Senior Infrastructure Analyst

”

SOLUTION

The security team conducted a full RFP to evaluate solutions from existing vendors, as well as Check Point solutions. Only Check Point delivered the single-pane-of-glass management needed with a suite of integrated solutions and additional capabilities, such as historical logging and unified policy management.

Connexus Energy deployed Check Point Quantum 15400 Next Generation Security Gateways with high availability for its core security gateway. Check Point Quantum 5600 Security Appliances protect the SCADA network, and Check Point Quantum 3200 Next Generation Security Gateways are deployed at multiple remote sites. Finally, Connexus Energy deployed Check Point Quantum 1200R Rugged Appliances with next-generation threat prevention for its ICS at all substations. A solid-state appliance, the Check Point Quantum 1200R Appliances protects all critical operational systems.

In addition to security protection, Check Point solutions provide Connexus Energy with a Check Point compliance software. Based on a library of more than 300 security best practices, the compliance software highlights configuration errors, identifies security weaknesses, and validates changes in real time. Not only does it enable real-time security policy audits, but it also ensures proper configuration and function of firewall, antivirus, IPS, and data loss prevention protections.

“The Quantum 1200R Rugged Appliances delivered ruggedization, comprehensive security, and centralized visibility in one product,” said Melissa Kjendle, Cybersecurity and Senior Infrastructure Analyst. “Its footprint is so small that it easily fit in every environment we needed to place it in.”

OUTCOME

In the past, the security team continually had to reboot substation security systems when they would go offline. The Quantum 1200R Rugged Appliances operates regardless of environmental conditions, saving the team time.

“The Quantum 1200R Rugged Appliances have delivered tremendous reliability,” said Kjendle. “That’s huge because we’re not spending time driving to remote sites to reboot systems. Even though those systems run

“



Check Point not only delivered outstanding security solutions and effective management capabilities, they have helped our entire company build a stronger security posture.

Melissa Kjendle, Cybersecurity and Senior Infrastructure Analyst

”

over a relatively slow network, they give us a reliable tunnel and logs, which we never had before.”

“Check Point delivered solutions that our entire security team uses, enabling them to manage security for everything down to individual devices and files,” said Rono. “I’m able to use our entire range of expertise much more effectively.”

Team members can view everything in the Check Point Security Management console. In the past, team members had to orchestrate different views across multiple systems and try to correlate meaningful data. With Check Point, they can see at a glance how many endpoints are compliant, ensure that all systems are updated, address any risks that have appeared, and push unified policy out to hundreds of devices in the field.

Unified logging features accelerate troubleshooting and threat investigation. For example, Connexus Energy had incidents during which more than 30 endpoints were not responding. Within a week of deploying Check Point, that number was reduced to four. Check Point combined gateway and endpoint protections also enabled Connexus Energy to completely replace its previous desktop security solution.

“Bringing security and management under Check Point changed our focus from reacting to becoming proactive,” said Rono. “I don’t have to use resources to do all of the work that Check Point does automatically for us. One solution did it all and delivered higher value.”

In the past, the security team continually had to reboot substation security systems when they would go offline. The Quantum 1200R Rugged Appliances operates regardless of environmental conditions, saving the team time.

“The Quantum 1200R Rugged Appliances products have delivered tremendous reliability,” said Kjendle.

“That’s huge because we’re not spending time driving to remote sites to reboot systems. Even though those systems run over a relatively slow network, they give us a reliable tunnel and logs, which we never had before.”

The Board of Directors had launched an initiative to increase cyber awareness across all levels of the organization. When the company implemented Check Point solutions, it also engaged the Infinity Platform Services Incident Response team to help develop an incident response plan.

The Check Point team first analyzed the company’s existing strategies and policies. They shared best practices and documentation with the Connexus Energy security team and presented security best practices for employees.

They also met with the executive team to conduct an Infinity Platform Services Incident Response tabletop exercise to help the company structure a comprehensive cyber incident response plan. Using a ransomware attack as a hypothetical situation, Check Point provided a response framework based on best practices, which Connexus Energy used to map out its incident response procedures and processes for stopping, mitigating, and remediating a cyber attack.

“Check Point not only delivered outstanding security solutions and effective management capabilities,” said Rono, “they have helped our entire company build a stronger security posture. That’s the kind of engagement we wanted to protect our systems, operations, and customers.”

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Platform Services for collaborative security operations and services.

[LEARN MORE](#)

Worldwide Headquarters

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters

100 Oracle Parkway, Suite 800, Redwood City, CA 94065

www.checkpoint.com

