Endpoint Security Services

Name	NTT Service Description – Endpoint Security Services
Owner	NTT
Status	APPROVED
Classification	UNCLASSIFIED-EXTERNAL
Version	V1.0
Date	24 April 2019

Contents

1 Service Matrix

Managed Security Services are available in packages consisting of a core set of Service Modules, associated Service Elements and Options.

Endpoint Security Services (ESS) is a service family from NTT Ltd. that provides three service levels of Managed Security Service (MSS) Enhanced support for Endpoint Detection and Response (EDR), Endpoint Protection Platforms (EPP) and other endpoint security solutions.

The three service levels are:

- Endpoint Monitoring
- Endpoint Detection
- Endpoint Response

Section	Service Elements	Service Levels		
		Endpoint Monitoring	Endpoint Detection	Endpoint Response
3	Service Elements			
3.1	24/7 Hours of Operation	✔	✔	✔
3.2	Security Operation Centers	✔	✔	✔
3.3	NTT Portal	✔	✔	✔
3.4	Client Portal Language Support	✔	✔	✔
4	Service Transition			
4.1	Engagement	✔	✔	✔
4.2	Planning	✔	✔	✔
4.3	Staging	✔	✔	✔
4.4	Integration	✔	✔	✔
4.5	Go-Live	✔	✔	✔
	Detection Types			
6.2.1	Security Best Practices and Basic Compliance Profile	✔	✔	✔
6.2.1	Enhanced Compliance Profile (PCI, HIPAA)	✔	✔	✔
6.2.1	Customized Event Detection	✔	✔	✔
7.3.1	Advanced Analytics with Proprietary Machine Learning / Behavioral Modeling		✔	✔
	Threat Intelligence			
7.3.2	Services Enhanced by NTT Global Threat Intelligence Center IR		✔	✔
7.3.2	Continuous Threat Intelligence Updates Driven by Production Investigations		✔	✔
	Security Analyst Interaction			
6.2.2	Automated Analysis with Security Analyst Verification	✔	✔	✔
7.3.3	Detailed Security Incident Investigation by Security Analyst		✔	✔
7.3.3	Event-Driven Threat Hunting		✔	✔
7.3.3	Vendor Integration and Evidence Collection for Key Security Technologies		✔	✔
8.5	Remote Isolation			✔
	Client Notification			
6.2.3	Automated Email Notifications	✔	✔	✔
6.2.3	24/7 Security Analyst Telephone Notifications	✔	✔	✔
7.3.4	Analyst-Created Security Incident Reports based on Detailed Investigation and Threat Hunting		✔	✔

Section	Service Elements	Service Levels		
		Endpoint Monitoring	Endpoint Detection	Endpoint Response
	NTT Portal and Reporting			
6.2.4	Web Portal	✔	✔	✔
6.2.4	Configurable Reporting	✔	✔	✔
6.2.4	Client access to 90 days of Security Compliance Event Data	✔	✔	✔
7.3.5	Client access to 90 days of Event Data and Lifetime Access (Life of Contract) to Security Incident Data		✔	✔
7.4	Policy Management			
7.4.1	Asset Tracking and Reporting		✔	✔
7.4.2	Co-Management		✔	✔
7.4.3	Service Request Fulfilment		✔	✔
9	Service Options			
9.1	[Option] Investigator – Enriched and Aggregated Log Search	✔	✔	✔
9.2	[Option] Secure Long-Term Log Storage and Management	✔	✔	✔

2 Service Prerequisites

2.1 General Requirements

2.1.1 Service Selection

Client is responsible for selecting services and ensuring that the selected services meet the compliance standards (e.g. PCI, HIPAA) applicable to Client operations.

2.1.2 Client Point of Contact

Client will assign a main Point of Contact (POC) to work with the NTT Ltd. Account Team to schedule all service-related activities and communicate with the SOC as needed for installation and ongoing tuning and support.

- To prevent delays during Implementation, Client will ensure completion of the Client Security Service Detail (CSSD) form.
- Client Point of Contact (POC) will be available during all scheduled activities.
- Client is responsible for providing NTT Ltd. with all contact information updates pertaining to Incident and Security Incident escalation instructions.
- Client is responsible for maintaining NTT Portal user list and rights.

2.1.3 Access and Connectivity Requirements

Client will ensure access and connectivity to all 'in-scope' devices, including the ability to receive source feeds and evidence data (packet capture, stack trace, etc.).

2.1.4 Client Staff and Resources Requirements

Client will provide knowledgeable technical staff, and/or third-party resources, to assist with hardware and software implementations, including:

- Configuring end-to-end connectivity to ensure the successful transport of all in-scope Log feeds and evidence data.
- Providing rack space and power for each in-scope NTT Appliance (if applicable).
- Providing an IP address for each NTT Appliance to be installed at Client site.
- Installing NTT Appliances on Client's network.
- Installing Log Transport Agents (LTAs) – NTT Ltd. will provide the Client with access to documentation via the NTT Portal and support in configuration and installation of LTA's during Service Transition
- Participate on Clients calls with third-party vendors and offer support as appropriate.

2.1.5 Source and LTA Configurations

Source device and LTA configurations must comply with NTT Ltd.'s standard setup requirements. NTT Ltd. provides Configuration Guides that provide configuration guidance for supported in-scope devices. If Client's configuration cannot or does not comply with NTT Ltd.'s configuration guidance, engineering consulting hourly rates will apply to develop a custom solution. Additionally, if any devices are not compliant with Configuration Guides, including use of supported versions of source devices only, Client agrees in good faith to work with NTT Ltd. to amend the Purchase Order accordingly.

2.1.6 Technologies that may impede delivery

If Client utilizes security technologies that block traffic, rotate Logs, or otherwise impede NTT Ltd.'s ability to receive Logs from in-scope devices, Client must notify NTT Ltd., and cooperate with NTT Ltd. to identify a mutually agreed upon mitigation to be developed.

Note: Loss of Log lines and interruption of monitoring capabilities may occur because of uncoordinated Log rotation.

2.1.7 Third-Party Vendors

Client will work directly with third-party vendors hosting any in-scope devices to allow NTT Ltd. to deliver services.

2.1.8 Maintenance, Support, and Licensing Agreements

Client is responsible for procuring all maintenance, support, and licensing agreements with third-party vendors for all non-NTT Ltd. provided in-scope devices for the term of the Client agreement, unless otherwise stated in the Purchase Order.

2.1.9 Software Modification

NTT Ltd. will not support altered, damaged, or modified software, or software that is not an NTT Ltd.-supported version.

2.1.10 Third-Party Device Failure

Client will work with third-party vendors to rectify device failure for all non-NTT Ltd. provided devices and is responsible for all associated expenses.

2.1.11 Responsibility for Data Privacy, Regulatory, and Administrative Policies and Procedures

Client is responsible for complying with all relevant data privacy, regulatory, and administrative laws and policies and procedures related to monitoring user traffic and communications.

2.1.12 Physical Security of NTT Appliances

Client is responsible for ensuring the physical security of all NTT Appliances located on-site at Client locations or hosted at third-party locations.

2.1.13 Internet Service Provider or Client Network Outages

Client is responsible for resolving Client Internet Service Provider (ISP) outages, or issues with Client internal network infrastructure.

2.1.14 System Backups

Client is responsible for performing full backups and restoration of relevant systems prior to the performance of services.

2.1.15 Closure of Incidents and Security Incidents

Client will work with NTT Ltd. to bring closure to each Security Event and Incident identified by the services presented in this Service Description.

2.1.16 Providing Required Information

Client's failure to provide any of the Service Requirement information on a timely basis can result in delays in Service Transition and NTT Ltd. shall not be liable for any consequences of such delays.

2.2 Communication Requirements

2.2.1 NTT Appliance

Managed Security Services require an NTT Appliance.

The NTT Appliance is available in multiple form factors, including a virtual image and physical appliance. All NTT Ltd. Appliances must be installed, initially configured and enrolled by the Client. NTT Ltd. will only be responsible for management and maintenance of the appliance software (in both physical and virtual form factors) and the physical appliance form factor if supplied by NTT Ltd.

NTT Appliances gather Logs, events, reports, and evidence data from in-scope Client devices and systems, then prepare the data for secure transmission and processing. The NTT Appliance also provides a secure communication path for Policy Management service delivery. Ongoing configuration and maintenance of the NTT Appliance is conducted by NTT Ltd. and therefore the appliance must be installed by the Client in a suitable location on the Client network infrastructure to facilitate both NTT Ltd. access and log collection.

The NTT Appliance requires:

- At least one static (non-dynamic) IP address
- Permanent LAN Connectivity
- Permanent Internet connectivity on TCP port 443

For the virtual form factor the NTT Appliance also requires:

- Must to be configured to power on automatically if the hypervisor is restarted
- Minimum resources from the hypervisor in the virtual environment as specified by NTT Ltd.

2.2.2 Configuration Item Requirements

All in-scope configuration items require:

- For internet-facing configuration items a static (non-dynamic) public IP address
- For non-Internet-facing configuration items – a static (non-dynamic) RFC 1918 IP address
- Necessary network connectivity to NTT Appliance as specified by NTT Ltd.

2.2.3 Connection to Client Network

The Client must supply all the necessary network hardware and cabling to connect the configuration item to the Client's own, third-party and ISP networks. All network interfaces connecting to the configuration items must be a minimum of 1 Gigabit Ethernet interfaces. The standard for Gigabit stipulates auto mode as mandatory. However, some vendors have deviated from this and do facilitate the hard coding of interface speed and duplex. Where this is enabled, it is imperative that both ends of the network cable are set to fixed speeds and duplex modes (in other words both Switch and Configuration Item). In this instance it is important that the Client discusses any potential infrastructure changes that may affect this setting.

3 Service Elements

3.1 Hours of Operation

Managed Security Services are delivered through the Security Operations Centers (SOCs) of NTT Ltd. Unless otherwise stated, MSS hours of operation are 24 hours a day, 7 days a week.

3.2 Security Operation Centers (SOCs)

NTT Ltd. will deliver services from its SOCs. NTT Ltd. may at its sole discretion deliver services from any of its SOCs, and Client data may be held in any of the SOC and MSS platform locations unless there is prior agreement and approval between NTT Ltd. and the Client.

3.3 NTT Portal

The NTT Portal is a globally available web-based application, which allows Clients to interact with, manage, and monitor Managed Security Services.

3.4 Language support

Services are provided in English language only, unless there is prior agreement and approval between NTT Ltd. and the Client.

4 Service Transition

Service Transition is executed in five phases, these are:

1. Engagement
2. Planning
3. Staging
4. Integration
5. Go-Live

The five phases and activities and procedures within them, ensure a consistent approach to management and completion of the transition and a framework for governance and communication. During the first four phases of the Service Transition period there will be no alerts, incidents, or cases generated for customer review and triage.

4.1 Engagement Phase

To initiate the Service Transition, a Purchase Order (PO) is submitted along with the Pricing Information from the approved quotation, a High Level Solution Design document, and the Client Security Services Detail (CSSD) to NTT Ltd.

NTT Ltd. reviews the provided documentation and confirms that all the requirements for commencement of the transition have been met.

A Kick-off meeting is held to communicate the Transition Process, the project tasks, roles and responsibilities and introduce the key stakeholders.

The Engagement Phase is expected to take 12 business days and can be accelerated if completed and accurate documentation is provided when submitting the Transition Service Request.

4.1.1 Engagement Phase Activities

The key activities during the Engagement Phase are as follows:

- Receive the Service Transition Request and PO and respond within three business days
- Review provided documentation within six business days
- Provide feedback and confirm content is complete and aligned to the Service Order
- Assign a Service Transition team including allocation of an NTT Ltd. Client Service Manager
- Create the Draft Service Transition Project Plan, including timeline and constraints within 10 business days
- Arrange a Kick-off meeting within 12 business days (if documentation is complete and confirmed)

4.1.2 Engagement Phase Deliverables

The deliverables provided during the Engagement Phase are as follows:

- Purchase Order Approval
- Kick-off meeting (face to face or call)
- Draft Service Transition Project Plan, including timeline, standard risks and issues

4.2 Planning Phase

The Service Transition Planning Phase validates the provided documentation and locks down the transition plan, scope, and timeline. The Planning Phase is expected to take six business days.

4.2.1 Planning Phase Activities

The key activities during the Planning Phase are as follows:

- Agree on final architecture, including devices and logs collection
- Assess Log Source Scope and Prioritization, including completing Log Source Inventory where applicable
- Client Approval of Final Service Transition Plan
- Confirm Services Delivery Model, including Incident Management and Steady State Governance

4.2.2 Planning Phase Deliverables

The Final Service Transition Plan (including timeline, risks, and issues) is provided as a deliverable during the Planning Phase.

4.3 Staging Phase

The Service Transition Staging Phase establishes the primary service elements for NTT Ltd. to provide the service. It includes connectivity, appliances for log collection, and Policy Management access, and NTT Portal and IT Service Management (ITSM) setup. The Staging Phase is expected to take 12 working days.

4.3.1 Staging Activities

The key activities during the Staging Phase are as follows:

- Install NTT Appliances (shipping, if required)
- NTT Appliance initial configuration and hardening
- NTT Appliance setup and validation of remote access
- Log(s) events/ monitoring setup (Client device)
- SOC Portal account(s) configuration
- SOC infrastructure preparation
- Testing of bi-directional ticket flow, if appropriate
- NTT Ltd. User Account and credentials setup for remote access (Client device, if applicable)

4.3.2 Staging Deliverables

The deliverables provided during the Staging Phase are as follows:

- NTT Appliance required to support Client services
- Client credentials for Portal
- Client Entitlement in NTT Ltd. ITSM
- Test results

4.4 Integration Phase

The Service Transition Integration Phase completes the required technical service elements for NTT Ltd. to provide the service. It includes configuration of threat detection (Advanced Analytics), advanced features for log collection, and final NTT Portal and ITSM integration. Additionally, during the Integration Phase, the NTT Ltd. CSM conducts the Welcome meeting and Portal training with the Client. The Integration Phase is expected to take 21 business days.

Following the Welcome meeting, the CSM becomes the interface into the NTT Ltd. services.

4.4.1 Integration Activities

The key activities during the Integration Phase are as follows:

- Final validation of connectivity to the SOC
- Device(s), log(s), and service testing and final verification
- Normalization and tuning (logs, not devices)
- Quality assurance review and activation of the service(s)
- Risk and Issue documentation
- Welcome meeting or call with Client (NTT Ltd. decision)
- Portal training meeting or call and Client (NTT Ltd. decision)
- Confirm Service Activation Date (in phases, if required), Billing Date, and SLA start date

4.4.2 Integration Deliverables

The deliverables provided during the Integration Phase are as follows:

- Client Welcome meeting and Portal training
- Service Activation Date

4.5 Go-Live Phase

The Service Transition Go-Live confirms that the service is live and closes the Service Transition Project. The Go-Live Phase is expected to take six working days.

4.5.1 Go-Live Activities

The key activities during the Go-Live Phase are as follows:

- Operational Check List review by SOC
- Conduct Service Transition Plan closure review meeting or call with Client (NTT Ltd. decision)
- Review all remaining open action items including lessons and risks/issues to be considered for Steady State (going forward)
- Receive Client Service Transition Plan closeout final approval

4.5.2 Go-Live Deliverables

The deliverables provided during the Go-Live Phase are as follows:

- Risks/Issues Register (if any)
- Commencement of service and Billing
- Lessons learnt (if any)

4.6 Service Transition Deliverable Acceptance

The Service Transition is considered complete on the Service Activation Date and after any Go-Live deliverables are provided. The deliverables are considered as being accepted at the completion of next phase. The Client will close the Service Transition by agreeing to the closure of the parent ticket in ITSM.

5 Service Detail

Endpoint Security Services (ESS) is a service family from NTT Ltd. that provides three service levels of Managed Security Service Enhanced support for Endpoint Detection and Response (EDR), Endpoint Protection Platforms (EPP) and other endpoint security solutions. The three service levels are:

- **Endpoint Monitoring** – Endpoint Monitoring (EPM) is designed for organizations with security best practice, business policy enforcement monitoring requirements and customized compliance for endpoint protection, detection and anti-virus products.
- **Endpoint Detection** – Reserved for EDR technologies, Endpoint Detection (EPD) offers advanced detection, investigation and reporting of Security Incidents, Event and Incident management, asset management and service request fulfilment in addition to service elements included in Endpoint Monitoring.
- **Endpoint Response** – Reserved for EDR technologies, Endpoint Response (EPR) exclusively delivers Remote Isolation for managed endpoint isolation based on known threats or Indicators of Compromise (IOC) using the Client's chosen EDR technology and supporting service elements also included in Endpoint Detection.

6 Endpoint Monitoring – Features

NTT Ltd. offers three service levels from Endpoint Security Services (ESS), a service family from the Managed Security Services:

- Endpoint Monitoring (EPM)
- Endpoint Detection (EPD)
- Endpoint Response (EPR)

This section presents the features of the ESS EPM service level.

6.1 Service Level Detail

EPM is the base-entry service level within ESS and is intended for more traditional vendor products that don't support advanced threat detection features such as API-driven threat hunting, automated response, custom indicator of compromise (IOC) enforcement, and other contemporary EDR features. Supported device types may include Endpoint Protection Platforms (EPP), Host Intrusion Prevention Systems (IPS), Host Intrusion Detection Systems (IDS) and Next Generation Anti-Virus (NG AV).

For a complete list of supported products available within this service level, please consult with your Sales representative.

6.2 Security Compliance

6.2.1 Detection Type

The EPM service uses customized rules and an anomaly-based security detection and compliance profiles to identify and report on the following categories of Security Events:

- **Compliance** - Events that indicate a deviation from a pre-defined baseline of a regulatory body's definition of compliance controls.
- **Security Best Practices** - Events that indicate a deviation from a pre-defined baseline of NTT Ltd.'s definition of security best practices.
- **Business Policy Compliance** - Events that indicate a deviation from a pre-defined baseline of an organization's custom business policy compliance requirements.

To ensure service quality, NTT Ltd. will continuously make detection tuning decisions based on the validity and relevance of service generated Events and Security Events.

- Use of the NTT Ltd. Standard Rule sets for existing supported device types is included in the EPM service level.
- Support for devices not currently supported by the EPM service level may be requested via the Non-Standard Request process (NSTAR) for EPM service level Clients.
- Up to fifteen (15) Standard or Compound Rules can be developed and implemented annually for EPM service level Clients.
- Additional Standard or Compound Rules can be purchased via the Move Add Change Delete (MACD) process at a rate of 6 MACDs per rule.
- Up to five (5) existing Analysers can be implemented annually for EPM service level Clients.
- Additional existing Analysers can be purchased via the Move Add Change Delete (MACD) process at a rate of 12 MACDs per Analyser.
- Development of new Analysers can be purchased via the MACD process at a rate to be determined based upon the level of effort associated with the development of the Analyser.

6.2.2 Security Analyst Interaction

The EPM service level utilizes automated detection for high confidence Security Events, with Security Analyst verification for custom high priority business use cases.

6.2.3 Client Notification

A mixture of automated and manually created notifications are utilized for the EPM service level. Clients are notified based on Client's selection of NTT Ltd. supported notification options, including e-mail and phone calls. Additionally, updates may be viewed on the portal.

6.2.4 Portal and Reporting

EPM Clients will have access to a portal that includes access to 90 days of Security Event Data. EPM Clients will also have access to monitoring and configurable reporting.

Use of standard NTT Ltd. reports is included as part of the EPM service level. Development of custom reports is not included as part of the EPM service level.

7 Endpoint Detection – Features

NTT Ltd. offers three service levels from Endpoint Security Services (ESS), a service family from Managed Security Services:

- Endpoint Monitoring (EPM)
- Endpoint Detection (EPD)
- Endpoint Response (EPR)

This section presents the features of the ESS EPD service.

7.1 Service Level Detail

The EPD service level is reserved for Endpoint Detection and Response (EDR) technologies and includes an advanced mix of customizable best practice and compliance monitoring alongside human-validated advanced threat monitoring and detection capabilities using our Machine Learning (ML)-based real-time threat detection and analytics engine.
Policy management of the vendor console is also included.

For a complete list of supported EDR technologies available within this service level, please consult with your Sales representative.

7.2 Security Compliance

The EPD service level includes all features defined within section 6.2 above.

7.3 Advanced Analytics

7.3.1 Detection Type

The EPD service level utilizes Advanced Analytics with proprietary machine learning / behavioral modeling to detect threats in the Client environment. Advanced Analytics leverages a combination of traditional threat detection techniques (e.g. correlation, pattern matching, reputation feeds) with Advanced Analytics (e.g. machine learning, statistical modeling, kill-chain modelling) and Threat Intelligence which enable detection of sophisticated threats.

7.3.2 Threat Intelligence

The EPD service level is enhanced by Threat Intelligence delivered by the Global Threat Intelligence Center.

Additionally, the EPD service level includes continuous threat intelligence updates driven by investigations of actual Security Incidents.

7.3.3 Security Analyst Interaction

The EPD service level includes detailed Security Incident investigation by Security Analysts in an NTT Ltd. SOC, including threat validation and threat hunting activities across the Client's in-scope log monitoring / telemetry environment to enable validation and assessment of the malicious nature of a threat and its potential impact. The EPD service level also includes vendor integration and evidence collection for selected security technologies, including packet capture data (PCAP) and malware execution reports. For details on availability refer to technology solutions guides.

7.3.4 Client Notification

Security Incident Reports for the EPD service level are based on detailed investigation and threat hunting and are prepared by a Security Analyst. Clients are notified based on Client's selection of NTT Ltd. supported notification options, including e-mail and phone calls.

7.3.5 Portal and Reporting

EPD Clients will have access to the NTT Portal that includes access to 90 days of Events, and Incidents for the lifetime of Client contract.

7.4 Policy Management

The EPD service level provides 24/7 Policy Management for EDR management consoles. NTT Ltd. provides co-managed support while the Client maintains full control and access to their security infrastructure.

7.4.1 Asset Tracking and Reporting

7.4.1.1 Configuration Item Recording

NTT Ltd. will record and track in-scope Client configuration items with information available within the NTT Portal.

7.4.2 Co-Management

NTT Ltd. provides Policy Management services to Clients in a co-managed scenario with specific conditions in place, as outlined below:

- Policy changes can only be made by specific contacts by raising a Case via the NTT Portal
- For NTT Ltd. to provide effective support it is recommended that Clients complete the following actions:
  - Notify NTT Ltd. in advance of changes being made to include scheduling and scope of changes being made to avoid 'lost transaction' or collision of change work
  - Record all modifications to be made via a Case within the NTT Portal
  - If applicable and upon completion the Client must provide a report/status update from their internal Change Management process to ensure NTT Ltd. is aware of all the changes occurring to configuration item(s)
  - The Client must make changes to configuration item such that there is a clear audit trail indicating the party responsible for the change, the date of the change and customer change control identification
  - Each change must be made in such a way as to provide the possibility of rolling back to the previous version. Failure to do this may render it impossible to recover the rule base if problems occur.
- Any changes to NTT Ltd.'s service administration rules must be agreed by NTT Ltd. in writing by means of a Case prior to their implementation

Clients accept any exception that may arise due to deviation from, or circumventing the processes described may result in an unsecured device(s) and/or non-compliant configuration(s) and, accordingly, Clients release NTT Ltd. from any liability resulting from outages, misconfigurations, exposures, loss of business, or other negative impacts directly related to changes implemented directly by Clients.

7.4.3 Service Request Fulfilment

Service Request Fulfilment focuses on request for information, advice or access.

7.4.3.1 Service Request Management

Service requests are managed through ITIL process and raised via a Case in the NTT Portal. Attainment of various key performance metrics are tracked, monitored and reported within NTT Ltd. on a monthly basis.

7.4.3.1.1 Request for Information

Clients may request information through the NTT Portal about the policy configuration of in-scope configuration items. NTT Ltd. shall deduct the commensurate number of MACD units (if applicable) and provide the information in the Service Request.

7.4.3.1.2 Service Request Reporting

All Incidents, Service Requests, Problems or Changes are recorded in the ITSM system and reported back through the NTT Portal.

7.4.3.1.3 Project Oriented Requests

NTT Ltd. will charge, and the Client agrees to pay, the then-current applicable hourly rates for work associated with PORs. If any Change performed by the Client results in adverse effects and requires remediation work be performed by NTT Ltd. to restore the software/configuration item to proper working service, the Client agrees to pay NTT Ltd. the then-current Engineering hourly rate to return the 'in-scope' device to normal operating run-state.

7.4.3.2 Move, Add, Change, Delete (MACD) Fulfilment

Policy Change Requests are administered through a Move, Add, Change, Delete (MACD) service unit model and are requested via the NTT Portal as outlined within Policy Change Management (see 7.4.3.3 below).

MACD service units are packaged within this service level offering with option to purchase additional MACD units and are based on configuration item sizing. MACDs are deducted in the execution of any Client sourced service requests pertaining to Request for Changes of configuration items. The number of MACD service units deducted per service request is based on a predefined list of standard tasks that NTT Ltd. has derived assessing level of complexity to route accordingly to an appropriate SOC engineer.

The MACD Service Unit Usage Tables per technology documentation is available upon request.

Where the usage of MACD service units for a service request exceeds 6 hours of effort, NTT Ltd. may charge additional MACD service units or propose a Project Orientated Request (POR) to perform the work on a time and materials basis.

MACD unit usage is tracked by NTT Ltd. and is included within any scheduled service reviews to ensure the Client account is operating in line with MACD availability. Should MACD unit balance drop below a certain threshold the Client will be notified for purchase of additional MACD service units.

7.4.3.2.1 Non-Standard Tasks utilizing MACD Service Units

In the unlikely event that there is not a pre-existing menu item for a Client request, NTT Ltd. considers this a non-standard task.

NTT Ltd. will review non-standard tasks requested by the Client to determine if:

- NTT Ltd. has the appropriate skills to action or implement the task
- Whether the non-standard task should become a standard task (based on demand/repeatability)

NTT Ltd. will assess the non-standard task to determine the correct number of MACDs. NTT Ltd. will provide the Client with the number of MACD service units the task will incur for approval to proceed. Once approved by the Client, NTT Ltd. will execute the Request for a non-standard pre-approved task. No service levels will apply to the execution of a non-standard task.

7.4.3.3 Policy Change Management

At a Client's request, NTT Ltd. will implement a request for change to in-scope configuration items in accordance to an associated MACD task or Non-Standard task outlined in section.

NTT Ltd. provide specific Operational Level Agreements for Request for Changes which can be found in the Endpoint Security Services Operational Level Agreements.

7.4.3.3.1 Client-Sourced Requests

Request for Change Cases must be submitted by valid Client contacts within the NTT Portal.

7.4.3.3.2 NTT Ltd.-Sourced Requests

NTT Ltd. may submit a Request for Change Case when a correct control change is necessary to resolve a Problem or Incident.

7.4.3.3.3 Change Reporting

All Changes must be reported and tracked via the NTT Portal.

The party making a Change is required to open an applicable Request for Change Case in the NTT Portal prior to implementation to ensure coordination between both parties.

7.4.3.3.4 Request for Change

All requests for change types follow the NTT Ltd. Change Management process and require approval by NTT Ltd. NTT Ltd. derive tasks per technology which corresponds to the number of Service Units utilized by each task. There are 3 (three) types
of request for change outlined below.

Normal Change

Normal Changes require approval (from both NTT Ltd. and Client respectively) before being implemented. Neither Client nor NTT Ltd. is authorized to apply Changes on behalf of the other without documented consent from appropriately authorized individuals (documented within a Change Approver Group on the NTT Portal) from both parties via a Request for Change Case resident in the NTT Portal.

Standard Change

NTT Ltd. is authorized by the Client to apply Changes without authorization from the Client when a standard change ticket is raised via the NTT Portal, though an NTT Ltd. internal approval process is still valid.

Emergency Changes

An emergency change is considered a request for change that must be implemented as soon as possible, for example to resolve an Incident or implement a security patch. NTT Ltd. will work with the Client during the Change Management process.

7.4.3.3.5 Cancelling a Request for Change

The Client may cancel a Request up to 2 hours before any scheduled changes being committed to the device configuration. In which case any MACD credit that would have been deducted shall be cancelled.

If the Client would like to reverse a Change that has already been implemented, the Client must submit a new Service Request for Change via the NTT Portal. In which case the commensurate MACD credits shall be deducted for both the original change and any subsequent reversal requested.

7.4.3.3.6 Change Implementation

NTT Ltd. strongly recommends that the Client making the Change completes and documents the following tasks associated with each Change:

- Backup the current running configuration(s) prior to the change or if co-managed must notify NTT Ltd. to ensure a backup is taken
- Ensure a copy of any applicable software and/or firmware is readily accessible
- Ensure a roll back plan is documented in the event there are issues with the Change
- Create a backup of the new configuration after the Change is implemented

The NTT Ltd. party making the Change must complete and document the following tasks associated with each change:

- Assign an internal ticket number (if applicable) to track the Change for auditing purposes
- Implement and test the Change (as far as is possible – testing responsibility is also shared with the Client) to confirm whether the change met the requirements as specified by the submitter
- Update NTT Ltd.'s Service Request ticket indicating whether the Change was successful or not

It is imperative each Change is fully documented within the NTT Portal to ensure a detailed record of Change is available for Client lead troubleshooting and audit purposes if/when unanticipated negative consequences arise.

Exceptions

The Client agrees that any exceptions that may arise due to deviation from or circumventing the processes described herein may result in unstable and/or unsecured configuration item(s) and/or non-compliant configuration(s) and accordingly, the Client releases NTT Ltd. from any liability resulting in outages, misconfigurations, exposures, loss of business, or other negative impacts directly related to any Change made by the Client.

The Client agrees any work performed by NTT Ltd. to troubleshoot issues directly attributable to a Client Change is billable at the current NTT Ltd. Engineer's hourly rate.

Client Responsibilities

The Client agrees only appropriately-trained and skilled engineers will perform Changes in a Co-Managed environment.

The Client agrees that NTT Ltd. reserves the right to bill for incremental troubleshooting work NTT Ltd. performs as a result of:

- Client not accurately recording changes on their in-scope configuration item(s)
- Client not notifying NTT Ltd. about changes being made with at least 1 full business day's notice
- Client performing work that violates OEM support agreements or leads to in-scope configuration items negatively effecting Client production environment

NTT Ltd. Responsibilities

NTT Ltd. will review Incident, service requests and documentation regarding changes performed by the Client and may seek clarification.

7.4.3.3.7 Change Impact Analysis

As part of the Change design process, NTT Ltd. conduct a Change Impact Analysis in accordance to all Requests for Change Cases (pre- and/or post-implementation). NTT Ltd. reviews Incident cases, service request cases and documentation regarding Requests for Change Cases in the event of a co-managed service and may seek clarification.

NTT Ltd. will conduct a Change Impact Analysis prior to implementation of any Request for Change Case – including request for change, or PORs to ensure:

- Hardware/software meets all prerequisites
- Any change is consistent with security best practices and does not compromise the Clients network, service or that of NTT Ltd.
- Any change is relevant to Client's environment
- Any change can be implemented within the requested timeframe

NTT Ltd. considers the Change Impact Analysis complete when Client has addressed all issues raised during the analysis (if applicable), and the engineer acknowledges receipt of a valid Request for Change via the NTT Portal.

8 Endpoint Response – Features

NTT Ltd. offers three service levels from Endpoint Security Services (ESS), a service family from Managed Security Services:

- Endpoint Monitoring (EPM)
- Endpoint Detection (EPD)
- Endpoint Response (EPR)

This section presents the features of the ESS EPR service level.

8.1 Service Level Detail

The EPR service level includes all features from the Endpoint Detection (EPD) service level and adds an automated and orchestrated endpoint quarantine feature as part of the human-validated advanced threat detection capability. This feature allows our SOCs to immediately respond to validated security incidents by remotely isolating compromised endpoints and / or blocking malicious IoCs at the network layer.

For a complete list of supported products available within this service level, please consult with your Sales representative.

8.2 Security Compliance

The EPR service level includes all features defined within section 6.2 above.

8.3 Advanced Analytics

The EPR service level includes all features defined within section 7.3 above.

8.4 Policy Management

The EPR service level includes all features defined within section 7.3.5 above.

8.5 Remote Isolation

Exclusively available in the EPR service level, Remote Isolation enables Security analysts from globally located NTT Ltd. SOCs to quarantine infected endpoints on the Client's network by remotely accessing a pre-configured EDR management console or associated 'Response' application. This feature puts Endpoint Detection and Response (EDR) capabilities front and center and provides NTT Ltd. Clients with all core service elements available from Managed Security Service and 24/7 detection and response management (MDR) using their chosen EDR technology.

This feature does not include remediation actions, processes or procedures that may occur following isolation of one or more infected endpoints.

8.4 Policy Management

By subscribing to the EPR service level, the Client is agreeing that NTT Ltd. may take responsive actions to isolate compromised endpoints by remotely logging into the Endpoint Detection and Response (EDR) management interface using secure credentials provided during staging (see Staging Phase).

8.5.2 Linked Access

NTT Ltd. may use alert links made available through the vendor to login and access alert pages directly within the management UI. Levels of automated access may vary by supported product.

9 Service Options

9.1 Investigator Client Log Search

ESS Clients have the option to purchase NTT Ltd. Investigator log search capabilities. Investigator provides the Client access to an interface to perform investigative searches on enriched logs.

9.2 Secure Long-Term Log Storage (SLTLS)

ESS Clients have the option to purchase secure long-term log storage.

10 Terminology and Definitions

Terminologies and Definitions for Endpoint Security Services are presented in the 'NTT Ltd. - Terminology and Shared Services Reference' document that accompanies this Service Description.

11 Operational Level Agreements

Operating Level Agreements for Endpoint Security Services are presented in the 'Operating Level Agreements – Managed Security Services' document that accompanies this Service Description.

12 Changes in Service

12.2 Method of Service Delivery

NTT Ltd. reserves the right to make changes to the service, provided these changes do not have a material adverse impact on functionality or performance.

12.3 Supported Devices

NTT Ltd. reserves the right to change Supported Devices over time as new manufacturer hardware models and software versions are released or announced by the manufacturer as End of Support and/or End of Life.

13 Service Exclusions

Unless otherwise stated in a Purchase Order, the services described in this document do not include the following:

- Configuration of in-scope security systems and devices to allow for Log, Events, and evidence collection.
- Support and Remedial Work which is not expressly stated in this Service Description. This includes any troubleshooting and problem solving related to issues arising from Client actions or Client's network.
- Project Orientated Requests (PORs) are not included in the Services described herein and are subject to additional fees. NTT Ltd. and the Client will develop a scope for the POR and NTT Ltd. will provide a separate quote to Client, which must be executed prior to performance of any such work.
- Client requests for advice or consultation regarding network or configuration item configuration not specifically outlined in this Service Description is not included are subject to additional fees.
- Client staff training unrelated to NTT Ltd. services (NTT Ltd. provides written and video training on the NTT Portal and the different functions that Client may use within the portal.).
- Software or hardware maintenance (unless otherwise stated).
- Software licensing (unless otherwise stated).
- Software or hardware upgrades.
- Network connectivity troubleshooting.
- On-site forensic services.
- Security policy or procedure establishment.
- Firewall rule set design, validation and troubleshooting.
- Remediation of a Security Incident or attack on a Client's network, server or application.

14 Controlling Terms

In the event of any conflict between the terms of this Service Description and the terms of the Client agreements, then terms of this Service Description shall control.

Together we do great things