Ontinue

# ION FOR ENHANCED PHISHING PROTECTION

SERVICE DESCRIPTION

Table of Contents

## 1. ABOUT THIS DOCUMENT

This service description of Ontinue ION for Enhanced Phishing Protection provides an overview of how the service enables enhanced protection against the threat of phishing attacks. **ION for Enhanced Phishing Protection is available exclusively as an add-on to the Ontinue ION Managed Extended Detection and Response (MXDR) service**. Subject to ordering and payment of applicable fees, this Ontinue ION for Enhanced Phishing Protection 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 MXDR Services ("MSA"). Notwithstanding anything to the contrary, the Customer acknowledges and agrees that Ontinue may modify or update the ION for Enhanced Phishing Protection Service over time, provided that any such modifications or updates do not materially degrade the security or function of the ION for Enhanced Phishing Protection Service.

This document covers the following:

| Section | Description |
|---|---|
| **ION for Enhanced Phishing Protection Service** | A high-level explanation of the ION for Enhanced Phishing Protection service. |
| **ION for Enhanced Phishing Protection Technology** | The technology deployments and licenses that are either prerequisites or recommendations for using the service. |
| **ION for Enhanced Phishing Protection Service Launch** | The details of how the service is configured and deployed for customers, designed to deliver value from the start. |
| **ION for Enhanced Phishing Protection Service Operations** | How ION for Enhanced Phishing Protection operates, including the responsibilities on both the Ontinue and customer side. |

## 2. ION FOR ENHANCED PHISHING PROTECTION SERVICE

**ION for Enhanced Phishing Protection is an add-on service to the ION MXDR service** that enables enhanced protection against the threat of phishing attacks. With ION MXDR, customers receive 24/7 detection, investigation, and response for phishing alerts generated by Microsoft security controls. The **ION for Enhanced Phishing Protection add-on service extends the same 24/7 protection to phishing alerts generated by users reporting suspected phishing emails, alleviating the need for customer security teams to manually investigate and respond to user-reported phishing emails**. This saves SecOps professionals hours of work each week while reducing the residual risk of a breach by detecting phishing attacks missed by other controls, including Microsoft. ION for Enhanced Phishing Protection also reinforces customer investments in end user awareness training by rewarding positive end user behavior.

## 3. ION FOR ENHANCED PHISHING PROTECTION TECHNOLOGY

The ION for Enhanced Phishing Protection service uses a variety of technologies and security controls to effectively protect customer environments. **In addition to the technologies required for the ION MXDR service, the following technologies are required for the ION for Enhanced Phishing Protection service.** It is the responsibility of the customer to procure the technology licenses and deploy the technologies listed as required below. In case the required technology has not yet been deployed by the customer, Ontinue's Consulting Services team offers a Readiness package to expedite the deployment of the necessary technology. The Readiness package is subject to additional consulting fees.

### Technology License Requirements for ION for Enhanced Phishing Protection

| Technology | License and pricing | Comments |
|---|---|---|
| **Microsoft Defender for Office 365** | Plan 2 license | Many Microsoft licensing SKUs include the Microsoft Defender for Office 365 Plan 2 License |

### Technology Deployment Requirements for ION for Enhanced Phishing Protection

Microsoft Defender for Office 365 Plan 2 must be deployed to activate the ION for Enhanced Phishing Protection add-on service.

### Technology Configuration Requirements for ION for Enhanced Phishing Protection

To activate ION for Enhanced Phishing Protection, customers need to have completed a predefined set of relevant Ontinue Security Posture Improvement (SPI) tasks. The specific set of tasks will be communicated to the customer during pre-sales, as they relate to the customer's specific Defender for Office 365 configurations.

If the SPI tasks have not yet been completed by the customer, Ontinue's Consulting Services team offers a Readiness package to expedite the implementation of the necessary configurations. The Readiness package is subject to additional consulting fees.

## 4. ION FOR ENHANCED PHISHING PROTECTION SERVICE LAUNCH

The ION for Enhanced Phishing Protection add-on service leverages the ION SecOps Platform, Microsoft Teams-based collaboration interfaces, and delivery teams of the ION MXDR service, which enables the add-on service to be easily activated. The same Cyber Advisors and Customer Operations Managers who deliver the ION MXDR service deploy and deliver the ION for Enhanced Phishing Protection service, as well. This ensures a consistent, cohesive experience for the customer.

The same service launch roles and responsibilities as the ION MXDR core service (detailed in the ION MXDR Service Description) hold true for the ION for Enhanced Phishing Protection service, with the addition of the responsibilities specified below:

| Key Party | Contact / Entity | Launch Responsibilities |
|---|---|---|
| **Ontinue ION** | Cyber Advisors | Confirm that the email security best practice configurations (part of the SPI framework) have been completed.<br><br>Note: the configuration work is not done by the Cyber Advisor. It can be executed by the customer (with guidance from the Cyber Advisor) or by Ontinue Consulting Services, for additional consulting fees. |

## 5. ION FOR ENHANCED PHISHING PROTECTION SERVICE OPERATIONS

The same ongoing operational roles and responsibilities as the ION MXDR core service (detailed in the ION MXDR Service Description) hold true for the ION for Enhanced Phishing Protection service, with the addition of the responsibilities specified below

| Key Party | Contact / Entity | Ongoing Operational Responsibilities |
|---|---|---|
| **Ontinue ION** | Cyber Advisors | Ensure ongoing, correct technical implementation of ION for Enhanced Phishing Protection. |
| | Customer Operations | Ensure that customer needs are heard, and feedback is integrated into ION for Enhanced Phishing Protection, as appropriate and relevant.<br>Proactively deliver updates on ION for Enhanced Phishing Protection's continuous development and ensure expectations alignment. |
| **Customer** | IT Security Operations | Notify Ontinue of any IT environment changes that may affect the execution of the ION for Enhanced Phishing Protection service.<br>User training and awareness on how to report suspected phishing emails.<br>Perform end-user follow up and verification if required (depending on organization). |
| | IT Team or designated MSP/CSP | Perform end-user follow up and verification if required (depending on organization). |

## Scope of Phishing Protection Service Operations

ION for Enhanced Phishing Protection leverages the ION SecOps Platform's proprietary automation engine (ION Automate), the human expertise and tooling of the Cyber Defense Center, and the native capabilities of the Microsoft Defender suite to investigate and resolve security incidents generated by user reported emails.

### Basic Automated Investigation

The Basic Automated Investigation is done by Automated Investigation and Response (AIR), a Microsoft Defender for Office 365 capability. The entities (data elements such as user accounts, hosts, mailboxes, IP addresses, files, or URLs) associated with each reported email are analyzed by AIR and given one of the following verdicts:

| Verdict | Description |
|---|---|
| **Phishing or Malware** | When entities associated with a reported email are found to be phishing or malware, AIR will take the remediation actions it is configured to execute.<br>Note: the best practice AIR configuration is done as part of the required configuration of the ION for Enhanced Phishing Protection service. |
| **Spam or no threats found** | Users often report emails that might be unsolicited or unexpected but are not malicious. In such cases, AIR can determine that the email does not pose a threat, and the incident can be resolved automatically. |

To provide feedback to the user who reported the email, customers can set up an automated email that informs the user of the verdict. While Ontinue can provide guidance on the configuration of the automated email, it is the responsibility of the customer to maintain the automated email.

### Advanced Automated Investigation

In cases where the Basic Automated Investigation is not able to resolve the incident, ION Automate will execute Advanced Automated Investigation to determine whether the user reported email is malicious. This includes checks of any URLs and the file hashes of attachments within the email.

- **Suspicious URL**: when a URL is found to be suspicious, ION Automate runs checks to determine whether the suspicious URL was clicked. If the URL was clicked, ION Automate checks whether the connection was blocked. If the connection was not blocked, the user(s) might be compromised. ION Automate will add the list of potentially compromised users to the incident and escalate to the Ontinue Cyber Defense Center, as well as trigger response actions.
- **Suspicious attachment file hashes**: when ION Automate finds the file hash of an attachment to be suspicious, it then runs checks to determine whether the suspicious file was opened. If the file was opened, ION Automate will trigger response actions.

Response actions are executed in accordance with the Rules of Engagement (RoE). In scenarios where the RoE requires that the action be approved by the customer, ION will execute the response action after Ontinue receives customer approval.

ION Automate can execute the following response actions:

- Add URL to a list of Indicators of Compromise (IOCs)
- Add file hash to a list of IOCs
- Add IPs to a list of IOCs
- Mark user as compromised
- Revoke user sessions
- Block sender
- Soft delete email

**Escalation to the Ontinue Cyber Defense Center (CDC)**

When ION Automate cannot close an incident, the incident is escalated to the CDC. The CDC triages, investigates, and responds to incidents (including executing pre-approved response actions) as defined in the Rules of Engagement. For a detailed explanation of incident handling and collaboration, please refer to the ION MXDR Service Description.

Note: Standard SLAs and SLOs apply to the incident at the point of escalation to the CDC, as such engagement is a part of the ION MXDR service.

**Escalation to the customer**

Ontinue aims to resolve every incident through to closure without having to involve the customer. However, there are some scenarios in which Ontinue will need to escalate the incident:

- **Customer requires their involvement for response action execution:** in taking response actions, Ontinue always adheres to the ION Escalation Matrix established as part of the ION MXDR service. For incident scenarios in which the customer dictates that Ontinue request approval before acting, Ontinue will escalate the incident to the customer requesting approval for the recommended response action.
- **More information needed:** in certain cases, ION's investigation might deem the incident to be suspicious but will require additional information to confirm the incident as a true positive. Ontinue will make use of all available information with the aim of not escalating the incident to the customer. If, however, the required information is not available, then Ontinue will escalate the incident with a summary of investigations steps and actions taken, along with the specific request for additional information.

## 6. ION FOR ENHANCED PHISHING PROTECTION LICENSING MODEL

ION for Enhanced Phishing Protection is licensed per Ontinue Unit, that the customer has procured for their subscription of the ION MXDR service. The Ontinue Units licensed for the ION for Enhanced Phishing Protection add-on service must match the number of units of the ION MXDR service.

For details on what constitutes an Ontinue Unit, please see the Ontinue ION License Guide.