International Health Center in Colombia Secures Its Critical Information and Medical Devices With Fortinet Platform

On the Colombian Caribbean coast, one of the best-known private clinics in the region has taken a critical step to secure the flow of sensitive information through its network. La Misericordia Clínica Internacional (LMCI) is one of the most modern health institutions in the region. LMCI provides complex health services to Colombians and foreigners in Barranquilla city through its 1,300 medical and administrative staff. The facility has 237 beds—70 of them intensive care—and 12 cutting-edge operating rooms, in addition to an emergency care unit. Today, it attends to approximately 8,000 patients per month and hospitalizes about 2,000 people, resulting in an occupancy rate exceeding 94%. The institution specializes in high-complexity surgery; neurosurgery; laparoscopic, cardiovascular, and pediatric surgery; and critical medicine.

With its reputation for modern healthcare, it is crucial that LMCI also implements innovative security and networking strategies to provide optimum service while complying with the government’s health institute regulations. “Information security is key for LMCI,” says Dieb Maloof Cusse, president of La Misericordia Clínica Internacional. “Handling so much sensitive data makes it possible to have security breaches and put the institution at risk. Thus, information security is one of the most important concerns for our organization.”

Security as a Business Driver

LMCI operates in a 55,000-square-meter facility comprised of six buildings. Fiber-optic links connect all the buildings to one another and to the main data center, which houses the core information and security system. In 2019, LMCI initiated a vendor review process to modernize its network and security infrastructure. The organization faced a pressing need to optimize its information security, gain access to 24/7 support, and eliminate system outages.

One of LMCI’s primary requirements was the technical support. As a nonstop medical institution, it relies on a technological ally to provide support at any time. Additionally, LMCI was worried about network performance. The health facility has multiple biomedical and intraoperative equipment that connects to wired or Wi-Fi networks, demanding high bandwidth. At times, the network equipment became saturated and LMCI experienced operational bottlenecks. Moreover, the network had to support high traffic in LMCI’s outpatient service, estimated at around 800 patients per day.

After evaluating different providers in the market, the health center turned to Fortinet. “We chose Fortinet because we realized that it is a competitive and robust brand compared to others. It also gives us peace of mind that our information and systems are protected,” says Maloof Cusse.

“Fortinet platform allows us to save a lot of time in management issues. Now we can focus on a more intelligent analysis of attacks and vulnerabilities, which is a sensitive issue for healthcare institutions today.”

– Dieb Maloof Cusse, President, La Misericordia Clínica Internacional

Details

Customer: La Misericordia Clínica Internacional (LMCI)
Industry: Healthcare
Location: Colombia

Business Impact

- Enables secure telemedicine services
- Up to 70% reduction in network leaks through the Wi-Fi network
- Less time spent on security administration with a simple graphical management interface
- 24/7 support to mitigate any network security issues
Security and Availability Improvements

Before Fortinet, LMCI utilized multiple point products and lacked a unified switch management system. It was difficult to solve any problems that arose, as access to each device was only possible directly from the device itself. This resulted in very long response times to incidents and greatly disrupted the network. Similarly, information security was not included in the network architecture, presenting a notable blind spot in the organization’s visibility and control of network vulnerabilities and risks.

In early 2020, LMCI implemented Fortinet’s secure access solution deploying FortiGate Next-Generation Firewalls and FortiSwitch secure Ethernet switches to take a step forward in network and security innovation. Fortinet’s solution also integrated well with LMCI’s multivendor wireless environment—the organization reduced its Wi-Fi network leaks by up to 70%, along with unauthorized device connections. LMCI’s new real-time security solution also minimized the risk for devices with outdated operating systems. Future plans for LMCI include looking at expanding its Fortinet Security Fabric approach end to end with FortiAP secure wireless access points.

Fortinet’s central security management capability overhauled the entity’s operations, allowing them to minimize management time spent directly administering the switches that were each previously managed independently. Now, LMCI’s security management is centralized—once a single configuration is implemented, it is immediately deployed over the entire system. On top of these integral changes, platform control is now much easier, as its graphical nature enables a faster and simpler operation.

“The Fortinet platform allows us to save a lot of time in management issues that previously demanded multiple resources of time and effort. Using FortiAnalyzer, we can focus on a more intelligent analysis of attacks and vulnerabilities, which is a sensitive issue for healthcare institutions today,” says Maloof Cusse. In addition, with Fortinet’s FortiCare service, LMCI has been able to rely on a security service that provides 24/7 support for any eventuality.

Fortinet’s solution strength also expands the protection capabilities of LMCI’s services. During the COVID-19 pandemic, the healthcare institution began offering telemedicine services, requiring a secure communication channel for doctors and patients at home. “Physicians needed to have continuous access to the clinic’s system to check diagnostic images and make crucial decisions from anywhere. With Fortinet, we can give users peace of mind that they are connecting securely, ensuring that all information is protected,” concludes Maloof Cusse.