CUSTOMER STORY

Infors effortlessly defends against cyber threats with Ontinue.

Infors HT has been developing and producing high-tech solutions for biotechnology for almost 60 years. The portfolio includes bioreactors, incubator shakers and the appropriate software for controlling bioprocesses. The family-run company, which has since become a public limited company, has sites in numerous countries in North America, Asia and Europe and is headquartered in Bottmingen, Switzerland. A special characteristic of the company is its employee and customer-oriented approach. Flat hierarchies foster a welcoming atmosphere for innovation and optimization suggestions. At Infors HT, our team comprises not only engineers skilled in valve construction but also seasoned scientists specializing in operational research. This diverse expertise ensures we understand customer needs and can effectively address their challenges.

What has changed drastically at Infors HT since it was founded in 1965 is the digital infrastructure. Over the years, the maturity of IT has steadily increased – and with it, its complexity. Today, around 90 percent of the IT infrastructure is in the cloud, while the company relies entirely on Microsoft technologies for its application software. As a global company, it goes without saying that Infors HT has networked its locations around the world with a very extensive WAN (Wide Area Network) infrastructure.

Challenges

- Establishment of a genuine Security Operations Center (SOC)
- 24/7/365 monitoring of the IT infrastructure
- Freeing up time for internal audits and IT administration

Solution

- Implementation of a holistic, Microsoft-based security infrastructure
- Outsourcing the monitoring of security tools to the Cyber Advisors and Cyber Defenders of the MXDR service Ontinue ION

Business Outcomes

- Consistent monitoring and first response by Ontinue – around the clock
- Better integration of in-house first-level support into the security processes
- Close cooperation between Ontinue and Infors HT via Microsoft Teams
- Holistic protection of the IT infrastructure
- The significant increase in employee time allocation provides ample opportunities to conduct internal audits and enhance security measures.

About Infors HT

Infors HT has been developing and producing high-tech solutions for biotechnology for over 55 years. The company is proud to be one of the best specialists in bioreactors, incubator shakers and bioprocess control software. Infors HT is committed every day to simplifying its customers' work processes using state-of-the-art technologies. To this end, the company involves its customers directly in product development and thus designs practical products, software solutions and services that not only deliver what they promise on paper but also in challenging everyday life.

"We are a family business, and you can see that in the way we treat each other," emphasizes René Schröder, the main person responsible for IT security. "And of course, I want to protect my company like my family – in this case from cyberattacks such as hacking or phishing attacks."

To enact this initiative, the IT team at Infors HT established a compact "Micro Security Operations Center" dedicated to managing alerts and incidents originating from Microsoft Defender and Sentinel tools. "Unfortunately, we quickly realized that we couldn't process all incoming alerts. At some point, we only concentrated on the high alerts and tried to automate the smaller alerts," Schröder continues. "To be honest, however, we lacked the know-how to really make full use of the tools available to us." What Infors HT needed were real cybersecurity specialists who had undergone specific further training in this area. The IT department's workload meant that it was out of the question to do this themselves and build up the necessary expertise to the full extent. Engaging a provider for Managed Extended Detection and Response (MXDR) emerged as the most prudent course of action.

A Security Package from a Single Source

When looking for the right provider, one thing was an absolute prerequisite: they had to have excellent knowledge of Microsoft technology, as Infors HT has been relying entirely on Microsoft for years, both on the client and cloud side and, of course, in terms of security technology. "It was particularly important to us that our security partner did not work against the manufacturer of our security software. Many MXDR service providers use their own tools, which override the tools used natively or hinder their work. We also didn't want any more complexity, but a complete package from a single source," says Schröder, explaining the most important core elements for the evaluation process.

"We then looked at a few companies and listened to presentations, but most of them did not understand and use Sentinel and the Defender suite, or only in a rudimentary way. Ontinue, on the other hand, won us over with its Microsoft expertise," Schröder continues. In addition, according to the main person responsible for IT security, Infors HT has relied on Open Systems, the provider from which Ontinue emerged, for network management and security for many years. He also praises the good communication that continues with Ontinue, despite the highly technical issues: "We always had contacts and Cyber Advisors at Ontinue who immediately knew what we needed, what we meant and how we could overcome the hurdles that inevitably arise when working with external service providers."

> " We always had contacts and Cyber Advisors at Ontinue who immediately knew what we needed, what we meant and how we could overcome the hurdles that inevitably arise when working with external service providers."

René Schröder
Head of IT Security
Infors HT

Not Too Expensive and Makes Perfect Sense

Infors HT has alleviated the need to investigate every security event and incident independently. The majority are intercepted directly by Ontinue's Security Operations Center (SOC), reducing escalations to Infors HT to just one in a hundred thousand events. This efficiency liberates resources for René Schröder and his team, allowing them to focus on infrastructure management, organizational clarifications, and internal audits. Moreover, the continuous monitoring of IT infrastructure provides René Schröder and his team with peace of mind, ensuring prompt detection of anomalies and cyberattacks every day of the week. Consequently, attackers have significantly less time to act before necessary countermeasures are implemented.

Communication between René Schröder, his team and Ontinue takes place via the shared channel in Microsoft Teams, which ensures smooth coordination between cyber defenders, cyber advisors, and internal security experts. The security professionals from MXDR partner Ontinue are so integrated into the in-house IT team that it feels like they are part of the company. “We can also better integrate our own first-level supporters into the security processes,” explains Schröder. “They can ask Ontinue’s Cyber Defenders and Cyber Advisors directly via Teams what recommendations they have for specific incidents. They respond immediately and already have suggestions on how we should react. This is particularly important because we don’t have any IT administrators in the USA, for example, which is a completely different time zone, but only first-level support.” Escalation matrices were created for the corresponding processes at the beginning of the collaboration, which define access authorizations, responsibilities and contact persons at all neuralgic points.

The experts from Ontinue and Infors HT have now grown together to form a Security Operations Center (SOC). René Schröder quantifies the increase in security performance based on the recommendations of the Federal Office for Information Security and the Swiss ICT standard as follows: “We have come around 50% closer to a secure IT infrastructure. This shows once again that MXDR services are neither too expensive nor pointless for small and medium-sized enterprises - on the contrary: they are a really good thing and SMEs in particular should not cut corners when it comes to their security.”

> ” MXDR services are not only affordable but also invaluable for small and medium-sized companies. They offer precisely what is needed to effectively secure their IT infrastructure without requiring enormous budgets.”

René Schröder
Head of IT Security
Infors HT

About Ontinue

Ontinue offers nonstop SecOps through an AI-powered managed extended detection and response (MXDR) service. Ontinue ION MXDR combines powerful proprietary AI with the industry’s first collaboration with Microsoft Teams to continuously build a deep understanding of our customers’ environments, informing how we prevent, detect, and respond to threats. Continuous protection. AI-powered Nonstop SecOps. That’s Ontinue.