Central hospital protected by NovaMDR

"NovaMDR was our way to evolve our IT security infrastructure quickly and efficiently."

ForeNova Customer Story

We had to evolve our IT security infrastructure to comply with the new security regulations. With the excellent and flexible support of ForeNova and the quick onboarding process, we could handle the transformation without having the trouble of creating our own technology platform or the complex processes of an internal Security Operation Center. NovaMDR gives us peace of mind and a future-proof solution against the ever-evolving cyberattacks on our hospital."

Head of IT Security of the hospital

Our customer is one of the biggest hospitals in the center of a major country. Directly attached to a worldwide recognized university, the hospital offers best-in-class medical services to thousands of patients per day. With more than 6000 employees, it is critical to ensure the region's safety and medical coverage.

The hospital experienced several waves of massive growth during the last twenty years. As a result of building up new departments and acquiring other regional hospitals, the IT infrastructure developed in a very heterogeny way. A significant pain point for the customer was keeping track and control of all the assets and creating a reliable IT inventory. **The Head of IT security states:** *"ForeNova's asset management system delivering real-time information on the whole IT infrastructure as part of NovaMDR was a significant part of our hospital's decision for this solution."*

The IT leaders couldn't prevent technology islands during the rapid parallel digitalization and evolution of different hospital departments and branches: *"We have a thousand devices from hundreds of manufacturers. In the beginning, every hospital deportment made its own IT decision. As a result, today, it is nearly impossible for us to patch all the systems in time to prevent security vulnerabilities. In addition, we have a lot of medical devices that a traditional endpoint protection solution can't cover."* NovaMDR even works without any software agent on the endpoint and therefore can easily detect all threats in the hospital network.

Central hospital protected by NovaMDR

"NovaMDR was our way to evolve our IT security infrastructure quickly and efficiently."

Supported by advanced technologies like machine learning and AI, NovaMDR analyzes millions of client & network activities per minute and delivers alarms & potential incident information to ForeNova's own Security Operation Center (SOC).

"We have a very complex system of policies covering the user scenarios of all the different medical departments. With our high standards of patient data privacy, we have a hybrid strategy for digitalization. While many processes can build upon cloud services, certain use cases cannot even use any kind of internet. For example, our doctors must use USB sticks to transfer patient data from one department to another to comply with data privacy regulations. From an IT security point of view, this is a major cybersecurity concern. With NovaMDR's endpoint detection & response solution, we have reliable protection against potential threats resulting from this use case. NovaMDR can use all collected information from endpoints and network to immediately give us an alarm in real-time if there are suspicious activities from a PC after the doctor has attached a USB stick." To manage all the alarms and incidents reported by NDR & EDR the hospital decided to leverage ForeNova's own security operation center: *"NovaMDR offers a 24/7 monitoring of our network and all our endpoints including all our medical devise with network capabilities. To be honest, we wouldn't have the personnel resources & expertise to handle all alarms & incidents. We need ForeNova's security analysts to guide us on what to do after they report an incident to us. They have the experience in handling cybersecurity attacks for many years, and that experience is important against more and more mature cyber criminals."*

Hospitals have become one of the main targets of cyberattacks in the last two years because they were regarded as easy targets. As a response, governments worldwide established new regulations & requirements for cybersecurity. *"We had to evolve our IT security infrastructure to comply with the new security regulations. With the excellent and flexible support of ForeNova and the quick onboarding process, we could handle the transformation without having the trouble of creating our own technology platform or the complex processes of an internal Security Operation Center."*