Trellix Managed Detection and Response Service Description

INTRODUCTION

This Trellix Managed Detection and Response Service Description (the "Service Description") describes the threat management services Trellix provides either directly to Customer or through Trellix authorized partner(s) ("the MDR Service(s)"), utilizing Trellix Endpoint Protection (ENS) and Endpoint Detection & Response (EDR) solutions, to provide continuous threat monitoring, endpoint incident response, and seamless remediation against sophisticated cyberattacks. All capitalized terms in this Service Description have the meaning ascribed to them in the Agreement (defined below) or in the Definitions section below.

This Service Description is part of and incorporated into, as applicable: (i) the agreement between Customer and Trellix covering the purchase of an MDR Service subscription; (ii) if no such signed agreement exists, this Service Description will be governed by the terms of the Trellix End User License Agreement posted at https://www.trellix.com/about/legal/ and, if applicable, the Professional Service Terms and Conditions also posted at https://www.trellix.com/about/legal/. The terms and conditions of this Service Description will take precedence over the terms and conditions of any other agreement between Trellix and Customer, in the event of a conflict(s).

Notwithstanding anything to the contrary in the Agreement, Customer acknowledges and agrees that:

- Trellix may modify or update the MDR Services from time to time without materially reducing or degrading its overall functionality.
- Customer agrees that Trellix has the right to modify this Service Description at any time without notice, and any updated Service Description will take the place of any previous Service Description, and will become effective, made part of and incorporated into the Agreement upon posting to https://www.trellix.com/about/legal/.

THE MDR SERVICES:

Trellix's MDR Services provides Customers with Trellix Endpoint Security management and threat response on a 24x7x365 basis. MDR Team experts align closely with Customers on operational goals and implement playbooks for streamlined threat detection and incident handling. The MDR Services extends to all Customer endpoints and systems managed within the Trellix ePO platform that have Trellix Endpoint Detection and Response installed in order to ensure protection that aligns with each Customer's security posture.

Endpoints managed under Trellix are configured and monitored using standardized security playbooks. Upon detection of a threat, the MDR team follows these playbooks to investigate and respond—whether by remote mitigation, notifying stakeholders, or escalation. Trellix automation in detection engineering allows for rapid threat identification and effective responses without manual intervention.

DEFINITIONS

The following capitalized terms are used in this Service Description and shall have the meanings set forth below:

1. **Agreement**: The contractual terms governing the relationship between Trellix and the Customer, including this Service Description, applicable order forms, and the Trellix End User License Agreement or other mutually agreed and signed terms including, when applicable, the Professional Service Terms and Conditions.
2. **Case**: A record created during the MDR Services that documents the analysis, investigation, or response to a Detection, Incident, or other security-related activity.
3. **Customer**: The organization subscribing to the MDR Services.
4. **Detection**: An alert generated by Trellix's systems indicating potentially malicious or suspicious activity within the Customer's environment.
5. **Endpoint Software**: Trellix-provided software installed on Managed Endpoints to facilitate threat detection, analysis, and response.
6. **Incident**: A confirmed security event that may require investigation, response, or remediation.
7. **Investigation**: The process of analyzing Detections, Cases, and related security data to determine the presence, scope, and severity of a potential Incident.
8. **Managed Endpoint**: A device or system within the Customer's environment that has Trellix Endpoint Software installed and is monitored as part of the MDR Services.
9. **Response Actions**: Actions taken by the MDR Team to mitigate, contain, or remediate identified threats, such as isolating endpoints, removing malicious files, or providing guidance for third party remediation.
10. **MDR Team**: Refers to the Trellix team or any third party contractors engaged by Trellix to deliver the MDR Services. This includes, but is not limited to, activities such as monitoring, investigation, response, and threat hunting.
11. **MDR Services**: Trellix Managed Detection and Response (MDR) subscription service offering, as described in this Service Description, including its associated features, activities, and deliverables.
12. **Service Level Targets (SLTs)**: Target timeframes for specific MDR Services actions, such as Case creation or initial Response Actions, designed to set timing expectations for the Customer.
13. **Third-Party Systems**: Non-Trellix systems, platforms, or software integrated with the Customer's environment that may transmit security telemetry to Trellix or require coordination for Incident response.

SCOPE OF MDR SERVICES

Activities Applicable to the Trellix MDR Services Offering

1.1 Onboarding

To receive the MDR Services, Customer must (i) provide Trellix with an authorized Customer contact information including an email address, (ii) install the Trellix Endpoint Security solution on all Managed Endpoints to be covered by the MDR Services, and (iii) classify Customer assets by risk level and agreed Response Actions.

1.2 Monitoring and Triage, Investigation, and Response Actions

The MDR Team will conduct the following activities for Cases originating from Managed Endpoints:

- Monitoring and Triage: Analyze Detections to enhance identification, aggregation, and prioritization of threats, leading to a Case.
- Investigation: Investigate confirmed threats and perform Response Actions where appropriate. Investigations will also improve detection accuracy by filtering out expected activities.
- Response Actions: Notify the Customer of Case details based on pre-selected communication preferences. For clarity, threat response includes (1) the containment and disruption of threats, (2) Endpoint isolation of Managed Endpoints, and (3) providing remediation guidance and recommendations where applicable.

1.3 Availability of MDR Services

All monitoring, investigation, and Response Actions described in Section 1.2 will be available 24/7/365. The Customer also has direct access to the MDR Team for suspected Incident reviews around the clock.

1.4 Trellix Products and Solution Coverage currently functional with MDR Services

- ePolicy Orchestrator (ePO) SaaS
- Endpoint Security (ENS)
- Endpoint Detection & Response (EDR)
- Threat Intelligence Exchange (TIE)
- Insights

1.5 Service Level Targets (SLT)

The following service level targets define timing expectations for Case creation and Response Actions:

Detection Level / Customer Request	**Response Time**
Critical	1 Hour
High	2 Hours
Medium	24 Hours
Customer general requests via email	Next Business Day

CUSTOMER RESPONSIBILITIES

The Customer acknowledges and agrees that the Customer must take the following actions to facilitate and enable the delivery of the MDR Services and Trellix shall not be liable for degraded, incomplete, or failed MDR Services delivery resulting from the Customer's failure to take the required actions described here. Trellix reserves the right to suspend MDR Services until the required actions are completed. Failure to complete these required actions after written notice from Trellix (including email notice from the MDR Team to the Customer's designated contacts) shall constitute a material breach of the Agreement.

1. Onboarding and Installation Requirements

The Customer must do the following in order to complete the onboarding process.

- Have a valid, active Trellix Endpoint subscription.
- Properly deploy and configure the applicable Endpoint Software on all Managed Endpoints.
- In relation to (b) above, review the Operating Guide and follow all instructions found therein in order to enable the MDR Services.
- Meet minimum system requirements for Trellix software installation.
- Ensure that only supported versions of Trellix software and/or third-party security tools are in use.

Trellix will not be responsible for issues, problems, or errors caused by the Customer's failure to properly configure or enable the recommended security settings or otherwise meet these requirements, nor will Trellix be responsible for an endpoint which is not a Managed Endpoint.

2. Remediating Known Threats

The Customer must take reasonable steps to remediate compromises reported by Trellix or other third party technologies in a timely manner. Trellix will not be liable for issues resulting from the Customer's failure to take remediation steps promptly. The MDR Team is not obligated to notify the Customer or generate new Cases for Detections where remediation recommendations have already been provided to Customer.

3. Customer Personnel

The Customer must identify a sufficient number of appropriately skilled personnel to collaborate with the MDR Team during MDR Services delivery. These personnel must possess the necessary technical and business knowledge and authority to make decisions related to use of the MDR Services.

4. Timely Response

The Customer must promptly acknowledge receipt of communications from Trellix and respond to requests in a timely manner.

5. Customer Systems

The Customer must ensure that all Customer systems function correctly throughout the MDR Services term and must immediately notify Trellix if any issues arise. Trellix will work with the Customer to address telemetry transmission issues from systems where feasible.

ACTIONS OUTSIDE THE SCOPE OF MDR SERVICES

Any activities not expressly and explicitly outlined as a Trellix responsibility in this Service Description fall outside the scope of the MDR Services. The Customer is solely responsible for:

- Taking actions outside the scope of the MDR Services (e.g., on-site response, litigation and e

Discovery support, and law enforcement collaboration, etc.).

• Directing any actions performed by the MDR Team outside the defined scope of this Service Description. This scenario would be covered under a separate SOW.

The MDR Services focus on **initial containment and remediation actions** for detected threats. The MDR Services do not include in-depth incident investigation, forensic analysis, or root cause analysis. In cases where advanced investigation is required, the MDR Team will notify the Customer and may recommend engaging a dedicated Incident Response team for forensic investigation.

The MDR Services do not cover, e.g., those security incidents, threats, or compromises that occurred prior to the start date of the MDR Services subscription, or, for example, which have originated from an endpoint which is not a Managed Endpoint.

Additionally, the Customer is responsible for neutralizing Incidents or confirmed threats in Third-Party Systems.

.

ADDITIONAL TERMS

1. MDR Services Exclusions and/or excusable delays

Customer assumes full responsibility for all actions or omissions by Customer and all parties acting on behalf of Customer. Trellix is not liable for such actions or omissions.

The Customer acknowledges and agrees that Trellix will not be liable or considered in breach of this Service Description or the Agreement (including any applicable SLT) under circumstances which include the below:

• Any delay or failure to perform obligations resulting from widespread ransomware, cyberwarfare, or other industry-wide cyberattacks that prevent the MDR Team from addressing an Incident in a timely manner.

• Unforeseen circumstances or causes beyond Trellix's reasonable control, including but not limited to war, strikes, riots, criminal acts, acts of God, or resource shortages.

• Legal prohibitions, such as new statutes, decrees, regulations, or orders.

• Any period of MDR Services suspension by Trellix in accordance with the terms of the Agreement.

• Customer's failure or delay in the performance of a specific task, obligation, or responsibility under the Agreement or this Service Description.

• The MDR Team's reliance on erroneous, insufficient, or incomplete instructions, authorizations, or information from Customer or a third party on behalf of Customer.

• Any updates or modifications to the Customer's environment that impact the MDR Team's ability to provide the MDR Services. This includes but is not limited to changes made to any Customer or third party products that may affect the MDR Services. Examples include updates in operating systems, deployment tools, changes in administrative rights, etc.

• The Customer being in breach of the Agreement, including but not limited to overdue invoices.

- During any scheduled maintenance windows.
- Outages of any nature that are not caused by Trellix.
    - No travel is included in MDR Services and if a Customer requires travel the Customer will be required execute a separate SOW with Trellix.

2. MDR Services Capabilities

The Customer acknowledges and agrees that while Trellix has implemented commercially reasonable technologies and processes as part of the MDR Services, Trellix makes no guarantee that the MDR Services will detect, prevent, or mitigate all Incidents. The Customer agrees not to make any representations or warranties to third parties suggesting that Trellix has provided such guarantees or warranties.

3. Language of Communication and Documentation

All communications, reports, and documentation provided under this Service Description and the Agreement shall be conducted in English. This includes but is not limited to status updates, deliverables, technical reports, training materials, and any correspondence related to the scope of work. Any translation needs or requirements shall be the responsibility of the requesting party unless explicitly agreed otherwise in writing.

4. Workforce and Data Storage Location

The majority of personnel performing the MDR Services described in this Service Description are based in the United States. Additionally, data storage and processing related to the MDR Services are primarily conducted within facilities located in the United States, unless otherwise specified. Any exceptions to this will be disclosed and mutually agreed upon in advance, ensuring compliance with relevant legal and regulatory requirements. At this time, the MDR Services does not include individuals who can perform Classified Work or require Security Requirements in the USA.