

Ontinue

Ontinue ION for Digital Forensics & Incident Response Service Description Product Management

Version: v1.01

Effective Date: 22.09.2026



Table of Contents

- 1. About the Service..... 3
- 2. Service Overview & Scope..... 3
 - 2.1. Service Overview..... 3
 - 2.2. Service Scope..... 4
- 3. Technology & Prerequisites..... 4
 - 3.1. Technology License Requirements..... 5
 - 3.2. Technology Deployment Requirements..... 5
 - 3.3. Technology Configuration Requirements..... 5
 - 3.4. Access and Permission Requirements..... 5
- 4. Service Launch..... 5
 - 4.1. Launch Roles & Responsibilities..... 5
 - 4.2. Service Launch Phases..... 6
- 5. Service Operations..... 6
 - 5.1. Ongoing Roles & Responsibilities..... 6
 - 5.2. Operational Mechanics..... 7
 - 5.3. Deliverables, Reports & Notifications..... 8
- 6. Subscription Metrics..... 9



1. About the Service

The Ontinue ION for Digital Forensics & Incident Response (DFIR) Service extends the ION Managed Extended Detection and Response (MXDR) Service by providing enhanced incident response and digital forensic capabilities that extend beyond the ION MXDR service scope. ION for DFIR is available exclusively as an add-on to the Ontinue ION MXDR Service.

Subject to ordering and payment of the applicable fees, this Service Description is incorporated into the Multi-Services Agreement available at www.ontinue.com/msa, or the equivalent agreement executed between Ontinue and Customer (the "MSA"). Ontinue may modify or update ION for DFIR from time to time, provided any such change does not materially degrade the security or core functionality of the Service.

This document covers the following:

Section	Description
Service Overview & Scope	What ION for DFIR does, the outcomes it is designed to deliver, and what is included and excluded.
Technology & Prerequisites	The technology deployments and licenses that are either prerequisites or recommendations for using ION for DFIR, together with the configuration and permissions Customer must have in place for Ontinue to deliver it.
Service Launch	How ION for DFIR is configured and deployed for Customer, including launch roles and the onboarding phases, designed to deliver value from the start.
Service Operations	How ION for DFIR operates on an ongoing basis, including the responsibilities of Ontinue's DFIR alliance partner, and Customer.
Subscription Metrics	Where to find the subscription metrics applicable to the Service.

2. Service Overview & Scope

This section describes the capabilities of ION for DFIR and defines the boundaries of the Service, distinguishing what is included from what is explicitly out of scope.

2.1. Service Overview

Purpose: With ION MXDR, Customer receives detection, investigation, and response for security incidents generated by Ontinue's and Microsoft's advanced threat detection. For the vast majority of security incidents, the containment actions delivered through the ION MXDR Service are fully sufficient to effectively remediate evolving security incidents and prevent any further impact.

However, rare, high-impact security incidents require a deeper level of forensics and response than those provided by standard MXDR operations.

A high-impact security incident refers to an exceptional event that has the potential to significantly disrupt business operations, compromise sensitive data, or otherwise extend beyond the scope of routine MXDR response. Such confirmed true-positive incidents may include, for example, lateral movement, compromise of multiple privileged identities or directory services, or ransomware activity.

ION for DFIR closes that gap for ION MXDR customers, alleviating the need for Customer's security teams to engage multiple service providers during these events.



Description: ION for DFIR extends the 24/7 response capabilities of ION MXDR into enhanced incident response and digital forensics, delivered in collaboration with hand-picked specialist alliance partners. It brings together Ontinue's ION MXDR Service — continuous, real-time detection, investigation, and proactive threat containment — with the advanced forensic expertise of Ontinue's DFIR alliance partners, whose hands-on experience, state-of-the-art forensic laboratories, evidence preservation practices, and close collaboration with law enforcement ensure that even the most complex and high-impact security incidents are managed effectively and with confidence. Customer interacts with ION for DFIR through the same Microsoft Teams-based collaboration interfaces and delivery teams as ION MXDR.

Outcomes: ION for DFIR delivers:

- Readiness for high-impact incidents established and maintained ahead of time, through a DFIR readiness workshop, defined escalation and engagement procedures, and recurring tabletop exercises.
- A single, coordinated response path from MXDR detection and containment into specialist forensic investigation, without the need to engage multiple service providers during a high-impact incident.
- In-depth forensic findings for high-impact incidents to support Customer's containment, remediation, and notification decisions.

2.2. Service Scope

Within Service Scope: ION for DFIR includes:

- Enhanced incident response and digital forensics for rare, high-impact security incidents, delivered in collaboration with Ontinue's DFIR alliance partner as an add-on to the ION MXDR Service.
- Escalation and engagement of the DFIR alliance partner by Ontinue's Cyber Defense Center for high-impact security incidents.
- An initial security incident assessment, a full security incident assessment where approved by Customer, and remote or on-site forensic support as agreed.
- An annual half-day DFIR review workshop, including a tabletop exercise, from the second year of service.
- All IT systems that are operated directly by Customer, by an outsourcing partner on behalf of Customer, or by a service provider for Customer. This includes SaaS, PaaS, and IaaS solutions, provided the security incident in question impacts IT systems in use and under Customer's direction or control.

Outside Service Scope: ION for DFIR does not include:

- DFIR support for incidents that occur entirely within an outsourcing partner's or service provider's own environment.
- Legal advice, regulatory breach notification on Customer's behalf, and any determination of Customer's notification obligations.
- Remediation and recovery actions executed outside the response actions delivered under the ION MXDR Service, other than those recommended by the DFIR alliance partner and executed by Ontinue's Cyber Defenders or by Customer.

3. Technology & Prerequisites

This section lists the technology, licensing, deployment, configuration, and permissions Customer must have in place for Ontinue to deliver ION for DFIR.



3.1. Technology License Requirements

Technology	License	Comments
As required for the ION MXDR Service.	As defined in the ION MXDR Service Description.	The ION MXDR licensing baseline applies.
DFIR alliance partner's forensic tooling.	As defined in DFIR alliance partner's service description.	Partner-dependent. There may be specific licenses required depending on which alliance partner is providing the DFIR services.

3.2. Technology Deployment Requirements

- The ION MXDR deployment baseline applies.
- Depending on which DFIR alliance partner is providing Customer with the DFIR services, there may be specific deployments required, as defined in that partner's service description.
- Where the selected DFIR alliance partner requires specific analysis or forensic tooling to be deployed during an incident, deployment is coordinated and supported by the DFIR alliance partner, with Customer's IT team or designated MSP/CSP acting as the primary technical contact.

3.3. Technology Configuration Requirements

- A dedicated Microsoft Teams channel for ION for DFIR, accessible to Customer, Ontinue, and Ontinue's DFIR alliance partner.
- Customer's DFIR Engagement Configuration updated to include Ontinue's DFIR alliance partner, enabling direct and timely escalation of high-impact security incidents.

3.4. Access and Permission Requirements

- Customer identifies and maintains a current list of individuals authorized to invoke the DFIR Service.
- Where a full security incident assessment is approved, Customer provides the DFIR alliance partner with the access required to conduct forensic investigation of the affected systems, including access to relevant telemetry, logs, and evidence sources.

4. Service Launch

This section describes how ION for DFIR is configured and deployed for Customer, including the roles involved and the onboarding phases.

4.1. Launch Roles & Responsibilities

The ION MXDR service launch roles and responsibilities (detailed in the ION MXDR Service Description) hold true for ION for DFIR, with the additional responsibilities specified below.

Key Party	Contact / Entity	Launch Responsibilities
Ontinue	Customer Operations	Ensure that the ION for DFIR launch advances on schedule, with key milestones successfully completed.
	Cyber Advisor	Ensure the correct update of Customer's Teams channel configuration, Escalation Matrix and Rules of Engagement. Participate in workshops to provide ION MXDR service insights.



Key Party	Contact / Entity	Launch Responsibilities
Ontinue's DFIR Alliance Partner	DFIR Specialist	Serve as the contact for all technical DFIR requests. Lead the initial kickoff, one-day DFIR workshop and half-day tabletop exercise. Responsible for initial kickoff, one-day DFIR workshop and half-day tabletop exercise outcomes and documentation.
Customer	CISO or Head of Security or equivalent	Provide details of Customer contacts authorized to invoke the DFIR service.
	IT Security Operations	Participate in workshops to provide Customer environment insights.

4.2. Service Launch Phases

The table below outlines the standard phases of the launch process, the outcome of each phase, and its typical duration. Actual timelines may vary depending on Customer's environment and responsiveness.

Phase	Outcome	Typical Duration
Initial Kickoff	Teams introduced and aligned, and the agreed service scope reviewed in detail with Ontinue's Cyber Advisor and Customer Operations Manager, Ontinue's DFIR alliance partner specialists, and Customer.	1 hour
One-Day DFIR Workshop	An initial assessment of Customer's DFIR readiness, a review of incident response and escalation procedures, key communication channels and operational workflows outlined, and a documented summary of key findings and outcomes.	1 day
ION Teams Configuration Update	A dedicated Microsoft Teams channel established for delivering ION for DFIR, accessible to Customer, Ontinue, and Ontinue's DFIR alliance partner to ensure seamless collaboration and communication.	Within the 15 business day launch window
DFIR Engagement Configuration	Operational procedures for ION MXDR are extended to include Ontinue's DFIR alliance partner, enabling direct and timely escalation of high-impact security incidents to DFIR specialists.	Within the 15 business day launch window
Half-Day Tabletop Exercise	A technical tabletop exercise conducted and documented, training cross-functional teams in coordinated incident response.	~10 business days after the Service is fully operational

5. Service Operations

This section describes how ION for DFIR operates on an ongoing basis, including the responsibilities of Ontinue and Customer.

5.1. Ongoing Roles & Responsibilities

The ION MXDR roles and responsibilities (detailed in the ION MXDR Service Description) hold true for ION for DFIR, with the addition of the responsibilities specified below.



Key Party	Contact / Entity	Operational Responsibilities
Ontinue	Cyber Defenders	Escalate high-impact security incidents, as needed, to Ontinue's DFIR alliance partner. Work with Ontinue's DFIR alliance partner to provide further investigation details as required. Execute response actions based on Ontinue's DFIR alliance partner recommendations as required.
	Threat Hunters	Execute threat hunting for high-impact security incidents based on recommendations provided by Ontinue's DFIR alliance partner.
	Detection Engineers	Maintain and enhance detection use cases in alignment with Ontinue's holistic detection coverage model, incorporating recommendations from Ontinue's DFIR alliance partner.
	Customer Operations	Ensure close collaboration between Ontinue, Ontinue's DFIR alliance partner, and Customer.
Ontinue's DFIR Alliance Partner	DFIR Specialist	Lead the annual half-day DFIR review workshop. Responsible for annual half-day DFIR review workshop outcomes and documentation. Provide and coordinate in-depth DFIR investigations, including timeline, determination of the attack path, indications of other affected objects, identification of IoCs and indications of data exfiltration. Provide status updates to Customer Management. Coordination and support of analysis tool installation. Responsible for in-depth DFIR investigations outcomes and documentation.
Customer	CISO or Head of Security or equivalent	Decide if advanced digital forensics & incident response services are invoked after the Initial Security Incident Assessment.
	IT Security Operations	Notify Ontinue of any IT environment changes that may affect the execution of ION for DFIR. Participate in workshops to provide Customer environment insights.
	IT Team or designated MSP/CSP	Act as the primary contact for the technical deployment of required IT forensics and incident response tools during high-impact security incidents.

5.2. Operational Mechanics

The following describes the core mechanics of how the ION for DFIR Service operates on a daily basis:

- **Standards and methods:** ION for DFIR is based on proven standards and checklists, complemented by proprietary methodologies developed by Ontinue's DFIR alliance partner. Depending on the nature of the high-impact security incident and specific Customer requirements, recognized standards and frameworks such as ISO, BSI, NIST, the ISECOM OSSTMM, and vendor-specific hardening guidelines (e.g., from Microsoft) are applied. Team members from Ontinue's DFIR alliance partner hold relevant academic degrees and industry-recognized certifications in digital forensics and incident response.
- **Initial Security Incident Assessment:** Ontinue's Cyber Defense Center escalates and engages Ontinue's DFIR alliance partner and Customer in case of high-impact security incidents as defined in the Escalation Matrix. To enable swift collaboration, a Microsoft Teams meeting is used, which is joined by the responsible Cyber Defenders from Ontinue's Cyber Defense Center and the DFIR specialists of Ontinue's DFIR alliance partner within one (1) hour. If Ontinue escalated the incident



on behalf of Customer, Customer receives 60 complimentary minutes per case for an initial assessment provided by Ontinue's DFIR alliance partner, free of charge. Ontinue's Cyber Defense Center provides required information to Ontinue's DFIR alliance partner to allow a detailed initial assessment. After the initial 60-minute assessment, Customer decides whether further digital forensics & incident response services are required.

- **Full Security Incident Assessment:** Once a Full Security Incident Assessment is approved by Customer, further remote support is provided by the alliance partner. Depending on which Ontinue DFIR alliance partner is providing Customer with the DFIR services, there may be specific deployments or licenses for further digital forensics and incident response required. When an on-site engagement is requested, the DFIR alliance partner will be dispatched to a mutually agreed Customer location, established in advance.
- **Annual Half-Day DFIR Review Workshop:** The annual half-day DFIR review workshop includes a review of interfaces and readiness, as well as a tabletop exercise to ensure that training is ongoing and interface definitions are up to date. An annual half-day DFIR review workshop is conducted starting in the second year of service.

5.3. Deliverables, Reports & Notifications

Deliverable	Trigger / Frequency	Audience	Purpose	Delivery Channel
One-Day DFIR Workshop summary	Once, during service launch	Customer CISO / Head of Security and IT Security Operations	Document the initial DFIR readiness assessment, escalation procedures, communication channels, and key findings.	Microsoft Teams
Half-Day Tabletop Exercise documentation	Once, during service launch	Customer CISO / Head of Security and IT Security Operations	Record the exercise outcomes and any identified improvements to readiness.	Microsoft Teams
Initial Security Incident Assessment outcome	Per high-impact security incident escalated	Customer CISO / Head of Security and IT Security Operations	Provide the initial but detailed assessment on which Customer decides whether to approve a Full Security Incident Assessment.	Microsoft Teams
DFIR investigation status updates	During an active Full Security Incident Assessment	Customer CISO / Head of Security and IT Security Operations	Keep Customer informed on investigation progress.	Microsoft Teams
In-depth DFIR investigation documentation	On completion of a Full Security Incident Assessment	Customer CISO / Head of Security and IT Security Operations	Document the timeline, attack path, affected objects, IoCs, and indications of data exfiltration.	Microsoft Teams



Deliverable	Trigger / Frequency	Audience	Purpose	Delivery Channel
Annual DFIR Review Workshop documentation	Annually, from the second year of service	Customer CISO / Head of Security and IT Security Operations	Record the review of interfaces and readiness and the outcomes of the accompanying tabletop exercise.	Microsoft Teams

6. Subscription Metrics

ION for DFIR is available exclusively as an add-on to the ION MXDR Service and cannot be purchased or delivered independently of it.

The fees charged for ION for DFIR are independent of the number of Ontinue Units that Customer has procured for their subscription of ION MXDR. Excluding the initial 60-minute complimentary assessment to which Customer is entitled, any DFIR services performed by the DFIR alliance partner will be charged on a time and materials basis, per 15-minute increment. All fees are payable to Ontinue for the DFIR services.

Nonstop SecOps

Questions? Let's talk.

European HQ

Grubenstrasse 54, 8045 Zürich,
Switzerland

Düsseldorf Office

Speditionstraße 2, 40221
Düsseldorf, Germany

North America HQ

450 Maple Street, Redwood City,
CA 94063, USA

Vienna Office

Kohlmarkt 8-10, 1010 Wien, Austria

UK Office

9 Holborn, London EC1N 2LL, United
Kingdom

APAC Office

World Trade Tower, Sector 16, Noida
201301, India

Toronto Office

6060-3080 Yonge St, Toronto ON
M4N 3N1, Canada

 **Continue**