Forcepoint

Customer Story

Forcepoint NGFW Helps the University of Münster Keep Its Network Open and Safe

This German university relies on Forcepoint to help manage its firewalls efficiently, keep its network open, and protect against ransomware attacks and other cybercriminal activity.

Article 5 of the German constitution guarantees freedom of science, research and teaching as fundamental right. This ensures German universities are at the forefront of research and education, but also creates a challenge for security teams tasked with staving off the cybersecurity threats they're facing. Defending against targeted attacks from cybercriminals and safeguarding the University of Münster's network is a daunting challenge for its small IT team. Yet, while other universities in Germany had to shut down essential systems and services due to ransomware attacks, the University of Münster stayed up, running and secure by relying on Forcepoint NGFW with IPS.

CUSTOMER PROFILE:
One of the largest universities in Germany with some 45,700 students and 7,100 employees, including 5,300 academics.

INDUSTRY:
Education

HQ COUNTRY:
Germany

PRODUCT:
Forcepoint Next Generation Firewall (NGFW)

Public organizations in Germany, and especially universities, are frequently targeted by cybercriminals looking to either deny and degrade services, steal personal data or intellectual property, or to extort money by interrupting educational activities. Unfortunately, specialized hacker networks and foreign organizations found universities a tempting target. These institutions often have modern, powerful and wide-ranging networks, enabling malware to spread very quickly, but the culture of open networks means that it is difficult to establish powerful security controls. Due to their prominence in research and development, universities also offer a rich trove of data, another attraction for bad actors. Over the last few years, multiple German universities have been forced to shut down large parts of their IT infrastructure for a period of time, leaving users with no access to email or remote connectivity.

This has caused massive disruptions in some cases and demonstrated how difficult it is to balance network freedom with the necessary security controls. The University of Münster, however, managed this very well. The IT team became aware of the risks early and has built up more than 15 years' experience of protecting the unprotectable.

The search for a new firewall and IPS leads to a solution that can handle more than 10 gigabits per second

Founded as a Jesuit seminary in 1588, the University of Münster plays a significant role in the city of Münster, the state of North Rhine-Westphalia, and German intellectual life. The university is housed in more than 300 buildings throughout the city and is home to the University of Münster Faculty of Medicine.

As one of the most prominent universities in Germany, the network security team always made security a priority. Since 2004, the university had an intrusion prevention system (IPS) and firewall in place, but in 2012 began looking for a new solution. They considered several vendors and went through proofs of concept with some of them. In the PoCs, Forcepoint (then known as Stonesoft) proved to be the most suitable solution.

One of the critical requirements was the need for an IPS that could handle the volume of traffic and speed the university required—more than 10 gigabits per second. The university has since upgraded their external internet connection to 30 gigabit per second and need to have full IPS protection on all that data without slowing traffic down. Forcepoint showed it could handle the load and after a successful proof of concept, the team moved forward with Forcepoint NGFW with systems integrator partner Avency.

The Forcepoint NGFW Security Management Center makes the grade

Today, the university has four NGFW firewall appliances in two clusters creating 6 virtual contexts. They've created secure network areas for the datacenter and workstations, voice over IP, guest and remote access services, internet of things, and internal management, and will soon add an area for administrative staff. Creating these separate virtual contexts allows the team to set custom security policies, rules and controls depending on the area's function and requirements. However, the IPS configuration is nearly the same across the contexts and nearly all traffic goes through the deep packet inspection engines..

Enabling the set up and easy configuration of the virtual contexts is Forcepoint's NGFW Security Management Center (SMC). "The SMC is one of the major benefits to the Forcepoint firewall solution—it was key to our decision to choose Forcepoint," said Guido Wessendorf, Head of Network Security. "It's very intuitive to configure and monitor the whole system."

"It was far better than the management tools of the other vendors we considered at that time," said Markus Speer, Head of Central Network Services.

Challenges

A culture of freedom for science and teaching means the network needs to stay open.

Required IPS for >10Gb internet traffic without slowing down.

Privacy rules prevent security controls on student, faculty and staff personal devices.

High profile ransomware attacks crippled other German universities.

Approach

Implement Forcepoint Next Generation Firewall with Intrusion Prevention System.

One of the ways the SMC makes managing the firewalls easier is via its API function. Forcepoint has built a robust community among the German universities in which security professionals connect and exchange tips and hints to best manage their Forcepoint firewalls. One of those tips was the usage of recommended IP blocklists—the user community exchanged scripts on how to import and install them via the Forcepoint API into the SMC. This led to University of Münster seeing 100 million discards (a firewall terminate or denial to malicious hosts) per day just due the IP block list, out of a total 150 million denials each day.

"With only a small team, we need systems that manage much of our daily activities automatically," Wessendorf said. "The import of the block list, automatic receiving of Forcepoint updates, and the intrusion prevention policies all help us manage our firewalls efficiently."

Even in an unusually difficult security environment, Forcepoint helps the University of Münster stay ransomware-free

Making the security situation even more challenging for the team is that a large number of the PCs, laptops, phones and tablets used by the students, faculty and staff are "user-managed" not "university-managed." This means that there can be no specific controls on the personal systems. Often firewalls will utilize HTTPs decryption to look into web traffic data packets and find malicious code, but it's not possible in this scenario because of privacy restrictions protecting personal PC usage.

During a normal study day, around 20,000 users are simultaneously connected with their own, unprotected laptops, tablets and smartphones to the university's WiFi network. Those devices and all the other approximately 30,000 registered university end systems could be infected with ransomware that needs to download additional keys or software in order to activate, but is blocked from doing so by the Forcepoint firewall solution.

"The IP block lists we imported along with the built in Forcepoint block lists, the Forcepoint Threatseeker Intelligence Network updates and the IPS functionality all work together to stop the attempts of malicious software on our systems to access command and control functions and establish ransomware locally," Wessendorf explains. "Therefore, we assume, we've had no ransomware situations yet, due to that fact."

A supportive university community delivers benefits to Forcepoint customers

When peers in similar security roles ask for a review of Forcepoint NGFW, "Normally I invite them to come to my desk and let them look at the solution," explains Wessendorf. "The SMC shows how easy it is to use, configure and manage—the demonstration speaks louder than words."

As one of the first universities in Germany to select and implement the Forcepoint NGFW, the longevity of the relationship also demonstrates the value. The university's network security team appreciates the ability to connect with the Forcepoint firewall product development team in Finland. "We have an open opportunity to share feature requests and give input into what we will require in the coming years," Speer said. "Having that direct contact and deep working relationship with Forcepoint is really an advantage."

In addition to the product itself, the support from Forcepoint and the community they've built around German universities using NGFW is unique. The members are all experts in using NGFW and the SMC so it's a very good resource, according to Wessendorf.

"I really have to say this kind of support and cooperation is unheard of in other university circles. It really produces benefits for its members," said Speer.

Results

- **150 million** firewall blocks of connections per day.
- No successful ransomware attacks.
- Part of a supportive German university community around Forcepoint network security.

"I really have to say this kind of support and cooperation is unheard of in other university circles."

MARKUS SPEER, HEAD OF CENTRAL NETWORK SERVICES

Forcepoint