Ontinue

CUSTOMER STORY

Hospitality Organization Achieves 90% Reduction in Cybersecurity Incidents by Partnering with Ontinue

DO & CO seemed an unlikely target for a cyberattack. As a gourmet catering company with three major business lines serving the airline industry, international event catering, and restaurants and hotels, DO & CO operates 32 gourmet kitchens in 12 countries, staffed by a highly mobile workforce of 12,000 that follows Formula One, FIFA World Cup and other international events.

As a moderately large and complex organization, DO & CO's business is often subject to last-minute changes — in numbers, venues, logistics, flights — as the company is essentially responsible for "making the impossible possible" each day. Yet, DO & CO had no formal cybersecurity program.

"The DO & CO environment was essentially a cyber incident waiting to happen," according to Johann van Duyn, Global CISO at DO & CO, who notes that day arrived on November 23, 2020.

"The organisation suffered a major ransomware incident from the DoppelPaymer group," he tells. "The screens all turned red. Three months of backups were corrupted. The decryptor provided to us failed. The short story — everything was very broken. The impact on DO & CO was not insignificant. The company could not even trust Active Directory anymore, which, as you can imagine, is not a great place to start from."

For a company with €935 million in annual revenue at the time, falling back on manual, ad-hoc processes meant failure on several contractual requirements, regulatory headaches, reputational damage — and, as a result, financial loss, as well.

DO&CO

Motivators

- 2020 ransomware attack highlighted need for a modern security strategy
- 24/7 threat coverage required
- In-house SOC not feasible due to talent shortage and pace of technology change

Solution

- Ontinue ION managed extended detection and response (MXDR) service
- Microsoft E5 Security
- Microsoft Defender for Endpoint
- Microsoft Defender for Officer 365
- Microsoft Sentinel

Business Outcomes

- Achieved 90% reduction in cybersecurity incidents
- Saved 40% year-over-year on SecOps data costs
- 75% of alerts closed via automation
- Streamlined communication and collaboration through Microsoft Teams
- Stayed ahead of attacks with a 24/7 service that evolves as attackers do
- Closed incidents via automation
- Improved prevention through automation and recommendations for hardening security environment
- Gained time for higher-value SecOps work

About DO & CO

DO & CO specializes in Airline Catering, International Event Catering, and Restaurants, Lounges & Hotels, providing unparalleled Gourmet Entertainment worldwide. With 32 locations across 12 countries spanning 3 continents, the company upholds the highest standards of quality in all its offerings. At the heart of its premium service is its dedicated staff, each embodying a unique personality and an unwavering passion for hospitality.

It was also a major wake-up call. In response, the company brought in a CIO and Van Duyn later joined as CISO. Together they devised a cyber strategy, migrated to the cloud and, among other strategic decisions, they took a Microsoft-first approach to cyber security, signing on for Microsoft E5 Security capabilities, with Microsoft 365 Defender taking center stage.

"That turns out to have been the best decision ever for us. E5 brings a lot of capability in one single purchase," says Van Duyn, who noted that Microsoft Defender for Office 365 immediately reduced the number of malware and phishing emails reaching user inboxes. "Defender for Endpoint has also been an absolute gold mine of picking up spurious activities within the environment — even sometimes picking up administrators trying to install software they shouldn't be and blocking them from doing that."

But as every SecOps team knows, threat actors don't keep business hours.

"They want to wake us up at all times of the day and night," says Van Duyn. "So, we had to talk to an organization that could provide us with 24/7 detection and response."

Ontinue ION: Improving detection, response and prevention

Managed detection and response very clearly became an operational imperative for DO & CO for Van Duyn and his team, Ontinue ION managed extended detection and response (MXDR) ticked all the boxes.

"Building a SOC in-house is just not an option for us," says Van Duyn. "We have a very small team. The cost, the capability requirements, the analyst churn and the need to keep up with constant technology change made it unfeasible for us. Ontinue came to us as an MXDR that was a Microsoft E5 and Sentinel specialist organization. Ontinue integrates with Microsoft Teams, provides automation backed by machine learning and AI, and provides Microsoft Sentinel in our Azure tenant."

For Van Duyn, the successful relationship with Ontinue started with implementation and has grown stronger ever since.

Even to the point where my Head of Infrastructure said to me during the implementation, 'You know what? This is probably the most professional and knowledgeable crowd I've ever worked with.'"

Van Duyn notes his team's Senior Analyst interacts with ION through Microsoft Teams, where all the details are communicated clearly, so there's no need to search. "We spend our time doing high-value work due to Ontinue taking over security detection and response," he says. "The alert enrichment by the Cyber Defenders at Ontinue is high value. It enables us to understand, and they get the alerts enriched a lot quicker than we were ever able to before we started on the Ontinue journey."

Automation improves prevention

Automation has proven to be a key to efficiency — and prevention, in some cases.

"I love incident closures by automation," says Van Duyn. "That is a pure win. Ontinue Cyber Defenders don't just take the incidents and tell us what happened. They also tell us how we prevent the next incident and how we can harden our environment, improve our security overall, and make us more resilient and more resistant to incidents as an organization."

Attackers evolve, and Van Duyn is happy to have a partner in Ontinue, which evolves to stay ahead of trending attacks. "We've also seen Ontinue step in with the latest load of phishing via QR codes," he adds.

What would Van Duyn say to other CISOs seeking a managed detection and response provider?

> "Would I recommend engaging with Ontinue? Absolutely. We are very, very happy that we met and that we engaged with Ontinue. Ontinue is proving to be a high-value partner on our cybersecurity journey."

Johann Van Duyn
Global CISO
DO & CO

Ontinue

About Ontinue ION: Nonstop SecOps

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.