



Customer-at-a-Glance

Superintendencia de Electricidad

Industry

Utilities

Number of Staff

More than 400 users at headquarter offices and 200 users at 42 remote offices

Challenges

- Improve service delivery to customers and employee productivity by reducing downtime resulting from ransomware and other advanced threats
- Increase threat visibility across the entire environment to enable faster response and better decision making
- Simplify and consolidate security management
- Protect against ransomware and today's advanced, evasive threats

Sophos Solutions

Sophos Central Endpoint
Sophos Intercept X
Sophos Intercept X for Server
Sophos XG Firewall
Sophos RED
Sophos Access Points

Sophos Helps Dominican Utility Company Improve Service Delivery and Expand Visibility





Superintendencia de Electricidad is a regulatory entity of the Dominican Republic's electric sub-sector. Founded in 1998, the organization is headquartered in Santo Domingo and has 42 offices distributed across the country. Its mission is to supervise compliance with legal provisions and technical regulations related to the generation, transmission, distribution, and commercialization of electricity. The organization is also responsible for establishing tariffs and tolls subject to price regulation. Superintendencia de Electricidad services a broad cross-section of users: regulated users, unregulated users, distribution companies, companies that generate electricity, companies that transmit electricity, and the private sector.

How do cyberthreats impact continuity of service in the utility sector?

Challenged by the complexities of the national electrical system and the diversity of actors involved with this sector, Superintendencia de Electricidad is in the process of reorganization and continuous improvement, as it strives to become more dynamic, modern, efficient, and effective. Security plays an important role in this effort, with the main focus on how to prevent ransomware and other advanced attacks from impacting endpoints, from spreading across the network, and from resulting in downtime for internal users and customers.

The organization's legacy antivirus solution was unable to detect advanced malware and ransomware, contributing to a perception that the organization was vulnerable and an easy target. Even though there was a backup policy in place to minimize the impact of ransomware, these types of attacks frequently resulted in service disruption and loss of productivity. When infected computers were hijacked, they had to be quarantined, repaired, or replaced, all of which took time and effort. Lacking 360-degree visibility across all endpoints and the network, CTO Fabricio Gómez and his team were unable to conduct forensic analysis, which could have prevented new infections.

Why are visibility and innovation so critical for a well-rounded security infrastructure?

After evaluating several security solutions, Gómez concluded that the Superintendencia de Electricidad needed an innovative and effective solution that included a broad set of security controls—anti-ransomware, traditional antivirus, anti-spam, web filtering, and firewall—along with a high level of vendor and local partner support. Gómez selected Sophos because it provides a unified and integrated security environment with single-console management and full visibility across the entire organization. In his eyes, Sophos was the only brand with a suite of products that combines maturity, a solid track record, and innovation.

To secure endpoints, Gómez implemented Sophos Central Endpoint, which integrates anti-malware, web filtering for users on and off the network, application control, data loss prevention, and more. The team also decided to extend the same capabilities to servers that house critical data and applications—all with minimal impact to performance and availability.

The Sophos Central cloud-based management platform offers Gómez and his team the ability to easily coordinate between the different security solutions and provides a simple, intuitive user interface that enables them to make clear, informed decisions when issues arise. Additionally, it offers visibility across the entire operation—at headquarters, at remote offices, and out in the field.

Superintendencia de Electricidad also deployed 120 licenses of Sophos Intercept X, which provides everyone in the organization—from business executives to employees—with comprehensive, enterprise-grade endpoint protection that combines anti-ransomware, next-generation antivirus, deep learning (a form of machine learning), and anti-exploit technology.



How do you provide consistent network security across remote locations?

For network security, Superintendencia de Electricidad invested in five Sophos Firewall XGs, recognized by NSS Labs, Gartner, and others for top protection, performance, and value. Among Sophos Firewall XG's many innovative features is the ability to gain insights into applications, users, and risks, along with rich, easy-to-access on-box reporting. It provides the organization with layered protection against ransomware and advanced threats, including intrusion prevention systems (IPS), sandboxing, dual antivirus, application control, antiphishing, and a web application firewall.

The organization relies on Sophos to protect the wireless network and remote locations as well. They deployed 10 Sophos Access Points, which they can manage via the Sophos Central console to get full visibility into the security health of their trusted wireless network. They also installed 50 Sophos Remote Ethernet Devices (Sophos RED). These plug-and-play devices encrypt all traffic and tunnel it from remote offices back to the firewall at the main facility, enabling a secure distributed network.

Since deploying Sophos, Superintendencia de Electricidad has been operating with all its services fully protected. While previously the security team had struggled with limited visibility and control, they now have a complete view to traffic across all networks and to user systems and servers. Additionally, the IT team are encountering fewer false positives, which saves time and allows the team to place their attention on what matters most. As a result, Gómez and his team can now take more efficient and effective action against attacks to their infrastructure and get closer to achieving their business goals.

**Start your free trial of Sophos
Intercept X today:**

Visit www.sophos.com/intercept-x

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com