

CASE STUDY

Efficient network infrastructure management Network Access Control (NAC)

The regional health care facilities of the Moravian-Silesian region requested an information system according to the following requirements: A comprehensive and highly reliable multi-tenant and multi-vendor system for network device management, network analytics, access policy management.

The regional health care facilities of the Moravian-Silesian region include Bílovec Hospital, Havířov Hospital, Karviná-Ráj Hospital, Třinec Hospital, Frýdek-Místek Hospital, the Krnov United Health Care Facility and Silesian Hospital in Opava.



SELECTED TECHNOLOGY

The ExtremeCloud IQ Site Engine, Extreme Analytics and Extreme Control fully met the required features. Together, these systems form a single functional unit.

CUSTOMER ACQUISITION

By deploying the systems, the individual hospitals have particularly gained the ability to efficiently manage their network infrastructure from a single location. The hospitals use the tool for tasks such as inventory, network map, firmware management, configuration management and fault management.

The access control tool provides previously unavailable insight into who is where on the network and enables simple network and security configuration based on the identity of the connected device and user.

The analytics tool then provides a detailed insight into the applications used by the user and their performance and is very helpful in case of problems. The system's automation capabilities will help IT staff streamline selected repetitive tasks.

SPECIFICATION

A comprehensive and highly reliable multi-tenant and multi-vendor system for network device management, network analytics, access policy management.

REQUIREMENTS

- Simplified administration
- High availability of solutions
- Delivery of technical support services
- Assistance in meeting the requirements of Sections 18 and 19 of the Cybersecurity Decree
- Ensuring network segmentation
- Ensuring communication management
- Identity verification

I appreciate that a large team of experienced professionals has been involved in the extensive analysis and implementation of NAC in our hospitals. What we got is a tool that not only increases security, but is also user-friendly, with a range of automation features. Our cybersecurity team now has a tool that simplifies their work and improves prevention/response to potential security accidents and incidents.



RNDr. Ing. Alois Slovák
director
Moravian-Silesian
Data Centre

The Moravian-Silesian region features 6 districts: Bruntál, Frýdek-Místek, Karviná, Nový Jičín, Opava and Ostrava-City and is divided into 22 administrative districts of municipalities with extended competence. Its area ranks 6th among all regions and it is the third most populated in the Czech Republic. The administrative centre of the Moravian-Silesian region is Ostrava, where about a quarter of the population lives. The Moravian-Silesian region is strongly dominated by industry, and in terms of the environment the region is one of the most polluted regions in the Czech Republic. Seven hospitals and other health care facilities also fall under the region.

SYSTEM UNIQUENESS

What is unique about the system is that it **supports any device** that can be encountered on the network. The communication infrastructure of hospitals consists of elements of different ages and from different manufacturers. Yet the ExtremeCloud IQ Site Engine is able to encompass most of these elements and provide unified and transparent management over them.

DETAILS OF DEPLOYED TECHNOLOGIES

The **ExtremeCloud IQ Site Engine** is a robust network management tool that enables unified management of network devices regardless of manufacturer or age. It allows you to perform common day-to-day management tasks through its user-friendly graphical interface, plus it supports task automation, conformity checking and other features to facilitate network operations. It also allows integration with other systems through the offered and documented API.

ExtremeAnalytics provides deep insight into application and network performance, providing proactive monitoring and rapid diagnostic tools.

Extreme Control is a network access control system that provides secure access for internal users, BYOD users, IOT devices or visitors and protects the network from external threats. The system can be integrated with other security systems such as NG firewalls, SIEM, MDM and others.

SYSTEM USERS

The supplied IT systems are used almost exclusively by hospital employees, yet it can be said that the deployment of the above systems has a direct impact on a patient as a visitor to the hospital. In general, the system contributes to higher security of the entire IT, so patient data is better protected against misuse or theft.

Hospital staff can also expect better functionality of existing IT technology and can thus have more time for a patient. In addition, it opens up the possibility of deploying modern and secure devices that will provide patients with a higher quality of healthcare services.

The IT teams of the hospitals have often communicated and collaborated with each other before.

Now they have another common theme. They can share their experience of working with the management and analytics system or the network access control system.

The biggest challenge was integrating network devices from a number of different manufacturers into the Extreme ecosystem.



Petr Mojžíšek
Head of Infrastructure Department, ANECT