UnderDefense CYBERSECURITY

German Healthcare Leader scales its IT security team with UnderDefense MDR

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.

€5,4M
saved daily by partnering with UnderDefense

25K
covered endpoints and servers

15
severe incidents prevented during the first months of cooperation

Client Introduction

Headquarters:	Germany	**Infrastructure:**	Hybrid
Industry:	Hospitals and Healthcare	**Annual Turnover:**	Over €2 billion
Company Size:	17,000+ employees	**Technologies and Tools:**	Fortinet/EnSilo EDR
Covered Endpoints:	25,000+	**Internal IT Security Team:**	Over 100 employees

Challenges

- Limited visibility on 25,000 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
- IT security team working 8-5 overwhelmed by alerts, viruses, malware, and ransomware attacks. Employees requested many changes, permissions, and whitelisting
- Increasing cyberattacks targeted at healthcare institutions

Results

- Complete visibility on 25,000 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. All automated or with delightful customer experience
- Comprehensive protection and response to all malicious security threats, including malware, ransomware, and viruses

The Challenge

Cyberattacks on healthcare organizations are escalating. Beyond financial and reputational damage, some attacks have tragically led to patient deaths, as seen at University Hospital Düsseldorf and Springhill Medical Center.

Our client knew that and had an in-house security team with over 100 IT engineers. Unfortunately, it wasn't enough as they were fighting a losing battle against:

- Relentless cyber threats from employee actions, malware, and phishing attacks.
- Staff burnout due to overwhelming alerts, incidents, and major hacks like the Emotet attack.
- Limited budget and talent shortages, preventing additional hires.
- A misconfigured Endpoint Detection and Response (EDR) tool that failed to reduce alert fatigue or operate effectively.

Consequently, various types of malware could easily sneak into the client's infrastructure and block all business functions. As it happened now and before.

All that only aggravated the situation for the in-house specialists.

Meanwhile, the stakes were high for the client. Their business security directly impacted the quality and timeliness of healthcare services. Additionally, sensitive medical records of European patients were at risk, threatening medical confidentiality and exposing the organization to GDPR penalties, violations of the Convention on Human Rights and Biomedicine, and more. Beyond legal issues, their reputation was on the line.

The Solution

The company realized they couldn't hire more employees in-house. So, they started looking for a reliable and professional cybersecurity partner to lessen the burden on the in-house employees and guarantee that no incident would go unnoticed. They needed solid cybersecurity experience and hands-on best practices to get maximum of their current and future security investments.

The client discovered UnderDefense, which provided not only relevant expertise but also a 24/7 security operation center (SOC) and a full team of elite cybersecurity engineers.

Since UnderDefense had a mature expert team and a well-established MDR service, we got to work nearly immediately, saving the client months of recruiting, interviewing, and onboarding. But most importantly, a quick collaboration kickoff prevented 15 severe incidents in the client's infrastructure.

To ensure comprehensive endpoint protection and deal with alert fatigue, we fine-tuned EnSilo (now Fortinet) across all Windows and MacOS systems within the hospital. Finally, the platform introduced automated incident detection, response, and prevention against modern malware and cyberattacks.

Meanwhile, we also started monitoring and fighting malware on over 20,000 endpoints.Maintaining compliance with strict European regulations and standards was another pressing issue for the company's IT Director and a high-priority task for the UnderDefense team. So, to improve data safety, we provided 8/5 or 24/7 security monitoring team Tier 1-3 with 20 minutes SLA for critical alerts with notification, reporting, and IR guidance.

During the first year of cooperation, the UnderDefense team analyzed 31.07 TB of data logs and 7.05 billion processes executed on 19,842 endpoints.

We also did the following:

- Reviewed **55,160** potentially threatening events
- Eliminated **37,508** false positive alerts
- Provided feedback on **7,722** events that were marked as allowed
- Notified the client about **73 confirmed attacks**
- Confirmed **27 attacks** (APT) that were remediated by our team
- Used the IR plan to respond to 3 threats
- Held 54 active communication sessions between the client's in-house and our SOC teams
- Conducted **89 calls** with the client's IT specialists
- Fielded **19** direct calls to the 24/7 SOC hotline
- Helped to increase CIS maturity level by 10 points

Outcomes

The collaboration with UnderDefense allowed the client to free up an expensive in-house security team and focus them on more strategic cybersecurity tasks unique to their industry and business. Internal engineers no longer need to spend time on the front-line monitoring alerts. Moreover, they don't get thousands of alerts with no context anymore. UnderDefense sends in-depth reports with instructions instead.

Better protection of sensitive assets and data	Fine-tuning of the endpoint detection and response solution, along with SOC provided by UnderDefense, added the missing security layer to the hospital's perimeter protection. Now the data of European patients are safe, and the client has eliminated the risk of becoming non-compliant.
Optimized security processes and workload	Professional configuration and orchestration of the entire security flow allowed the client to lower the number of false positives, reduce alert fatigue, and lessen the burden on the internal staff. The UnderDefense team not only notifies about important security incidents but also provides detailed remediation guidance.
End-to-end visibility and readiness for threats	Seeing and understanding what's actually happening in the environment is crucial for any business. Visibility is the key that gives c-level peace of mind and confidence to make important decisions. Working with UnderDefense, the client certainly has that. Additionally, our team provides threat investigation, advanced analytics, and custom monthly reports.

> *"We feel much more secure knowing that there is someone 24/7 watching our backs."*
>
> Hans, IT Director