Customer Story

BAYERNOIL Meets Strict German Regulations for Critical Infrastructure with Forcepoint NGFW

Bavaria-based oil refinery uses Forcepoint Next Generation Firewall from partner Software Symbiose to gain better visibility, improve network security management, support cloud applications and, most importantly, meet regulatory requirements.

Bavaria may be known for beer and brats and Oktoberfest, but BAYERNOIL is also a major regional producer of something not so tasty but arguably just as important: oil. Designated critical infrastructure ("KRITIS") by the German government, Bavaria-based refinery BAYERNOIL needed to upgrade its network security to meet the stringent performance and auditing requirements of the nation's Federal Office for Information Security (BSI). BAYERNOIL turned to Forcepoint and trusted reseller Software Symbiose to architect a security framework centered on Forcepoint NGFW to protect new cloud applications, provide network segmentation and improve reporting—all to comply with BSI and fuel its business.

CUSTOMER PROFILE:
Largest refinery in the Bavarian region, producing high-quality liquefied gases, fuels, petrol, jet, diesel, heating oil and bitumen from around 10.3 million tons of crude oil per year.

INDUSTRY:
Oil and gas

HQ COUNTRY:
Germany

PRODUCTS:
Forcepoint NGFW with Forcepoint One Endpoint

In Germany, energy companies, transportation, food processing plants and oil refineries are designated as critical infrastructure ("KRITIS" in German) that require sophisticated cybersecurity toolsets. Operators of critical infrastructure like oil refinery BAYERNOIL have to show the BSI that they can meet the standards specified by the 2015 IT Security Act including ISO 27001 under the country's National Strategy for Critical Infrastructure Protection, and report any security incidents to the BSI.

After Marcus Waatsack, Manager Information Technologies at BAYERNOIL, was presented with BSI's regulatory requirements for separated networks, high performance and granular auditing, he sat down to evaluate options with Franz Hermann, CEO at Software Symbiose, a trusted solution provider. Waatsack also wanted to transition part of BAYERNOIL's on-premises infrastructure to Microsoft Office 365 and Citrix File Services cloud-based applications. The network security architecture needed to evolve to deliver strong security and meet both regulatory and performance requirements.

Determining the path to comply with BSI's regulations and enable a hybrid cloud turned out to be an easy choice for Waatsack and Hermann. Several years prior, BAYERNOIL deployed Forcepoint Next Generation Firewall (NGFW) appliances as the foundation of its network security, so Waatsack was already familiar with its capabilities. BAYERNOIL decided to upgrade to the latest Forcepoint NGFW appliance with a unified endpoint solution, implemented by Software Symbiose. "Forcepoint's technology simply did a great job for our company, and we were convinced of its power," recalled Waatsack. "Why should we change the firewall when our people were trained and we believed in the technology? We were confident Forcepoint was the right choice to solve our current and future challenges."

One endpoint allows for a people-focused perimeter

Right out the gate, BAYERNOIL quickly executed a pilot to install Forcepoint One Endpoint agents on several client systems connected to the new Forcepoint NFGW appliance; the BAYERNOIL team then observed logs and adjusted policies through the Forcepoint Security Management Center (SMC). One Endpoint provides visibility into applications and devices attempting to connect to BAYERNOIL's network and the internet through the Forcepoint NGFW. The endpoint identifies users through information delivered to NGFW, so access can be managed by group membership, rather than specific IP address, regardless of where users log on from. As BAYERNOIL adds new Forcepoint security capabilities, they can leverage the One Endpoint to connect to additional solutions.

Forcepoint's SMC also enabled a seamless transition from the previous network security platform to the new one: Waatsack's team could swap out hardware while the system was running, simply update policies for authorized user groups and actions, and restrict unsafe URLs and apps. The Forcepoint NGFW automatically distinguished between an allowed browser or application and blocked unauthorized software from executing or connecting on BAYERNOIL's network.

"The upgrade from the Forcepoint NGFW 1000 Series to the 3000 Series appliance went off better than expected," said Waatsack. "We were able to take advantage of Forcepoint's high availability features to install one firewall node at a time in an active/active cluster and completely replace the hardware without any network downtime."

Challenges

Comply with German IT and security policies for critical infrastructure.

Support migration to cloud applications.

Establish network segmentation and network zones.

Meet mandated auditing requirements.

Approach

Deploy Forcepoint NGFW.

Segmentation for improved security and compliance

Besides granular visibility, the NGFW SMC also made it easy for Waatack's team to segregate networks to keep up with KRITIS and ISO 27001 as required by the government. Forcepoint NGFW allows administrators to divide BAYERNOIL's network into separate segments with different access credentials. Because data traffic and user access are physically separated, Forcepoint increases the protection levels and keeps bad actors from running rampant through the network, even if one segment is breached.

Forcepoint SMC controls also help Waatsack's team meet audit requirements–the security analysts can pull reports to show that network segmentation is enforced and fulfill required checkpoints for incident management on a weekly, monthly or quarterly basis when needed.

"Reporting has become very important for us during the audit process," said Waatsack. "We've never been able to separate data traffic and users physically from our network before, and now we are able to and can meet the BSI's strict policies. The usability is really key. We need software that that's easy to use so we can accomplish and then maintain our goals."

Taking strides on the journey to the cloud

The upgrade in NGFW performance not only raised the bar for security, it also helped the company seamlessly move some applications that were strictly on-premises to the cloud, including the transition to Office 365. As Microsoft dynamically updated its IP addresses and domain names as part of Office 365 application services, the Forcepoint NGFW could keep up with ease.

"The granular control is a necessity," observed Waatsack. "In the past, we could not support Microsoft apps like Teams because the challenge was maintaining communication with Office 365 resources that constantly cycled for security reasons. That's all changed for the better, because Forcepoint NGFW meets us at the intersection between the networking and security requirements of the cloud application and user. We can ease some restrictions to keep our employees productive but still be safe and secure."

Future-proofing with Forcepoint cybersecurity

Forcepoint is helping BAYERNOIL get ready for a hybrid cloud future. According to Herrmann, Forcepoint offers BAYERNOIL a completely novel approach to cybersecurity, one that integrates network security, data loss prevention (DLP), web security and cloud access security broker (CASB) to deliver a holistic solution that is ready for greater expansion into secure cloud services.

"Forcepoint understands our needs are pretty simple: get applications up fast and keep them running," summarized Waatsack. "With our current hybrid cloud strategy, we need our security partners to help us focus on how we can future proof BAYERNOIL with capabilities down the road like CASB, DLP or Dynamic Edge Protection. This is a road we can feel confident traveling on with partners like Forcepoint and Software Symbiose."

> "Forcepoint understands our needs are pretty simple: get applications up fast and keep them running."
>
> **MARCUS WAATSACK,** MANAGER INFORMATION TECHNOLOGIES

Results

- Physically separated network segments to limit data traffic and access only to authorized users.
- Leveraged unified endpoint to streamline intelligence on users, apps and access on the network.
- Improved network performance to enable cloud services for the first time.
- Created verifiable audit trails supported by automated reporting.