Ontinue

BROCHURE

Ontinue and NIS2

24/7/365 Expert-Managed SecOps for Microsoft Customers

With unparalleled mastery of the Microsoft Security portfolio and an advanced AI-powered security and collaboration platform, our security experts work around the clock in a follow-the-sun model to prevent, detect, and respond to all the threats coming at you.

Today, most MDR is a miss.

Evolving threats. Complex infrastructure. Limited budgets. And ongoing staff shortages. In today's cybersecurity landscape, managed detection and response (MDR) has become a go-to option for overburdened SOCs. But while managed security vendors promise 24/7 coverage, they consistently fail to deliver. That's because a strong security posture requires a deep understanding of your unique environment, something most MSSPs and MDR providers can't achieve.

We understand you. And your environment.

Ontinue ION, our managed extended detection and response (MXDR) service, is different. We've developed a proprietary customer data model that we use to tailor our services to your unique environment's assets, processes, rules of engagement, users, and more. Mapping your environment onto our customer data model in this way allows us to harness the power of AI and the speed of automation. That translates to faster, higher quality, and more transparent incident resolution - delivered by our 24/7/365 globally distributed Cyber Defense Center.

> " Consistent reviews, coupled with data science and automation, can help customers get faster, more accurate and higher quality responses. Managed security providers who take a more proactive approach will be able to deliver a stronger security posture for their client, helping to build better trust in their security offering"

Craig Robinson
Research Vice President, Security Services
IDC Research

Deep optimization. Higher ROI.

Our comprehensive managed security service is tailored for businesses using the Microsoft Security portfolio, and we go deep to optimize both your SecOps and your ongoing data costs. In other words, not only will you see fortified security for fewer incidents, faster resolution times, and a reduced workload; you'll also achieve higher ROI—allowing your team to focus on critical security tasks while we handle the rest.

Navigating the NIS2 Directive with Confidence

Respond faster, report sooner, and collaborate more easily—with Ontinue

With the introduction of the updated Network and Information Systems Directive (NIS2), the EU is raising the bar on cybersecurity—requiring stronger defenses, faster incident reporting, and closer collaboration with authorities. It's a smart move for protecting citizens and businesses, but it's a big lift for your team. And non-compliance can result in hefty fees, even up to 2% of your global turnover.

Without a fully staffed, highly skilled, 24/7 SOC, how can you stay compliant? With Microsoft and Ontinue.

Our Microsoft Security experts deliver around-the-clock services, protecting your business from the latest threats while optimizing your tech and keeping you compliant.

- **You can't protect what you can't see.** Ontinue enables visibility of your operational environment and allows you to understand and protect your critical assets. Ontinue AI-powered MXDR is backed by real people, 24/7. We have your back.
- **Ensure consistency in reporting time.** Speed response time with real-time Teams collaboration and increase efficiency of your team and ensure consistent reporting within the given deadline in NIS2.
- **Reduce the reporting effort for NIS2.** Ontinue MXDR's AI-powered forensic capabilities will significantly reduce processing time needed for NIS2 reporting, saving your employees' time, so you can focus on what's important for your organization.
- **It's not about detection, but prevention.** Threats continue to evolve in complexity, number and speed. Ontinue ION MXDR service brings together the ION platform, the ION Cyber Defense Center, and the power of generative AI with ION IQ for continuous protection.

NIS2 and Ontinue

Chapter IV, Article 21, Cybersecurity risk-management measures		
2. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems… based on a) policies on risk analysis and information system security;	**Ontinue ION MXDR**	Leverages an AI-powered system that is constantly learning, not just about threats, but about the optimal way to defend against threats before they get on your network. AI-driven automation offers faster detection and response. We continuously measure every aspect of your day to-day operations incl. servers, apps, endpoints, email and docs, IoT, containers and network to identify new opportunities for automation and optimization. ION automation engine filters out false positives, while also triaging true positives up front. If ION Automate determines it can investigate and resolve the incident on its own, it will. For incidents that require human judgement to resolve, ION Automate elevates them to our Cyber Defense Center for further investigation. We analyze your environment 24/7/365 and deliver that information through Teams, reducing MTTD, enabling you to neutralize advanced cyber-attacks.
	Ontinue ION MVM	Enables to effectively reduce risk by surfacing the small percentage of IT vulnerabilities that pose the greatest risk.
	Ontinue ION MXDR	Leverages dedicated teams of experts in threat hunting, vulnerability management, and threat intelligence, backed by AI to enhance defenders and neutralize advanced cyber security threats.
	Ontinue ION IoT	Delivers 24x7 monitoring of your IoT and OT assets, correlating alerts across your IoT/OT and IT environments for maximum visibility and minimal false positives, enabling your team with ressources to fight real threats and not alerts.
2. b) incident handling;	**Ontinue ION MXDR**	Shares live health status, enabling coordinated isolation, detection, and malware remediation across servers, apps, endpoints, email and docs, apps, IoT, containers and network. Continuous monitoring of signals from across the entire security environment enables quick and accurate detect and respond to potential cybersecurity events, eliminating false positives through automation.

Chapter IV, Article 21, Cybersecurity risk-management measures		
	Ontinue ION MXDR	Leverages dedicated teams of experts in threat hunting, vulnerability management, and threat intelligence, backed by AI to enhance defenders and neutralize advanced cyber security threats.
	Ontinue ION MXDR	24/7/365 incident response, recovery engineering, and advanced security services, to reduce the severity, impact and cost of a breach.
2. c) business continuity, such as backup management and disaster recovery, and crisis management;	**Ontinue ION MXDR**	Ensures the information security aspect of business continuity management with 24/7/365 detection of and response to security incidents across the IT environment, leveraging AI-powered human expertise, and automation. 24/7/365 incident response, recovery engineering, and advanced security services, to ensure business continuity.
2. e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	**Ontinue ION MXDR**	Human threat-hunting experts backed by AI monitor and investigate alerts from across the network and information systems to identify and investigate suspicious activities and protect personal data wherever it resides. Ontinue ION MXDR generates exceptional actionable signals across the network infrastructure to optimize cyber defenses and proactively responds to any vulnerability disclosures. On notification, a full investigation is initiated that looks for signs of exploitation. If necessary, Sophos MDR will remediate the incident and provide guidance on how to harden the environment against future exploitation. A full human-authored report is provided in response to the disclosure investigation.
	Ontinue ION MVM	Provides tailored recommendations and guidance on how to mitigate urgent vulnerabilities that impact your IT environment.
2. f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	**Ontinue ION MXDR**	24/7/365 investigation and assessment of potential security risks across your entirel environment, leveraging exceptional threat intelligence to identify risk levels and prioritize response.
2. i) human resources security, access control policies and asset management;	**Ontinue ION MXDR**	Threat-hunting experts monitor and correlate information system activity across the full IT security environment, identifying and investigating suspicious activities by regularly reviewing records of information system activity, such as audit logs, access logs, access reports, and security incident tracking reports. Your organisation's critical assets and log sources, as well as defining operational procedures, are mapped and monitored. The response procedures are agreed upon and documented in Rules of Engagement.
Chapter IV, Article 23, Reporting obligations		
	Ontinue ION MXDR	Ontinue ION delivers 24/7/365 security with eyes on glass continuous monitoring — backed by Ontinue employees supporting the entire security lifecycle with threat hunting, intelligence, automation and engineering.
4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority: d) a final report not later than one month after the submission of the incident notification under point (b), including the following: **(i) a detailed description of the incident, including its severity and impact;**	**Ontinue ION MXDR**	On notification, an investigation is initiated that looks for signs of exploitation. If necessary, Ontinue ION will resolve the incident automatically and provide guidance on how to advance your cyber security against future exploitation.
	Ontinue ION MXDR	A complete incident investigation is initiated unveiling the initial point of compromise, a full analysis of all in-scope systems and log data, together with a human executive summary of findings and recommendations to remediate and prevent future attacks.
(ii) the type of threat or root cause that is likely to have triggered the incident;	**Ontinue ION MXDR**	Ontinue ION MXDR investigates and assesses potential security risks across the full environment 24/7/365, leveraging sepreme threat intelligence from Ontinue ION Cyber Defense Center. Full root cause analysis by Ontinue ION MXDR enables improvement of cyber security plans and strategies on the basis of the incorporated learnings.
	Ontinue ION Incident Response	In case of an incident, a complete incident analysis is presented including the initial point of compromise and concrete knowledge to remediate and prevent future attacks.

What Makes Us Different

Tailored to you, automated for you

With our proprietary AI-powered platform, we localize service and accelerate automation based on insights into your environment and operations.

Delivered by experts

Looking to consolidate your security stack using Microsoft's XDR and SIEM ecosystem? Our unmatched expertise with Microsoft 365 Defender and Sentinel empowers you to remove redundant controls and reduce your data ingestion costs.

Built for transparent collaboration

You can collaborate in real time with our Defenders, Advisors, and AI chatbot—right in Microsoft Teams—for faster decision-making and easy access to information.

Prevention-focused

ION isn't just reactive. Our service includes prioritized, measurable recommendations for posture-hardening and threat prevention.

Stronger security. Faster resolution. Easier operations.

With an entire SecOps team backed by proprietary AI that tailors security to your needs, ION delivers faster mean time to resolve and lower security TCO—while driving prevention. Here's what you can expect from our MXDR.

Faster detection and response

Our Cyber Defense Center is more than a SOC: it brings together security experts, PhDs in data science, and software developers to continually execute, measure, and optimize security operations on your behalf.

Greater efficiency and transparency

Real-time collaboration and AI-powered automation eliminate noise, focus efforts, and keep everyone on the same page. We reduce the burden on your team while giving them insight into what's happening at any time.

Higher ROI

Our platform and expertise are based on the Microsoft Security portfolio, and we optimize your tech so you get the most out of your investment. Retire redundant controls, reduce SecOps data costs, and lower your security TCO.

Lighter burden. Faster responses.

- **2 days/week saved by analysts** thanks to AI-driven automation, which accelerates threat detection and response
- **99.5% of alerts ingested by our SOC** are resolved without customer escalation

Microsoft Security

Deep Expertise in Microsoft

As the winner of both the Microsoft Security Services Innovator of the Year Award and the Microsoft Social Impact Partner of the Year Award for 2023, Ontinue ION and our add-on services are purpose-built for the Microsoft Security product portfolio. Ontinue has also been recognized by the Microsoft Intelligent Security Association (MISA) as a Microsoft Certified Managed XDR Solution.

Member of Microsoft Intelligent Security Association
Microsoft Security

Microsoft Intelligent Security Association
Microsoft Security
Microsoft Verified Managed XDR Solution

Ontinue

About Ontinue ION: Nonstop SecOps

Ontinue, a leading provider of AI-powered managed extended detection and response (MXDR) service, 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.