Forcepoint

Customer Story

GNZ Securely Powers Research at Max Planck Society Institutes

Next-Generation Firewall helps the GNZ protect its high-speed network and the work of its scientists.

Lack of true centralized management for its Next-Generation Firewall (NGFW) led the Joint Network Center (GNZ) for the Max Planck Society to review other vendors in the market. Following a collaborative effort between the IT administrators in participating institutes, Forcepoint's NGFW emerged as the top solution due to its ease of use and comprehensive functionality. Now, the GNZ seamlessly secures the traffic of four institutions to support their ground-breaking research.

CUSTOMER PROFILE:
The Joint Network Center (GNZ) for the Berlin-Brandenburg Max Planck institutions is a regional IT competence center, located and managed at the Fritz Haber Institute. The group focuses on networking, data storage and IT security services. The GNZ supports all institutes and facilities of the Max Planck Society (MPG) in Berlin and Brandenburg.

INDUSTRY:
Education

HQ COUNTRY:
Germany

PRODUCT:
› Next-Generation Firewall

Protecting MPG Institutions from One Location

Since the academic foundation's inception in 1948, the Max Planck Society (MPG) in Germany has grown to accommodate roughly 25,000 scientists across over 80 institutions. The Joint Network Center (GNZ) for the Berlin-Brandenburg Max Planck Institutes is responsible for eight of these institutes, as well as some smaller facilities.

"We support around 10 percent of the scientists who belong to the MPG through our core work with networking, data management and IT security,"

GERD SCHNAPKA, HEAD OF THE GNZ

"Each institute has its own IT department—some smaller, some larger—and we all work together closely."

The GNZ maintains a high-speed connection for its scientists to meet the needs of their research, experiments, and other web-based projects. Additionally, the GNZ has to manage a separate policy for its guest network that provides open access to the internet on campus. The open research environment policy makes the MPG network a target for threat actors as members can work from their own devices.

As its previous firewall solution came up for renewal, the GNZ's Firewall Administrator, Robert Gruppe, learned that the GNZ's prices and hardware costs would rise too. Given that the platform didn't provide true centralized management across all institutes, Robert Gruppe, who is responsible for IT security at the GNZ, consulted with other vendors to find greater functionality and cost savings.

Seamless and Straightforward Migration

Forcepoint has been a longstanding member of the German educational community, with ties to many of the country's universities.

During a security day for universities' IT staff, a representative from RWTH Aachen spoke highly of Forcepoint's NGFW during a presentation. This, combined with a previous demo Robert Gruppe had taken part in years before, convinced the GNZ to explore Forcepoint's platform.

After carefully reviewing four other vendors, the GNZ chose Forcepoint's NGFW. The Security Management Center (SMC), which would allow Robert Gruppe and his colleagues to administrate across all institutions from a central location, and straightforward functionality made it an easy choice.

"We felt very comfortable with the user interface and the rule setup—even though we hadn't used it before, we were used to a similar kind of policy configuration and building in our firewall," Robert Gruppe said.

The GNZ expected to spend considerable time and resources migrating from its old platform to Forcepoint's NGFW, but the similarities in functionality made the knowledge transfer seamless.

"The migration was unbelievably easy. We gave our policies to our partner magellan and one day later, we received the complete set of policies."

ROBERT GRUPPE, GNZ FIREWALL ADMINISTRATOR

Challenges

- Maintain consistent network uptime across four sites.
- Find cost savings over previous vendor.
- Centralize management.
- Protect the high-speed network from infiltration and threats.

Initially, Robert Gruppe thought the GNZ might have to integrate Forcepoint in parallel with its old platform, which can often lead to issues with routing because there would be two gateways running at the same time. With the migrated policies in hand, Robert Gruppe's colleagues were instead able to focus completely on swapping out the old solution for Forcepoint's NGFW.

Stopping Threats and Saving Budget

The GNZ successfully deployed the NGFW across four institutions in less than two weeks. Downtime lasted only minutes, and nobody on the network realized there was a switch to a new firewall.

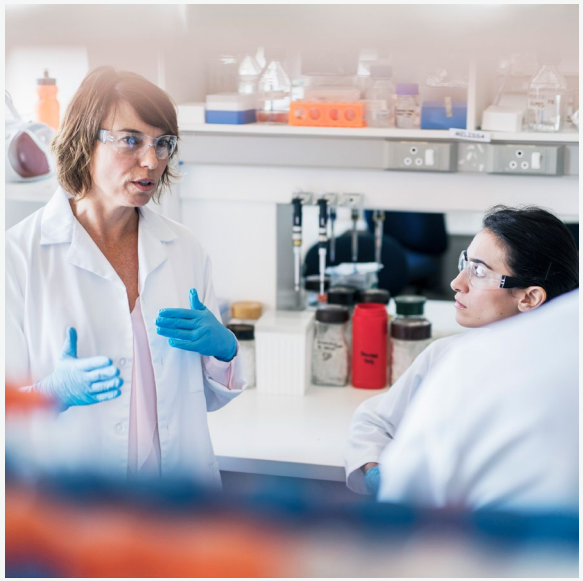
With the SMC, the GNZ can now easily add and manage from one location should more Berlin-Brandenburg MPG institutions adopt the NGFW.

Robert Gruppe has taken full advantage of the blocking functionalities, using a mix of private and public blacklists to block over 4 million IP addresses per day from accessing the network. Similarly, the NGFW also stops users from visiting roughly 10,000 blacklisted websites per week. This is especially valuable considering the institutions' Bring Your Own Device (BYOD) policies, where the GNZ cannot always apply protection to the devices connected to the network.

"Of course, any savings we find from our NGFW, we're able to give back to the scientists."

ROBERT GRUPPE, GNZ FIREWALL ADMINISTRATOR

The GNZ enjoys the strong support it receives from its partner magellan and Forcepoint. Due to quick vendor support and the supplying of new signatures, the GNZ was able to activate the integrated IPS functionality to mitigate Log4j exploitation. The IPS helps identify the attacks and automatically blocks the IP addresses of the threat actors.



Approach

- Deploy Forcepoint's NGFW.
- Leverage migration tool to automatically migrate policies from replaced solution.
- Attend two-day training with Forcepoint partner magellan on platform.

Results

- Successful NGFW migration completed in just two weeks.
- Block 4 million IP addresses daily and 10,000 malicious web addresses weekly.
- Seamless knowledge transfer due to similarity of platforms.
- Substantial decrease in planned downtime due to maintenance windows.
- Best cost-value ratio in comparison to other market-leading vendors.