WatchGuard Managed Detection and Response
Service Description

Last Updated: June 30, 2025

This Service Description describes WatchGuard Technologies, Inc.'s ("**WatchGuard**") Managed Detection and Response ("**MDR**") services offered to Clients by WatchGuard to help identify and validate Detections of security threats to the Client's (or where the Client is an MSP, the Managed Service Recipient's) Covered Assets, conduct Investigations, provide Alerts, and, where applicable, take Response Actions (the "**Service**"). This WatchGuard MDR Service Description ("**Service Description**") is part of and incorporated into the WatchGuard Managed Detection and Response Terms of Service entered into by and between Client and WatchGuard (the "**Agreement**"). To the extent there is a conflict between the terms and conditions of the Agreement and this Service Description, the terms and conditions of this Service Description will take precedence to the extent the conflict pertains to the Service.

1. **Definitions**. Capitalized terms used in this Service Description will have the meanings given to them below or in the Agreement, as applicable.

    1.1. "**Alert**" means a notification and information about a Detection, Investigation or Incident shared by WatchGuard with Client or, where applicable, Delegated Managed Service Recipient.

    1.2. **"Covered Assets"** means any physical or virtual environment, system, or cloud services where MDR Compatible Products are installed and that send security telemetry to the WatchGuard Managed Services Security Stack.

    1.3. "**Detection**" means a condition where data generated by Covered Assets is identified as a potential indicator of malicious or suspicious activity.

    1.4. "**End User**" means: (i) each individual in the Client's organization; or (ii) where Client is an MSP, each individual in the Managed Service Recipient's organization.

    1.5. "**Health**" means the state of configurations and settings for a Managed Endpoint running WGT EDR that affects the efficacy of the security of that Managed Endpoint.

    1.6. "**Health Check**" means the act of reviewing Health to identify configurations and settings that may negatively impact the efficacy of the security of a Managed Endpoint.

    1.7. "**Incident**" means (i) a Detection that, after Investigation, resulted in a confirmed security compromise or unauthorized access to Covered Assets that poses an imminent threat to Covered Assets, or (ii) confirmed security compromise of Client's or, where applicable, Managed Service Recipient's assets reported to Managed Services Team by the Client.

    1.8. "**Incident Response**" is the technical processes performed by the Managed Services Team to take Response Actions with regard to an Incident.

    1.9. "**Investigation**" means a process of gathering and analyzing Detections by Managed Services Team when a Detection or a set of Detections warrant such review.

    1.10. "**Managed Endpoint(s)**" means any physical or virtual endpoint or a server system where WGT EDR or other MDR Compatible Products are installed, up-to-date, and operational in support of delivery of the Service.

    1.11. "**Managed Services Security Stack**" means security stack used by the Managed Services Team to (i) ingest and review Client's (or the relevant Managed Service Recipient's, if applicable) security telemetry data and Detections, (ii) conduct Investigations, and (iii) initiate Response Actions, in each case in connection with providing the Service to Client. For the avoidance of doubt, in no event will Client (or its Managed Service Recipient(s) and/or End User(s)) be permitted to access the WatchGuard Managed Services Security Stack.

1.12. "**Managed Services Team**" means the WatchGuard team conducting security Investigations, Threat Hunting, Response Actions, and Incident Response.

1.13. "**MDR Compatible Products**" means any WatchGuard or third-party products that send security telemetry to the WatchGuard Managed Services Security Stack and can be used in support of the Services as further described in Section 2 and/or Documentation.

1.14. **"MDR Portal"** means web-based interface that consolidates and displays key Service information and allows Client or, where applicable, relevant Managed Service Recipient, to review and monitor Detections, Investigations, and reports, and communicate with Managed Services Team about Investigations.

1.15. "**Remediation Guidance**" means guidance, if any, provided by WatchGuard regarding actions that Client may need to take on Client's and/or Managed Service Recipient's (if applicable) systems or security tools (a) during Threat Response, (b) after WatchGuard's completion of Threat Response.

1.16. "**Response Action**" means action taken by Managed Services Team as a part of Threat Response or Incident Response.

1.17. **"Service Mode"** means Client's or, where applicable, Delegated Managed Service Recipient's business hours and availability during which Managed Services Team can reach the Client.

1.18. "**Threat Hunting**" means the process of proactively and iteratively searching through data originating from the WGT EDR and other MDR Compatible Products using a combination of semi-automated and manual activities to identify the signals and indicators of malicious activity that may have bypassed existing prevention and detection controls.

1.19. "**Threat Intelligence Data**" means any information about malware, threats, actual or attempted security events, including but not limited to their frequency, source, associated code, general identifiers, or attacked sectors or geographies. Threat Intelligence Data includes any indicators of compromise ("**IOCs**") or indicators of attack ("**IOAs**") generated by WatchGuard in connection with the Service.

1.20. "**Threat Response**" means the methods, processes, communications, and Response Actions utilized by WatchGuard to provide the Service in accordance with this Service Description.

1.21. "**Threat Response Mode**" means the type of Response Actions to be taken by the Managed Services Team during delivery of the Service as determined by Client during onboarding.

1.22. "**WGT EDR**" means one or more of the following WatchGuard products, as applicable: WatchGuard Endpoint Protection Detection and Response ("WatchGuard EPDR"), WatchGuard Endpoint Detection and Response ("WatchGuard EDR"), Panda Adaptive Defense, Panda Adaptive Defense 360, WatchGuard Advanced Endpoint Detection and Response, WatchGuard Advanced Endpoint Protection Detection and Response ("WatchGuard Advanced EPDR"), or another endpoint protection product or similar such product offered by WatchGuard or one of its Affiliates and designated by WatchGuard from time to time as being compatible with the Service. WGT EDR expressly excludes WatchGuard Endpoint Protection.

2. **Service Tiers.**

2.1. **Service Tiers.** WatchGuard offers the Service in one of the tiers described below. MDR Compatible Products required for each of the Service tiers are as follows:

Service Tier	MDR Compatible Products
Core MDR	WGT EDR Microsoft 365
Core MDR for Microsoft	Microsoft Defender for Endpoint Microsoft 365
Total MDR	Endpoint security services: WatchGuard EDR, WatchGuard EPDR, and WatchGuard Advanced EPDR (further for the purposes of this Service Description "**WatchGuard Endpoint Security**") Network security services: Firewall Security Services, Network Detection and Response (NDR) Identity security: AuthPoint MFA Cloud services: Microsoft 365, Amazon Web Services, Google Workspace

3. **Clients. Contractual Relationships.**

3.1. WatchGuard will only provide the Service to Clients described in this Section 3.1.:

a) **Direct Clients,** where Client is an organization contracting directly with WatchGuard and receiving the Service directly from WatchGuard for its own purposes ("**Direct Client**").

b) **MSP Clients,** where Client is an MSP that provides Managed Service to Managed Service Recipients, including Delegated Managed Service Recipients ("**MSP Client**").

3.2. **License Agreements.** Client acknowledges and agrees that the use of MDR Compatible Products is subject to the terms of the applicable end user license agreement or such other WatchGuard or third-party terms or written documentation that may be included with the relevant MDR Compatible Products and/or the packaging for any of the foregoing (collectively, the "**License Agreements**").

3.3. **No Contractual Relationship with Managed Service Recipients**. MSP Client shall enter into a written agreement with each Managed Service Recipient as described in Section 16.8. MSP Client hereby acknowledges that WatchGuard has no contractual relationship with the Managed Service Recipients, including Delegated Managed Service Recipients, and WatchGuard's sole liability shall be to the MSP Client.

3.4. **No Warranties by MSP Clients**. MSP Clients shall not, and shall ensure that its employees or agents do not, make any representation, warranty, promise, or guarantee to any Managed Service Recipients, their End Users, or any other party with respect to specifications, features, or capabilities of the Service, WGT EDR, or other MDR Compatible Products that is not contained in or is otherwise inconsistent with, the applicable License Agreement, this Service Description, or other written WatchGuard Documentation. MSP may, however, give instructions for the use of the Service, as well as WGT EDR or MDR Compatible Products that are contained on the applicable product packaging, in the applicable License Agreement, or approved in writing by WatchGuard.

4. **Managed Service Recipient Account Delegation.**

4.1. MSP Clients may delegate certain Managed Service Recipients ("**Delegated Managed Service Recipients**") to WatchGuard by requesting WatchGuard to provide Service to them directly. MSP Clients may delegate a Managed Service Recipient as long as the MSP Client ensures that the requirements described in this Section 4 and Section 5 are met.

4.2. **Service Communications.** MSP Client and Delegated Managed Service Recipient understand and acknowledge that after MSP Client has delegated Managed Service Recipient and such Delegated Managed Service Recipient's onboarding has been completed, WatchGuard will send Alerts, reports and all other communications that form a part of the Service (including, where applicable, requests for approval of certain Response Actions) directly to Delegated Managed Service Recipient and/or per Delegated Managed Service Recipient's preferences communicated to WatchGuard by MSP Client or Delegated Managed Service Recipient during onboarding.

4.3. **MSP Client Role.** For the avoidance of doubt, Delegated Managed Service Recipient is not a party to the Agreement. It is MSP Client's obligation to ensure that:

a) MSP Client and Delegated Managed Service Recipient comply with the terms of the Agreement and this Service Description.
b) MSP Client and Delegated Managed Service Recipient enter into a written agreement as required by Section 16.8.
c) MSP Client and/or Delegated Managed Service Recipient carries out actions described in this Service Description and follows WatchGuard instructions.
d) Delegated Managed Service Recipient understands what actions required to facilitate and enable delivery of the Service have been delegated by MSP Client to Delegated Managed Service Recipient and what actions will be carried out by the MSP Client.

MSP Client is solely responsible for Delegated Managed Service Recipients' non-compliance with this Service Description or WatchGuard's instructions. WatchGuard shall have no liability for any degraded, incomplete, or failed delivery of the Service which may result from Delegated Managed Service Recipient's failure to take the required actions.

5. **Service Minimum Requirements.**

5.1. **Minimum Requirements for Direct Clients.** Direct Client must ensure that Direct Client (a) has previously acquired and installed or is acquiring and will install, prior to commencement of the Service WGT EDR (for Core MDR), WatchGuard Endpoint Security (for Total MDR) or Microsoft Defender for Endpoint (for Core MDR for Microsoft) licenses for at least twenty five (25) Managed Endpoints, and (b) has a dedicated internal team that consists of an appropriate number of suitably skilled IT personnel who will work with WatchGuard during the provision of the Service. Direct Client's identified personnel must have the necessary technical and business knowledge and authority to make decisions concerning the Service.

5.2. **Minimum Requirements for MSP Clients**. Where Client is an MSP Client, Client must ensure that each Managed Service Recipient has previously acquired and installed or is acquiring and will install, prior to commencement of the Service WGT EDR (for Core MDR), WatchGuard Endpoint Security (for Total MDR), or Microsoft Defender for Endpoint (for Core MDR for Defender) licenses for at least five (5) Managed Endpoints.

5.3. **Minimum Requirements for Delegated Managed Service Recipients.** In addition to minimum requirements in Section 5.2. above, for Delegated Managed Service Recipients, MSP Clients shall ensure that Delegated Managed Service Recipient has or, prior to commencement of the Service, will have a dedicated ***internal*** team that consists of an appropriate number of suitably skilled IT personnel who will work with WatchGuard during the provision of the Service. Delegated Managed Service Recipient's identified personnel must have the necessary technical and business knowledge and authority to make decisions concerning the Service.

6. **Service Scope.** WatchGuard will provide the Service in accordance with the Agreement entered into by and between Client and WatchGuard and this Service Description. Service scope is further described in Sections 7 through 15. All activities that are not expressly provided in this Service Description are outside of the scope of the Service. Client is solely responsible and liable for: (i) taking any actions that are outside of the scope of the Service (e.g., remediation, litigation and e-Discovery support, and collaboration with law enforcement); and (ii) for any actions undertaken by WatchGuard under Client's specific direction that are not provided in this Service Description. Client acknowledges and agrees WatchGuard is not responsible for any security incidents, threats or compromises that occurred or existed prior to Service start date or on Client's systems that were not Covered Assets. In addition, Client is responsible for neutralizing any Incidents and/or confirmed threats in third-party systems.

7. **Client Onboarding.**

   7.1. All Clients must be onboarded by WatchGuard prior to receiving or receiving and reselling the Service. During the onboarding process, and as a pre-condition to the delivery of the Service, Client must perform the activities described in this Section 7.1. MSP Clients may be required to perform some or all of the activities described in this Section 7.1 for each Managed Service Recipient, as directed by WatchGuard.

   a) Contact Information. Client will (i) provide contact information of the individuals designated by Client to receive communications from WatchGuard, and (ii) determine Client communication preferences (i.e., email, phone, etc.). For clarity, MSP Clients must act as the contact for any Service to be provided to its Managed Service Recipient, except where Service is provided to Delegated Managed Service Recipient who, per MSP Client's instructions, is contacted by WatchGuard directly as described in Section 4.2. Client is solely responsible for ensuring it notifies WatchGuard of any changes to any contact information provided to WatchGuard during the onboarding process (either its own or its Delegated Managed Service Recipient's), and Client expressly acknowledges and agrees that WatchGuard shall not be responsible or liable for any delays or Service delivery failures arising out of Client's failure to update its or its Delegated Managed Service Recipient's designated contact information.

   b) Threat Response Mode. Where applicable, Client must select the desired Threat Response Mode for the Managed Services Team's interaction with Client's or, where applicable, with Delegated Managed Service Recipient's Covered Assets as further described in Section 10.

   c) Service Mode. Client must select 24/7 or 8/5 Service Mode for itself and/or, where appliable, its Delegated Managed Service Recipient.

   d) Installation of MDR Compatible Products. Client will ensure that, where applicable, MDR Compatible Products are installed on all Covered Assets to be covered by the Service prior to commencement of the Service.

   e) Configuration Requirements. WatchGuard may provide a list of configuration requirements to Client or, where applicable, Delegated Managed Service Recipient. Client will ensure all such configuration requirements are implemented and notify WatchGuard when all configuration requirements have been met. If Client's, Managed Service Recipient's, or, where applicable, Delegated Managed Service Recipient's environment has any incompatibility with configuration requirements designated by WatchGuard, Client must promptly notify WatchGuard thereof, and WatchGuard will determine what changes, if any, Client must make in order to meet the configuration requirements and receive the Service. Client acknowledges and agrees that, to ensure Service continuity, upon Service activation, WatchGuard will have access to Client's Service configuration and the configuration of Covered Assets to the extent necessary to provide the Service.

   f) Initial Health Check. The Managed Services Team will run a Health Check on all Managed Endpoints running WGT EDR as part of the onboarding process. Client or, where applicable, Delegated Managed Service Recipient will be notified of any configurations or issues that

could diminish Client's, Delegated Managed Service Recipient's or other Managed Service Recipient's security posture along with any required steps to remediate the issues identified by the Health Check. Client or, where applicable, Delegated Managed Service Recipient must remediate any known issues before the onboarding process is considered completed.

8. **Monitoring, Detection, and Threat Hunting**. WatchGuard will monitor and conduct analysis of Client's or Managed Service Recipient's security telemetry data to identify, aggregate, and prioritize Detections. WatchGuard will also make reasonable efforts to conduct proactive Threat Hunting to search for threats that may have evaded existing detection controls based on threat intelligence and relevant indicators of compromise observed in Threat Response engagements and Investigations. Threat Hunting will only be provided in relation to data collected from Covered Assets and will focus on identification of attacker behaviors and tactics. If Threat Hunting reveals indicators of malicious activity, an Investigation will be performed.

9. **Investigations.** WatchGuard will perform Investigations as needed to review and assess threats or malicious activity within Detections and in case of a confirmed Incident. During the course of performing the Service, WatchGuard may use the results of Investigations to filter out expected activity to enhance the visibility of suspicious activities in Client's or Managed Service Recipient's environment.

10. **Threat Response.**

    10.1. WatchGuard will interact with Covered Assets to perform Investigations and conduct Threat Response by taking Response Actions such as, without limitation, quarantining Managed Endpoints, terminating processes, or blocking IP addresses or authentications. Response Actions are determined based on the nature of the threat and Covered Assets. Depending on the Service tier and Covered Assets involved, Client may have the option to select preferred Threat Response Mode.

    10.2. Threat Response Modes for Managed Endpoints – Applicable Only to Core MDR and Total MDR. When an Investigation in relation to Detections from Managed Endpoints warrants Threat Response, WatchGuard will take the following Response Actions depending on the Threat Response Mode selected by the Client during onboarding:

        a) **Alert**: WatchGuard will conduct Investigations and, where applicable, will provide Alerts to Client or, where applicable, Delegated Managed Service Recipient, but WatchGuard will not quarantine Managed Endpoints without Client's or, where applicable, Delegated Managed Service Recipient's prior consent or active involvement. WatchGuard will notify Client or, where applicable, Delegated Managed Service Recipient of Alerts in accordance with the pre-selected communication preferences.

        b) **Conditionally Quarantine**: WatchGuard will perform the Response Actions identified in Section 10.2(a) above. WatchGuard will quarantine Managed Endpoints only if, after these Response Actions are performed, (A) there is no response or active involvement from the Client or, where applicable, from the Delegated Managed Service Recipient within a twenty-four (24) hour period, OR (B) Response Actions are performed outside of Client's or, where applicable, Delegated Managed Service Recipient's Service Mode that has been selected during onboarding or otherwise communicated to WatchGuard in writing. WatchGuard will notify Client or, where applicable, Delegated Managed Service Recipient of quarantine actions taken in accordance with the pre-selected communication preferences.

        c) **Quarantine**: WatchGuard will perform the Response Actions identified in Section 10.2(a) above and quarantine Managed Endpoints. WatchGuard will notify Client or, where applicable, Delegated Managed Service Recipient of quarantine actions taken in accordance with the pre-selected communication preferences.

10.3. Threat Response for Assets of Interest – Applicable Only to Core MDR and Total MDR. With regard to Managed Endpoints, Client or, where applicable, Delegated Managed Service Recipient may identify to WatchGuard any specific Managed Endpoints to which rules and/or Responses Actions that are different from, or in addition to, the Threat Response Mode may apply ("**Assets of Interest**"). Client or, where applicable, Delegated Managed Service Recipient and WatchGuard will agree on the rules and/or Response Actions (if any) that will apply in respect of any Assets of Interest.

10.4. Threat Response Mode for Microsoft 365 – Applicable to Core MDR, Core MDR for Microsoft and Total MDR. WatchGuard will be able to disable Microsoft 365 accounts if Client chooses to provide such access to WatchGuard during onboarding and Service configuration.

10.5. Threat Response for Covered Assets under Total MDR. Except as otherwise provided above, for Total MDR, WatchGuard will take Response Actions in accordance with applicable Documentation without any specific authorization from Client.

10.6. Remediation Guidance. Where possible, WatchGuard may also provide Remediation Guidance as part of Threat Response, updating the Remediation Guidance, if any, periodically for a maximum of three (3) days from the first date an Alert was communicated to Client.

11. **Authorization to Take Response Actions.**

11.1. Where Client selected a Threat Response Mode that authorizes WatchGuard to take Response Actions such as, but not limited to quarantining Managed Endpoints, killing processes, disabling accounts, or where WatchGuard takes such actions by default (e.g. as a part of Total MDR), WatchGuard may utilize WatchGuard tools to take such Response Actions. Apart from conditions identified in Section 10, Response Actions will not require any additional approval, unless otherwise agreed to by the parties in relation to any Asset(s) of Interest. Where the parties previously agreed that different/additional rules or Response Actions apply in respect to Assets of Interest, WatchGuard will request any necessary authorization before performing Response Actions with regard to those Assets of Interest.

11.2. CLIENT ACKNOWLEDGES AND AGREES THAT CLIENT'S AUTHORIZATION FOR WATCHGUARD TO TAKE RESPONSE ACTIONS COULD RESULT IN INTERRUPTION OR DEGRADATION OF CLIENT'S AND/OR THE MANAGED SERVICE RECIPIENT'S SYSTEMS AND INFRASTRUCTURE. WATCHGUARD WILL HAVE NO LIABILITY TO THE CLIENT OR MANAGED SERVICE RECIPIENT, IF APPLICABLE, FOR ANY DAMAGES ARISING FROM OR RELATED TO SUCH INTERRUPTION OR DEGRADATION OF CLIENT'S AND/OR THE MANAGED SERVICE RECIPIENT'S SYSTEMS AND INFRASTRUCTURE. CLIENT FURTHER ACKNOWLEDGES THAT FAILURE TO GRANT AUTHORIZATION FOR SUCH RESPONSE ACTIONS COULD RESULT IN NEW MALICIOUS ACTIVITY OR THE WORSENING OF EXISTING MALICIOUS ACTIVITY. WATCHGUARD WILL HAVE NO LIABILITY TO CLIENT OR MANAGED SERVICE RECIPIENT, IF APPLICABLE, FOR ANY DAMAGES ARISING FROM OR RELATED TO SUCH NEW OR WORSENED MALICIOUS ACTIVITY IF CLIENT HAS DENIED WATCHGUARD'S REQUEST FOR AUTHORIZATION TO TAKE A CERTAIN RESPONSE ACTION.

12. **Incident Response**.

12.1. If Client or Managed Service Recipient experiences an Incident, Managed Services Team will conduct Incident Response. During Incident Response, Managed Services Team will make reasonable efforts to mitigate the Incident by prioritizing Incident related Response Actions, Investigations, and Client communications. Incident Response will be limited to a period of twenty-four (24) hours from the moment WGT or Client were alerted about an Incident, unless otherwise agreed by WatchGuard and Client in writing.

12.2. In no event, will Incident Response include Incident remediation, discovery of assets that are not Covered Assets, ad hoc vulnerability or Dark Web scans, attacker negotiation, actions related to law enforcement or victim notification, forensics, insurance reporting, or system hardening.

13. **Service Availability.** All monitoring, detection, Investigation, and Threat Response described in Sections 8,9, and 10 will be provided on a 24/7/365 basis. Client will also have direct call-in access and email access to the Managed Services Team to review suspected Incidents on a 24/7/365 basis. The contact details for such access to the Managed Services Team, as of the date of this Service Description are as follows:

    Americas: +1 646-435-0011

    EMEA: +34 919037244

    Email: support.mdr@watchguard.com

14. **Service Level Targets**. The following service level targets are intended to provide Client with guidelines around timing expectations for various aspects of the Service (the "**Service Levels**"). These targets only apply to Investigations on Covered Assets.

Issue	**Target Notification Time**	**Notification method***
Ongoing intrusion	In real-time	By email By phone
Red team tests or internal tests (where WatchGuard is notified of Red team testing ahead of time)	In real-time	By email
Critical Detections	In real-time	By email By phone
Non-Critical Detections	In real-time	By email
Detections that require more context from the Client	In real-time	By email
Protection Errors	Monthly reports	
Bad administration or software usage practices	Monthly reports	
Issues relating to devices that are not Managed Endpoints	Monthly reports	
Non conformant settings	Monthly reports	

*The notification method above shall control unless Client selects a different notification method during the onboarding process.

As used in the table above, the following terms have the meanings given below:

a) "**business hours**" means the customary business hours in the Client's location.

b) "**In real-time**" means that the Managed Services Team will notify the Client promptly upon confirmation of the relevant issue.

c) "**Protection Error**" means an error related to the protection behavior for one or more Managed Endpoint(s) that WatchGuard can or has detected in connection with a Health Check.

d) "**Red team test**" means an exercise reflecting real-world conditions that is conducted as a simulated adversarial attempt to compromise organizational missions or business processes

to provide a comprehensive assessment of the security capabilities of an organization and its systems.

15. **Reporting.**

15.1. Incident Reports. Periodically, WatchGuard may provide Client or, where applicable, Delegated Managed Service Recipient with reports relating to Detections, Investigations, and Response Actions.

15.2. Monthly Status Report. WatchGuard will, on a monthly basis, provide to Client a status report that provides information for the previous month's Service activity.

15.3. All reports provided by WatchGuard to Client in connection with the Service are hereby deemed WatchGuard Materials, as that term is defined and used in the Agreement.

16. **Client Responsibilities**. Client acknowledges and agrees that Client or, where applicable, Delegated Managed Service Recipient must take the following actions to facilitate and enable delivery of the Service, and WatchGuard shall have no liability for any degraded, incomplete, or failed delivery of the Service which may result from Client's failure to take the required actions.

16.1. **Onboarding**. Client will perform all required activities during the onboarding process.

16.2. **Installation Requirements**. Client or, where applicable, Delegated Managed Service Recipient must:

a) have a valid and active account for the applicable MDR Compatible Products;

b) deploy and configure the applicable MDR Compatible Products;

c) maintain compliance with all requirements identified in the Health Checks;

d) meet minimum system requirements to install the MDR Compatible Products; and

e) run only supported versions of the MDR Compatible Products.

Additionally, Client will use best efforts to ensure that: (i) MDR Compatible Products are deployed on at least eighty percent (80%) of Client's serviceable environment or (ii) where Client is an MSP, MDR Compatible Products are deployed on at least eighty percent (80%) of the applicable Managed Service Recipient's serviceable environment, as this is necessary to provide the Managed Services Team with sufficient visibility into the environment for delivery of the Service.

16.3. **Remediating Known Threats**. Client must and must ensure that Managed Service Recipients make reasonable efforts to timely remediate any threats and compromises reported by WatchGuard or by other third-party technologies that Client or the Managed Service Recipient, if applicable, utilizes for cybersecurity detection and protection. WatchGuard will not be responsible or liable for any issues caused by Client's or the applicable Managed Service Recipient's failure to take remediation steps in a timely manner. Additionally, WatchGuard shall have no obligation to notify Client or Delegated Managed Service Recipient and generate new Alerts for Detections where WatchGuard provided an Alert for Covered Assets if Client or Delegated Managed Service Recipient fails to take remediation steps or follow WatchGuard's Remediation Guidance (if such Remediation Guidance was provided).

16.4. **Time and Date Settings**. Client or, where applicable, Delegated Managed Service Recipient must ensure that all Managed Endpoints and, if applicable, other Covered Assets have accurate time and date settings. WatchGuard will not be responsible for errors, issues, or residual risk experienced or incurred by Client or Managed Service Recipient for Detections generated by Managed Endpoints or, if applicable, other Covered Assets with inaccurate time and date settings.

16.5. **Client Personnel**. Client must identify an appropriate number of suitably skilled personnel who will work with WatchGuard during the provision of the Service. Client's identified personnel must have the necessary technical and business knowledge and authority to make decisions concerning the Service.

16.6. **Timely Response**. Client or, where applicable, Delegated Managed Service Recipient must promptly acknowledge receipt of WatchGuard's communications in writing (via email, MDR Portal or other agreed method) and must timely respond to WatchGuard's requests.

16.7. **Actions taken by Third Parties**. Client may allow third parties to take certain actions within the scope of the Service on behalf of Client, in which case Client is responsible for all actions and omissions of such third party, including Delegated Managed Service Recipient. WatchGuard will not be liable for any actions or omissions of third parties. WatchGuard will also not be liable for any actions or omissions caused by MSP Client's failure to perform its duties as to Delegated Managed Service Recipient as described in Section 4.

16.8. **Managed Service Recipient Agreement**. MSP Clients must enter into written agreements with Managed Service Recipients (each, an "**Managed Service Recipient Agreement**"). As part of the Managed Service Recipient Agreement, MSP must present this Service Description and the Agreement to the Managed Service Recipient and obtain their acceptance of the terms and conditions of this Service Description and the Agreement. MSP will provide copies of such Managed Service Recipient Agreements to WatchGuard upon request. MSP is solely responsible for: ensuring that any Managed Service Recipient for which MSP receives this Service has agreed to accept all risks described in this Service Description or otherwise inherent in the Service. MSP Client will indemnify and hold WatchGuard harmless for any claim brought against WatchGuard by a Managed Service Recipient if such claim results, in whole or in part, from MSP's failure to fully perform its obligations under this Section 16.8.

17. **Threat Intelligence Data.** WatchGuard may collect, access, use, process, transmit, or store Threat Intelligence Data, including in connection with its provision of the Service, for: (a) product improvement; (b) research and development purposes; and (c) deriving statistical data using information that is aggregated, anonymized, de-identified, or otherwise rendered not reasonably associated or linked to an identifiable individual or to Client or End Users. WatchGuard retains all intellectual property rights in such Threat Intelligence Data. WatchGuard may share Threat Intelligence Data with selected reputable members of the IT industry for the purposes of promoting awareness of security risks, and anti-spam and security threat research.

18. **Service Language**. WatchGuard offers the Service in English.

19. **Exclusions**. WatchGuard is not responsible for (a) any activities that are not expressly provided in this Service Description, including, without limitation, remediation of Incidents; (b) any Incidents, threats, or compromises that occurred or existed prior to the Service start date; (c) any Incidents, threats, or compromises that exist in Client's or Managed Service Recipient's systems that are not Covered Assets. Client agrees and acknowledges that WatchGuard will not be liable or be considered in breach of this Service Description (including any applicable Service Level targets): (i) due to any delay or failure to perform its obligations hereunder as a result of industry or infrastructure wide ransomware, cyberwarfare, or other cyberattacks that causes WatchGuard to be unable to provide resources to address an Incident in a timely manner; (ii) due to unforeseen circumstances or any Force Majeure event; (iii) due to legal prohibition, including but not limited to, passing of a statute, decree, regulation, or order; (iv) during any period of Service suspension by WatchGuard in accordance with the terms of this Service Description; (v) if Client is in breach of the Agreement or failed to perform actions required under this Service Description; or (vi) during any scheduled maintenance windows for MDR Compatible Products.

20. **Modifications to the Service; Modifications to Service Description**. Notwithstanding anything to the contrary in the Agreement or this Service Description, Client acknowledges and agrees that WatchGuard may from time to time modify, replace, update, or improve the Service or any portion thereof in WatchGuard's discretion at any time during or after the Term and that WatchGuard may discontinue or limit the sale of the Service at any time in its sole discretion. Changes to the Service may be applied automatically and with or without notice to Client, though WatchGuard will use commercially reasonable efforts to notify Client of any changes within a reasonable period of time where practicable. Additionally, some changes to the Service may require action on the part of Client or the Managed

Service Recipient, where applicable (for example, but not by way of limitation, configuration changes). The terms and conditions of this Service Description and the Agreement shall continue to apply to the Service as modified, replaced, updated, or improved. Notwithstanding the foregoing, WatchGuard may modify or update this Service Description at any time to accurately reflect the Service being provided by providing notice of the modifications or updates to Client (but without Client's approval or consent). Unless WatchGuard says otherwise in its notice, the modified or updated Service Description will become effective immediately, and Client's continued use of the Service after WatchGuard provides Client with such notice indicates Client's acceptance of the updated/modified Service Description. If Client does not agree to the updated or modified Service Description, Client must terminate the Agreement and its access to and use of the Service.

21. **Suspension**. WatchGuard reserves the right to immediately suspend its provision of, and Client's access to, the Service if Client, Managed Service Recipient, or Delegated Managed Service Recipient fails to perform any of its obligations set forth in this Service Description or the Agreement, including, without limitation, (i) Client's failure to pay fees for the Service when due, (ii) Client's or Delegated Managed Service Recipient's failure provide or keep up-to-date any information required by WatchGuard to provide the Service, (iii) non-renewal or termination or expiration of Client's, Managed Service Recipient's, or Delegated Managed Service Recipient's license(s) to use WGT EDR or other MDR Compatible Products, or (iv) Client's or Delegated Managed Service Recipient's failure to investigate or remediate any issues identified by WatchGuard during a Health check or Remediation Guidance provided to Client. WatchGuard will resume provision of the Service to Client when Client cures the event giving rise to the suspension to WatchGuard's reasonable satisfaction. Any suspension by WatchGuard under this Section 21 will not relieve Client of its obligations under the Agreement or this Service Description, including Client's obligation to pay the fees (whether to WatchGuard or an Authorized Partner) for the Service.

22. **Disclaimer**. Without limiting Section 6 of the Agreement, WatchGuard does not guarantee that the Service (a) will detect, prevent, or mitigate all Incidents, or (b) be uninterrupted, timely, or error-free. Under no circumstances shall WatchGuard be held responsible (i) for any error or malfunction caused by external elements, including MDR Compatible Products other than WGT EDR and/or other external hardware or software, related to or otherwise used in connection with the Service; (ii) for any issues arising out of any assets that are not Covered Assets; (iii) for any issues arising due to Client's or Managed Service Recipients failure to comply with this Service Description; (iv) for any issues arising out of or relating to Client's and Managed Service Recipients, where applicable, failure to comply with the terms of the Agreement or relevant License Agreements. Client acknowledges that for the Services to be effective, WGT EDR and other MDR Compatible Products on all Covered Assets must always be up to date, which may require involving the IT resources of Client or the Managed Service Recipient, where appropriate. For this reason, WatchGuard expressly disclaims any and all liability and responsibility arising from or in connection with Client's or the Managed Service Recipient's failure to allow or facilitate the provision of the updates required to achieve said maximum effectiveness. Client accepts responsibility for any losses and/or damages and costs arising from any incompatibility between WGT EDR or MDR Compatible Products and any other third-party software or service that Client, or Managed Service Recipient, may have installed on its Managed Endpoints, as well as any other problems that may arise due to the interaction between programs or services.