Trustwave®

SERVICE DESCRIPTION

Managed Phishing for Microsoft – Add-On to MXDR for Microsoft

Overview

Trustwave's Managed Phishing for Microsoft service ("**Service**") is an add-on service to Trustwave's Managed Extended Detection & Response (MXDR) for Microsoft service ("**MXDR for Microsoft**"). Delivered by Trustwave's Global Security Operations Centers (SOCs) and backed by SpiderLabs threat intelligence, the Service enhances phishing detection, user awareness, and response capabilities. Designed to work natively within the Microsoft Defender platform, the Service extends organizational resilience to email-borne threats and supports comprehensive risk reduction strategies—delivering continuous protection, visibility, and education across the user base. The following description sets out the parameters of the Service.

Core Trustwave Features

The Service includes threat-based prevention, managed detection, investigation, and response for the following Client owned Microsoft Security products ("**Managed Technology**"):

- Microsoft Defender for Office

The Service includes the following core features:

Phishing Threat Response

Trustwave will analyze, investigate, and respond to both user-reported and system-detected phishing threats, operating directly within Microsoft Defender, including

- Triage and response to high and medium priority XDR Incidents from the Defender for Office portal. Note: this feature and related definitions are included in MXDR for Microsoft.
- Triage and response to user-reported phishing emails via Microsoft's "Report Phishing" button or mailbox (classified as low priority XDR Incidents)
- Email containment and response actions, e.g., soft delete

Reporting and Intelligence

Client will receive ongoing insights into phishing trends and recommendations for improvement in performance, including

- Weekly summaries of user-reported and system-detected phishing attacks
- Monthly phishing simulation reporting key metrics and trends
- Monthly service readouts with key findings, recommendations, and performance metrics

Phishing Simulation and Training

Trustwave will develop and deliver tailored phishing simulations and awareness campaigns scoped based on Client's environment and evolving threat landscape, including

- Pre-built monthly phishing simulation campaigns targeting the organization and/or prioritized user segments
- Quarterly ad-hoc campaigns focused on emerging threats or specific departments
- Bi-annual all-staff training campaigns using curated educational content based on recent simulation and threat data
- Creation of targeted training follow-ups for users who fail simulations

Technology Management

Trustwave will provision and manage phishing-related tools and integrations, including

- Initial setup and configuration of simulation, training, and Trustwave's proprietary, machine - learning email security engines
- Continuous policy management within Microsoft Defender for Office
- User provisioning, role assignment, and ongoing tool administration
- Configuration of the API-based Trustwave's proprietary, machine-learning email security engines for enhanced phishing detection

Enhanced Detection

Trustwave extends native Microsoft protection with its proprietary detection technologies, including

- Deployment of Trustwave's proprietary, machine-learning email security engines
- Enhanced layered email engines identifying and blocking inbound advanced phishing attacks

Consumption Overages

The Service is provided and priced according to 1) monthly Defender for Office emails reported by users as malware or phish– related XDR Incidents, and 2) users protected within the Defender for Office Plan 2 Licenses, as set forth in the applicable SOW or Order Form. Trustwave will periodically review the volume of alerts processed for Client in relation to the Service.

Client will regularly review its alert volumes associated with 1) and 2) above in the Microsoft Defender platform and work with Trustwave to tune its configurations to stay within purchased volumes. Where Client's Defender alert volumes spike and are found to signal that Client will or has exceeded the agreed threshold for the current month, Trustwave may

- evaluate excess alerts and determine if increased volume is (i) a signal of an attack and related alert information that can be consolidated under an alert, or (ii) a configuration error documented in a ticket that requires Client to take corrective action within 24 hours; or
- suppress, filter, throttle, consolidate, or send notification of excess Defender alerts from Client's systems at Trustwave's discretion.

Where Client's alert volumes are found to exceed the agreed threshold persistently by five percent (5%) or more on average over a thirty (30) day period, Trustwave may either

- charge Client for the excess data and event volumes at current list price; or
- suppress, throttle, or filter excessive data and events from the Managed Technology.

Trustwave will notify Client of the overage and will select the method that is expected to limit impact to the Service.

Systems Management

Trustwave will manage and monitor the security configuration of those Client security applications running on the Managed Technology which are included in the Service, as indicated in the applicable SOW or Order Form ("**Managed Technology Security Applications**") and as further described in MXDR for Microsoft.

Service Features

The Service includes the following features:

Onboarding

Trustwave's obligations to provide the Service depend on Client completing the onboarding processes described in MXDR for Microsoft, including (1) Client-side implementation and (2) MSS Transition. Additionally, Trustwave and Client will review Client's email authentication, protection policies, and allow/block lists according to Trustwave's golden policy, assign permissions and apply priority accounts and user tags, configure user reported settings, and provision Trustwave's proprietary, machine-learning email security engines within Client's environment.

Service Level Objectives (SLOs)

The following SLOs apply to this Service:

Service Activity	SLO and Frequency
Phishing submission triage	Response initiated within 1 business day
Phishing simulation campaigns	Conducted monthly (up to 12 per year)
Ad-hoc phishing simulation campaigns	Conducted quarterly (up to 4 per year, only on Client request)
All-staff phishing training	Conducted bi-annually (up to 2 per year, only on Client request)
Weekly phishing report	Delivered weekly summarizing user-submitted and detected threats
Monthly reporting readout	Delivered monthly with performance metrics and recommendations
User and tool provisioning	Completed during onboarding and maintained continuously

Service Delivery and Platform Integration

The Service operates natively within Microsoft 365 Defender. All remediation, policy management, and simulation orchestration is executed within the Microsoft ecosystem, enhanced by Trustwave's

proprietary, machine-learning email security engines. Trustwave's global SOC analysts and SpiderLabs threat researchers work together to ensure timely, accurate, and effective threat response and user education.

Hosting Region

If Trustwave gives Client the option to select the region in which Trustwave's proprietary, machine-learning email security engines account will be hosted, then Client understands it must select the region in its sole discretion. Client is responsible for all appropriate analysis to verify Client selects the region appropriate for its account (including any legal or regulatory analysis). The country where Trustwave accounts are hosted for each region is as follows:

Region	Hosting Country
AMS	United States
EMEA	Ireland and the Netherlands
APJ	Australia

Threat Response

As part of Onboarding and during the Term, Trustwave and Client will agree to one of the following client-level response authorization protocols. These response authorization protocols are actions Trustwave may take on the Managed Technology natively or in the Trustwave Fusion platform. Such pre-authorizations comprise Client's "Response Authorization Protocol" and are further described in MXDR for Microsoft.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in MXDR for Microsoft, Trustwave's Master Terms and Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/, or in the applicable Statement of Work or Order Confirmation between Trustwave and Client.