opensystems

WHY FRANKE COMBINES MEP WITH ZTNA
FOR SECURE REMOTE ACCESS

"
The managed service not only relieves us of work, but also gives us flexibility and scalability.
"

Ronny Hammel, Team Leader of the Global Network Services team, Franke

FRANKE

SUMMARY

Franke is a leading global provider of solutions for domestic kitchens, foodservice, convenience stores, and professional coffee making with nearly **8,000 employees across 60+ sites worldwide**. As security demands grew, its legacy remote access setup became unsustainable. To ensure secure, high-performance access for users worldwide, Franke implemented a managed **ZTNA and MEP solution** – reducing complexity, boosting transparency, and supporting global operations with minimal overhead.

CUSTOMER DETAILS

- Manufacturing
- Aarburg, Switzerland
- 5 continents
- 7,000+
- franke.com

PRODUCTS USED

- ZTNA
- MEP
- SD-WAN

RESULTS

100%
VISIBILITY
of user access via
Open Systems Portal

~90%
REDUCTION
in manual
troubleshooting

24x7
GLOBAL SUPPORT
via Open Systems'
Mission Control

~3500
INTERNAL USERS
on MEP

400
EXTERNAL USERS
on ZTNA

We recently sat down with **Ronny Hammel, Team Leader of the Global Network Services team at Franke**, to discuss the company's past challenges and goals, and how Open Systems provided a comprehensive solution.

CAN YOU DESCRIBE YOUR ROLE IN THE COMPANY – PARTICULARLY IN RELATION TO NETWORK SECURITY?

As Team Leader of the Global Network Services team at Franke, my team and I are responsible for global SD-WAN operations, supported by Open Systems. We oversee everything from firewalls to global WiFi and remote access.

The latter has become an increasing challenge for manufacturing companies in recent years, as it involves managing access not only for internal employees but also for external suppliers in the supply chain who require tightly regulated access to our resources. With growing regulatory requirements, this has also become a compliance issue.

WHAT WERE THE KEY REASONS FOR IMPLEMENTING MEP AND ZTNA – AND WHICH SPECIFIC CHALLENGES WERE YOU AIMING TO ADDRESS?

Franke's decision to adopt MEP and ZTNA from Open Systems came in direct response to recurring issues with our previous MEP solution. Critical security vulnerabilities repeatedly emerged, often requiring urgent patching during evenings or off-hours. For our small internal team, this constant "firefighting" became unsustainable. When the end-of-life for the old solution was brought forward, we needed a reliable replacement – and fast.

While we provide broad network access to internal users, including remote employees, we want to give external users highly restricted, regulated access. The challenge: these external users are globally dispersed – across Europe, the U.S., South Africa, India, China, and South America. To reduce the team's workload, we previously used only a few central access points. This simplified maintenance but negatively impacted performance.

The combined ZTNA and MEP solution offers local access points to users, which, while not a direct security concern, led to a noticeable performance boost.

Currently, MEP is used for internal users – around 3,000 to 4,000 colleagues worldwide. A smooth transition was crucial, and MEP was ideal in this regard: a near one-to-one replacement for the previous solution, requiring minimal changes for end users.

ZTNA, on the other hand, was rolled out specifically for around 400 external users – set up correctly from the start and fully managed by Open Systems. The zero-trust approach is not a one-off project but an ongoing journey, which makes it even more important to establish a scalable and future-proof ZTNA foundation right from the beginning.

In a global enterprise, one-size-fits-all solutions don't work. Some regions require tailored approaches and flexibility. For example, in some countries, we deployed ZTNA directly for colleagues with managed devices, as alternative solutions weren't feasible under the given conditions.

The close collaboration with Open Systems and the ability to combine solutions were critical: together, we found a solution that could be implemented quickly – without disrupting ongoing operations.

And we're already looking ahead: in the long term, Franke is considering a gradual shift from MEP to ZTNA internally as well – based on clean inventories of applications, devices, and users. The groundwork for this transition is already in place.

WHY DID FRANKE CHOOSE OPEN SYSTEMS?

We've been working successfully with Open Systems for several years in the area of managed SD-WAN – and especially when it comes to complex, global network and security topics, Open Systems has proven to be a reliable partner. In addition, Franke also handles all firewalling in collaboration with Open Systems.

> ## "The Zero Trust approach is not a one-time project, but a continuous process – which makes it all the more important to establish a scalable and future-proof ZTNA foundation from the start."

The consistent service quality stands out at every level – from a dedicated account team that knows our infrastructure inside and out, to Mission Control, the global support team that is available 24x7.

In the past, we attempted to implement a MEP solution in-house – but the effort was simply too high. It would have required building up new expertise and tying up resources that we needed elsewhere. Whenever something went wrong, someone could end up being blocked for days – which is nearly impossible to manage with a small team, especially when dealing with globally used IT services like remote access. In this case, 24x7 service and support are essential. The managed service from Open Systems not only relieves this burden but also provides us with the flexibility and scalability we need.

Another advantage: since we already had well-distributed SD-WAN infrastructure in place globally, ZTNA didn't require new hardware. This helped save costs, accelerated the rollout, and simplified ongoing operations – especially crucial given the time pressure we faced.

Ultimately, it was also the seamless integration of the MEP and ZTNA solutions into our existing SASE ecosystem that sealed the deal. Everything comes from one provider – reducing complexity and boosting efficiency.

HOW DID THE IMPLEMENTATION GO?

The implementation was focused, efficient, and smooth – exactly what we've come to expect from Open Systems. Our Technical Account Managers know both our infrastructure and team very well, which makes the collaboration incredibly effective. Even after hours, there's always someone available who takes care of things. The support isn't just technically strong – it's also reliable and committed, which truly makes a difference for us.

Whenever there were questions or minor issues, we could simply pick up the phone – direct communication made everything much easier.

We also value Open Systems' hands-on approach and their quick response times, especially when security vulnerabilities emerge. Not having to manage this ourselves has been a huge time-saver.

The rollout itself happened in two phases: first, the solution was rolled out and the most important requirements were implemented. Then we entered a collaborative fine-tuning phase – in close, constructive collaboration between our team and Open Systems to tailor the solution precisely to our specific needs.

WHAT POSITIVE EXPERIENCES OR INSIGHTS DID YOU GAIN DURING THE PROJECT?

One of the biggest surprises for us was how fast and flexibly Open Systems responded to our requirements – even in challenging scenarios like operations in China.

With the sudden end-of-life of our previous solution, we were under enormous time pressure to find and implement a new solution quickly. We had expected a long gap between contract signing and rollout – especially since we went through a formal tender process.

Instead, we were able to move directly from the proof of concept into live operation. Open Systems demonstrated impressive agility here, which helped us tremendously in staying on schedule. Not only did the initial rollout go smoothly, but the ongoing collaboration has also been highly cooperative and solution-oriented.

A particularly notable example was the implementation in China. Initially, performance there was limited because all traffic was routed through the Singapore hub. Open Systems responded quickly and deployed a local solution within just a few days – leveraging our existing SD-WAN infrastructure, including the setup of a hub in China. This kept all data traffic within the country, avoiding issues with the Great Firewall. The turnaround was remarkable: identified on Friday, resolved by Monday. Since then, the ZTNA performance in China has been stable.

And perhaps the best part: our users barely noticed the switch. Despite the rapid rollout, there was no negative feedback – a clear sign of how cleanly the technical transition was executed.

HOW HAS NETWORK TRANSPARENCY AND YOUR CONTROL OVER USER ACCESS CHANGED WITH ZTNA AND MEP? WHAT IMPROVEMENTS HAVE YOU SEEN?

We've seen clear improvements in transparency, performance, and a significant relief in our day-to-day operations.

Performance

End-user performance has improved substantially, as we now theoretically have 90 access points worldwide – meaning MEP and ZTNA access is much closer to the end users.

We received very positive feedback from locations in South Africa and South America, where we now have access points for the first time – something that simply wasn't available before.

The biggest benefit, however, is that we don't have to worry about it anymore. We no longer need to check vendor websites every morning to see if new vulnerabilities have been announced, and then rush to patch vulnerabilities. Open Systems monitors everything for us and acts quickly and reliably when needed.

Visibility

The Open Systems customer portal shows us exactly who logged in, when, and how – providing critical and much-needed visibility. While we could technically extract similar data before via Syslog, Microsoft Sentinel, and other tools, it was far more cumbersome and time-consuming. The integration of this functionality into the Open Systems Portal has significantly simplified troubleshooting.

> " We sleep better and start our days more relaxed – Open Systems has definitely lifted a weight off our shoulders. "

Operational Relief

With the old solution, dealing with constant vulnerabilities often felt nerve-wracking – every morning started with checking the news and hoping no new critical issue had emerged that required immediate patching. Often, as soon as one was resolved, the next would appear.

Now, we can easily monitor our security posture via the Open Systems Mission Control Portal. If a vulnerability does arise, it's handled transparently and quickly. We sleep better and start our days more relaxed – Open Systems has definitely lifted a weight off our shoulders.

Time Savings

We've also achieved significant time savings in daily operations. Previously, we managed five to six security gateways on our own. Patching and testing each one used to take about two hours per device. Today, we benefit from around 190 security gateways across approximately 90 locations worldwide – all managed by Open Systems. This means that maintenance effort on our side has dropped to zero. As a result, we now have noticeably more time to focus on strategic tasks.

opensystems

A FINAL **SUMMARY**

THE CHALLENGE

As a global company with growing security demands, Franke needed more secure, high-performance access for its nearly 8,000 employees across 60+ sites worldwide.

THE SOLUTION

A fully managed ZTNA and MEP solution from Open Systems, reducing complexity, boosting transparency, and supporting global operations with minimal overhead.

THE RESULTS

✓ **Significant reduction** in manual troubleshooting

✓ Reduced complexity through **managed services**

✓ Clear **visibility** of user access

✓ 24x7 **global support**

About Franke

With its three divisions, Franke is a global leader in products and services for domestic kitchens, system catering, the convenience store sector, and professional coffee preparation. Operating through more than 60 companies across five continents, nearly 8,000 employees continuously explore new perspectives to identify opportunities and turn them into inspiring, innovative solutions to meet the challenges of tomorrow.

opensystems

Open Systems provides Managed SASE solutions that combine networking and security functions on a cloud-native platform, securely connecting hybrid IT environments for greater efficiency, enhanced security, and maximum scalability.