Ontinue

ION FOR IOT SECURITY
SERVICE DESCRIPTION

Table of Contents

1. ABOUT THIS DOCUMENT

This service description of Ontinue ION for IoT Security provides an overview of how the service helps mitigate threats and reduce risk in Operational Technology (OT) environments. **ION for IoT Security is available exclusively as an add-on to customers of the ION Managed Extended Detection and Response (MXDR) service**. Upon ordering Ontinue ION for IoT Security, for the applicable term this service description is incorporated into the Master Services Agreement available at www.ontinue.com/msa, or if applicable the agreement executed by and between Ontinue and Customer for ION Services ("MSA"). Notwithstanding anything to the contrary, the Customer acknowledges and agrees that Ontinue may modify or update the ION for IoT Security service add-on over time to accurately reflect the services being provided, provided that any such modifications or updates do not materially degrade the security or function of the Services. Specifically, this document covers the following: over time to accurately reflect the services being provided, provided that any such modifications or updates do not materially degrade the security or function of the Services. Specifically, this document covers the following:

Section	Description
ION for IoT Security Components	An explanation of the component parts of ION for IoT Security, covering both the platform and the human teams.
ION for IoT Security Technology	The technology deployments and licenses that are either prerequisites or recommendations for using the service.
ION for IoT Security Service Launch	The details of how the service is operationalized for customers, designed to deliver value from the start.
ION for IoT Security Service Operations	How ION for IoT Security runs security operations, including the roles and responsibilities on both the Ontinue and customer side.

2. ION FOR IOT SECURITY SERVICE

ION for IoT Security is **an add-on service to the ION MXDR service** and is centered on Microsoft Defender for IoT telemetry. Together the ION MXDR and ION for IoT Security services offer Ontinue customers a unified security view of their IT and OT environments. ION for IoT Security customers also benefit from the Cyber Defense Center and Cyber Advisory services.

3. ION FOR IOT SECURITY SERVICE TECHNOLOGY

The ION for IoT Security service is based on telemetry from Microsoft Defender for IoT, which enables customers to discover, manage, and monitor OT devices across their organization. **It is the responsibility of the customer to procure the required technology licenses and deploy the required technologies**, as listed below.

Technology License Requirements for ION for IoT Security

Technology	License and pricing
Microsoft Defender for IoT	Details of Defender for IoT licensing and pricing can be found here

Technology Deployment Requirements for ION for IoT Security

Deployment
Customers are required to deploy Microsoft Defender for IoT network sensors, on either virtual machines or physical appliances, across all the sites they would like monitored and protected.

Access
Customers must provide Ontinue access to the Microsoft Defender for IoT Azure Portal, so alerts can be properly triaged.

4. ION FOR IOT SECURITY SERVICE LAUNCH

ION for IoT Security Service Launch Key Parties and Responsibilities

Key Party	Contact / Entity	Responsibilities
Ontinue	Sales Engineers	Review the technical implementation of the service, including appropriate configurations.
	Security Consultants	Provide Microsoft Defender for IoT deployment support through Ontinue Consulting Services if required.
	Cyber Advisors	Ensure the Escalation Matrix is updated to reflect any OT escalation contacts that might need to be included with the addition of the ION for IoT Security service.
Customer	CISO or Head of Security or equivalent	Serves as the security strategy and IR policy owner. Provides approvals and drives onboarding forward from the customer side. Onboards third-party providers, e.g. Defender for IoT deployment support partner. Ensures all required technology is licensed and deployed.
	IT Security Operations	Ensures accuracy of Critical Asset inventory. Ensures accuracy of Escalation Matrix, including the addition of OT escalation contacts. Ensures that the Microsoft Defender for IoT configuration is based on Ontinue's best practices.
	OT Engineers	Provide detailed information of the customer OT environment for the ION for IoT Security service. Serve as an escalation contact when appropriate.
	IT Team or designated MSP/CSP	Serves as the Azure Global Admin for technical onboarding with Cyber Advisors and for access package approvals.

ION for IoT Security Service Launch Phases

ION for IoT Security customers benefit from a fast launch, as the service is built to leverage existing components from the ION MXDR service. For consistency, customers get the benefit of the same designated Cyber Advisor as the ION MXDR service and the same 24/7 Cyber Defense Center. The key launch milestones are:

Phase	Description	Supported by
Planning and solution design	During this phase, Ontinue supports customers with guidance and solution design of their Microsoft Defender for IoT deployment. This could include, but is not limited to, understanding how Defender for IoT could best fit into customers network architecture, planning the site and zone to be assigned to each sensor, blueprint definition and guidance on purchasing the appropriate number of licenses.	Ontinue Sales Engineering
Sensor deployment	During this phase, the customer deploys the Microsoft Defender for IoT sensors at the relevant locations with support of Ontinue's Consulting Service or a 3rd party deployment partner if required and for an additional cost. This could include, but is not limited to, the creation of virtual machines or the assembly and cabling of a hardware sensor, the configuration of the Microsoft Defender for IoT sensors and the subsequent initial alert baselining.	Ontinue Consulting Services or 3rd party deployment partner
Deployment review	Review of the correct technical implementation of Microsoft Defender for IoT deployment, including appropriate configuration based on best practices to ensure the correct functioning of Ontinue's ION for IoT Security service.	Ontinue Sales Engineering
Service Setup	Service parameters, such as the Rules of Engagement and Escalation Matrix are configured. Ontinue will guide customers on how which escalation criteria can be used to ensure the correct person is contacted in the event of a security incident in the OT environment. Microsoft Defender for IoT log connector and playbooks are enabled. Additional configuration and installation occur in the backend without need for customer interaction. **Outcome**: Service Setup for ION for IoT Security is completed, and the customer's environment is ready for Operational Start.	Ontinue Cyber Advisory
Operational Start	The Cyber Advisor validates that ION for IoT Security is functioning. **Outcome**: The customer OT environment is now under the protection of ION for IoT Security. In case of distress, the customer may raise critical incidents to the Ontinue Cyber Defense Center 24/7 through ION ENGAGE. The Threat Detection Team begins work on continuous detection optimization & localization. During this phase,	Ontinue Cyber Defense Center

	the Cyber Defense Center responds to any incidents raised through ION ENGAGE.	
Calibrate and fine-tune	Alerts generated by Microsoft Defender for IoT are optimized with respect to their signal to noise ratio, to enable accurate and relevant detection of threats. **Outcome:** Curated set of use cases deployed and baselined. Escalation Matrix updated. The customer's environment is stable and ready for SLA (Service Level Agreement) start.	Ontinue Threat Detection team
SLA-start	The Cyber Advisor enables alert-based incident handling in the Cyber Defense Center. **Outcome:** The Cyber Defense Center monitors and responds to in-scope OT alerts 24/7. SLAs now apply to the Ontinue ION for IoT Security service.	Ontinue Cyber Defense Center

Microsoft Access

ION gains authorized access to the customer's Microsoft Sentinel instance and Microsoft Defender for IoT through Azure Lighthouse, which is based on Azure delegated resource management. With Azure delegated resource management, authorized Ontinue users can work directly in the context of customer subscriptions without having an account in, or being a co-owner, of the customer tenant. Data in transit as well as data at rest is encrypted. To onboard customer tenants, an active Azure subscription is required.

5. ION FOR IOT SECURITY SERVICE OPERATIONS

Key Party	Contact / Entity	Responsibilities
Ontinue	ION Automation	Executes incident enrichment and initial incident triage. Works on the continual reduction of benign positives. Escalates incidents, as needed, to Cyber Defenders and customers.
	Detection Engineers	Design and maintain the coverage model designed to ensure customer environments are comprehensively protected. Evaluate the Defender for IoT alert categories and alerts to be included in the scope of the ION for IoT Security service.
	Cyber Defenders	Perform incident investigations. Escalate incidents, as needed, to customers. Serve as the strategic contact on responding to identified incidents. Provide containment recommendations, when possible, based on other preventive technologies that are in place.
	Cyber Advisors	Serve as the customer interface for the service in general. Ensure ongoing, correct technical implementation of all Ontinue services.
	Customer Operations	Support Cyber Advisors with action tracking and non-technical activities in service delivery to the customer.
	Account Manager	Questions on pricing and renewals.
Customer	CISO or Head of Security or equivalent	Serves as the security strategy and IR policy owner. Provides approvals, serves as a key point of escalation. Onboards third-party providers, e.g. legal advisors. Serves as the link to a Steering Committee, if needed.
	IT Security Operations	Serve as the incident peer for Cyber Defenders. Take emergency decisions and provides verifications. Notify Ontinue of any IT environment changes that may affect the execution of the ION MXDR service.
	OT Engineers	Serve as the incident peer for Cyber Defenders, in the case of incidents affecting OT environments. Take emergency decisions and provides verifications, in the case of incidents affecting OT environments. Notify Ontinue of any OT environment changes that may affect the execution of the ION for IoT Security service.

Third Parties	Law Enforcement	Perform filing of global digital criminal complaints, as needed. Ensure prompt transmission to international parties and liaises with relevant authorities (e.g. INTERPOL).
	Forensics	Serve as an on-demand emergency contact. Perform analysis and recovery of hard drives and files. Gather evidence, ensures collaboration with law enforcement.
	Incident Response on Demand	Serve as an on-demand emergency contact. Deliver IR capabilities – e.g. large, on-site investigations.

Note: Ontinue is not a provider of any of the services listed under "Third Parties". In case any such service is required, for example Incident Response, that would be the responsibility of a third party. Ontinue can recommend an Incident Response provider in the customer's region if needed.

Scope of ION for IoT Security Service Operations

Microsoft Defender for IoT produces alerts in 5 categories. The coverage associated with each category of alerts is detailed below:

Alert Category	Description	ION for IoT Security Coverage
Malware	Triggered when the Malware engine detects malicious network activity. For example, the engine detects a known attack such as Conficker.	**Covered** including ticket generation, requires baselining and subject to AAA methodology.
Anomaly	Triggered when the Anomaly engine detects a deviation. For example, a device is performing network scans but isn't defined as a scanning device.	**Covered** including ticket generation, requires baselining and subject to AAA methodology.
Protocol violation	Triggered when the Protocol Violation engine detects packet structures or field values that don't comply with the protocol specification.	Alerts in this category **do not trigger an incident**. They are available for correlation and context in investigations.
Policy violation	Triggered when the Policy Violation engine detects a deviation from traffic previously learned.	Not in scope.
Operational	Triggered when the Operational engine detects network operational incidents or a device malfunctioning.	Not in scope.

For more details on the continuously growing set of threat detections provided out-of-the-box by Microsoft Defender for IoT, please see the official Microsoft documentation on the topic.

Ontinue investigation and response capabilities as part of the IoT and MXDR services are limited to information provided in Microsoft Sentinel. Microsoft Defender for IoT is **deployed as a passive network sensor by design to ensure no interference with sensitive and critical OT system components**. Ontinue will provide containment recommendations based on other preventive technologies owned by the customer where possible.

Incident Escalation and Escalation Matrix

Ontinue aims to minimize the number of security incidents escalated to the customer. When an incident does need to be escalated, Ontinue follows the protocol jointly defined with the customer in the Escalation Matrix.

The Escalation Matrix defines the escalation contact(s) based on various criteria, including incident severity. Each escalation contact has an associated email address and phone number, as well as their preferred medium of communication. The Escalation Matrix also captures the trigger for escalating notification to the next level. Typically, this will be following no response after a certain number of attempts to communicate with the contact.

The customer is responsible for ensuring the ongoing accuracy of and availability of contacts included in the Escalation Matrix, including notifying their Cyber Advisor/Customer Operations if changes need to be made. **The ION for IoT Security service uses the same Escalation Matrix as the ION MXDR service. Thus, OT specific escalation contacts should be integrated into the Escalation Matrix, using the supported escalation criteria to ensure the correct person is reached.**

Supported notification mediums are Microsoft Teams, phone, and email.

The process of incident collaboration, reporting, and tracking, as well as interaction with Cyber Advisors, is the same as the ION MXDR Service. The processes are described in detail in the ION MXDR Service Description, available at: https://www.ontinue.com/service-descriptions/

6. ION FOR IOT SECURITY LICENSING MODEL

The licensing model of the ION for IoT Security add-on service is **based on the number of devices at a site and the total number of sites monitored**, following Microsoft's Defender for IoT model.

A site is defined as a specific physical location, such as a factory, facility, campus, office building, or hospital. A site can contain any number of Defender for IoT sensors, all of which monitor devices detected in connected networks.

A device is defined as an IP address, excluding the subnet mask and network address.

The site pricing tiers are as follows:

Site size	Devices per site
XS	Includes up to 100 devices per site
S	Includes up to 250 devices per site
M	Includes up to 500 devices per site
L	Includes up to 1'000 devices per site
XL	Includes up to 5'000 devices per site