Ontinue

SOLUTION BRIEF

ION for Enhanced Phishing Protection

CISOs need to handle more phishing emails that slip through security controls

Over 3 billion phishing emails are sent daily, 65% of which target organizations. To protect themselves, defenders invest in security controls that detect and block phishing attempts. While this serves to block most phishing emails, an average of over 2k phishing emails per 1k users slips through defenses annually. Once a malicious email is in a mailbox, users interact with it within minutes. The challenge is growing as the volume and sophistication of phishing emails increases, and along with it the number of malicious emails that get through to user mailboxes.

In turn, CISOs have mobilized their users as an additional layer of detection, enabling individuals to report emails they find suspicious. While users often correctly identify phishing emails, they also report many benign emails, which creates a high operational load of user reports for security teams.

Your outcomes with Ontinue ION for Enhanced Phishing Protection

Comprehensively block phishing attacks

Shield your organization against phishing by extending detection and response to user-reported phishing attempts.

Free Up Your Team

Your security team gets to focus on what matters most, while we take on the operational load of investigating thousands of user-reported phishing attempts.

Maximize Microsoft Security ROI

We operationalize Defender for Office 365 on your behalf, so you can squeeze more value out of the Defender XDR suite.

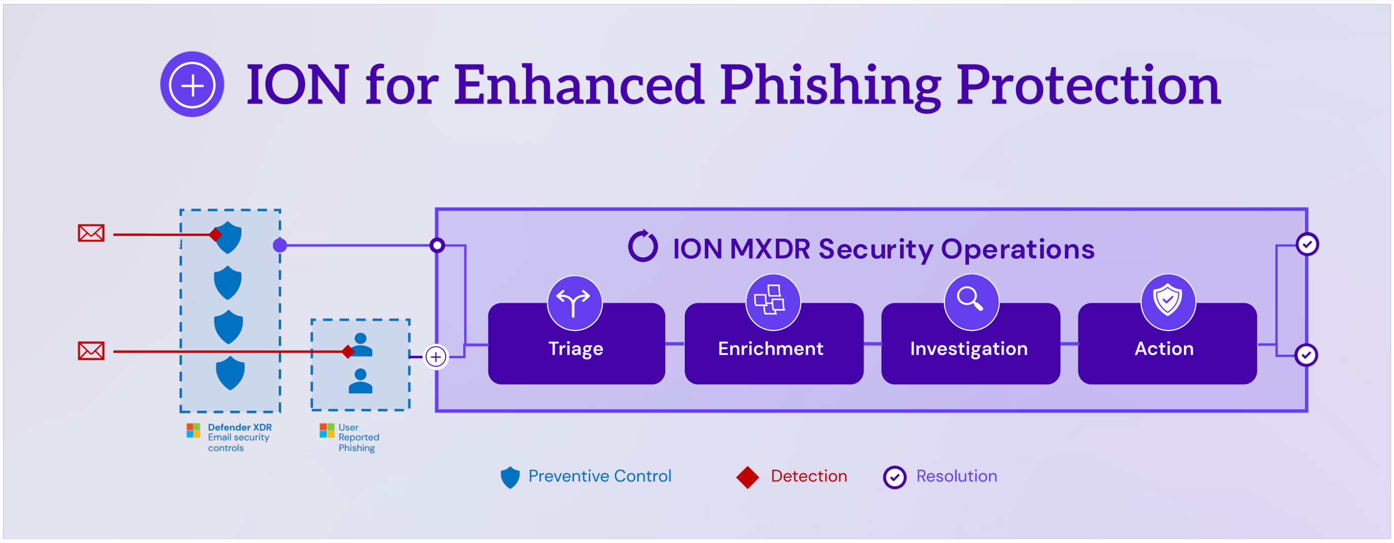
High effort, slow triage, ineffective user training

CISOs face several challenges in operationalizing user reports to more effectively stop phishing attempts:

1. **High effort to triage and analyze** – Security teams need to deal with a high monthly volume of user reports. Each reported email typically takes 15-60 minutes to resolve, with a very high false positive rate.
2. **Slow to investigate and respond** – User reports are typically handled on a best-effort basis, with the time to triage and resolve measured in hours or days, rather than minutes.
3. **Ineffective user training** – When organizations invest in training users to report suspicious emails, it results in a massive increase of reports. Because of the high volume, security teams struggle to effectively use these additional reports to detect and block phishing attempts.

Comprehensively shield your organization against phishing by extending detection and response to user-reported phishing attempts.

Ontinue ION for Enhanced Phishing Protection (ION for EPP) is an add-on service to Ontinue ION MXDR that extends the 24/7 triage, enrichment, investigation and response to phishing attacks, delivered in ION MXDR, to user-reported phishing emails. This enables you to better protect your organization against phishing attempts, without additional effort, all while maximizing your Microsoft Security investments.


ION for Enhanced Phishing Protection
ION MXDR Security Operations
Triage
Enrichment
Investigation
Action
Defender XDR Email security controls
User Reported Phishing
Preventive Control
Detection
Resolution

Key capabilities of Ontinue ION for Enhanced Phishing Protection include:

Robust phishing prevention

Ontinue ION for EPP leverages Defender for Office 365 email security controls, including best practice configurations to safely handle unknown links and attachments, to block phishing attempts well before they reach user inboxes.

Effective triage, enrichment, and investigation of user-reported emails

Ontinue ION for EPP uses multiple layers of automation to weed out false positives, while enriching and investigating actual phishing emails within minutes. For more complex incidents, our security experts in the 24/7 Ontinue Cyber Defense Center (CDC) take over and run the incident to ground.

Faster, tailored response to phishing emails

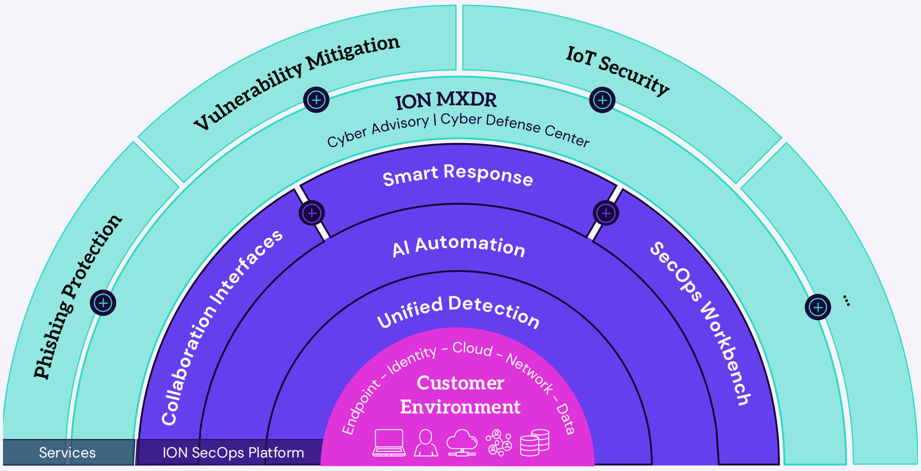
Ontinue ION for EPP executes email-specific responses at machine-speed when pre-authorized in the ION MXDR Rules of Engagement. When customer approval is needed, ION for EPP uses the ION MXDR Escalation Matrix to request response approval from the preferred escalation contact using the preferred contact method

Actionable insights on phishing protection

Ontinue ION for EPP delivers insights and trends on detected phishing incidents, with reports visualizing the breakdown by detection source (security control or user report) and submission status, to track and reduce your Mean Time to Resolution (MTTR) on phishing incidents.

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.



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.

Ontinue | Microsoft
Social Impact
Winner: Ontinue AG
Partner of the Year Awards

Microsoft Security
Excellence Awards 2023
Microsoft Intelligent Security Association
WINNER
Ontinue
Security Services Innovator

Microsoft Security
Excellence Awards 2022
Microsoft Intelligent Security Association
WINNER
Ontinue
Security MSSP of the Year

Copilot for Security
Private Preview Partner

Member of
Microsoft Intelligent Security Association
Microsoft Security
Microsoft Verified Managed XDR Solution

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.

Ontinue

CONTACT US

LEARN MORE