Ontinue

ION FOR
DARK WEB MONITORING
SERVICE DESCRIPTION

Table of Contents

1. ABOUT THIS DOCUMENT

This Service Description of Ontinue ION for Dark Web Monitoring (DWM) provides an overview of how the service extends the Ontinue ION Managed Extended Detection and Response (MXDR) Service by adding monitoring capabilities across hard-to-access areas such as the deep and dark web. This enables early detection of compromised credentials and typosquatting domains associated with Customer, providing actionable insights that allow potential risks to be mitigated quickly.

Ontinue ION for DWM 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 Master Services Agreement for ION MXDR Services available at www.ontinue.com/msa (the "MSA").

Notwithstanding anything to the contrary, Customer acknowledges and agrees that Ontinue may modify or update the ION for DWM Service over time, provided that any such modification or update does not materially degrade the security or function of the service.

This document covers the following:

Section	Description
ION for DWM Service	A high-level explanation of the ION for DWM service.
ION for DWM Technology	The technologies, deployments, and licenses that are prerequisites or recommendations for using the service.
ION for DWM Service Launch	How the service is configured and deployed for customers, designed to deliver value from the start.
ION for DWM Service Operations	How ION for DWM operates, including the responsibilities of Ontinue and Customer.

2. ION FOR DWM SERVICE

ION for Dark Web Monitoring (ION for DWM) is an add-on to the ION MXDR Service, designed to proactively identify threats emerging from the deep and dark web. Following a security incident, sensitive information such as credentials may surface in hidden online spaces, often without Customer's awareness. Such exposures can result not only from direct attacks but also from third-party breaches or the personal use of corporate credentials by end users. Even without a known incident, organizations face persistent risk from inadvertent data leaks.

ION for DWM addresses these risks by continuously monitoring selected sources across the clear, deep, and dark web to detect compromised credentials and typosquatting domains. These insights enable the Ontinue Cyber Defense Center to conduct swift investigations and execute tailored ION MXDR Service response actions in accordance with the established Rules of Engagement.

Confirmed findings are surfaced as security incidents in Customer's Microsoft Sentinel environment and through the ION SecOps Platform and Microsoft Teams interfaces in near real time, following the same notification and severity handling as the ION MXDR Service.

3. ION FOR DWM TECHNOLOGY

ION for DWM leverages the technologies already in place for the ION MXDR Service and requires no additional deployments or licenses from Customer.

Technology Configuration Requirements for ION for DWM

To ensure a swift response to identified threats, the following Response Actions in Ontinue's Rules of Engagement must be set to Pre-Approved:

- Mark User as Compromised
- Revoke User Sign-in Sessions
- Custom Indicator Blocking

If a Customer's policy does not permit one or more of these actions to be pre-approved, ION for DWM operates in a notify-only mode for the affected action(s): Ontinue investigates and notifies Customer with recommended remediation, but the corresponding containment is performed by Ontinue only after approval or by Customer. This increases the time required to contain an exposure, and Customer accepts responsibility for that increased risk.

4. ION FOR DWM SERVICE LAUNCH

ION for DWM leverages the ION SecOps Platform, the Microsoft Teams-based collaboration interfaces, and the delivery teams of the ION MXDR Service, which allows the add-on to be easily activated. The same Cyber Advisor and Customer Operations Manager who deliver the ION MXDR Service also deploy and deliver ION for DWM, ensuring a consistent, cohesive experience for Customer.
The service launch roles and responsibilities of the ION MXDR Service apply to ION for DWM, with the additions specified below:

Key Party	Contact / Entity	Launch Responsibilities
Ontinue ION	Cyber Advisors	Ensure correct technical implementation of ION for Dark Web Monitoring.
	Advanced Threat Operators	Lead the Initial Findings Assessment Session.

Service Launch Phases

Service launch typically takes 15 business days from the Initial Kickoff to enter the fully operational phase of the add-on service. ION for DWM launch milestones are as follows:

Step	Launch Responsibilities
The following steps are completed during the onboarding phase.	
Initial Kickoff	Initial workshop with Ontinue's Cyber Advisor and Customer Operations Manager. It begins with team introductions and alignment, followed by a detailed overview of the agreed service scope.
Key Asset Update	ION Key Assets are reviewed to ensure that search parameters such as domains remain accurate and up to date.
Microsoft Sentinel Configuration	The customer's Microsoft Sentinel environment is configured to receive Dark Web Monitoring raw telemetry from Ontinue directly into the Log Analytics workspace, with an Analytic Rule deployed to generate incidents from validated findings.

Engagement and Escalation Update	DWM-specific operational procedures are reviewed and integrated into the existing engagement and escalation paths to ensure direct and timely response actions.
Initial Findings Assessment Session	An initial review of DWM findings that establishes the service's baseline.

5. ION FOR DWM SERVICE OPERATIONS

The ongoing operational roles and responsibilities of the ION MXDR Service apply to ION for DWM, with the additions specified below:

Key Party	Contact / Entity	Operational Responsibilities
Ontinue ION	Cyber Advisors	Ensure ongoing, correct technical implementation of ION for DWM.
	Customer Operations Manager	Ensure that Customer needs are heard and that feedback is integrated into the service, as appropriate and relevant. Proactively deliver updates on the continuous development of the service and keep expectations aligned.
	Advanced Threat Operators	Lead the annual, one-hour ION for DWM review session.
Customer	IT Security Operations	Notify Ontinue of any IT environment changes that may affect the execution of the service. Own end-user follow-up and verification (for example, password resets and account checks) arising from findings, unless this is delegated to Customer's IT Team or MSP/CSP.
	IT Team or designated MSP/CSP	Perform end-user follow-up and verification where Customer has delegated this responsibility.

Scope of ION for DWM Operations

Step	Service Responsibilities
Continuous Monitoring	Relevant platforms are systematically observed, and findings are ingested into Customer's Microsoft Sentinel environment. Ontinue's Threat Detection use cases curate and deduplicate these findings, generating security incidents that are processed by ION Automate and the Ontinue Cyber Defense Center, ensuring swift remediation and escalation where required.
Annual DWM Review Session	The annual one-hour DWM review session includes a comprehensive review of the global threat landscape and the findings identified within the customer's environment. Note: An annual one-hour DWM review session is conducted starting in the second year of service.

6. ION FOR DWM FEES

Please refer to the ION License Guide for details: http://ontinue.com/ion-license