Ontinue

SOLUTION BRIEF

Ontinue ION for IoT Security Add-On Service

CISOs increasingly accountable for OT security

With the convergence of OT and IT environments, as well as IoT adoption accelerating, CISOs are increasingly tasked with securing these expanding attack surfaces. In 2024, 27% of organizations assigned OT security to CISOs, up from 10% in 2022. This shift aligns with the surge in attacks affecting both OT and IT, which jumped from 21% to 49% in the same period.

The challenge is growing as IoT and OT devices proliferate faster than IT assets, tripling the attack surface CISOs must secure in the coming years.

Limited visibility, minimal expertise and, siloed operations

CISOs face distinct challenges when integrating OT and IoT security into their existing security operations:

1. **Limited Visibility** – Security teams lack comprehensive OT/IoT asset inventories, making it difficult to assess their attack surface. Disparate security controls and the absence of integrated telemetry prevents unified threat correlation across OT and IT environments.
2. **Expertise Gaps** – OT teams excel in industrial processes but often lack security expertise, while IT security teams struggle to understand OT/IoT alerts, protocols, and the operational constraints inherent to OT environments. This disconnect slows security integration initiatives.

Your outcomes with Ontinue ION for IoT Security

Gain visibility into your IoT and OT assets

Discover and inventory your IoT and OT assets to get quick visibility into your attack surface and satisfy audit requirements.

Quickly and easily extend 24/7 protection to IoT/OT environments

The Ontinue Cyber Defense Center delivers 24/7 detection and response using correlated telemetry from across your IoT/OT and IT environments.

Realize fast time-to-value for Microsoft Defender for IoT

Get up and running with Defender for IoT in minimal time with expert, tailored guidance on architecting, deploying, and configuring your IoT/OT sensors for each site.

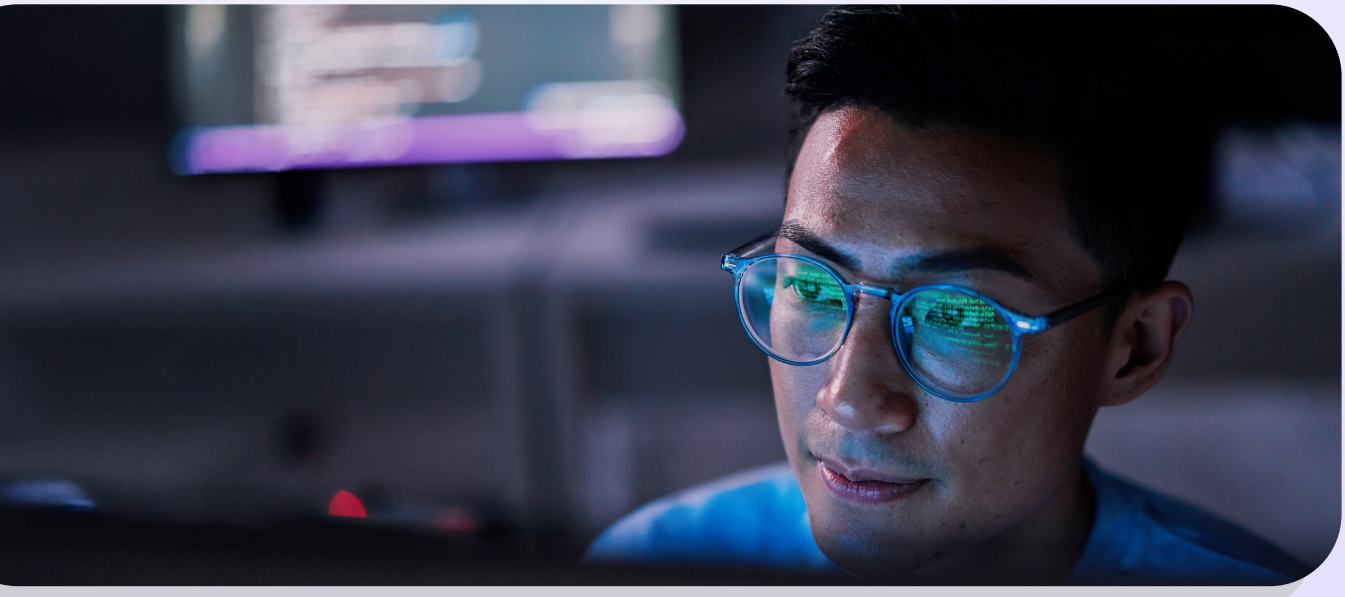
3. **Siloed Operations** – OT and IT security teams operate separately, leading to unclear roles, responsibilities, and escalation processes, even when threats are identified.

24/7 OT and IoT protection that's part of a holistic security program

Ontinue ION for IoT Security is an add-on service to Ontinue ION MXDR that extends continuous protection to your OT and IoT environments. ION for IoT Security delivers 24x7 monitoring and investigation of OT/IoT incidents and tailored automatic escalation processes to bridge the gap between IT security and OT operations teams. The Ontinue Cyber Defense Center provides expert response recommendations while allowing your team to retain full control over response decisions and execution, minimizing the potential for business disruption. Built on Microsoft Defender for IoT, ION for IoT Security also helps maximize the value of your Microsoft security investments.

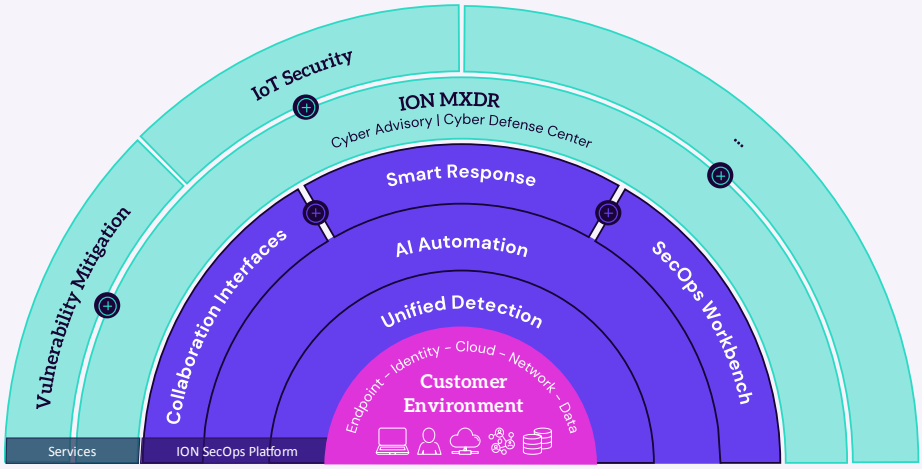
Key capabilities of Ontinue ION for IoT Security include:

- **Real-time asset discovery and management:** ION for IoT Security enables you to maintain an up-to-date inventory of all network connected devices. By leveraging the passive network sensor of Defender for IoT, we enable you to discover unmanaged devices along with relevant details such as manufacturer, serial number, firmware, and more.
- **24/7 threat detection, investigation, and containment for IoT/OT environments:** ION for IoT Security extends the 24/7, follow-the-sun protection of ION MXDR to your IoT/OT environments. Every incident is investigated holistically, analyzed within the broader context of your technology environment. ION for IoT Security extends the tailored incident escalation and handling processes of ION to IoT/OT incidents. With the Environment Mapping, Rules of Engagement, and Escalation Matrix, you define exactly who to involve, in which situations, and how to communicate.
- **Expert, real-time response recommendations:** IoT/OT-enabled Cyber Defenders offer expert response recommendations, based on best-practices and practical experience. Using ION Engage, customers can get on a Microsoft Teams call with the Cyber Defense Center within minutes to get hands-on assistance when needed.



A New Approach to Managed SecOps

Ontinue ION MXDR combines human experts with AI automation to ensure every incident is detected, investigated, and resolved with minimal involvement from your team. Built to maximize the value of your existing Microsoft security investments, ION MXDR provides 24/7 protection across hybrid and multi-cloud environments that extends beyond reactive detection and response into proactive prevention and posture hardening. ION's innovative collaboration model and transparent architecture ensure that security analysts always have instant access to eyes-on-glass SecOps support and complete control of their data. With ION handling the daily security operations, CISOs and their teams get more time back in their day to focus on the next big initiative to propel their organization forward.



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.

Microsoft Security

Our Deep Expertise in Microsoft

As the winner of Microsoft Security Services Innovator of the Year and Social Impact Partner of the Year, and a finalist in the Healthcare category, Ontinue is recognized for our commitment to empowering organizations with advanced threat detection and response, seamlessly integrated into the Microsoft ecosystem, while driving meaningful impact and success alongside Microsoft and our customers.

Copilot for Security
Private Preview Partner

Microsoft Intelligent Security Association
Microsoft Security
Microsoft Verified Managed XDR Solution

Ontinue

CONTACT US

LEARN MORE