



# Herdecke Community Hospital Relies on Forcepoint to Protect Sensitive Patient Information and Hospital Systems From Cyber Attacks

This German hospital uses Forcepoint NGFW and DLP to cost-effectively ensure patient data is securely stored in compliance with strict privacy requirements and hospital systems are protected from malicious hackers.

Herdecke Community Hospital wants to protect its patients' data in the best possible way while reducing costs and workload. The hospital chose a cost-effective, integrated solution from Forcepoint that combines Next Generation Firewall (NGFW) and Data Loss Prevention (DLP). This protects the highly sensitive data against both external attacks and uncontrolled data flow by the hospital's own employees.

**CUSTOMER PROFILE:**

German community hospital treating more than 50,000 inpatients and outpatients annually.

**INDUSTRY:**

Healthcare

**HQ COUNTRY:**

Germany

**PRODUCTS:**

- › Forcepoint NGFW
- › Forcepoint DLP

Information about the health of a person is among the most sensitive and therefore worthy of the strongest protection. As such, it is subject to the strict rules of the European basic data protection regulation, or EU-DSGVO for short, and other special guidelines. In the healthcare sector, the correct and secure handling of such sensitive information is essential, simply because hospitals and other institutions have long been targeted by hackers. Using phishing, ransomware or brute force attacks, they attempt to penetrate the network in order to extract data or paralyze the entire IT infrastructure. In the worst case, operations have to be shut down. At the same time, the sensitivity of this data also requires careful handling internally, so that it is not simply sent by email for the exchange of information between doctors, for example.

This was the challenge facing the Herdecke Community Hospital in the Ruhr area. In the acute care hospital with 492 beds serving the cities of Herdecke and Wetter, around 1,250 employees care for more than 50,000 patients annually, both outpatients and inpatients, including those with private health insurance. This ranges from all the specialist departments required for standard care to psychiatric treatment and emergency medical care for Herdecke and surrounding regions. At the same time, it is also open nationwide to all patients who choose to take advantage of the anthroposophically extended medicine practiced there.

As such an important part of the community, it was vital to protect hospital systems from cyber threats. Although a firewall existed, over time, those responsible were no longer satisfied with its performance.

"We were no longer happy with our solution. We had regular outages, the performance no longer fitted, and in short, reliability was no longer guaranteed in this highly critical security environment," explains Mr. Hirtzbruch, project manager at Herdecke Community Hospital.

When the existing licenses for maintaining the firewall expired, the hospital decided it was time to replace them with a modern next-generation firewall. At the same time, the hospital wanted to counter potential data loss with a convergent solution for network security and data protection. This solution should protect locally stored files, ensure DSGVO-compliant data exchange with other healthcare organizations, and prevent data from being accidentally uploaded to unauthorized websites or otherwise leaving the hospital through carelessness.

### **An integrated solution from Forcepoint is the Proof of Concept winner**

Initially, the Herdecke Community Hospital considered combining the solutions of two different providers for external communication and internal communication. After a Proof of Concept (PoC), however, it quickly became clear that a fully integrated solution from Forcepoint was the best possible answer to all requirements, while at the same time meeting the strict cost constraints to which hospitals are subject. During the needs assessment, another sticking point came to light: sensitive patient data must be prevented from leaking to the outside world. This is the case, for example, when doctors send unsecured electronic files to the family doctor for further treatment. At the same time, communication, and thus the ability of medical staff to work, must not be restricted by strict measures.

After a six-month test installation, the Herdecke Community Hospital decided in favor of the Forcepoint Next Generation Firewall (NGFW), which was installed on the local devices. Integrated into the firewall is Forcepoint Data Loss Prevention (DLP) to monitor and, if necessary, block data transactions to prevent unwanted outflow. The project—including data classification, processes, and works council approval—was completed in a very short time, with all components implemented by the end of 2019. DLP alerts and other controls were aligned using Forcepoint's comprehensive policy libraries.



## **Challenges**

- › Healthcare facilities have come to the attention of cyber criminals.
- › The DSGVO and other guidelines require special protection of sensitive patient data.
- › Given tight staffing and cost constraints, data security must be easy to manage.



## **Approach**

- › Forcepoint Next Generation Firewall (NGFW) analyzes data traffic and protects the network and computers against attacks.
- › Forcepoint Data Loss Protection (DLP) prevents uncontrolled data movement by employees.

## Cluster functionality, easy management and complete data protection

In Hirtzbruch's view, functions and administrative effort are convincing arguments for Forcepoint's solutions: "First of all, the cluster functionality of Forcepoint NGFW is a decisive advantage over the systems of other suppliers. If the performance is no longer sufficient and we need higher throughput, we can simply add another node. This guarantees us investment security. At the same time, the integrated intrusion prevention system allows us to very granularly define in which areas we use which signatures to detect anomalies, abnormalities, or attack patterns".

One advantage of an Intrusion Prevention System (IPS) is its simple, user-friendly management. The IPS is directly able to influence firewall rules in case of detected attacks without the need to configure complex connections and rule sets for communication between IPS and firewall. At the same time, the Forcepoint solution analyzes the stream in real time in order to react to threats at an early stage.

The IT managers of the Herdecke Community Hospital are particularly enthusiastic about Forcepoint Data Loss Prevention: Data transactions via email or the internet are monitored, controlled, and logged. An understanding of what is worth protecting simplifies the entire IT security strategy and minimizes the risk of data loss from the outset. Critical transactions are blocked or an alarm is triggered.

"Patient data, i.e. doctors' letters, findings, and similar documents, must not be exchanged in an uncontrolled manner. Our previous solution only covered Word and PDF documents—and PDFs only if they supported full text search. With Forcepoint's DLP solution, these restrictions have been removed and we can analyze scanned documents or screenshots of monitors to determine whether or not the documents are allowed to leave the house," Hirtzbruch continues. This prevents data from being downloaded by email, and documents cannot be uploaded to the Internet.

## An enterprise security platform that is scalable for the future and within budget

In the next phase, the Herdecke community hospital plans to install Forcepoint Email Security. The solution, which uses real-time behavioral sandboxing, provides comprehensive protection against multi-level, complex threats that often attempt to penetrate IT landscapes via email.

"Everything works perfectly. Managing network security has become much easier. We have a unified security platform that is scalable to future needs, has enterprise functionality, and still hasn't exceeded our budget. The cooperation was also very good—we had a reliable and competent contact person at our side at all times," Hirtzbruch notes with satisfaction. "I can't put it any other way: It's a pleasure to work with Forcepoint."



## Results

- › DSGVO-compliant protection of highly sensitive patient data
- › Significantly simplified IT security with scalability for the future



**"I can't put it any other way: It's a pleasure to work with Forcepoint."**

MR. HIRTZBRUCH, Project Manager,  
Herdecke Community Hospital.