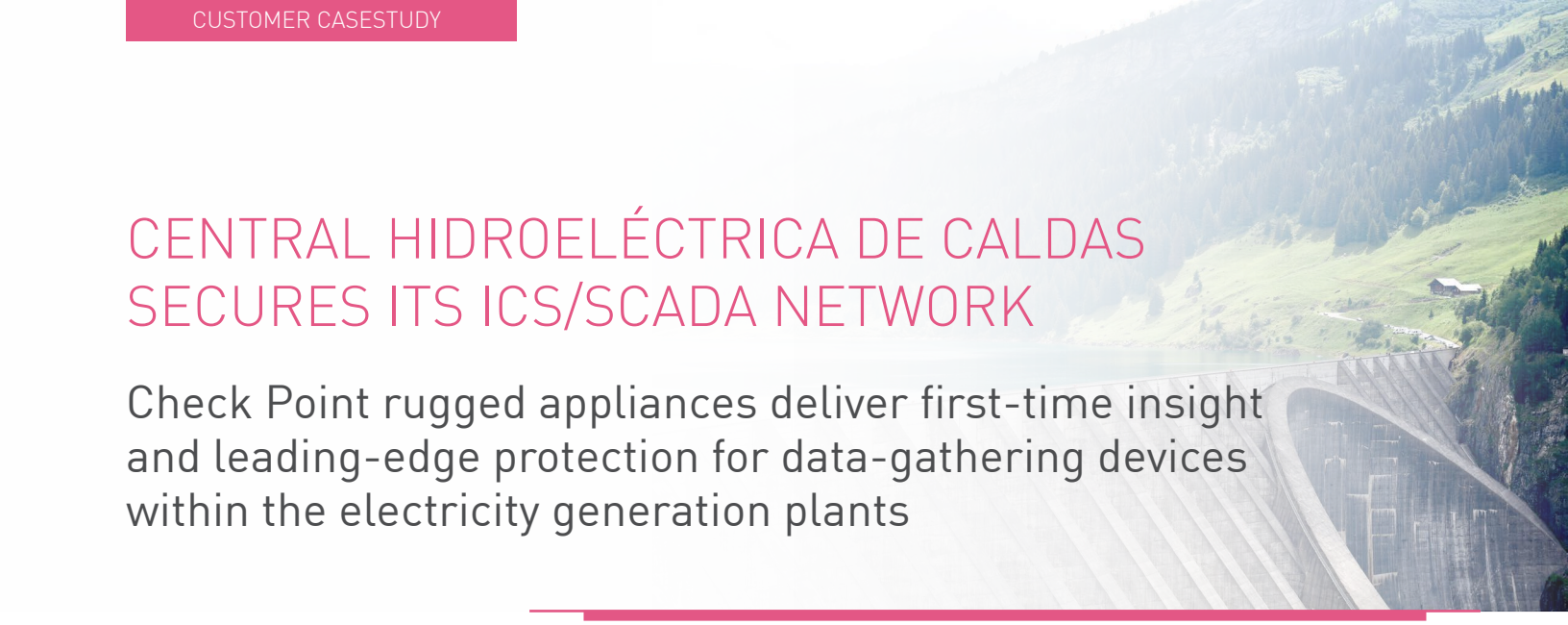


CENTRAL HIDROELÉCTRICA DE CALDAS SECURES ITS ICS/SCADA NETWORK

Check Point rugged appliances deliver first-time insight and leading-edge protection for data-gathering devices within the electricity generation plants

Customer Profile

Central Hidroeléctrica de Caldas generates and distributes electricity in Colombia.

Challenge

- Meet governmental security requirements for power generation plants
- Secure traffic delivered from SCADA devices to prevent network infiltration by attackers
- Enable highperformance security in harsh, inhospitable environments

Solution

- Check Point 1200R Ruggedized Gateways
- Check Point R80 Cyber Security Management

Benefits

- Gained visibility and control of SCADA monitoring traffic
- Consolidated SCADA security management across locations
- Blocked threats to ensure high availability of monitoring and control data

"The Check Point 1200R gateways performs exceptionally well. It gave our team visibility into SCADA traffic for the first time, enabling us to identify potential security threats, analyze incidents, and monitor compliance."

- Maria Jose Bernal Zuluaga, Security Professional, Central Hidroeléctrica de Caldas

Overview

Central Hidroeléctrica de Caldas

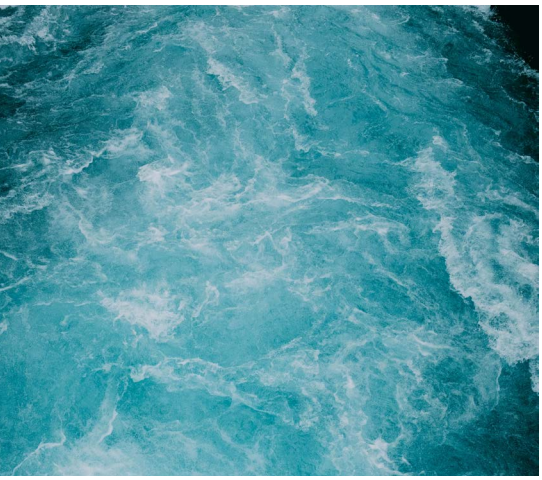
Central Hidroeléctrica de Caldas (CHEC) generates and distributes hydro-and thermoelectric power across the Caldas and Risaralda departments of central-west Colombia. As part of the country's vital energy grid, CHEC launched a project to extend cyber protection to its substations and power plants. It turned to Check Point to accelerate success.

Business Challenges

Securing the Farthest Edge

Headquartered in Caldas, Colombia, CHEC is part of Grupo EPM, the second-largest business group in Colombia. Founded in 1944, CHEC pioneered the delivery of electricity for street lighting in this coffee- growing region. Today CHEC powers 40 municipalities with 100% electricity coverage in urban areas and 99.62% in rural areas—providing power and illumination for almost a half million customers.

As the company grew and consolidated its power generation capabilities, it built transmission and distribution networks to deliver power across the regions. These networks are monitored and controlled by Supervisory Control and Data Acquisition (SCADA) devices located in power plants and substations.



Since the SCADA systems were deployed, cyber security of the country's energy facilities has become a significant concern. Power plants generating more than 100 megawatts of power, and substations transfer more than 115 KW must now comply with security controls required by Ministerio de Minas y Energía de Colombia and the Comisión de Regulación de Energía y Gas. The company's corporate infrastructure is well protected, but SCADA devices were deployed years ago, before cyber security controls were needed. Cyber attackers could potentially compromise one or more SCADA devices and gain control of vital systems.

"As an energy company, we see every type of cyber attack on our systems," said Maria Jose Bernal, Security Professional at CHEC. "Our SCADA systems represented a significant security vulnerability. We began seeking a way to mitigate the risk of threats gaining access to our networks through these devices."
A new solution had to put controls in place without being installed on the SCADA devices themselves. It also had to function in industrial environments—plants and substations are located in areas of high heat, humidity, and rugged terrain. CHEC turned to Check Point as a trusted advisor for its solution.

> "It gave our team visibility into SCADA traffic for the first time, enabling us to identify potential security threats, analyze incidents, and monitor compliance."
>
> -Maria Jose Bernal Zuluaga, Security Professional, Central Hidroeléctrica de Caldas

Solution

Newfound Visibility into SCADA Traffic

The CHEC team designed a proof of concept to test Check Point 1200R Rugged gateway in its environment. They installed a gateway in one substation in Monitor Mode and a second system in another substation in online mode. In Monitor Mode, the Check Point 1200R gateway monitors and analyzes traffic without affecting the production environment. In online mode, the Check Point appliance enables full visibility and granular control of SCADA traffic.

"The rugged appliance performs exceptionally well," said Ms. Bernal. "It gave our team visibility into SCADA traffic for the first time, enabling us to identify potential security threats, analyze incidents, and monitor compliance."

The 1200R gateway delivers proven, integrated security for deployment in harsh environments as part of a complete end-to-end Industrial Control System (ICS) security solution. The CHEC team now has granular functional control of SCADA protocols and can log SCADA protocols, including commands, for check forensic analysis. The available Compliance technology enables organizations to translate thousands of complex regulatory requirements into actionable security best practices
CHEC deployed Check Point 1200R Appliances in its power generation plants and substations to protect SCADA traffic. The team also uses Check Point R80 cyber security management for managing security across the SCADA environment in a single pane of glass. With policy, logging, monitoring, event correlation, and reporting in a single system, the security team can easily identify security risks across the organization. Multiple team members can work in Check Point R80 simultaneously without conflict, simplifying management across locations.

Check Point Smart-1 5050 Appliances consolidate management for up to 50 systems, delivering full threat visibility and control of SCADA traffic. Hardened to meet the rugged environment, Check Point Smart-1 5050 Appliances enable the team to install policy up to five times faster and achieve outstanding log collection performance. Check Point Smart-1 Appliances send traffic and management data to the CHEC Point centralized Security Management console.

Results

Protect Investment with Compliance

Prior to the Check Point 1200R Appliances, CHEC could not effectively monitor security for SCADA traffic to identify potential threats. Now they have complete visibility into application traffic from substations and devices.

"With Check Point, even if we cannot capture and control all of the SCADA protocols in substations that have not yet been migrated to IP, we still can control the traffic," said Ms. Bernal. "We have strong access controls for each substation, so we can still achieve our compliance objectives."
CHEC has not had any disruption from cyber attacks. Check Point solutions effectively block threats and enable CHEC to maintain high performance for data collection, energy distribution monitoring, and power delivery.

Peace of Mind

Ms. Bernal says that her team relies on Check Point expertise to help them overcome current environmental challenges and ensure that its SCADA systems are protected. When CHEC needs assistance, the Check Point team is right there. "We have peace of mind knowing that the Check Point solutions are working well," she said. "In addition to our own security and technical teams, we have the Check Point experts standing behind us to work on cyber security issues with us. It's a huge relief."

> "In addition to our own security and technical teams, we have the Check Point experts standing behind us to work on cyber security issues with us. It's a huge relief."
>
> -Maria Jose Bernal Zuluaga, Security Professional, Central Hidroeléctrica de Caldas

For more information, visit:
https://www.checkpoint.com/products/