Forcepoint

Customer Story

HUBER+SUHNER Builds a Layered Network Defense to Safeguard Critical Data

HUBER+SUHNER, a global leader in connectivity solutions, is navigating the complexities of digital transformation while safeguarding its most valuable asset: **data.** With operations spanning defense, transportation and medical sectors, the company faces a unique challenge—balancing innovation with rigorous data security and compliance.

Christian Keller, Chief Information Security Officer (CISO) at HUBER+SUHNER, is leading the company's transformation into a cybersecurity-forward organization. With a background in next-generation firewalls and decades of experience in IT security, Keller brings a strategic vision to one of Switzerland's most established industrial companies.

HUBER+SUHNER

CUSTOMER PROFILE:

A global provider of high-performance connectivity solutions for communication, transportation, and industrial applications.

INDUSTRY:

High-tech manufacturing (Cables, Connectors, Antennas)

HQ COUNTRY:

Switzerland

PRODUCT(S):

- Forcepoint Next-Generation Firewall (NGFW)
- Forcepoint SD-WAN

The Challenge: Complexity and Compliance

As a global manufacturer operating in highly regulated sectors including defense, transportation and medical, HUBER+SUHNER manages a uniquely complex data environment shaped by diverse and evolving compliance requirements.

The company protects a broad spectrum of sensitive information, from proprietary engineering designs and regulated industry data to operational infrastructure, employee credentials and insider activity. This globally distributed and highly varied data landscape demands a robust, adaptive security strategy to ensure confidentiality, integrity and compliance at scale.

> "We needed more than just compliance, we needed clarity, control and confidence in how our data is handled. Forcepoint gave us all three."

— Christian Keller, CISO

This complexity is compounded by the rapid pace of regulatory change. New data protection laws, export controls and industry-specific mandates are introduced frequently across jurisdictions, making it difficult to maintain a consistent and compliant security posture.

> "Some new regulations, some new sensitivities and new classification… pop up nearly every day."

— Christian Keller, CISO

The Strategy: A Multi-Layered Approach to Data Security

To address this, HUBER+SUHNER has adopted a risk-based approach to compliance. The company focuses on identifying and protecting the most critical assets first, enabling a more strategic and efficient approach to data security.

> "We don't have enough resources for tagging all of those, so we look for which is the highest risk for our company."

— Christian Keller, CISO

This prioritization is essential in a landscape where the volume of data is growing exponentially, and the threat surface is expanding. The company's strategy involves continuous monitoring of regulatory developments, close collaboration with legal and compliance teams and the use of automation and artificial intelligence (AI) to support classification and risk assessment.

Moreover, the challenge isn't just external. Internally, the company must manage the tension between innovation and control. Engineers and developers often create "shadow IT" systems—unofficial tools and platforms designed to accelerate innovation—which can inadvertently introduce security vulnerabilities

> "Most of the things they want to look [for] are new technologies, new ways to work… like shadow IT or shadow systems… which is going to be innovative. But this also causes a threat to the company, to the security posture."

— Christian Keller, CISO

This dual pressure, from both regulatory bodies and internal innovation, demands a flexible, intelligent and deeply integrated data security strategy.

HUBER+SUHNER's approach is to build a unified framework that can adapt to evolving requirements while enabling the business to move forward with confidence. HUBER+SUHNER's cybersecurity strategy is built on a layered defense model that integrates advanced technologies, adaptive policies and human-centric processes. This approach ensures that the company can respond to evolving threats while maintaining operational agility and regulatory compliance.

Forcepoint NGFW and Forcepoint Secure SD-WAN

To support its global cybersecurity strategy, HUBER+SUHNER relies on two foundational technologies from Forcepoint: NGFW and Secure SD-WAN.

Forcepoint NGFW for Deep Visibility

HUBER+SUHNER has deployed Forcepoint NGFW to gain deep, contextual visibility into network traffic and enforce granular, content-aware policies around data access.

These firewalls go beyond traditional perimeter defenses by inspecting the actual payload of communications, allowing the company to detect threats that might otherwise bypass conventional filters. This is particularly important in a hybrid environment where cloud services, remote work and legacy systems coexist.

> "Even if the communication is legitimate by source and destination, the data transferred might still be malicious."

— Christian Keller, CISO

Keller emphasized the operational advantages of Forcepoint's clustering and high availability features:

> "The biggest benefit was the reliability and the possibility to cluster in a way that nobody else can do… we don't even need a maintenance window for updates."

– Christian Keller, CISO

This ensures continuous protection without disrupting business operations, even during upgrades or configuration changes.

Forcepoint NGFW: These firewalls provide deep packet inspection, application-level visibility and adaptive policy enforcement. They allow HUBER+SUHNER to detect and block threats based not only on source and destination but also on the content and behavior of the data itself. The NGFWs are also praised for their clustering capabilities and seamless updates, which ensure high availability without disrupting operations and minimizing data threats.

> "It's not just who's talking to who, it's also what they're talking and what is the content of the data."

Secure SD-WAN for Global Flexibility and Performance

To support its decentralized operations and improve connectivity across 45+ global sites, HUBER+SUHNER implemented Forcepoint Secure SD-WAN. This technology allows the company to dynamically route traffic based on performance, security, and compliance needs.

> "We changed our strategy from a centric to a de-centric localization… spreading it across continents where connectivity is more reliable."

The Forcepoint Secure SD-WAN architecture integrates seamlessly with the company's firewall infrastructure, enabling consistent policy enforcement across both physical and cloud environments. It also reduces latency, improves application performance and enhances the user experience for remote and distributed teams.

This shift has allowed HUBER+SUHNER to modernize its IT infrastructure without compromising on security or compliance, even in regions with strict data residency requirements.

Forcepoint Secure SD-WAN: This solution enables HUBER+SUHNER to transition from a centralized IT infrastructure to a decentralized, globally distributed model. By dynamically routing traffic based on performance and security needs, Secure SD-WAN ensures consistent policy enforcement across all locations—whether on-premises or in the cloud—while improving connectivity and reducing latency.

Together, these tools form the backbone of HUBER+SUHNER's secure, scalable and resilient IT environment.

The Outcome: Resilience Through Visibility and Agility

By implementing a layered, intelligence-driven security strategy supported by Forcepoint NGFW and Secure SD-WAN technologies, HUBER+SUHNER has achieved measurable improvements in both operational efficiency and cyber resilience.

The company's security team now has the tools and visibility needed to proactively manage threats, enforce compliance and support innovation across a globally distributed infrastructure. What was once a reactive, resource-intensive process has evolved into a streamlined, strategic function that empowers the business rather than slowing it down.

HUBER+SUHNER's strategy has delivered:

- → Greater visibility into network and data flows, enabling faster detection of anomalies and better understanding of system behavior.
- → Faster response to emerging threats, through real-time inspection, adaptive policies and AI-assisted threat detection.
- → A scalable, flexible infrastructure capable of supporting decentralized operations and cloud integration without compromising control.
- → A culture of security awareness , driven by employee training, cross-functional collaboration and security-by-design principles.

> "We gained so much visibility... and better understanding with really low amount of resources."
>
> – Christian Keller, CISO

These outcomes not only strengthen HUBER+SUHNER's security posture but also position the company to innovate with confidence—knowing that its data, systems and people are protected by a modern, resilient cybersecurity foundation.

Conclusion

HUBER+SUHNER's cybersecurity journey demonstrates how an industrial company can evolve into a digitally resilient enterprise. By strategically integrating Forcepoint NGFW and Secure SD-WAN technology, the company has built a security architecture that is not only robust but also agile enough to support global innovation.

Forcepoint's solutions have empowered HUBER+SUHNER to gain deep visibility into their network, enforce adaptive security policies and decentralize their infrastructure without compromising control. These capabilities are critical in a world where data volumes are exploding, threats are becoming more sophisticated and compliance demands are constantly shifting.

> "There is no 100% security... so we need to focus our effort on the crucial points."
>
> – Christian Keller, CISO