SERVICE DESCRIPTION

NTT

Web Security Service

Name	NTT Ltd. Ltd. Service Description – Web Security Service
Owner	NTT Ltd. Ltd.
Status	APPROVED
Classification	UNCLASSIFIED-EXTERNAL
Version	V1.18
Date	29 March 2019

Contents

1 Service Matrix

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

Section	Service Elements	NTT Ltd. Cloud Web Security Service
3	Core Service Elements	
3.1	24/7 Hours of Operation	✓
3.2	Security Operation Centers	✓
3.3	Client Portal	✓
3.4	Language Support	✓
3.5	WSS Management	✓
3.6	Communications	✓
3.7	Escalation Management	✓
4	Service Transition	
4.1	Engagement	✓
4.2	Planning	✓
4.3	Staging	✓
4.4	Integration	✓
4.5	Go-Live	✓
5	Web Security Service Features	
5.1	Threat Detection	
	Advanced Analytics with proprietary machine learning / behavioural modelling	✓
5.2	Threat Prevention	
	Advanced Threat Protection	✓
	Advanced Authentication	✓
	URL Filtering and Categorization	✓
	Encrypted Traffic Inspection	✓
5.3	Threat Intelligence	
	Leverage NTT Ltd. Global Threat Intelligence Center (GTIC)	✓
	Enriched by Symantec Global Intelligence Network	✓
5.4	Security Analyst Interaction	
	Detailed Security Incident investigation by Security Analyst	✓
	Event-driven Threat Hunting	✓
5.5	Security Engineer Interaction	✓
5.6	Client Notification	
	Analyst-created Security Incident Reports based on detailed investigation and Threat Hunting	✓
5.7	Portal and Reporting	
	Web portal	✓
	Client access to Events (90 days)	✓
	Client access to Incidents (lifetime of contract)	✓
	Actionable and Detailed Reporting (Symantec WSS Portal)	✓
	Scheduled reporting and triggered alerts with e-mail delivery (Symantec WSS Portal)	✓
	Pre-configured and custom reporting (Symantec WSS Portal)	✓
	Web Security Hosted Reporting (Symantec WSS Portal)	✓
5.8	Health and Availability Monitoring	✓
5.9	Incident Management	
	Incident Generation	✓
	Incident Diagnosis	✓
	Incident Resolution	✓
	Incident Reporting	✓
5.10	Service Request Fulfilment	
	Service Request Management	✓
	Move, Add, Change, Delete (MACD) Fulfilment	✓
	Change Management	✓
5.11	Problem Management	
	Problem Identification and Recording	✓
	Solution Identification and Recording	✓
	Solution Implementation	✓
	Problem Reporting	✓
5.12	Service Options	
	[Option] Investigator – Enriched and aggregated Log Search	✓
	[Option] Secure long-term log storage and management	✓
	[Option] Web Security Mobile	✓
	[Option] WSS Hybrid	✓
	[Option] Malware Analysis Advanced Service (MAAS)	✓

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 their security requirements and 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 communications with the SOC as needed for installation and ongoing tuning and support.

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

2.1.3 Client Staff and Resources Requirements

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

- Configuring end-to-end connectivity of in-scope devices to Symantec WSS cloud infrastructure (via Public Internet)
- Working with third-party vendors for support or provide authorization for NTT Ltd. Account Team to contact third-party vendors on behalf of Client as appropriate
- Having sufficient bandwidth to provide an acceptable level of authorized user web experience
- Having an operational Domain Name Service (DNS) in place
- Only allowing the agreed number of authorized users to use the Service as identified to NTT Ltd. and paid for
- Using the Service via the provisioned portal(s) or such other means as directed by NTT Ltd. or its nominee
- Not reselling, renting, or leasing the Service to any third party without prior written consent from NTT Ltd.

2.1.4 Third-Party Vendors

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

Note: NTT Ltd. will procure maintenance, support, and licensing agreements for Symantec WSS.

2.1.5 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 services for the term of the Client agreement, unless otherwise stated in the Purchase Order.

Note: NTT Ltd. will procure maintenance, support, and licensing agreements for Symantec WSS.

2.1.6 Software Modification

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

2.1.7 Third-Party Device/Service Failure

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

2.1.8 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.

2.1.9 Internet Service Provider or Client Network Outages

NTT Ltd. is not responsible for resolving Client’s Internet Service Provider (ISP) outages, or issues with Client’s internal network infrastructure which is not under NTT Ltd. management.

2.1.10 Closure of Service Request, Incidents and Security Incidents

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

2.1.11 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 Service Delivery by NTT Ltd. and NTT Ltd. shall not be liable for any consequences of such delays.

2.2 Communication Requirements

2.2.1 NTT Ltd. LTA/Fetcher

NTT Ltd. Web Security Service (WSS) is a cloud-based service that does not require any Client premise equipment.

WSS LTAs are deployed within the NTT Ltd. infrastructure. NTT Ltd.'s is responsible for configuration, management and maintenance of the LTAs and enrolment of the Client into the service. The LTAs collect Logs from Symantec WSS proxy and malware logs, and then prepare the data for processing.

2.2.2 Connection to Client Network

Client must supply all the necessary network interfaces to connect the Client’s own, third party and ISP networks to Symantec WSS Infrastructure (via Public Internet).

2.2.3 Connectivity and System Configuration

The Client must select at least one traffic-forwarding option and one Authentication method to direct their traffic to Symantec WSS infrastructure. To view a list of available Access Methods and Authentication Methods, refer to:

http://portal.threatpulse.com/docs/am/AMDash.htm

Client is responsible to manage the devices and configurations, where the device is not a NTT Ltd. Ltd. managed device.

The Client is solely responsible for monitoring and controlling access to the service, maintaining the confidentiality of the passwords and for any use of the Services that occur using such passwords.

3 Core 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 Operations Centers (SOCs)

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

3.3 Client Portal

For the WSS offering, Clients have access to the following web-portals:

- The NTT Ltd. Portal
- The Symantec WSS Portal

In the Standard Management (default) set up, all user lists and rights are owned and managed by NTT Ltd. for all portals.

3.3.1 NTT Ltd. Portal

The NTT Ltd. Portal is a globally available web-based application, which allows Clients to interact with, manage, and monitor NTT Ltd. Managed Security Services. Clients can use the NTT Ltd. Portal for NTT Ltd. Advanced Analytics capabilities for WSS
e.g. Security Incident Reports, and Service and Change/Issue Management requests.

3.3.2 Symantec WSS Portal

A globally available web-based application provided by Symantec, which provides management, reporting and role-based access for the Symantec WSS configuration and service functionalities.

The Symantec WSS portal is available for NTT Ltd. WSS Clients. The portal provides complete access for management, reporting and role-based access for the Symantec WSS solution, service functionalities, and WSS optional features including Malware Analysis Advanced Service (MAAS).

NTT Ltd. configures the Symantec WSS portal for the Client with all relevant service information. An account is created for the nominated service administrator and its operation verified by the Client.

Clients can be assigned Admin or Reviewer role based on their management service deployment.

In a Standard Management set up, the Client will be assigned a Reviewer role (Read-Only).

In a Co-Management set up, the Client can be assigned the Admin role (Read/Write) and may configure and manage the Symantec WSS, access reports, and view data and statistics through Portal.

In a Co-Management set up, specific conditions applies. For more information, see Co-Management (available on request) section.

3.4 Language support

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

Note: The Symantec WSS Portal is available in English and Japanese.

3.5 WSS Management

NTT Ltd. offers two types of management set ups for Symantec WSS Portal and WSS Proxy configurations:

- Standard Management
- Co-Management

Responsibilities for the management of the Symantec WSS Portal are dependent on the type of management set up selected by the Client in the Planning phase.

3.5.1 Standard Management

NTT Ltd. has privileged access to configurations within scope. The Client can be provided with up to 3 read-only accounts to access configurations within scope.

If the Client expects more (>3) read only accounts, NTT Ltd. will create a read-only account via MACD consumption.

NTT Ltd. will create one administrator account ('Break Glass account') for the Client and will securely store the credentials and password. In the event of an emergency where NTT Ltd. is unable to make a Change or access the configurations/ management infrastructure, the Client Nominated Service Administrator (primary Client security contact) will be provided with the credentials and password.

Each time the Client uses the Break Glass account, NTT Ltd. will reset the account with a new password.

3.5.2 Co-Management (available on request)

NTT Ltd. and the Client and/or its nominated third party and/or an NTT Ltd. Group Operating Company have access to the in-scope WSS configurations with the ability to make updates and configuration changes.

In a Co-Management set up, Client can be assigned the Admin role and may configure and manage the Symantec WSS Portal, WSS policies, access reports, and view data and statistics through the Symantec WSS Portal.

In this case, the Client is responsible for maintaining Client user accounts and rights for Symantec WSS Portal. For more information about portal, refer to NTT Ltd. Portal section in this document.

Note: WSS management set up must be selected during 'Planning' phase. Clients cannot switch between management set ups after the service 'Staging' phase.The Client agrees only appropriately-trained and skilled WSS and Proxy engineers will have Admin account access and perform changes in a Co-Managed environment.

In a Co-Managed scenario, specific conditions and responsibilities apply as outlined below:

- Co-management is only available as an option when the Client has an appropriately-trained and skilled WSS and Proxy engineer in house
- WSS configuration and policy changes can only be made by the specific Client's WSS engineer, outlined within the CSSD or added by raising a service request via the NTT Ltd. Portal
- In order for NTT Ltd. to provide effective support the Client shall:
  - 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 Ltd. Portal
  - If applicable and upon completion, the Client shall provide a report/status update from their internal Change Management process to ensure NTT Ltd. is aware of all the changes occurring to the WSS configurations
  - The Client shall make changes to WSS configurations such that there is a clear audit trail indicating the party responsible for the change, the date of the change and Client change control identification
- Any changes to NTT Ltd.'s service administration rules must be agreed by NTT Ltd. SOC in writing prior to their implementation.
- Any changes in Clients' accounts rules must be agreed by NTT Ltd. SOC prior to their implementation.
- All Changes must be reported and tracked via the NTT Ltd. Portal, this includes Co-Managed scenarios.

Clients accept any exception that may arise due to deviation from, or circumventing the processes described may result in an unstable configuration(s) and service. 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.

3.6 Communication

3.6.1 Email

For security and data privacy reasons, email notifications from NTT Ltd. will only contain minimal information to notify Clients about creation of, or updates to, Incidents, Service Requests, Changes and Problems. Such emails shall not contain any sensitive information apart from the appropriate ticket reference number (and where possible not to disclose any private information a short description of the ticket).

Clients may send emails relating to new or existing Incidents, Service Requests, Request for Changes and Problems to NTT Ltd.. In the case where no reference number is provided as formatted by NTT Ltd., NTT Ltd. shall create a new Incident, Service Request or Request for Change with a short description based on the subject line provided.

When a Client is replying to an email with an existing reference number (as provided by NTT Ltd. and unchanged by the Client), the message body text shall be copied (upon receipt) to the timeline of the relevant Incident, Service Request or Request for Change and shall be marked as updated by the Client and waiting on NTT Ltd.'s further input. For security reasons, if Clients wish to send sensitive information to NTT Ltd. or provide approval workflow.

3.6.1.1 File attachments

Diagrams, images, PDFs, executables and any other attachments must not be attached to any Incident, Service Request or Request for Change via email. Where file attachments are necessary, the Client must log in to the NTT Ltd. Portal and attach the file securely through their web browser connected to the NTT Ltd. Portal.

3.6.2 Telephone

SOC staff may contact Clients and Clients may contact SOCs by telephone. In both cases an authentication shall be completed to verify Client identity.

3.6.3 NTT Ltd. Portal

Unless otherwise stated and agreed, all other communications originating from SOCs shall be secure and follow security best practices via the NTT Ltd. Portal.

3.6.4 ITSM (Service Management) Tool

NTT Ltd.'s ITSM manages all Incidents, Service Requests, Change Request, and Problems following ITIL wherever appropriate. Access is provided to appropriate NTT Ltd. staff.

3.6.5 Engineering

3.6.5.1 MSS Infrastructure

NTT Ltd. utilizes a regional based infrastructure built with security by design. The infrastructure is highly resilient and secured using best practice methodologies tools and techniques. It is fully managed by NTT Ltd. Global Services staff and monitored using our Device Management (DM), Enterprise Security Monitoring (ESM) and Threat Detection (TD) security services.

3.7 Escalation Management

NTT Ltd. utilizes escalation processes and defined responsibilities for addressing Client escalations. To escalate a configuration Incident, Request for Change or Service Request, the Client may telephone or email the service desk (quoting the reference number). An NTT Ltd. Escalation Manager is then assigned who is responsible for:

- Monitoring escalated matters through to resolution
- Creating and maintaining an action plan for each escalation
- Making any decision appropriate to the resolution of the escalation
- Arranging escalation meetings and/or phone conferences (as appropriate) between the Client, NTT Ltd. and relevant third parties
- Regularly communicating escalation status to:

  - The Client
  - The NTT Ltd. Client Services Manager (if assigned)
  - Any other parties relevant to the escalation
- Regularly updating and seeking the advice and support of NTT Ltd. management
- For the duration of an escalation, ensuring all appropriate personnel are available to support the agreed action plan

NTT Ltd. may downgrade an escalated Security Incident, Incident, Change Request or Service Request if it is being managed to a scheduled timeframe, or resolution has been provided to the Client and is in the process of being tested. If the Client initiated the escalation, NTT Ltd. will obtain the Client's approval prior to downgrading an escalated Security Incident, Incident, Change Request or Service Request.

Clients may request their Incident, Service Request or Problem be escalated to a higher priority at any time provided that they give sufficient justification. Upon review, the SOC manager shall be responsible for agreeing any urgent change.

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, the Client will submit a Purchase Order (PO) with the Pricing Information from the approved quotation, a High-Level Design document, and the Client Security Services Detail (CSSD) to NTT Ltd..

- Purchase Order (PO)
- Pricing Information
- Client Security Services Detail (CSSD)
- High Level Solution Design
- Symantec Purchase Order

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 the Client provides completed and accurate documentation when submitting the Transition Service Request. For WSS, the following aspects of the design must be reflected in the High Level Design document.

- Connectivity (e.g. VPN/Forward Proxy etc.)
- Authentication (e.g. AD integration/SAML etc.)
- Authentication server addresses, VPN Gateway addresses, Forward Proxy Locations and addresses.
- Policy design e.g. Specific URL Categories to be blocked, black/white lists required, exempt or special user's security groups as defined in AD. Safe Search Restrictions.
  Mobile Client's policy. (See appendix for example/template)

Failure to provide this level of detail at the start could delay the transition of the service to an active state.

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
- Register Symantec Purchase order
- 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 (CSM)
- 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)

NTT Ltd. Service Transition

- NTT Ltd. Portal account(s) configurations
- Symantec WSS Portal account(s) configuration

4.1.2 Engagement Phase Deliverables

The deliverables provided during the Engagement Phase are as follows:

- Purchase Order Approval
- Symantec Purchase Order Approval
- Kick-off meeting (face to face or call)
- Draft Service Transition Project Plan, including timeline, standard risks and issues
- Client Entitlement in Symantec ITSM
- Client credentials for NTT Ltd. Portal
- Client credentials for Symantec WSS Portal
- Client Entitlement in NTT Ltd. ITSM

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
- Low level design produced and documented
- 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, authentication validation, and setting up the LTA system, Portals and IT Service Management (ITSM) setup.
The Staging Phase is expected to take 12 business days.

4.3.1 Staging Activities

The key activities during the Staging Phase are as follows:

NTT Ltd. Tech Ops

- Log Transport Agents (LTAs) set up and configuration
- NTT Ltd. MSS infrastructure and Symantec WSS cloud infrastructure integration
- Backend Provisioning
- MSS SOC infrastructure preparation

NTT Ltd. Service Transition

- Web Security Service (WSS) initial configuration
  - Connectivity
  - Authentication
  - Mobile Client policy

Client

- Configuration of Client infrastructure to support connectivity and authentication
  - Connectivity
  - Authentication

Client/Professional Services/Partners

- Define/Design the WSS policy for all selected service elements including:
  - If not already provided, specifying categories to be blocked/allowed
  - Creation of white lists: specific URLs that should be allowed even if they exist within a denied content category
  - Creation of black lists: specific sites that should be blocked even if they exist within an allowed content category
  - Source white list: specific IP addresses, users or groups that should be excluded from content filtering
  - Business critical cloud applications or web sites that must always be allowed

The Client re-categorizes URLs into the groups it deems most appropriate, verifies the accuracy of all information presented in the Symantec WSS Portal, and advises NTT Ltd. SOC of any errors and/or required changes.

Note: Client is responsible for performing and signing off User Acceptance Test (UAT) for the WSS initial policy prior to 'Go live'.

NTT Ltd. SOC

- WSS Proxy Policy Configuration

4.3.2 Staging Deliverables

The deliverables provided during the Staging Phase are as follows:

- Client connectivity
- Client authentication
- Client WSS Policies are verified
- 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 Monitoring and Threat Detection, advanced features for log collection and policy/device management, and final 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 10 business days.

Following the Welcome meeting, the CSM becomes 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/log flow towards the SOC
- Final validation of connectivity towards Symantec WSS infrastructure
- Log(s) and service testing and final verification
- CMDB instantiation (where appropriate) for Contracts, Entitlements, Assets and CI's
- Test ticket creation and validation to NTT Ltd. ITSM via phone, email and NTT Ltd. Portal by Client
- Final validation of reachability to Client POC and Client's accounts access to the Portals
- Quality assurance review and activation of the service(s)
- Risk and Issue documentation
- MSS SOC Welcome meeting or call with Partners and Client (NTT Ltd. decision)
- NTT Ltd. Portal training meeting or call with Partners and Client (NTT Ltd. decision)
- Symantec WSS Portal training meeting or call with Partners and Client (NTT Ltd. decision)
- Confirm Service Activation Date (in phases, if required), Billing Date, and OLA start date

- NTT Ltd. SOC/Tech Ops verifies the format and spelling of domains provided by the Client and configures access to the domains within the Symantec WSS Portal. Inbound server or network host IP addresses and preferences, outbound network IP addresses (where applicable), and the service policy settings are verified by NTT Ltd..

4.4.2 Integration Deliverables

The deliverables provided during the Integration Phase are as follows:

- Client Welcome meeting and Portals training
- Service Activation Date
- Confirmation of WSS Readiness
- Confirmation of WSS log transfer to NTT Ltd. MSS Infrastructure
- Client review and acceptance of the Risk and Issue Register

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 business days.

4.5.1 Go-Live Activities

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

- Operational Check List review by SOC

Note: SOC to confirm with Client and Client to acknowledge that they have solid process to inform their employees on expectation of privacy and have a suitable privacy notice in place.

- Conduct Service Transition Plan closure review meeting or call with Partners and 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 is 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 ServiceNow.

5 NTT Ltd. Web Service Features

Web Security Service (WSS) consists of the following key features:

- Cloud Web Security Service powered by Symantec
- Advanced Analytics for WSS Proxy logs
- Policy Management for WSS

Following service options are offered as add-on features to WSS service. Clients can procure and add them to their WSS instance:

- Malware Analysis Advanced Service (MAAS) and Advanced Analytics for MAAS logs. Advanced Analytics is automatically enabled once MAAS is added to service.

In the Cloud WSS suspicious and malicious access is detected in real-time, by categorizing and analysing web traffic behavioural and threats posed to the Clients and examining malware-prone file types in detail.

With extensive web and cloud application controls and detailed reporting features, the WSS enables administrators to create and enforce granular policies that are instantly applied to all covered users, including fixed locations and roaming users.

Applying advanced Threat Detection capabilities to the WSS proxy and Malware logs, suspicious activities and all relevant contextual information are presented to a skilled Security Analyst, who engages in Threat Hunting and Threat Validation activities to verify the threat, its impact and to identify additional information associated with the potential breach. Once verified, the Security Analyst creates a detailed Security Incident Report and initiates Security Incident notifications in accordance with documented Client procedures, providing a detailed description of the Security Incident combined with scenario-specific actionable response recommendations, which significantly assist businesses in reducing the time to take informed responsive measures, lowering associated risks.

The following sections discuss the features of NTT Ltd. Web Security Service.

5.1 Threat Detection

NTT Ltd. WSS utilizes Advanced Analytics with proprietary machine learning / behavioural modelling to detect additional threats in the Client environment. WSS leverages a combination of traditional threat detection techniques (e.g. correlation, reputation feeds) with Advanced Analytics (e.g. machine learning, kill-chain modelling) and Threat Intelligence which enable detection of sophisticated threats.

5.2 Threat Prevention

WSS enforces granular access and security policies that manage internet usage by user, application, location, and device.

5.2.1 Advanced Threat Protection

The Symantec Advanced Threat Protection capability allows the WSS to be delivered using one multi-level policy, from the same console, through one Global Fully Meshed Cloud Security Fabric. This ensures gap-free protection against advanced threats, zero-day attacks and the ability to design the Client's security policy for its business. With Symantec Advanced Threat Protection, the Client has the ability to leverage the Global Intelligence Network to provide negative day defense, identifying malware networks prior to their active deployment.

Advanced Threat Protection utilizes:

- Multi-layered dual anti-virus and heuristic analysis combines to block malware
- Customized White-List/Black-List capabilities and file reputation analysis

5.2.2 Advanced Authentication

The Advanced Authentication allows versatile selection of authentication methods. This reduces the need for complex system integration, while incorporating the latest industry standards to enable authentication and authorization.
The Service supports SAML 2.0, including support for ADFS, SiteMinder, Cloud IDP, and Centrify solutions.

5.2.3 URL Filtering and Categorization

The Dynamic and Multi-layer URL Filtering provides flexible and granular URL filtering that aids the Client to achieve compliance by consistently enforcing acceptable use policies. Users can accurately filter web traffic by assigning multiple categories to any given URL, based on ratings from the Symantec Global Intelligence Network.

WSS URL Filtering and Categorization:

- Leverage security categories to block majority of the threats,
- Classify URLs in one of 72 categories covering approximately 50 languages
- Dynamic, real time ratings for the latest information
- Other features delivered by this capability include:
  - Multi-Dimensional Ratings: Multi-dimensional ratings are designed to enable more accurate categorization of URLs and reduce the risk of over-blocking content.
  - Dynamic Real-Time Rating (DRTR): DRTR dynamically categorizes new Web content in many different languages and in real-time to maximize categorization coverage.
  - User Control Granularity: URL categorization can be combined with user identifiers such as Active Directory (AD) username, AD group, and location and in some cases, IP addresses to allow the implementation of a very granular policy.

5.2.4 Encrypted Traffic Inspection

The SSL Interception feature provides the ability to apply policies to SSL-encrypted sessions for web access, mobile and web applications, and reports on these inspected sessions.

The Client agrees that encrypted malware traffic can only be inspected and analysed after decryption.

The SSL Interception service is intended to provide granular control of SSL interception by:

- **Category:** Decrypting traffic to webmail and social networking sites, but not online banking and health care sites.
- **Destination:** Exempt specific-destination domains or IP addresses from SSL interception.

This SSL Interception service is enabled by a 'Root Certificate' being distributed to the user devices so that the Service may decrypt and re-sign the SSL certificate without generating a browser warning.

Note: The Client is solely responsible to include exception from privacy policy practice in their employee's privacy notice.

5.3 Threat Intelligence

The WSS leverages Threat Intelligence delivered by the NTT Ltd. Global Threat Intelligence Center. WSS includes continuous threat intelligence updates driven by investigations of actual Security Incidents.

5.3.1 Symantec Global Intelligence Network

Connected to Symantec Global Intelligence Network, WSS is enabled to perform real-time threat analysis on sophisticated web traffic behaviour using globally derived intelligence. Symantec Global Intelligence Network is fed by threat information from enterprises, consumers and enterprise endpoints, and threat researchers and engineers.

Symantec Global Intelligence Network provides users with up-to-date protection by using a dynamic rating algorithm to identify and categories web content in real-time.

5.4 Security Analyst Interaction

The WSS 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.

5.5 Security Engineer Interaction

The WSS includes Change and Incident Management delivered by Security Engineers in NTT Ltd. SOCs.

Note: Symantec is responsible for Health and Availability management of the Symantec WSS features, portals (including Symantec WSS Portal), and Symantec cloud infrastructure.

5.6 Client Notification

Security Incident Reports for the WSS 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.

5.7 Portal and Reporting

The WSS Clients have access to following web portals:

- The Symantec WSS Portal: supporting WSS features including MAAS. Clients have access to 90 days proxy logs.
- NTT Ltd. Portal: supporting NTT Ltd. Advanced Analytics capabilities (e.g. Security Incident Reports for WSS Proxy and MAAS logs) and Change/Issue Management requests for WSS. Clients will have access to a web portal that includes access to 90 days of Advanced Analytics generated Events.

5.7.1 Web Security Hosted Reporting

Web Security Hosted Reporting allows the Clients to host log files in the Symantec WSS cloud, providing extended configurable data retention period (2-365 days).

The service can host log files (files can be uploaded from other sources), as well as report on any reporting data that exists in the service (imported or collected via the WSS user browsing activity).

5.8 Health and Availability Monitoring

The NTT Ltd. SOC monitors the overall Health and Availability of MSS infrastructure.

The Client will be notified and kept up to date of issues with overall health and availability via the Incident ticket available on the NTT Ltd. Portal.

Note: NTT Ltd. is not responsible for:

- Health and Availability on connectivity between the Client network and Symantec WSS cloud infrastructure.
- Health and Availability of WSS and Symantec WSS cloud infrastructure.

Refer to section 7 Operational Level Agreement for more information.

NTT Ltd. informs the Client about any planned and scheduled maintenance or probable outage of Symantec WSS infrastructure and Portal, via Incident ticket available on the NTT Ltd. Portal. During these periods, no OLA applies.

5.9 Incident Management

Incident Management focuses on responding to any unplanned interruption to service and operation to minimize any impact to business operations and ensure service quality and availability.

5.9.1 Incident Generation

Incidents may be generated by the SOC or Client raising an Incident related ticket via the NTT Ltd. Portal or telephone call to the SOC. For Incident tickets raised via the NTT Ltd. Portal, with a provided Impact and Urgency, the SOC team will validate the ticket and reserves the right to modify the Impact and Urgency as deemed necessary. For Incidents raised via a telephone call to the SOC, the SOC will create an Incident ticket on behalf of the Client with the relevant Impact and Urgency.

5.9.2 Incident Diagnosis

Incidents are managed based on the priority of the Incident ticket raised on the NTT Ltd. Portal. Priorities are calculated based on Impact and Urgency of an Incident ticket, leading to a specific priority. Priorities are defined as Major, High, Moderate and Low as outlined in the table below

		Urgency/Impact		
		1 Work blocked	2 Work degraded	3 Work not affected
Scope	1 Organization wide	Major=P1	Major=P1	High=P2
	2 Multiple Departments	Major=P1	High=P2	Moderate=P3
	3 Single Department	High=P2	Moderate=P3	Low=P4
	4 Individual	Moderate=P3	Low=P4	Low=P4

The SOC will triage the Incident to assess the priority. Incidents will be assigned to the appropriate SOC engineer who will investigate and analyses further to identify a correction plan to resolve the Incident. Clients are notified of updates to an Incident via the NTT Ltd. Portal and any restoration plan to resolve.

5.9.3 Incident Resolution

The SOC will work to resolve incidents and move to a 'resolved' state to allow Clients to confirm resolution. Incidents will then remain in a resolved state until:

- Client confirms resolution and the incident will be moved to a 'Closed' state
- Client confirms incident is not resolved, the ticket will be moved back to a 'In Progress' state
- Client does not respond, and the incident will be auto closed after 10 days.

NTT Ltd. will keep Clients updated on any Incident resolution plans via the NTT Ltd. Portal. Resolution targets are outlined in the NTT Ltd. Operating Level Agreements – Managed Security Services.

5.9.4 Incident Reporting

Clients are notified of all Incidents via a notification email which contains very minimal information for security purposes, with the full Incident details only available via the NTT Ltd. Portal.

5.10 Service Request Fulfilment

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

5.10.1 Service Request Management

Clients may request information through the NTT Ltd. Portal about the performance or other aspects of in-scope services where applicable. NTT Ltd. shall deduct the commensurate number of MACD credits (if applicable) and provide the information in the Service Request.

5.10.1.1 Request for Information

Clients may request information through the NTT Ltd. Portal about the performance or other aspects of in-scope services where applicable. NTT Ltd. shall deduct the commensurate number of MACD credits (if applicable) and provide the information in the Service Request.

5.10.1.2 Service Request Reporting

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

5.10.1.3 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.

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

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

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, however will still be entitled to raise any changes as required.

MACD service units are bundled offerings with the option to purchase additional MACD units. MACD's are deducted in the execution of any service requests pertaining to Request for Changes of configurations with the Client's approval. 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.

Where the usage of MACD service units for a service request exceeds 6 hours of effort or for non-standard tasks, 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.

5.10.2.1 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:

- What the apparent risk is associated with performing the task
- What impact the change is likely to have
- 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 Service Request for a Non-Standard pre-approved task. No service levels agreement will apply to the execution of a Non-Standard pre-approved task.)

5.10.3 Change Management

At a Client's request, NTT Ltd. will implement a request for change to WSS in accordance to an associated MACD task or Non-Standard task outlined in section 6.11.2.

5.10.3.1 Client sourced requests

Requests for Change must be submitted by valid Client contacts within the NTT Ltd. Portal.

5.10.3.2 NTT Ltd.-Sourced Requests

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

5.10.3.3 Change Reporting

All Changes must be reported and tracked via the NTT Ltd. Portal, this includes Co-Managed scenarios.

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

5.10.3.4 Request for Change

All requests for change types follow the NTT Ltd. Change Management process and require approval by NTT Ltd. NTT Ltd. classify each Request for Change as Simple or Complex which corresponds to the number of Service Units utilized by each task. There are 4 (four) 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 Ltd. Portal) from both parties via a request for change resident in the NTT Ltd. 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 Ltd. 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.

Cancelling a Request for Change

The Client may cancel a Service Request up to 2 hours before any scheduled changes being committed to the WSS configuration. In such a 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 Ltd. Portal. In which case the commensurate MACD credits shall be deducted for both the original change and any subsequent reversal requested.

5.10.3.5 Change Implementation

The party making the Change must complete and document the following tasks associated with each Change:

- Ensure that all changes are documented so that the previous change can be identified and reverted back as no rollback feature is available in WSS.
- Implement and test the change (as far as is possible – testing responsibility is also shared with the Client) to confirm whether the change was successful or not.
- Update NTT Ltd.'s Service Request ticket indicating whether the change was successful or not

- It is imperative each Change is fully documented via a Service Request in the NTT Ltd. Portal to ensure NTT Ltd. can quickly troubleshoot 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 that only appropriately-trained and skilled WSS and Proxy 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 days' notice
- Client performing work that violates OEM support agreements or leads to in-scope configuration items negatively effecting Client production environment

5.10.3.6 Change Impact Analysis

As part of the Change design process, NTT Ltd. conducts a Change Impact Analysis in accordance to all Requests for Change (pre- and/or post-implementation) (except changes made by the Client under Co-Management). NTT Ltd. reviews Incidents, service requests and documentation regarding Requests for Change 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 – including request for change, Patch and Version Management, or PORs to ensure:

- 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 Ltd. Portal.

5.11 Problem Management

5.11.1 Problem Identification and Recording

NTT Ltd. follows ITIL best practices for Problem identification and recording. Problem identification is performed in a number of ways and will typically result in a Problem Ticket in the NTT Ltd. ITSM tool and NTT Ltd. Portal. Typically, Problems are derived from a number of factors such as:

- Repeated Incidents of same or similar nature within single Client or across multiple Clients
- Compound problems caused by multiple Incidents of different nature within single Client
- Notification of problem from Vendor
- Lack of timely patch from Vendor to address security vulnerability
- Trend analysis

5.11.2 Problem Reporting

All Problems are recorded in the ITSM system and reported back through the NTT Ltd. Portal.

5.11.3 Solution Identification and recording

Once a problem is identified and recorded, a suggested plan or where appropriate a number of suggested options for resolution will be recorded in the problem ticket.

5.11.4 Solution Implementation

The Client and NTT Ltd. shall discuss and agree on the best or most appropriate solution and implement as a controlled change or series of changes in line with the standard change process.

5.12 Service Options

5.12.1 Investigator – Enriched and Aggregated Log Search

WSS Clients have the option to purchase NTT Ltd. Investigator log search capabilities. Investigator provides the Client access to an interface to perform historical log searches for Events triggered by NTT Ltd. Advanced Analytics capabilities for WSS.

5.12.2 Secure Long-Term Log Storage and Management

WSS Clients have the option to purchase secure long-term log storage and management for Events triggered by NTT Ltd. Advanced Analytics capabilities for WSS.

5.12.3 Web Security Mobile

Web Security Mobile extends the WSS to incorporate mobile devices and provide a consistent approach to securing mobile users.

5.12.4 WSS Hybrid

NTT Ltd. WSS can be purchased in conjunction with TD-E for on -premise ProxySG. Possible options are as follows:

1. Client purchases both an on-premise proxy and WSS
2. Client has deployed on-premise proxy and adds WSS

5.12.5 Malware Analysis Advanced Service

The Malware Analysis Advanced Service (MAAS) is delivered as an optional add-on service to WSS.

The service is only available if the Client has selected the Malware Analysis Advanced Service option. The MAAS is enabled in the Symantec WSS portal, once the service is procured.

Note: There are no additional configuration options. After the MAAS license is added to the Client account, the relevant Threats report provides indications of which technology blocked the malware: the standard service Threat Protection (AV) or the MAAS (sandboxing).

MAAS utilizes sandboxing resources that are hosted in Symantec data centers to identify suspicious samples and block malicious content from entering Client networks.

Utilizing a set of advanced analysis techniques and capabilities, unknown items/file are sent for sandboxing and detonations. During the detonation phase, the file is held in the sandboxing environment. However, if the detonation takes more time than expected, users may download the file before analysis is complete.

For the initial detection, an email notification is sent to the admin of the service to allow for Client remediation. Detonation email notifications can be sent to more than one recipient.

In both Standard and Co-management set up, Client admin email address must be added to distribution list of MAAS notification to take appropriate actions.

MAAS utilizes sandboxing to detonate suspicious samples in both virtual and emulated environments. Virtual sandbox supports detonation of EXE, DLL, MSI, JAR, RTF, Office, PDF and other file types. MAAS provides advanced analysis (leveraging static code, YARA rules, and behavioural analysis technologies) with notification on risky file detections. MAAS provided full Windows emulation, Office documents and PDF support. The Client receives a full detonation report.

Key Capabilities	Advanced Service
Static Code Analysis	
YARA Rule Analysis	✓
Behavioural Analysis	✓
Emulation of Windows Platform	✓
Inline, Real-time Blocking	✓
File and URL Reputation	✓
Windows Emulation	✓
Full Windows OS Detonation	✓
EXE and DLL Support	
Office Documents and PDF Support	✓
Full Detonation Report	✓

Clients are provided with threat reports indicating of which technology blocked the malware:

- The standard service Threat Protection (AV)
- Malware Analysis Advanced (sandboxing)

5.12.5.1 Cloud-Based Malware Analysis and Protection

Malware Analysis service utilizes a flexible subscription-based cloud service to actively identify and block malware from entering Clients networks and protect mobile users going who are going to direct-to-net to access apps.

5.12.5.2 Identify and Block Zero-day threats

MAAS utilizes sandboxing with virtual and emulation detonation environments to analyses unknown or suspicious files. If the file is identified as malicious, it is immediately blocked, and WSS proxy settings are updated to block any future access to the same object. Also, the object's URL, file hash, timestamp and filename are added to the Global Intelligence Network.

The following are therefore important considerations:

- For zero day threats, if the detonation takes more time than expected, a Client may download a potential threat, open and execute the item and become infected.
- If the file subsequently receives a malicious verdict, MAAS updates Symantec Global Intelligence Network and WSS to block all future downloads
- If the detonation result declares that the file is malicious, an entry is added to 'post-download detection' events section in Symantec WSS portal.

6 Terminologies and Definitions

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

7 Operational Level Agreement

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

8 Changes in Service

8.1 Regulatory Change Requirements

If regulatory changes (e.g., changes by a regulatory agency, legislative body, or court of competent jurisdiction) require NTT Ltd. to modify the Services described herein, NTT Ltd. will modify the Services and this Service Description accordingly without diminishing the features, functionality or performance. In the event a modification in response to regulatory changes results in a diminishment of features, functionality or performance, Client agrees in good faith to work with NTT Ltd. to amend this Service Description accordingly and execute any additional agreement which may be reasonable requested by NTT Ltd. to document such amendment.

8.2 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.

8.3 Unanticipated Log Volume

Client agrees in good faith to work with NTT Ltd. to amend the contract accordingly, if the Client environment generates an inordinate number of Logs or Events processed by the NTT Ltd. MSS.

8.4 Changes in MACD

NTT Ltd. has the right to modify/change MACD lists and associated service unit.

9 Service Exclusions

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

Unless otherwise expressly agreed by NTT Ltd. in writing, 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 Ltd. 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.

10 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.

Appendix A - WSS URL Filtering Categories

https://support.symantec.com/en_US/article.HOWTO54164.htm

Appendix B – WSS Policy Management MACD

Task	MACD	Comments
AD Integration Configuration	6	The scope of AD integration configuration is on Symantec WSS Portal Only. The Client's side of changes needs to be delivered by the Client. If the task cannot be delivered due to additional scope of works or complexity, it should be switched to 'Other' delivered via Project (T&M) rather than fixed MACD service units
Report - Single	2	Create or Modify a single simple Report or provide Access logs or create new Report Filter, does not include Scheduled Reports.
Report - Single Complex	4	Create or Modify a Complex report, including multiple reports & or Scheduling a report
Bypass URL / Domain – Single	1	Examples: Malware, Proxy (PAC), SSL bypasses
Bypass URL / Domain – List Provided	3	Examples: Malware, Proxy (PAC), SSL bypasses. Client provides a list for import, this may need correct formatting & deduplication.
Option Change	1	Quick Changes to settings. Examples: Unified Agent, Authentication Policy, DLP, Reporting, Integration tokens MDM API keys, Non-Custom Error Pages,
Delete Item	1	Examples: Policy, User, Object, Location, Report, Bypass.
Policy Change - Simple	3	Create or Modify a Simple single line of Browsing Policy containing few objects or insignificant amount of change, may include updates email distribution lists such as Malware.
Policy Change - Complex	6	Complex policy changes, including updates of multiple objects and rules, or re-organizing policy. More complex changes would need to be negotiated as 'Other'.
Policy Backup	2	NOTE: This is currently unavailable; expect to be a future option.
User or Group Create – Single item	1	Most likely to be Admin Portal Users, most browsing users will be defined in Customer Managed User repositories like Active Directory. This item can also include a single list import. NOTE: User / Group deletions are covered by 'Delete Item' task.
PAC File Management	4	This is becoming increasingly complex due to new functionality. This may involve testing or duplicating of PAC for specific locations.
Other	0	Non-Standard Service Requests or Exceed amount of estimated efforts; Service Requests will be delivered via Project (T&M) Utilized for many of the 'ad-hoc' tasks and can be negotiated with the Client once the Engineer has provided an estimate. Can also be utilized for the major changes to deployment which would have normally been completed by the on-boarding or Professional Services teams.

NTT

Together we do great things