ProDentist

Elevating Data Protection and Network Efficiency at Polish Dental Clinic

Customer at a glance

Customer Name
ProDentist

Industry
Healthcare

Location
Warsaw, Poland

Customer Background

ProDentist, a prestigious dental clinic in Warsaw, Poland, is dedicated to delivering comprehensive treatment and preventive care of the highest quality by harnessing cutting-edge materials and advanced equipment. In recent times, the healthcare industry in Poland has witnessed a staggering 60 percent increase in cyberattacks within a year. Hospitals, clinics, and medical facilities are increasingly becoming prime targets for hackers, as their IT security measures often fall behind those of financial institutions and energy companies.

"We had to consider the integration of the cloud-based medical system with the on-site database application and ensure compliance with GDPR. The clinic's management decided to use Zyxel's devices after the evaluation. Our team was pleased to work with the Zyxel Poland team, primarily for their post-sales support. I would like to highlight that ProDentist has also appreciated this support, and therefore, we are jointly planning to connect another ProDentist facility using Zyxel devices."

Krzysztof Kowalski, Owner
Kowalski ORG

Summary

ProDentist has decided to enhance network security to protect patient data and medical records in response to rising cyber threats on healthcare organizations. This involved implementing a zero-trust architecture for seamless integration with critical electronic devices like anesthesia systems, dental radiographs, and CBCT computer tomography while ensuring uninterrupted operations. For the medical staff, maintaining seamless communication with the SaaS medical system and encrypted VPN connections for remote access was of paramount importance. Zyxel USG FLEX 100 firewall was used to offer robust protection, extending from firewalls to access points with automated responses and multi-layer defense against a range of threats. External protections included URL threat filtering, malware protection, and intrusion prevention. Internally, application control and web filtering services prevented unauthorized network access and misuse of applications. The firewall detected and isolated threats on devices, synchronized data with the Nebula Control Center, and provided protection at the wireless access point level. VLANs were employed to segment the network into smaller, more secure subnets, improving traffic management and adaptability to organizational changes. Furthermore, the use of the 24-port GS1915 series switch enhanced efficiency with plug-and-play technology, and the Power over Ethernet feature powered connected devices directly from the ports.

Challenges

- Integrate the security solution with a diverse range of electronic medical devices without disrupting clinic operations
- Ensure unauthorized access could not compromise patient data

Benefits

- Enhanced security of patient data and medical records
- Seamless communication and remote access that allows medical staff to securely access critical information from anywhere
- The use of VLANs and the PoE switch makes the network more efficient and flexible to accommodate evolving healthcare needs

Products used

- USG FLEX 100 Firewall
- GS1915-24EP Smart Managed Switch