Forcepoint

Customer Story

Industry-leading Medical Device Company Imagines a Secure Future For its Networked Devices

Forcepoint Next Generation Firewall delivers more stable, effective, and flexible security for Internet of Things medical devices.

When this global leader needed a way to keep its internet-connected medical imaging devices secure from cyber-infection and malicious attacks, Forcepoint provided an innovative solution: next-generation firewalls that deliver stable, easily updated, and centrally managed security for thousands of devices doctors and patients rely on every day around the world.

CUSTOMER PROFILE:
Innovative medical device company with more than 120 years of experience offering medical imagining, laboratory diagnostics, and advanced therapies.

INDUSTRY:
Manufacturing

HQ COUNTRY:
Germany

PRODUCT:
Forcepoint Next Generation Firewall (NGFW)

Medical imaging has come a long way since German physics professor Wilhelm Röntgen discovered the medical use of X-rays when he captured a picture of the inside of his wife's hand in 1895. Today, diagnostic medical imaging devices like computed tomography and magnetic resonance imaging help enable early and precise diagnosis without invasive surgery. To provide optimal care for patients, the large amount of data generated has to be shared quickly, accurately, and safely throughout the healthcare ecosystem.

Unfortunately, this connectivity opens the door to risk of cyber-infection. The U.S. Department of Homeland Security recently warned that medical imaging files could be used for transmitting malware. And in a new report detailing cyberattacks on medical imaging devices, researchers at the Ben-Gurion University of the Negev Malware Lab noted that attackers could hack a computed tomography device and cause "severe damage" to a patient.

Or, as Forcepoint Account Manager Frank Limberger explained: "Imagine a doctor doing open-heart bypass surgery by viewing the live output of a medical imaging device. If there were an attack during such an operation, it would be catastrophic."

> "Imagine a doctor doing open-heart bypass surgery by viewing the live output of a medical imaging device. If there were an attack during such an operation, it would be catastrophic."
>
> **FRANK LIMBERGER,** FORCEPOINT ACCOUNT MANAGER

A Germany-based leader and visionary innovator in the medical devices industry faced this critical challenge when it needed to find a solution that would keep thousands of imaging devices worldwide secure. Forcepoint proposed a solution as innovative as the company.

An innovative security solution for a visionary company

In order to protect the connected medical imaging devices it sells, the company provided third-party anti-virus endpoint security software running on Windows operating systems. However, over time, that software was no longer supported on legacy operating systems used by the machines. Updating or changing any software on the devices themselves is difficult, time-consuming, and opens the door to risk of machine downtime and failures. Yet the company needed to provide alternative protection against infection to its customers.

When Forcepoint's Limberger heard about the challenge, he proposed an innovative solution: placing a Forcepoint Next Generation Firewall (NGFW) on the network in front of each connected medical device. This would provide comprehensive protection against cyberthreats but wouldn't require the installation of new operating systems or endpoint security on the machines themselves. The company was intrigued, but, as part of its due diligence, also evaluated two other security vendors. The company's technical support team, with the approval of the customer service team that needed to ensure customer satisfaction, confirmed that Forcepoint was the right choice.

Challenges

Deliver solution to protect critical internet-connected medical devices from cyber threats, without requiring changes to the device software.

Approach

Install Forcepoint Next Generation Firewalls between devices and the internet.

Forcepoint NGFW proves itself the most stable, most effective, and easiest to manage

Third-party validation and a proof of concept (POC) demonstrated that Forcepoint NGFW best fit the company's list of requirements. First, no time outs are acceptable for these devices; the firewall could not go down and interrupt imaging device activity in the middle of a procedure or while sharing images or data with the network. During the POC, the technical support team found Forcepoint NGFW the most stable—a competitor firewall crashed and never came back up, while the Forcepoint firewall was able to restart on its own. This stability is especially critical for remote hospital locations with no technical staff to troubleshoot locally, or even regionally.

Next, the team was impressed with the security effectiveness as demonstrated by NGFW's recommendation by the independent agency NSS Labs for the seventh year in a row. The NGFW Security Management Center was another deciding factor: the centralized management portal allows the company to manage all firewall appliances easily from one console and remotely update them quickly as needed to keep pace with security threats. As there would be thousands of firewalls in the systems eventually, this manageability was critical. Finally, NGFW's "zero-touch" deployment means firewalls can be sent to hospitals, plugged in, and activated by hospital staff, without requiring end customer technical staff or a company technician onsite for complicated install processes.

The potential to secure hundreds of thousands of devices on the Internet of Things

The company has begun offering the upgraded/extended security service for 7,000 MRI devices running on Windows XP. In fact, it has prioritized the project, adding a dedicated customer service team that conducts tests, proofs of concept, and training. Going forward, the company expects to expand the offering to 27,000 tomography devices running on Windows 7.

And this innovative use of NGFWs isn't limited to just medical devices; the concept can easily be expanded to other industries. "There are hundreds of thousands of IoT machines with legacy Windows systems, and the question is how you can secure those," explained Limberger. "The firewall doesn't care if it's a medical instrument or an elevator, but the business need, the pain point, is always the same."

> "The firewall doesn't care if it's a medical instrument or an elevator, but the business need, the pain point, is always the same."
>
> **FRANK LIMBERGER,** FORCEPOINT ACCOUNT MANAGER

Results

- Easy rollout, centralized management, and updates of globally dispersed firewalls, allowing extended cyber protection for thousands of MRI devices.
- Potential to guard hundreds of thousands of Internet of Things medical devices.