Managed Detection and Response for Endpoint

1 Overview of the Service

NTT's Managed Detection and Response for Endpoint (MDR for Endpoint) provides enhancements to the Managed Detection and Response (MDR) Service by utilizing Endpoint Detection and Response (EDR) technologies to expand detection capabilities, improve the visibility for Security Analysts and optionally include endpoint response actions.

The services described herein are in addition to the MDR Services described in the Managed Detection and Response Service Description. MDR for Endpoint is not a standalone service and is only in scope if Managed Detection and Response has also been contracted and is in scope.

In addition to services included in MDR Service, MDR for Endpoint service may provide depending on system configurations:

(a) Isolation of detected compromised and malicious endpoints

(b) Inclusion of user behavior analytics into the existing threat hunting platform

(c) Enhanced identification of lateral movement of potential threats within the enterprise

All capabilities are limited to the technology capabilities, NTT supported technologies, and in-scope systems.

2 Client Responsibilities

(a) Client warrants that it has obtained all consents necessary for the data to be collected and used on its behalf for MDR service and that it has a legal basis for requesting such information (excluding consents from NTT employees and agents) and shall indemnify, defend and hold harmless NTT for the use of this information for this service.

(b) Client will procure and install a supported EDR technology prior to Service Transition tasks and provide licensing, use and access rights to NTT as required for this service.

(c) Client will provide NTT a list of acceptable and authorized tasks in a form acceptable to NTT, in the event Client does not provide a list of acceptable and authorized tasks, no isolation activities will be performed. Any updates to this list must have 30 days written notice.

(d) Client will remediate actions post isolation of compromised / malicious endpoints, unless the DFIR service is invoked.

(e) Client will install additional agents, or configuration changes as required for the DFIR services and provide any required licensing.

(f) Client is responsible for any impact to any NTT SLAs, due to the use of Client procured third party security tools during an incident or investigation.

(g) Client will provide access to the Client's EDR technology console for the purposes for DFIR event investigation and any other reasonable request by NTT.

(h) Client will manage EDR technology agent, and all policies managed within the agent.

3 Service Specific Operations

As part of the Service, the following tasks are included:

Task	Description
Enhanced Detection of Events	Enhanced detection of events using endpoint and end user telemetry, generated by the EDR technology into the MDR Base platform.
Incident Investigation	Using capabilities of the supported EDR technologies, provide indicators of attack to Security Analysts as part of investigation activities.
Endpoint Isolation	Perform remote actions for isolation of compromised / malicious hosts following security analyst validation.
Monthly Reporting	Provide monthly service overview and license count review. Validation of endpoint isolation special handling notes.

4 Supported Technologies

Only the following technologies are supported

(a) CrowdStrike Falcon Insight EDR

(b) Microsoft Defender for Endpoint

(c) VMware Carbon Black Enterprise EDR

5 Supported Environments

Only the following environments are supported.

(a) CrowdStrike security cloud and Events Stream API

(b) Enterprise wide, where supported EDR agents are deployed

(c) NTT managed client on-premises data center

6 Limitations

(a) EDR technology license is not included/bundled in the MDR for Endpoint service. The client must Bring Your Own License (BYOL) for the supported EDR technologies.

(b) The minimum number of endpoints this service can support is 500 per client. Any increase in number of endpoints will be in multiples of 250 endpoints.

(c) NTT reserve the right to confirm the total number of endpoints supported within the EDR console to ensure alignment with the statement of work (SoW) on a quarterly basis. If the total number of endpoints exceeds what is defined within the SOW, NTT shall have the right in its sole discretion to adjust the pricing based on these changes.

7 Out of Scope

(a) MDR for Endpoint service does not include further remediation actions post isolation.

(b) Other log events from the supported technologies not pertaining to the specific EDR service.

(c) Any policy management, management of the agent, or any other requirement to maintain the health and availability of the EDR technology.

(d) Any task that hasn't been explicitly mentioned.

(e) Any customization of the MDR for Endpoint service.

(f) Any transmission, processing, or storage of any data, information or otherwise that requires any license, authorization, certification or attestation.

8 Tasks Included in the Standard Transition

(a) Client will notify NTT of the EDR-related information, such as Customer ID, Basic Authentication Username/Password, API Client/Password, and Base URL for the API connection and Client agrees to the use and storage of the EDR-related information by NTT.

(b) Agreement of any automated isolation activities with the Client.

(c) Implementation of SIEM collector within the Events Stream API.

9 Tasks not Included in the Standard Transition

(a) Deployment of any EDR technology, or any setup or creation of policies unless separately procured within Professional Services

(b) License procurement and renewal of Client provide M365 subscription