

Swiss Appliance Innovator Franke Turns to Ontinue for 24/7 Cybersecurity



Protecting an innovative company and its data and assets was the goal of Victor Andreu, Chief Information Security Officer for Franke, a smart systems supplier for residential kitchens and professional food services.

Franke's coffee systems are well known in retail and workplace locations, with the company providing digital services for real-time data that provides operational and commercial transparency. These connected systems can share data across multiple sites and regions, giving customers control, with all the data in one central place.

And wherever data exists, there are potential threats – requiring detection and response. Andreu wanted to enhance the company's threat detection capabilities and move from a traditional protection and prevention paradigm to become more proficient at detecting and responding. And he knew they needed to collaborate with a managed detection and response (MDR) service provider.

"My strategic objective is to safeguard Franke assets and reputation by remaining agile and supporting the business," says Andreu.

Andreu wanted to add more professional rigor and proficiency to detecting and responding to cyber threats. Adding a 24/7 professional security operations center (SOC) was another goal, but he knew building the competency internally would be much more



Motivators

- Needed a service to protect Franke's assets and reputation
- At the same time, enable the business and remain agile

Solution

- Enhanced detection capabilities
- Actionable threat intelligence
- Expertise on Microsoft technology already in use

Outcomes

- Enables research-based decisions on threats that pose risks
- Retains data and logs in Franke's environment
- Improves visibility and response time
- Provides 24/7 SOC coverage

About Franke

As a manufacturer and supplier of smart systems and appliances for residential kitchens, professional food services, and coffee preparation, Franke was founded on innovative engineering, unique design, and outstanding Swiss quality. That same emphasis on quality extends to the company's approach to its security decisions. Started over 100 years ago in Switzerland, Franke is world-renowned, with more than 60 subsidiaries in about 40 countries.

challenging – and costly. And finally, he sought actionable threat intelligence so the Franke team could act quickly on potential threats.

In addition, as an Open Systems SASE+ customer, Franke had relied on Open Systems for their secure access service edge to protect the network, so adding Open Systems MDR+ – now Ontinue ION – for managed detection and response had other benefits. “We saw that there were very good synergies for us to have the MDR and SASE services under the same service provider. This was fundamental for us,” Andreu says.

Franke was able to fully leverage its existing SASE infrastructure and combine it with their Microsoft security technology, which was optimized by the Ontinue ION managed extended detection and response (MXDR) service.

“We wanted a vendor who could adapt to our needs, operate on a 24/7 basis, and keep our logs and our data in our Franke environment, and Ontinue provided everything we were looking for,” Andreu recalls.

Maximizing the Microsoft Tools

Since Franke’s ecosystem is Microsoft based, it was important to have the MDR service provide insights on the tools Franke already had in place and was using. “It was extremely important that there was a close partnership between our MDR service and Microsoft – and Ontinue provided the Microsoft know-how,” says Andreu.

Leveraging Franke’s existing infrastructure combined with the Microsoft security technology allows the Ontinue Cyber Defense Center to provide not just alerts, but qualified outcomes. Franke gets actionable feedback they can ingest into their processes and procedures, which helps the risk posture improve over time. Franke’s security specialists can then focus on protecting their business, users and applications. “With Ontinue, we are now better equipped to respond to incidents in a systematic, consistent, and professional manner,” Andreu says.

Driving Decision-Making for Better Outcomes

Time is a critical factor when responding to a cyberthreat. And by working with Ontinue, Andreu notes that the speed of response to threats has increased significantly.

“Franke has established best-in-class and faster incident response because they’ve connected the managed service to the individuals who are responsible for responding to the incidents,” Andreu says. “Ontinue has delivered on its promise and has helped us to remain agile and enhance our existing protection against key risks.”

The key result: Andreu says the organization has greatly improved its security posture.

“I can say I sleep better at night,” he says. “Today, we have a more professional service, with 24/7 support and we have faster decision-making thanks to the threat intelligence we are getting from Ontinue.”

For Andreu, it was important to find a vendor that could not only solve their problems, but take a collaborative approach, as well. He experienced this with the Ontinue team, and he valued the open discussions that occurred between the two companies and praised the “learning mindset” that everyone demonstrated throughout the process. “We both want to improve and make the service better,” says Andreu. “There’s a spirit of partnership and collaboration that we highly appreciate.”

As Andreu sums up his experience: “If you want to work with a partner, instead of just a vendor, and if you want really to build collaboration, a fast MDR service, you can’t go wrong by working with Ontinue. I would strongly recommend them.”

“ If you want to work with a partner, instead of just a vendor, and if you want really to build collaboration, a fast MDR service, you can’t go wrong by working with Ontinue. I would strongly recommend them.”

Victor Andreu
Chief Information Security Officer
Franke



About Ontinue ION: Nonstop SecOps

Ontinue ION is AI-powered MXDR that accelerates mean time to resolve and lowers security total cost of ownership while driving smarter proactive prevention for Microsoft security customers. Only ION localizes managed protection to your environment using proprietary AI and dedicated Cyber Advisors and streamlines daily SecOps collaboration using Microsoft Teams.