ThreatDown Managed Detection and Response (MDR)

Service Description – May 2026

This Service Description, with any attachments incorporated by reference, is provided under and subject to the ThreatDown Managed Services Agreement online at https://www.threatdown.com/legal/managed-services-agreement/ and the ThreatDown Software License Agreement online at: https://www.threatdown.com/legal/eula, in addition to any terms and conditions referenced in an order confirmation issued by ThreatDown ("Order Confirmation") related to Customer's purchase of Service or any similar document published by ThreatDown which further defines Customer's rights and obligations related to the Service (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 ThreatDown. The MDR Service is conditioned on Customer's continuous satisfaction of the deployment, configuration, access, support, and operational prerequisites set out in this Service Description, the Agreement, the Order Confirmation, and the Documentation. ThreatDown may suspend, limit, or decline performance of the MDR Service, in whole or in part, where those requirements are not satisfied.

I. Service Overview

ThreatDown 'Managed Detection and Response' ("MDR Service") is a cloud-based service designed to provide detection of potential attacks, correlated with threat intelligence and automated and orchestrated responses, security incident analysis and escalation via a team of security personnel.

Features of the MDR Service include:

- 24x7x365 ThreatDown EDR monitoring, analysis, reporting, remediation, guidance, and threat hunting
- Trained security personnel with backgrounds serving customers of various sizes and verticals
- Onboarding Assistance
- 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
- Bi-directional communication with ThreatDown trained security personnel via our Nebula® portal
- Customer-driven tiered notifications based on incident severity

Additional Features applicable to the MDR Plus Service level include:

- Contractual Service Level Agreement (SLA) for response times to critical incidents
- Post-incident Root Cause Analysis (RCA) investigations into critical incidents

II. TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

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

B. Out of Scope/Additional Terms.
Anything not specifically described in this Service Description is out of scope and is not included in the Service. Without limiting the foregoing, any on-site response, forensic imaging beyond the expressly described scope, litigation support, eDiscovery, regulator engagement, law enforcement coordination, insurer coordination, public relations support, and actions in third-party systems not expressly assumed by ThreatDown are out of scope and remain solely Customer's responsibility unless separately agreed in writing. Customer (the "Customer") acknowledges, understands, and agrees that ThreatDown does not guarantee or otherwise warrant that the Service, or ThreatDown's recommendations and plans made by ThreatDown 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 ThreatDown 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).

Formal Incident Response/Forensic Investigations. The following services are also explicitly excluded from the MDR Services provided under this Service Description:

- Full-scope fly-to-site or remote incident response services, including root cause analysis (excepting MDR Plus service), full/complex forensic examinations, or formal incident reporting
- Corporate forensic investigations
- Malware reverse engineering

III. 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 MDR Service as indicated in the Order Confirmation and as defined in this Service Description or the Agreement, and in compliance with the Documentation. Customer acknowledges and agrees that the quality, completeness, timeliness, and efficacy of the MDR Service depend on Customer's full and continuing compliance with the following responsibilities. If Customer does not promptly provide or perform the following responsibilities in the required manner, ThreatDown's performance of the MDR Service may be delayed, impaired, incomplete, prevented, suspended, or terminated, and ThreatDown will have no liability for any resulting degradation, missed detection, delayed response, or worsened malicious activity.

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

- EDR Product Requirement, Full Deployment, and Configuration: MDR Service works by protecting all endpoints in an environment. Failure to monitor and protect all endpoints in an environment creates the risk

that a security threat may enter the environment via the unprotected endpoint. Accordingly, MDR Services require an active subscription to both MDR and EDR, with associated implementation on 100% of Customer's endpoints. Customer shall be responsible for ensuring that its endpoints have EDR and MDR enabled on all endpoints at all times so that Customer can utilize the intended benefits of the MDR Services. Customer shall also ensure that EDR is fully deployed, healthy, connected, updated, supported, and properly configured on all covered endpoints at all times in accordance with the Documentation and Malwarebytes' deployment and configuration guidance. Any endpoint, server, workload, account, tenant, or environment not fully deployed or properly configured may create visibility gaps, reduce Service efficacy, and increase the likelihood that threats may enter or persist in the environment without detection or timely response. ThreatDown will have no liability for any such visibility gaps, reduced efficacy, or resulting threats, compromises, losses, or damages.

- Configuration and Health Requirements: Customer is responsible for implementing and maintaining all policies, settings, exclusions, permissions, integrations, logging, communication paths, and other technical prerequisites required or recommended by ThreatDown for MDR Service delivery. Customer must promptly remediate any health, coverage, or configuration issues identified by ThreatDown. Failure to do so may reduce the quality or timeliness of the MDR Service and may result in suspension, limitation, or termination of the MDR Service.

- Onboarding/Technical Enablement of MDR Service in Nebula/OneView console: Customer must enable MDR Service in its Nebula console by completing the MDR setup process. MDR Service is not enabled until completion of this process.

- Multifactor Authentication and Access Control: Customer must use Multifactor Authentication (MFA) to access its Nebula and/or OneView console. If Customer cannot use SSO, ThreatDown highly encourages Customer to enable MFA through its identity provider. Customer must also maintain appropriate administrative access controls, credential hygiene, and account security at all times and is solely responsible for all access to and activity within its consoles, tenants, and related accounts, including any failure to prevent unauthorized access.

- Respond to ThreatDown Alerts and Escalations: To ensure effective MDR Service protection against threats, Customer must respond to alert escalations and requests for contextual information relevant to alerts in a timely fashion.

- Complete Reasonable Remediation Actions: Customer must use reasonable efforts to address security gaps identified by ThreatDown and take recommended remediation actions. ThreatDown has no obligation to notify Customer or generate new Incidents for new Alerts that are directly related to previously published Incidents for which ThreatDown has already provided recommended remediation steps, when Customer has acknowledged the prior Incident but cannot, or chooses not to, remediate the cause of these Alerts.

- MDR Access to Customer Nebula and/or OneView Environments: ThreatDown MDR Service requires access to Customer Nebula and/or OneView environments, as applicable. Customer must provide and maintain all permissions, roles, connectivity, communication channels, and technical access required for ThreatDown to deliver the MDR Service, including access to related telemetry, case management, and response functionality. ThreatDown may rely on the permissions, account assignments, and access pathways made available by Customer unless and until revoked in writing by an authorized Customer contact.

- Reasonable Assistance: Customer must provide assistance to ThreatDown in delivery of the MDR Service upon reasonable request by ThreatDown including, but not limited to, providing technical and license information related to the MDR Service, and enabling MDR Service and other functions within the Nebula and/or OneView environments. Customer must designate and maintain an appropriate number of trained contacts with sufficient authority to receive notices, make decisions, and authorize containment, remediation, isolation, or other response actions. ThreatDown may conclusively rely on instructions and approvals from such designated contacts.

- Accurate Emergency Point of Contact Information: Customer must provide ThreatDown 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 must also promptly monitor and respond to ThreatDown

communications, alerts, and requests for input, authorization, or action. ThreatDown will have no liability for any delay, incomplete response, increased impact, or worsened malicious activity caused by Customer's failure to timely respond or act.

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

- Monthly Service Summary: Customer must review the Monthly Service Summary to understand the current status of Service delivered and actively work with ThreatDown to resolve any issues requiring Customer input or action. This includes deployment gaps, misconfigurations, unresolved incidents, and recommended remediation steps. ThreatDown may treat Customer's failure to address such issues as a failure to satisfy the prerequisites for MDR Service delivery.

- Customer Infrastructure and Third-Party Systems: 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). ThreatDown is not responsible for any degradation, incompatibility, or Service issue caused by third-party products, unsupported versions, third-party integrations, customer-side changes, or vendor actions or omissions.

- Pre-Existing Conditions: ThreatDown is not responsible for any threat, compromise, vulnerability, malicious activity, misconfiguration, or other condition that existed before the MDR Service became active for the applicable environment or before Customer completed full deployment and configuration of the required Software and settings.

- Event Notifications: As part of the MDR Service, Customer 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, ThreatDown will endeavor to use commercially reasonable efforts to provide Event Notifications within ten (10) minutes of ThreatDown confirming the Event. Event Notifications will include information known to ThreatDown 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 ThreatDown that it has obtained all applicable consents and authority for ThreatDown to deliver the Service; (ii) giving ThreatDown explicit permission to perform the MDR 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, and 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, and 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); (iii) representing that such access and processing by ThreatDown 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 ThreatDown performs the Service ("Customer Systems"), which may be visible as Customer Data in connection with the Service, and that Customer is authorized to instruct ThreatDown to perform the Service on such Customer Systems. Customer shall defend, indemnify, and hold harmless ThreatDown for any claims

by any third parties relating to: (i) the Service; (ii) Customer's failure to obtain required consents, permissions, or legal authority for ThreatDown to perform the Service; (iii) any allegation that ThreatDown's access to, processing of, or actions within Customer Systems or Customer Data as authorized by Customer violates applicable law or third-party rights; (iv) Customer's breach of its representations, warranties, or responsibilities under this Service Description or the Agreement; or (v) any third party's reliance on Customer's description of the Service that is inconsistent with this Service Description or the Agreement.

- Reporting: Customer acknowledges and agrees that in the course of delivering the Service, ThreatDown 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 to which Customer is subject in one or more territories in which Customer operates. Accordingly, Customer shall remain solely responsible for all such reporting requirements and ThreatDown shall have no liability in this regard whatsoever. Customer is also solely responsible for determining whether any notice to regulators, law enforcement, insurers, customers, employees, vendors, or other third parties is required, appropriate, or advisable.

- Prohibited Uses. Customer agrees that Customer will not use the MDR 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 MDR Services;
  - To use the MDR Services in a way that has a materially detrimental effect upon the performance of the MDR Services for other users;
  - To use or attempt to use the MDR 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 MDR Services by other users;
  - To alter, tamper with or circumvent any aspect of the MDR Services;
  - To test or reverse engineer any of the software or items included as part of the MDR Services in order to find limitations or vulnerabilities.

IV. SERVICE LEVEL OBJECTIVES (SLO)

ThreatDown Managed Services service level objectives ("SLOs") establish non-binding operational targets for certain response-related activities in connection with the delivery of MDR Services. These SLOs are provided solely to help set customer expectations regarding typical service timing and are not warranties, guarantees, service level commitments, or contractual obligations. ThreatDown will use commercially reasonable efforts to work toward these SLOs where Customer has satisfied all applicable prerequisites. Failure to meet any SLO will not constitute a breach of the Agreement, will not give rise to any service credit, refund, termination right, damages claim, or other monetary or equitable relief, and will not expand any warranty, representation, or other obligation of ThreatDown.

Service Level Objective	Target Timeframe
Analyst Engagement Target	30 Minutes
Customer Notification Target	10 Minutes

"Analyst Engagement Target" means the time elapsed between creation of a qualifying MDR case and assignment of that case to an MDR Analyst.

"Customer Notification Target" means the time elapsed between ThreatDown's determination that a significant issue exists requiring customer notification and ThreatDown's initial attempted notification to the designated customer contact of the issue. This notification may take place via case escalation in Nebula, e-mail message to the customer, phone calls to the designated customer POC(s), or some combination thereof. Customer Notification Target measures first attempted outbound notification only and does not measure receipt, delivery, successful contact, customer acknowledgment, or completion of any escalation path.

These SLOs do not apply, and ThreatDown will have no responsibility for any failure to achieve them, to the extent any delay or failure results from: (i) Customer's failure to satisfy the prerequisites for MDR Services; (ii) incomplete deployment, improper or incomplete configuration, or use of unsupported versions or devices, network or connectivity issues outside of ThreatDown's control; (iii) unavailability or degradation of Customer systems, third-party systems, or communications channels; (iv) delays in Customer responses, approvals, access grants, or other required cooperation; (v) outages, maintenance, or emergency conditions; (vi) force majeure events or legal or regulatory restrictions; or (vii) events, alerts, or incidents outside the scope of the MDR Service.

V. SERVICE LEVEL AGREEMENT [MDR PLUS ONLY]

MDR Plus includes a Service Level Agreement (SLA) related to timely notification of Critical Incidents, as defined below. This SLA only applies to customers who have purchased entitlements to the MDR Plus service level. This SLA shall not apply during the first ninety (90) days following the MDR Plus service activation date (the "Onboarding Period"), and no SLA failure may be claimed for any Critical Incident occurring during the Onboarding Period. Customer is not eligible for Service Credits during any period in which Customer is in material breach of the Agreement, this Service Description, or any Order Confirmation, including any period in which Customer has outstanding overdue invoices.

An alert is classified as a "Critical Incident" when a ThreatDown MDR analyst validates that the event meets one or more of the following criteria:

Category	Description	Examples
Ransomware / Destructive Malware	Active execution of ransomware, wiper malware, or any destructive payload confirmed to be running on one or more in-scope assets.	Ransomware file encryption activity, Destructive malware execution
Active Attacks	Any alert determined by the ThreatDown MDR team to be indicative of an active, high-level threat requiring immediate action.	Active intrusion, hands-on-keyboard adversary activity

An alert does not qualify as a Critical Incident until a ThreatDown MDR analyst has reviewed the alert and confirmed it meets the above criteria. For the avoidance of doubt, Customer's own assessment or characterization of an event as critical shall not constitute or substitute for a ThreatDown MDR analyst's determination. Once an alert is determined to be related to a Critical Incident by the ThreatDown MDR team, the team will attempt notification to the customer's designated contact(s) within 45 minutes. Elapsed time shall be measured from ThreatDown's internal system timestamp recording the Critical Incident determination to ThreatDown's internal system timestamp recording the first attempted notification via any of the following channels: case escalation in Nebula, email to the customer's designated contact, or telephone call to the designated point(s) of contact. ThreatDown's internal records shall be the sole and authoritative source for all SLA measurement purposes.

Failure to Meet SLA

An SLA failure occurs when more than 45 minutes elapse between ThreatDown MDR determination of a Critical Incident and attempted notification of the customer's designated contact(s). No failure shall be deemed to have occurred where customer has failed to designate a contact in the ThreatDown system. A single Critical Incident that spans or recurs across multiple calendar months, or multiple alerts, detections, or notifications that ThreatDown reasonably determines arise from or are attributable to the same underlying root cause, threat actor, campaign, vulnerability, misconfiguration, or related series of events, shall be treated as a single SLA event and shall be eligible for a Service Credit only for the calendar month in which the Critical Incident was first determined by ThreatDown. ThreatDown shall have sole and reasonable discretion to determine whether multiple alerts or incidents constitute a single event for purposes of this provision. In the case of a verified SLA failure, the customer is entitled to a Service Credit applied to their account. Service Credits are calculated based on the total number of confirmed SLA Failures in

that calendar month:

SLA Failures in a Calendar Month	Target Timeframe
1-2 late/missed critical notifications	2.5% of Monthly Fee
3 or more late/missed critical notifications	5% of Monthly Fee

Requests for Service Credit
To receive a Service Credit, the customer must:

- Submit a written credit request to ThreatDown at MDR_SLA@threatdown.com within 30 calendar days of the SLA failure occurring, with the subject line "MDR SLA Credit Request" to MDR_SLA@threatdown.com
- Reference the MDR Case number(s) associated with the alleged SLA failure(s)
- Provide any logging or additional supporting evidence of SLA failure

ThreatDown will review the request within 10 Business Days and, if the SLA failure is confirmed in ThreatDown's sole discretion, a credit will be applied to the customer's account. ThreatDown's determination regarding whether an SLA failure has occurred and whether a Service Credit is owed shall be final and binding. Customer's failure to submit the credit request in accordance with the foregoing requirements, including the required content and applicable deadline, shall disqualify Customer from receiving a Service Credit for the applicable SLA failure.

Limits on Credits
Service Credits are subject to the following limitations:

- The maximum total Service Credit in any single Calendar Month is 5% of the Monthly Service Fee, regardless of the number of SLA Failures in that month.
- Customer may claim Service Credits no more than three times during a calendar year.
- Service Credits are the customer's sole and exclusive remedy for any SLA failure and for any failure by ThreatDown to meet the notification timeframes set forth in this Section V. No SLA failure shall constitute a breach of the Agreement, give rise to any termination right, damages claim, or other monetary or equitable relief beyond the Service Credits expressly provided herein.
- Service Credits have no cash value and may not be exchanged, redeemed, or converted into cash, refunds, or any other form of monetary payment. Service Credits do not constitute a debt, accounts payable obligation, or payment obligation of ThreatDown. Service Credits may not be transferred, assigned, or applied to any other customer account, entity, or subscription. Under no circumstances shall Customer be entitled to a refund, offset against amounts owed, rebate, or any other monetary remedy in connection with an SLA failure.
- Service Credits are only a portion of monthly fees related to MDR+, or the bundle it is within, and shall be applicable and issued only if the calculated credit amount for the applicable Calendar Month exceeds one dollar ($1.00 USD).
- Any Service Credits will be applied solely as a discount toward the subscription fees for renewal of the same MDR Plus service (or any successor bundle that includes MDR Plus as a component) for the immediately following subscription term. Service Credits may not be applied to any other ThreatDown product, service, or subscription.
- Each Service Credit shall expire on the later of: (a) twelve (12) months from the date of the SLA failure that gave rise to the Service Credit, or (b) the expiration of the then-current subscription term for the MDR Plus service. Any Service Credit not applied before its expiration date shall be forfeited without further obligation by ThreatDown. **If Customer does not renew its MDR Plus subscription before the applicable expiration date, all outstanding Service Credits shall be forfeited.**

This SLA does not apply, and ThreatDown will have no responsibility for any failure to achieve it, to the extent any delay or failure results from: (i) Customer's failure to satisfy the prerequisites for MDR Services; (ii) incomplete

deployment, improper or incomplete configuration, or use of unsupported versions or devices, network or connectivity issues outside of ThreatDown's control; (iii) unavailability or degradation of Customer systems, third-party systems, or communications channels; (iv) delays in Customer responses, approvals, access grants, or other required cooperation; (v) outages, maintenance, or emergency conditions; (vi) force majeure events or legal or regulatory restrictions; (vii) events, alerts, or incidents outside the scope of the MDR Service; (viii) industry-wide or infrastructure-wide ransomware, cyberwarfare, distributed denial-of-service attacks, zero-day exploits, or other large-scale cyberattacks that impair the ability of the ThreatDown MDR team to address Critical Incidents in a timely manner; (ix) any period in which Customer is in material breach of the Agreement, this Service Description, or any Order Confirmation, including any period in which Customer has outstanding overdue invoices; or (x) Customer's failure to designate a contact in ThreatDown's systems or to maintain accurate and current contact information for its designated contact(s).

VI. ROOT CAUSE ANALYSIS INVESTIGATIONS [MDR PLUS ONLY]

MDR Plus includes limited Root Cause Analysis (RCA) investigations as part of the service. RCA investigations are only provided to customers who have purchased entitlements to the MDR Plus service level and only as expressly described in this Section VI.

Root Cause Analysis Investigation Defined

A Root Cause Analysis investigation is defined as a limited, post-incident operational review performed after a Critical Incident (as defined in the SLA section, above) occurs. The purpose of an RCA investigation is to provide a clearer understanding, based on information reasonably available to ThreatDown, of how an incident may have occurred and to identify potential ways to strengthen the customer's security posture and reduce the likelihood of future incidents.

The RCA investigation delivers a targeted post-incident analysis with suspected root cause findings and remediation guidance, to the extent reasonably determinable from information available to ThreatDown. It is purpose-built for speed and clarity, rather than the depth required by full-scope incident response engagements. Where an investigation requires on-site deployment, advanced forensic examination, live memory analysis, malware reverse engineering, data recovery, chain-of-custody evidence handling, legal or regulatory analysis, or more expansive investigation, the Customer must engage a qualified incident response or other provider to address those needs.

No RCA investigation, finding, report, recommendation, communication, or other assistance provided by ThreatDown will expand the scope of the MDR Plus service, create any obligation to perform additional investigation or remediation, or require ThreatDown to provide incident response, forensic, legal, regulatory, recovery, restoration, remediation, monitoring, consulting, or support services beyond those expressly stated in this Section VI. ThreatDown may identify matters for Customer's consideration, but Customer is solely responsible for determining whether, when, and how to implement any remediation, security, legal, operational, or other response measures.

RCA INVESTIGATIONS ARE OPERATIONAL SERVICE REVIEWS AND ARE NOT FORENSIC INVESTIGATIONS, LEGAL ANALYSES, REGULATORY ASSESSMENTS, OR EXPERT REPORTS. THREATDOWN DOES NOT PRESERVE EVIDENCE FOR LITIGATION, MAINTAIN FORENSIC CHAIN OF CUSTODY, PROVIDE LEGAL ADVICE, DETERMINE WHETHER A LEGAL OR REGULATORY BREACH HAS OCCURRED, OR DETERMINE WHETHER CUSTOMER HAS ANY NOTIFICATION, REPORTING, DISCLOSURE, INSURANCE, LAW ENFORCEMENT, OR SIMILAR OBLIGATION. CUSTOMER REMAINS SOLELY RESPONSIBLE FOR MAKING ALL LEGAL, REGULATORY, INSURANCE, PUBLIC RELATIONS, LAW ENFORCEMENT, AND THIRD-PARTY NOTIFICATION DETERMINATIONS AND FOR ENGAGING ITS OWN COUNSEL, FORENSIC INVESTIGATORS, INCIDENT RESPONSE PROVIDERS, INSURERS, OR OTHER ADVISORS AS CUSTOMER DEEMS APPROPRIATE.

Initiation of RCA Investigation

An RCA investigation may be initiated in ThreatDown's sole discretion upon discovery by the ThreatDown MDR team of a Critical Incident impacting the Customer's environment covered by the ThreatDown MDR Plus service. Customer is not entitled to an RCA investigation unless ThreatDown determines that the applicable incident qualifies for an RCA investigation under this Service Description and that sufficient relevant telemetry, access, and customer cooperation are available to perform the investigation. Upon initiation, a ThreatDown MDR team member will be assigned to lead the investigation, providing a central customer point of contact and continuity throughout the course of the investigation.

The Customer's cooperation is essential to ThreatDown's ability to investigate and respond effectively. Accordingly, the Customer agrees to provide reasonable assistance as requested, including facilitating access to impacted systems, furnishing relevant information in a timely manner, designating personnel with authority to provide approvals and technical information, and accommodating other reasonable requests made by the ThreatDown MDR team in connection with an active investigation. **ThreatDown may suspend, limit, or conclude an RCA investigation if Customer fails to provide timely access, information, approvals, or cooperation requested by ThreatDown.**

RCA Findings Report

Upon completion of an RCA investigation, a formal report will be generated and provided by ThreatDown to Customer within a commercially reasonable period. An RCA investigation will be deemed complete upon the earliest of: (i) ThreatDown's delivery of the RCA report; (ii) exhaustion of the applicable analyst investigative hours; (iii) ThreatDown's determination that further investigation is not reasonably likely to identify additional material findings based on available information; (iv) ThreatDown's determination that further work would require services outside the scope of this Section VI; or (v) Customer's failure to provide required access, information, approvals, or cooperation. This report will contain, as applicable to the specific investigation and to the extent reasonably determined by ThreatDown:

- Executive Summary
- Narrative of Events related to the Incident
- Timeline of Relevant Events
- List of Impacted Hosts and Impacted User Accounts
- Relevant Indicators of Compromise (IOCs)
- Suspected Root Cause (if identified)
- Related Technical Misconfigurations and/or Other Contributing Factors
- Security and Remediation Recommendations

RCA Limitations

The following limitations apply to RCA Investigations:

- RCA investigations are provided on a "best effort" basis, with no guarantees made, of any kind, including but not limited to RCA identification, confirmation, completeness, accuracy, or exhaustiveness of any root cause, initial threat vector, impacted asset, affected account, indicator of compromise, timeline, recommendation, or other finding
- ThreatDown RCA investigations are limited to telemetry available to the ThreatDown MDR team via ThreatDown products and do not include review of data, systems, logs, networks, applications, cloud environments, identity systems, third-party tools, or other sources not made available to and supported by ThreatDown as part of the MDR Plus service
    - These data sources include ThreatDown EP, ThreatDown EDR, and any data fed to ThreatDown via ITDR and/or any future product offerings.
- An RCA investigation is limited to a maximum of 20 analyst investigative hours per investigation, inclusive of investigation, analysis, internal review, customer communications, report preparation, and related activities. Unused hours do not roll over, accrue, or apply to any other investigation, incident, subscription period, or customer account, and ThreatDown has no obligation to extend an RCA investigation or provide additional hours.
- No more than 3 RCA investigations will be performed per customer in a given calendar year. Multiple alerts, detections, incidents, hosts, accounts, or events that ThreatDown reasonably determines arise from or are attributable to the same underlying root cause, threat actor, campaign, vulnerability, misconfiguration, or related series of events will be treated as a single RCA investigation for purposes of this limitation.

If ThreatDown determines that an RCA investigation has reached the applicable hour limit or otherwise requires work outside the scope of this Section VI, ThreatDown may conclude the RCA investigation and, as applicable, identify in the RCA report that additional investigation by Customer or a third-party provider may be appropriate. ThreatDown will have no obligation to continue investigating, preserve or collect additional evidence, review additional data sources, participate in any third-party investigation, or verify findings made by Customer or any third party after the RCA investigation is concluded.

Customer acknowledges that RCA findings are based on information available to ThreatDown at the time of the investigation and may be incomplete, inconclusive, or superseded by later information. Customer shall not represent to any third party that ThreatDown has certified, verified, guaranteed, or conclusively determined the root cause, scope, containment, eradication, recovery, or legal effect of any incident. Any use, disclosure, or reliance on an RCA report by Customer or any third party is at Customer's sole risk and responsibility, subject to the Agreement.

VII. ASSISTANCE AND TECHNICAL SUPPORT

Technical assistance for the Service is provided by ThreatDown:

- ThreatDown Product Support information is located at: https://support.threatdown.com/hc/en-us/articles/4413809450003-Contact-ThreatDown-Support-for-Nebula
- For ThreatDown MDR Support, contact the MDR team via the MDR 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.

VIII. DEFINITIONS

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

"ThreatDown" 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