Malwarebytes Managed Threat Hunting (MTH)

Service Description – August 2023

This Service Description, with any attachments incorporated by reference, is provided under and subject to the Malwarebytes Managed Services Agreement online at: www.malwarebytes.com/legal in addition to any terms and conditions referenced in the order confirmation issued by Malwarebytes related to Customer's purchase of Service or any similar document published by Malwarebytes which further defines Customer's rights and obligations related to the Service, such as the "Order Confirmation" which incorporates this Service Description by reference (the Order Confirmation, this Service Description and any other documents referenced therein collectively, the "Agreement"). Any terms that are used but not defined herein shall have the meaning set forth in the Agreement. This Service Description may be updated from time to time by Malwarebytes.

Service Overview

Malwarebytes 'Managed Threat Hunting' ("MTH Service") is a cloud-based service designed to provide detection of potential attacks, correlated with threat intelligence and automated and orchestrated responses, indicator of compromise summary and escalation via a team of security personnel.

Features of the MTH Service include:

- 24x7x365 Malwarebytes EDR active threat hunting and remediation guidance
- Trained security personnel with backgrounds serving customers of various sizes and verticals
- Back-end artificial intelligence and machine learning supported by a proprietary analytics engine
- Cloud-based, proprietary back-end platform with integrated intelligence sources
- 31-day lookback of critical indicators of compromise (IoCs)
- Incidents are discreetly raised in our Nebula® portal
- Customer driven tiered notifications based on incident severity

TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Features
In addition to the information and attributes associated with the MTH Service outlined above, the following service features apply to the Service:

Out of Scope/Additional Terms.
Anything not specifically described in this Service Description is out of scope and is not included in the Service. Customer (the "**Customer**") acknowledges, understands, and agrees that Malwarebytes does not guarantee or otherwise warrant that the Service, or Malwarebytes' recommendations and plans made by Malwarebytes as a result of that Service, will result in the identification, detection, containment, eradication of, or recovery from all of Customer's system threats, vulnerabilities, malware, malicious software, or other malicious threats. Customer agrees not to represent to anyone that Malwarebytes has provided such a guarantee or warranty.

Litigation Support Services. The following services ("**Litigation Support Services**") are explicitly excluded from the Service provided under this Service Description:

- Depositions, fact witness testimony, expert witness testimony, affidavits, declarations, expert reports
- Responding to discovery requests, subpoenas
- eDiscovery services; and/or
- Other forms of litigation support or participation in any legal proceeding relating to the subject matter of the engagement (including those involving a governmental entity).

CUSTOMER RESPONSIBILITIES

Customer may use the Service only in accordance with the terms, the endpoints and versions under which Customer has obtained use of the MTH Service as indicated in the Order Confirmation and as defined in this Service Description or the Agreement, and compliance with the Documentation.

If Customer does not provide/perform per the following responsibilities, Malwarebytes' performance of the MTH Service may be delayed, impaired, prevented, or terminated.

- EDR Product Requirement and Network Saturation: MTH Service works by protecting all the endpoints in an environment. If an endpoint in an environment is not protected, there is a chance that a security risk may breakthrough the environment through the unprotected endpoint. Accordingly, MTH Services requires an active subscription to EDR and associated implementation on 100% of Customer's endpoints. Customer shall be responsible for ensuring that its endpoints have EDR enabled on all endpoints at all times so that Customer can utilize the intended benefits of the MTH Services.
- Multifactor Authentication: Customers must use Multifactor Authentication (MFA) to access their Nebula and/or OneView console. If Customer can't use SSO, we highly encourage customer to enable MFA through their identity provider.
- MTH Access to Customer Nebula and/or OneView Environments: Malwarebytes MTH Service requires access to Customer Nebula and/or OneView environments, as applicable.
- Reasonable Assistance: Customer must provide assistance to Malwarebytes in delivery of the MTH Service upon reasonable request by Malwarebytes including, but not limited to, providing technical and license

information related to the MTH Service, and enabling MTH Service and other functions within the Nebula and/or OneView environments.

- Accurate Emergency Point of Contact Information: Customer must provide Malwarebytes with accurate and up-to-date emergency point of contact information, including the name, email, and phone number(s) for all designated emergency points of contact.

- Customer's Outage: Customer must provide Malwarebytes notice at least twenty-four (24) business hours in advance of any scheduled outage (maintenance), network, or system administration activity that would affect Malwarebytes' ability to perform the Service.

- Customer Software and Hardware: It is Customer's sole responsibility to maintain current maintenance and technical support contracts with Customer's software and hardware vendors for any Device(s) affected by Service. It is Customer's responsibility to interact with Device(s) manufacturers and vendors to ensure that the Device(s) are scoped and implemented in accordance with manufacturer's suggested standards. Customer is also responsible for interactions with Device(s) manufacturers or vendors regarding the resolution of any issues related to Device(s) scoping, feature limitations or performance issues. Customer is responsible for remediation and resolution of changes to Device(s) which negatively impact the Service or the functionality, health, stability, or performance of Device(s).

- Event Notifications: Customer has MTH, it may opt-in to receiving Event Notifications (provided Customer has the required additional technology to receive such notifications including email servers). Where Customer has opted-in to Event Notifications, Malwarebytes will endeavor to use commercially reasonable efforts to provide Event Notifications within twenty (20) minutes of Malwarebytes confirming the Event. Event notifications will include information known to Malwarebytes at the time the Event is identified but may not include impact and severity details customarily determined through an Investigation or Incident report.

- Consent and Authorization: Customer acknowledges, understands, and agrees that unauthorized access to computer systems or data or intrusion into hosts and network access points may be regulated and/or prohibited by applicable local law. Customer is: (i) explicitly confirming to Malwarebytes that it has obtained all applicable consents and authority for Malwarebytes to deliver the Service; and (ii) giving Malwarebytes explicit permission to perform the MTH Service and to access and process any and all Customer Data related to the Service, including without limitation, if applicable, consent to analyze host forensics including but not limited to, memory, disk, logs, data, network traffic in real time to detect evidence of known malicious communication patterns and traffic containing unrecognized malicious code (malware), connect to Customer's computer network, archive and retain all host forensics data including but not limited to, memory, disk,logs, data, network traffic captured as part of Service (including to store any malware and metadata supplied by Customer, or anyone else working with or for Customer), and (iii) representing that such access and processing by Malwarebytes does not violate any applicable law or any obligation Customer owes to a third party; and (iv) accepting sole responsibility and liability with respect to engagement of such Service. Accordingly, Customer warrants and represents that it is the owner or licensee of any network, systems, IP addresses, software, appliances, code, templates, tools, policies, records, working papers, data and/or computers upon which Malwarebytes performs the Service ("Customer Systems"), which may be visible as Customer Data in connection with the Service, and that Customer is authorized to instruct Malwarebytes to perform the Service on such Customer Systems. Customer shall fully indemnify and hold harmless Malwarebytes for any claims by any third parties related to the Service.

- Reporting: Customer acknowledges and agrees that in the course of delivering the Service, Malwarebytes may become aware of issues such as data breaches, network intrusions, or the presence of malware, and that such issues may give rise to regulatory reporting obligations which Customer is subject to in one of more territories in which Customer operates. Accordingly, Customer shall remain solely responsible for all such reporting requirements and Malwarebytes shall have no liability in this regard whatsoever.

- Prohibited Uses. Customer agrees that Customer will not use the MTH Services for any of the following purposes:
    - Any unlawful, invasive, infringing, defamatory or fraudulent purpose;
    - To send unsolicited bulk commercial email (commonly referred to as "spam") of any kind, regardless of the content or nature of such messages;
    - To send any harmful code or attachment through the MTH Services;
    - To use the MTH Services in a way that has a materially detrimental effect upon the performance of the MTH Services for other users;
    - To use or attempt to use the MTH Services in breach of the Agreement;
    - To transmit harassing, obscene, racist, malicious, abusive, libelous, illegal, or deceptive messages or files;
    - To commit or attempt to commit a crime or facilitate the commission of any crime or other illegal or tortious act;
    - To interfere with the use of the MTH Services by other users;
    - To alter, tamper with or circumvent any aspect of the MTH Services;
    - To test or reverse engineer any of the software or items included as part of the MTH Services in order to find limitations or vulnerabilities.

ASSISTANCE AND TECHNICAL SUPPORT

Technical assistance for the Service is provided by Malwarebytes:

- Malwarebytes Product Support information is located at: https://service.malwarebytes.com/hc/en-us/articles/4413809450003-Contact-Malwarebytes-Business-Support
- For Malwarebytes MTH Support, contact the MTH team via the MTH Portal

Notwithstanding the foregoing, if Customer is entitled to receive technical support from an authorized reseller, please refer to Customer's agreement with that reseller for details regarding such technical support.

DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement or this Service Description, have the meaning given below:

"**Malwarebytes**" means the Malwarebytes entity named in the Order Confirmation and/or its affiliates.

"Customer" means the Customer identified in the Order Confirmation.

END OF SERVICE DESCRIPTION