

German Healthcare Leader Scales Its IT Security Team with UnderDefense MDR

About the client

The client is Germany's biggest and oldest healthcare organization, with 100+ different centers, institutes, and departments. They offer a wide range of healthcare services with state-of-the-art equipment and highly-qualified personnel. The institution is regularly listed among the best hospitals locally and globally.

Headquarters:	Germany
Industry:	Hospitals and Healthcare
Company Size:	17,000+ employees
Annual Turnover:	Over €2 billion
Client Since:	2019
Technologies and Tools:	EnSilo EDR (now Fortinet)
Internal IT Security Team:	Yes, 100+ employees
Infrastructure:	Hybrid

Data-Driven Outcomes

Over

€5,400,000

It is the daily cost of IT downtime caused by cybersecurity attacks

20,000+

Covered endpoints and servers

15

Severe incidents prevented during the first months of cooperation

"Even though the market is full of vendors, we had found it hard to get a top-notch ally whose services would align with our business goals and priorities until we met UnderDefense, which amazed us with their ability to understand all of our "headaches". We feel much more secure knowing that there is someone 24/7 watching our backs."

Hans
IT Director

CHALLENGES

- Limited visibility on 20,000 endpoints and weak cybersecurity posture
- Prevalent alert fatigue demoralizing the entire security system and burning out expensive internal IT security employees
- Heavy reliance on out-of-the-box configurations of security tools
- Small IT security team working 8-5 overwhelmed by alerts, viruses, malware, and ransomware attacks
- Increasing cyberattacks targeted at healthcare institutions

SOLUTION AND RESULTS

- ✓ Complete visibility on 20,000 endpoints and across the entire network
- ✓ Ability to identify and act quickly on important alerts
- ✓ Over 30,000 alerts reviewed and resolved to reduce alert fatigue and optimize the workload
- ✓ Professional fine-tuning of endpoint detection and response solution to maximize its value for the business
- ✓ 24/7 coverage delivered by talented cybersecurity engineers with constant access to unique domain expertise
- ✓ Comprehensive protection and response to all malicious security threats, including malware, ransomware, and viruses