Managed Security Services

Service Description

November 2018

Service Overview

The Managed Security Services (each a "**Service**" or collectively, "**MSS**" or "**Services**") comprise one or more of the following services, depending on the offering purchased by Customer as indicated in the Order Confirmation and as further described in this Service Description.

- **Advanced Security Monitoring Service** provides 24x7 real-time security monitoring, analysis and reporting, and early warning intelligence. Symantec does this by leveraging a combination of skilled analysts and proprietary technology in conjunction with Symantec's global intelligence network. Symantec works with Customer to identify known and emerging threats to Customer's critical infrastructure and to protect Customer's assets.

- **Hosted Log Retention Service** provides log collection and storage in a resilient and secure environment which Symantec hosts for Customer.

- **Managed IDS/IPS Intrusion Detection System (IDS) and Intrusion Prevention System** provides 24x7 alarm and incident management, lifecycle management support and emergency access to security experts. It also includes full security management with unlimited changes and policy recommendations.

- **Managed Endpoint Detection and Response Service** ("**MEDR**") provides Customer proactive responses by investigating suspicious activities by using Symantec's proprietary MEDR tool in an effort to provide additional context and refine incident severity.

    - MEDR is for customers who also use both Symantec Advanced Threat Protection: Endpoint ("**ATP**") [1] and Symantec Endpoint Detection ("**SEP**") [2]. Alternatively, Customer may use Symantec Endpoint Detection and Response ("**SEDR**")[3] instead of ATP. Separate purchases are required for ATP, SEDR and SEP.

    - MEDR is also available for customers who use the MSS Advanced Security Monitoring Service (separate purchase required). Except for *MEDR* and *Incident Response Retainer Services (Base)* described in this Service Description, the version of the service description for MSS that has applied to you prior to purchasing MEDR will continue to apply during Customer's use of MEDR.

This Service Description, with any attachments included by reference, is part of: (i) any signed agreement between Symantec and Customer which governs the use of the Services; or (ii) if no such signed agreement exists, the Symantec Online Services Terms and Conditions **(each, an "Agreement").**

This Service Description shall apply to Services purchased by Customer on or after July 19, 2017.

For Services purchased by Customer prior to July 19, 2017, the Service Description dated April 2017 shall apply, a copy of which is available at https://www.symantec.com/about/legal/repository or upon request to Symantec.

[1] Must be ATP version 3.0 or above.
[2] Must be SEP version 14.x.
[3] Must be SEDR version 4.0 or above.

For Services purchased by Customer prior to November 1, 2016, the Service Attributes dated January 1, 2015 shall apply, a copy of which is available at http://www.symantec.com/docs/TECH131855 or upon request to Symantec.

Table of Contents

TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

Service Features

- The MSS Offerings Chart, contained in Attachment 1 of this Service Description ("**MSS Offerings Chart**"), details certain information and attributes associated with each of the Service(s). In addition to those services features identified in the Service(s) Offerings Chart, the following service features apply to all the Service(s):

- ***MSS Portal***. Each of the Service(s) includes access to and use of the MSS portal ("**Portal**"), which is made available to Customer for use during the Term.
- ***Managed Security Services Operations Manual***. The Operations Manual, which is available on the Portal, provides further description of the Service(s), and details additional Customer responsibilities which may be applicable to the Service(s). Symantec will use commercially reasonable efforts to give Customer thirty (30) days' notice through the Portal of any material change to the Operations Manual.
- ***Security Operations Centers***. All Service(s) are performed remotely from Security Operations Centers ("**SOC(s)**").
- ***Scheduled Outages***. Symantec will, from time to time, schedule regular maintenance on the SOC Infrastructure (defined below) or on Device(s) (defined below) receiving Management Service(s) (defined below), requiring a maintenance outage. The protocol for any such maintenance outage is described in the Operations Manual.

- **TECHNICAL SERVICES COORDINATOR**. Customer may optionally purchase the services of a Technical Services Coordinator ("**TSC**"). The TSC is a remote resource responsible for fulfilling tasks that directly support the Service(s) in a manner tailored for the Customer. The TSC and Customer will mutually agree to tasks which support the delivery of Service(s), such that these tasks may not exceed twenty (20) hours per week of the TSC's time and must fall within the technical expertise of the TSC.

- **HOSTED MANAGEMENT CONSOLES**. Customer may renew the use of Hosted Management Consoles located at the SOC for centralized management of certain Device(s) receiving Service(s). Customer is responsible for obtaining any required license(s) from the technology vendor to allow applicable use of the Hosted Management Console (Hosted Management Console is no longer available for new purchases.)

- **REPAIR AND REPLACEMENT OF THE OUT-OF-BAND MANAGEMENT SOLUTION HARDWARE**. The "**Out-of-Band Management Solution**" means a third-party hardware product which Symantec may provide, at its sole discretion, for Customer's use to facilitate the remote configuration and management of Device(s) for a Customer who has purchased Management Service(s). Customer acknowledges and agrees that Symantec and/or its licensors are the owner(s) of any Out-of-Band Management Solution and only grants Customer the right to use the Out-of-Band Management Solution during the Term. In the event the Out-of-Band Management Solution fails due to a defect during the Term, Symantec will replace it subject to notification and reasonable cooperation from Customer. Customer acknowledges and agrees that Symantec is not responsible for any outages that may occur during the time that the Out-of-Band Management Solution is being replaced. Customer further acknowledges and agrees that Customer is responsible for the cost of replacing the Out-of-Band Management Solution if failure is due to misuse or negligence of Customer.

- **INCIDENT RESPONSE RETAINER SERVICES (BASE).** To minimize the impact of security incidents and shortens the timeframe between incident identification and incident resolution, *Incident Response Retainer Services (Base)* is now part of MSS. Customer can activate the benefits of Incident Response Retainer Services (Base) by paying an additional fee. For more details, please refer to the *Incident Response Retainer Services (Base) - Service Description*, a copy of which is available at https://www.symantec.com/about/legal/repository or upon request to Symantec.

- **MANAGED NETWORK FORENSICS SERVICE.** With Managed Network Forensics Service ("**MNF**"), MSS security analysts provide Customer proactive responses by investigating suspicious activities in an effort to provide additional context and refine incident severity. Additional fees are required. MNF is for customers who also use the Advanced Security Monitoring Service of MSS to enhance its service features and own Symantec approved Network Forensics Investigation

Devices (defined below). For more details, please refer to **Attachment 2**. NOTE: The version of the service description for MSS that applies to you continues to apply during Customer's use of MNF.

- **ADDITIONAL / OUT OF SCOPE SERVICE(S); TOKENS**. From time to time, Customer may request and Symantec may provide, certain services not currently described in the Service(s) Offerings Chart (hereinafter "**Exception Services**"). Customer may pay for such Exception Services by purchasing Tokens which can be applied to the cost of such Exception Services. The description and cost in Tokens of any Exception Services must be mutually agreed and attached to the Agreement. Tokens are valid for twelve (12) months from the date of purchase. Unused Tokens will expire after the validity period is over.

Customer Responsibilities

Customer may use the Services only in accordance with the use meter or model under which Customer has obtained use of the Service: (i) as indicated in the Order Confirmation; and (ii) as defined in this Service Description or the Agreement.

Symantec can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following responsibilities, Symantec's performance of the Service may be delayed, impaired or prevented, and/or eligibility for Service Level Agreement benefits may be voided, as noted below.

- Adequate Customer Personnel: Customer must provide adequate personnel to assist Symantec in delivery of the Service, upon reasonable request by Symantec.
- Device Registration: To access the Service(s), Customer must first register the serial number(s) identified in the Order Confirmation on the Symantec licensing portal located at https://licensing.symantec.com and designate its authorized points of contact for the Service(s) ("**POC(s)**"). Upon serial number registration, Customer will be given access to the Portal and SOC technical staff. Customer must provide all technical and license information for each firewall, server, intrusion detection device, or other hardware or software (each, a "**Device**") reasonably requested by Symantec, prior to such Device being recognized by the Service(s) and connected to the SOC ("**Device Registration**"). Customer acknowledges and agrees that the Term will expire upon the last day of the Term, even if no Devices undergo Device Registration or receive Service(s) during the Term.
- Reasonable Assistance: Customer must provide reasonable assistance to Symantec, including, but not limited to, providing all technical and license information related to the Service(s) reasonably requested by Symantec, and to enable Symantec to perform the Service(s). For management Service(s) (as further described in the MSS Offerings Chart ("**Management Service(s)**"), Customer must provide Symantec remote access to the managed Device(s) and necessary administrative credentials to enable Symantec to perform the Service(s).
- Use of Log Collection Platform: For monitoring Service (as further described in the MSS Offerings Chart ("**Monitoring Service(s)**"), Customer must successfully install a Symantec Log Collection Platform ("**LCP**") image within the Customer's environment, and establish the necessary network access to allow the SOC to remotely manage the LCP, and to allow the collector to extract log data of the Device(s) and transport such log data back to the SOC. LCP must be a supported version as specified in the Supported Product List ("**SPL**") available on the Portal (requires log-in). Customer must provide all required hardware or virtual machines necessary for the LCP, and enable access to such hardware or virtual machines by Symantec (as specified in the Operations Manual). In addition, for select logging technologies (as specified in the SPL), Customer may also be required to install collectors on customer provided systems other than the LCP and enable access to/from the LCP. Customer understands that Symantec must have access to log data of the Device(s) in a format that is compatible with Symantec's collectors and in some cases this may require configuration changes to Device(s). Customer agrees to make any necessary changes to the configuration of the Device(s), as described by SOC personnel, to conform with the supported format.

- Accurate Information: Customer must provide Symantec with accurate and up-to-date information, including, the name, email, landline, mobile, and pager numbers for all designated, authorized points of contact who will be provided access to the portal. Customer must provide the name, email, and phone numbers for all shipping, installation and security points of contact.
- Customer's Outage: Customer must provide Symantec at least twelve (12) hours in advance of any scheduled outage (maintenance), network, or system administration activity that would affect Symantec's ability to perform the Service(s).
- Daily Service Summary: Customer must review the Daily Service Summary to understand the current status of Service(s) delivered and actively work with the SOC to resolve any tickets requiring Customer input or action.
- Customer Software and Hardware: It is Customer's sole responsibility to maintain current maintenance and technical support contracts with Customer's software and hardware vendors for any Device(s) affected by Service(s). Customer must ensure any Device(s) receiving Service(s) conform to the version requirements stated in the SPL. It is Customer's responsibility to interact with Device(s) manufacturers and vendors to ensure that the Device(s) are scoped and implemented in accordance with manufacturer's suggested standards. Customer is also responsible for interactions with Device(s) manufacturers or vendors regarding the resolution of any issues related to Device(s) scoping, feature limitations or performance issues. For those Service(s) where Symantec is not solely responsible for the management of Customer's Device(s), Customer is responsible for remediation and resolution of changes to Device(s) which negatively impact the Service(s) or the functionality, health, stability, or performance of Device(s). Symantec may charge additional fees (Tokens) in the event that Customer requires Symantec's assistance for remediation or resolution activities.
- Acceptable Use Policy: Customer is responsible for complying with the *Symantec Online Services Acceptable Use Policy*, a copy of which is available at https://www.symantec.com/about/legal/repository or upon request to Symantec.

Supported Platforms and Technical Requirements

Supported platforms for the Service are defined at
https://mss.trm.symantec.com/SIINextGen/Home/DownloadFile?fileNumber=2113592 (requires log-in)

Hardware requirements can be found in the MSS Deployment Guide (and such other applicable guide based on your purchase) distributed by Customer's Service Manager.
The SPL describes the supported versions of the Device(s) that may receive Service(s). In the event the SPL indicates a Device can only be supported at a lower level of Service than what was purchased (i.e., Hosted Log Retention or Advanced), Customer shall receive the highest supported level of Service indicated on the SPL, not to exceed the level purchased.

Service Enabling Software

The Service includes the LCP Software as a Service Component, upon payment of the applicable fee.

Customer's use of the LCP Software shall at all times be in accordance with the LCP EULA accompanying the LCP Software, and shall be for the limited purpose of collecting and/or storing logs from a log source and forwarding those logs to Symantec for retention and/or security analysis in connection with the Services. Customer's system administrator may accept the terms of the LCP EULA on behalf Customer for all Customer Devices leveraging the LCP Software. By agreeing to this Service Description, Customer is also agreeing to the terms of the LCP EULA, if installed.

The license rights granted to Customer to the LCP Software under the LCP EULA will terminate upon the earlier of Customer's breach of any term contained in the LCP EULA or the expiration or earlier termination of the Service(s). Upon expiration or earlier termination, Customer shall immediately stop using and destroy all copies of the LCP Software.

Depending on your purchase, the Service may include additional enabling software, which should be used only in connection with Customer's use of the Service during the Term. Use of the enabling software is subject to the license agreement accompanying such software ("**Software License Agreement**"). If no Software License Agreement accompanies the software, it is governed by the terms and conditions located at http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf. In the event of conflict, the terms of this Service Description prevail over any such Software License Agreement. Customer must remove enabling software upon expiration or termination of the Service.

Assistance and Technical Support

- Technical assistance for the Service(s) will be provided by the SOC as described in the Operations Manual available on the Portal.
- Notwithstanding the foregoing, if Customer is entitled to receive technical support from a Symantec reseller, please refer to Customer's agreement with that reseller for details regarding such technical support, and the technical support described in the Operations Manual will not apply to Customer.

SERVICE-SPECIFIC TERMS

Changes to Subscription
If Customer has received Customer's subscription directly from Symantec, communication regarding permitted changes of Customer's subscription must be sent to the following address (or replacement address as published by Symantec): DL-CSS-BusinessOperations@symantec.com, unless otherwise noted in Customer's agreement with Symantec. Any notice given according to this procedure will be deemed to have been given when received. If Customer has received Customer's subscription through a Symantec reseller, please contact Customer's reseller.

Use Model

Use of the Service(s) is limited to the *Enterprise Wide Model* or *Per Unit Model* as set forth in the Order Confirmation, and as further described below:

- **Enterprise Wide Model**.
    - End User(s); Nodes. For Service(s) identified in the Order Confirmation as 'Enterprise Wide' ("**Enterprise Wide Service(s)**"), Customer warrants and represents that the quantity of Service(s) purchased by Customer reflects the total number of Nodes owned or used by Customer or the legal entity or entities benefiting from the Service(s) (each, an "**End User**", collectively, "**End User(s)**") at the time of purchase, regardless of whether each such Node directly interacts with or is protected by the Service(s) ("**Node Count**"). Each "**Node**" is a virtual or physical unique network address, such as an Internet protocol address. Enterprise Wide Service(s) entitle the End User to receive Service(s) for an unlimited quantity of Device(s) owned or used by End User, subject always to End User's Node Count Compliance as set forth below and each such Device conforming to the version requirements stated in the SPL.
    - Node Count Compliance. If, during the Term, End User(s)' applicable Node Count increases by more than five percent (5%) over the Node Count associated with the Service(s) purchased, then Customer agrees to promptly, but no later

than thirty (30) days following the increase in Node Count, purchase additional Service(s) to become compliant with such expanded Node Count. Symantec may, at its discretion, but no more than once every twelve (12) months, request Customer to validate the End User(s)' Node Count to Symantec in writing.

- Outsourcer Purchases. If Customer is a provider of outsourced services and purchases Enterprise Wide Service(s) for the benefit of an End User pursuant to an outsourcing agreement with such End User, Customer warrants and represents that the quantity of Service(s) purchased by Customer reflects the total Node Count for such End User receiving Customer's outsourced services.

- **Per Unit Model.**
  - For Service(s) not identified in the Order Confirmation as 'Enterprise Wide' ("**Per Unit Services**"), Symantec will provide the Service(s) to Customer commensurate with the quantity of Service(s) entitlement purchased as identified in the Order Confirmation. Per Unit Services are offered on a per Device pricing basis.

- **MEDR Model.**
  - For MEDR, Symantec will provide the MEDR Service to Customer commensurate with the quantity of entitlement purchased as identified in the Order Confirmation. Customer must purchase one license per each endpoint to be included in the MEDR Service ("**Endpoint**"). All Endpoints must be running a Windows® operating system of Windows 98 or above - whether on premise or in cloud (Amazon EC2 or Azure VM).

Termination Due to End of Service Availability

- The Service(s) (or a portion) may be terminated upon ninety (90) days prior written notice by Symantec, in the event that the Service(s) (or a portion) are affected by Symantec's cessation of, or designation of 'end of life' of, such Service(s) (or a portion). In the event that Symantec exercises its termination rights above, as good and valuable consideration, Symantec will credit Customer's account any prorated, unused fees received by Symantec for the impacted Service(s) (or a portion).

Service Conditions

- The use of any Service Component in the form of software shall be governed by the license agreement accompanying the software. If no EULA accompanies the Service Component, it shall be governed by the terms and conditions located at http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf). Any additional rights and obligations with respect to the use of such Service Component shall be as set forth in this Service Description.
- Except as otherwise specified in the Service Description, the Service (including any Service Components provided therewith) may use open source and other third-party materials that are subject to a separate license. Please see the applicable Third Party Notice, if applicable, at http://www.symantec.com/about/profile/policies/eulas/.
- Symantec may update the Service at any time in order to maintain the effectiveness of the Service.
- The Service may be accessed and used globally, subject to applicable export compliance limitations and technical limitations in accordance with the then-current Symantec standards.
- Customer shall comply with all applicable laws with respect to use of the Service. In certain countries it may be necessary to obtain the consent of individual personnel. Configuration and use of the Service is entirely in Customer's control,

therefore, Symantec is not liable for Customer's use of the Service, nor liable for any civil or criminal liability that may be incurred by Customer as a result of the operation of the Service.

SERVICE LEVEL AGREEMENT.

SERVICE LEVEL WARRANTIES & SERVICE CREDITS.

The service level warranties ("**SLWs**") listed below will apply to those Service(s) listed in the MSS Offerings Chart. The MSS Offerings Chart additionally details the SLW(s) applicable for each of the Service(s). Symantec's sole and exclusive obligation and Customer's sole and exclusive remedy for failure to meet the SLWs listed below shall be limited to the payment of Service Credit(s), as further described below.

- **Device Registration Warranty**.
  - The *Customer Responsibilities* set forth above must be met for Device(s) prior to Device Registration ("**Registration Requirements**").
  - Symantec will register each Device(s) upon the later occurrence of the following:
    - fifteen (15) business days after completion of the Registration Requirements; or
    - upon the Start Date identified in the Order Confirmation; or
    - in accordance with the registration date or timeline identified in a mutually agreed upon deployment schedule. A deployment schedule created by Symantec may be required, in Symantec's sole discretion, in the event that the Service(s) require registration of ten (10) or more Device(s).
  - If Symantec fails to register one or more Device(s) as required above, then Symantec will credit Customer's account for each day the deadline is missed, as follows:
    - for Enterprise Wide Service(s), one (1) Service Credit for each day the deadline is missed; or
    - for Per Unit Service(s) and solely with respect to a Device Block, one (1) Service Credit for each day the deadline is missed, regardless of how many Device(s) are contained within such Device Block. A "**Device Block**" refers to the unit of measure in which certain Per Unit Service(s) are purchased (e.g., a block of 2500 endpoints, a block of 10 HIDS/HIPS, a block of 150 servers of applications/OS); or
    - for all other Per Unit Service(s), one (1) Service Credit for each day the deadline is missed for each Device.

- **Severe Event Notification Warranty**. For Monitoring Service(s) (as further described in the MSS Offerings Chart), Symantec will initiate contact to notify Customer of Emergency and Critical incidents (as defined in the Operations Manual) within the specified Severe Event Notification Time identified in the MSS Offerings Chart, once the determination that an Emergency and Critical incident has occurred (as specified in the Operations Manual). If Symantec does not initiate contact within the specified time, Symantec will credit Customer's account with one (1) Service Credit(s) for impacted Enterprise Wide Service(s) or one (1) Service Credit for each impacted Device Block or Device, as applicable, unless the Device(s) subject to the Emergency or Critical incident is deemed to be a "**Runaway Device**," as defined in the Operations Manual.

- **Managed Device Availability Up-Time Warranty**. For Management Service(s), Device(s) shall be available in accordance with the Managed Device Availability Up-time Percentage, as identified in the MSS Offerings Chart, of each calendar month during the Term (excluding scheduled outage, hardware/software failures, failures resulting from changes made by Customer, and circumstances beyond SOC control, as further described I the Operations Manual). If the Device(s) is not available as specified in the preceding sentence, Symantec will credit Customer's account with one (1) Service Credit for each 24-hour period, or portion thereof for which this SLW is not met. If the Device(s) does not meet the version prerequisites as specified in the

current SPL or the immediately prior supported version prerequisites (as specified in a prior version of the SPL), then Symantec will not be liable for this SLW for such non-conforming Device(s).

- **Standard Changes Completion Time Warranty**. For Management Service(s), Symantec will complete Standard Changes within the Standard Changes Completion Time, as identified in the MSS Offerings Chart. If Symantec does not meet this SLW, Symantec will credit Customer's account with one (1) Service Credit.

- **Minor Changes Completion Time Warranty**. For Management Service(s), Symantec will complete Minor Changes within the Minor Changes Completion Time, as identified in the MSS Offerings Chart. If Symantec does not meet this SLW, Symantec will credit Customer's account with one (1) Service Credit.

- **Emergency Change or Assistance Response Time Warranty**. For Management Service(s), when an emergency change request or other emergency assistance is required, a SOC engineer will be made available to begin work on or assist with the emergency request in accordance with the timeline identified in the MSS Offerings Chart. If Symantec does not meet this SLW, and Customer has not exceeded their contracted Emergency Change or Assistance Requests for the month as specified in MSS Offerings Chart, Symantec will credit Client's account with one (1) Service Credit.

- **SOC Infrastructure Up-Time Warranty**. Symantec warrants that the SOC data storage, SOC log analysis processing, any Hosted Management Consoles, the Portal, and SOC customer communication methods (i.e., phone, email, the Portal) (together, the "**SOC Infrastructure**") shall be available in accordance with the SOC Infrastructure Up-time Percentage identified in the MSS Offerings Chart, for each calendar month during the Term (excluding scheduled outage, hardware/software failures, failures resulting from changes made by Customer, and circumstances beyond SOC control, as further described in the Operations Manual). If any or all of the SOC Infrastructure is not available as specified in the preceding sentence, Symantec will credit Customer's account with one (1) Service Credit for each 24-hour period, or portion thereof for which the warranty is not met.

- **Monthly Reporting Warranty**. If Symantec does not provide the applicable monthly reports, as specified in the Operations Manual, to Customer by or before the Monthly Reporting Time, as identified in the MSS Offerings Chart, of the immediately following calendar month, Symantec agrees to credit Customer's account with one (1) Service Credit.

- **Service Credits**. The process for requesting a Service Credit for an SLW failure is set forth in the Operations Manual and must be initiated by the Client within thirty (30) days of occurrence of the SLW failure. A service credit shall be calculated as follows:

    - For Enterprise Wide Service(s): A Service Credit shall be calculated as ten percent (10%) of the prorated daily fee payable to Symantec for the affected Enterprise Wide Service(s). For avoidance of doubt, Symantec will issue one (1) Service Credit per verified SLW failure, regardless of the number of affected Device(s).
    - For Per Unit Service(s): For Per Unit Service(s) purchased for a Device Block, a Service Credit shall be calculated as the prorated daily fee payable to Symantec for the affected Device Block, regardless of how many Device(s) within the Device Block are affected. For all other Per Unit Service(s), a Service Credit shall be calculated as the prorated daily fee payable to Symantec for the affected Device(s) (excluding Tokens and any one-time fees).
    - Service Credit(s) granted hereunder will first be applied towards Customer's next invoice due for the applicable Service(s) during the Term, or if no additional invoices are due for such Service(s), shall be provided as a payment.

- **Limitation of Service Credit Obligation.** Notwithstanding anything to the contrary in this Service Description, in no event will Symantec be required to credit Customer more than the value of the prorated Service(s) fees received by Symantec for the affected Service(s) for the period of time in which any SLWs were missed. Symantec's sole and exclusive obligation and Customer's sole and exclusive remedy for each respective SLW set forth in this Service Description will be limited to the issuance of Service Credit(s).

DATA PRIVACY NOTICE.

Customer may be required to supply certain business information which is necessary for Symantec to provide the Service and which may contain personally identifiable information (**"Personal Information"**), including but not limited to, names, e-mail address, IP address and contact details of designated users and contacts for the Service, Personal Information provided during configuration of the Service(s) or any subsequent service call and other Personal Information as described in the Agreement (**"Provisioning Data"**). Additionally, Customer acknowledges that in performing certain Service(s), Symantec may, on behalf of Customer, collect and process log data which may include certain source and destination IP addresses, host name, username, and policy names which may be classed as Personal Information (**"Log Data"**). Customer acknowledges that it is the controller of such Log Data and Provisioning Data, and agrees that it is will take all necessary measures to ensure that it, and all of its employees, are aware that their Personal Information may be processed as part of the Service(s) and that they have given their consent to such processing as well as complied with their responsibilities as data controller or data subjects, as applicable, in accordance with applicable laws and/or regulations. By providing Personal Information, Customer consents, for itself, its users and contacts, to the following: Personal Information will be processed and accessible on a global basis by Symantec, its affiliates, agents and subcontractors for the purposes of providing the Service(s), to generate statistical information about the Service(s), for internal research and development, and as otherwise described in the Agreement, including in countries that may have less protective data protection laws than the country in which Customer or its users are located. Symantec may disclose the collected Personal Information as required or permitted by law or in response to a subpoena or other legal process. Customer understands and agrees that Symantec has no control or influence over the content of the Log Data processed by Symantec and that Symantec performs the Service(s) on behalf of Customer and that Symantec will only process the Personal Information provided by Customer in both Log Data and Provisioning Data accordance with the instructions of Customer, provided that such instructions are not incompatible with the terms of the Agreement. Symantec will also take appropriate technical and organizational measures to protect personal information against accidental loss or destruction of, or damage to, that Personal Information. Contact the following for any questions or to access Customer's Personal Information: Symantec Corporation – Privacy Program Office, 350 Ellis Street, PO Box 7011, Mountain View, CA 94043, U.S.A. Email: privacyteam@symantec.com**.**

DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement, this Services Description or the Operations Manual, have the meaning given below:

"Credit Request" means the notification which Customer must submit to Symantec by email with the subject line "Credit Request" (unless otherwise notified by Symantec).

"Customer" means the customer identified in the Order Confirmation.

"**End User License Agreement (EULA)**" means the terms and conditions accompanying Software (defined below).

"Operations Manual" means the Managed Security Services Operation Manual.

"**Service Component**" means certain enabling Software, hardware peripherals and associated documentation which may be separately provided by Symantec as an incidental part of a Service.

"**Service Credit**" means the amount of money that will be credited to Customer's next invoice after submission of a Credit Request and validation by Symantec that a credit is due to Customer.

"**Software**" means each Symantec or licensor software program, in object code format, licensed to Customer by Symantec and governed by the terms of the accompanying EULA, or this Service Description, as applicable, including without limitation new releases or updates as provided hereunder.

"**Symantec**" means Symantec Corporation and/or its subsidiaries.

"Symantec Online Service Terms and Conditions" means the Online Services Terms and Conditions located at or accessed through https://www.symantec.com/about/legal/repository.

"**Term**" shall mean the term of the subscription of the Service(s) as specified in the applicable Order Confirmation.

"**Tokens**" means the total number of units purchased and redeemable for Exception Services.

END OF SERVICE DESCRIPTION

ATTACHMENT 1

MSS OFFERINGS CHARTS

	SYMANTEC MSS SECURITY MONITORING SERVICES	
Feature	**Log Retention Service**	**Advanced Security Monitoring Service**
Service Use Model[1]	Per Unit or Enterprise Wide	Per Unit or Enterprise Wide
Service Level Warranty Metrics		
Device Registration	As described in the Service Level Warranties	
Severe Event Notification Time	N/A	10 minutes
SOC Infrastructure Up-Time Percentage	99.90%	99.90%
Monthly Reporting Time	by 5th business day	by 5th business day
Hosted Log Retention (duration @ SOC during Services Term only):		
Online portal access to logs	3 months (92 days)[2]	3 months (92 days)[2]
Extended online portal access to logs from 3 months to 12 months[3]	optional	optional
Offline Log Retention[4]	12 months	12 months
Online Incident Data Retention	Service Term	Service Term
Security Incident Analysis		
Log/Alert data collection, aggregation, and normalization	X	X
Logs available for SOC Analyst inspection	X[5]	X

Feature	SYMANTEC MSS SECURITY MONITORING SERVICES	
	Log Retention Service	Advanced Security Monitoring Service
Analyze security data and customer context to detect signs of malicious activity, as applicable based on the log output received from the monitored Device(s): •Identify firewall port scans and brute force threshold exceptions •Identify host and network intrusions or suspect traffic •Identify connections to backdoors and Trojans •Identify events detected by endpoint security solutions •Identify internal systems attacking other internal systems •Identify connect to/from customer-specified bad/blocked URLs •Identify threats through parsing of web proxy data for connections to malicious URLs •Identify Emerging Threats (as defined by the Operations Manual)	N/A	X
Analyze security data and customer context to detect signs of malicious activity, as applicable based on the log output received from the monitored Device(s): •Identify threats that connect to/from IP addresses or URLs that are identified by Symantec's Global Intelligence Network (GIN) as malicious. •Identify anomalous traffic to/from an IP address within a registered network •Advanced Threat Protection – Detect[6] (automatic correlation of networking and endpoint events with Symantec GIN to assist in detection of malicious activity)	N/A	X
Vulnerability Data Correlation Integration	N/A	X
Validate, Assess and Prioritize impact of Incident to Enterprise	N/A	X
Security Incident Escalation		
Method of Notification of Security Incidents:		
Voice (as defined in the Operations Manual), Portal, Email (per Incident or Digest)	N/A	X

Feature	SYMANTEC MSS SECURITY MONITORING SERVICES	
	Log Retention Service	Advanced Security Monitoring Service
Method of Notification of Outage Incidents:		
Voice (as defined in the Operations Manual), Portal, Email (per Incident or Digest)	N/A	X
General Service Features		
Detection and response updated for emerging threats	N/A	X
Daily Service Summary delivered by e-mail	N/A	X
Log/device unavailability alerting and notification[7]	X	X
Online logs may be queried by customer via the Portal	X	X
Compliance reporting available on the Portal	X	X
Access to the Secure Internet Interface	X	X

[1] Refer to SPL to determine which Service(s) are available in Per Unit or Enterprise Wide models, at which level of service, and for which supported technologies.
[2] Subject to run away Device limits per the Operations Manual.
[3] Available for Per Unit Services only (on a per Customer basis). This option extends, for all licensed Devices, the time period that respective logs are available for viewing in a Customer's MSS portal from 92 days to 365 days during the Term of Customer's subscription for the applicable Services. For multi-year Terms of Services, Customer must purchase this option for each and every year of the Term.
[4] Restoral of offline log data done on best-effort basis. Restoral fees may apply, as advised by the Symantec team.
[5] Log Retention alone performs no security analysis. However, the retained log data is automatically associated with security incidents generated by other devices under Security Monitoring service(s) and is available for SOC analyst inspection.
[6] Refer to SPL to determine which technologies are required for Advanced Threat Protection – Detect.
[7] Notification of outage incidents for the HIPS/HIDS and Endpoint monitoring technologies shall apply to Manager/Management consoles only. Notification of outage incidents for all other technologies registered in netblock ranges shall be based on outage monitoring of the netblock range, Log Collection Platform, or Remote Importer.

	SYMANTEC MSS SECURITY MANAGEMENT SERVICES				
Feature	**Essential Management Firewall or UTM[7]**	**Advanced Management Firewall or UTM[7]**	**Essential Management Endpoint Protection[7]**	**Advanced Management Endpoint Protection[7]**	**Advanced Management IDS or IPS**
Service Use Model	Per Unit only	Per Unit only	Per Unit only	Per Unit	Per Unit only[5]
Service Level Warranty Metrics					
Device Registration	As described in the Service Level Warranties				
Managed Device Availability Up-Time Percentage	99.90%	99.95%	N/A	N/A	99.95%
SOC Infrastructure Up-Time Percentage	99.90%	99.90%	99.90%	99.90%	99.90%
Monthly Reporting Time	by 5th business day	by 5th business day	by 5th business day	by 5th business day	by 5th business day
Standard Changes Completion Time	6 hours for changes performed and completed by SOC				
Minor Changes Completion Time	24 hours for changes performed and completed by SOC				
Emergency Change or Assistance Response Time	Symantec will attempt to make SOC engineer available immediately; but not later than within 30 minutes of request				
Change Management					
Standard Changes (Includes a single, low-risk configuration or policy change using Portal standard change request templates. For endpoints, includes basic administrative tasks on the Management Console)	Customer Responsibility (The SOC will complete up to 5 Standard or Minor changes each calendar month).	Unlimited Requests	Customer Responsibility[2] (The SOC is available to assist in up to 5 Standard changes each calendar month).	Unlimited Requests	Updates to detection definitions occurs automatically when the signature update is released by the vendor.
Minor Changes (Includes a single change that is too complex to be requested thru the Portal standard change request templates. Includes endpoint Anti-virus / Firewall / IPS / Application Control / Device Control / Host Integrity policy management)	Customer Responsibility (The SOC will complete up to 5 Standard or Minor changes each calendar month).	Unlimited Requests	Customer Responsibility[2] (The SOC is available to assist in up to 2 Minor changes each calendar month).	Unlimited Requests	Unlimited Requests

	SYMANTEC MSS SECURITY MANAGEMENT SERVICES				
Feature	**Essential Management Firewall or UTM[7]**	**Advanced Management Firewall or UTM[7]**	**Essential Management Endpoint Protection[7]**	**Advanced Management Endpoint Protection[7]**	**Advanced Management IDS or IPS**
Significant Changes (Includes software changes or high-risk policy changes that interrupt device functionality. Includes Endpoint patch and maintenance updates to Management Console and Endpoint Protection Database)	SOC will initiate change requests for software upgrades/patches and schedule with customer. Customer initiated change requests require 5 business days' advance notice.				
Major Changes (Includes changes that modify architecture, technology or that require advance design)	Not included in scope of Services (Available with purchase of Help Desk Service Tokens)				
Emergency Change or Assistance Requests	2 per calendar month[1]	5 per calendar month[1]	2 per calendar month[1]	5 per calendar month[1]	5 per calendar month[1]
Service Features					
Provide management and configuration assistance for the features listed[3]	• Firewalling • Network address translation (NAT) • Anti-virus • Intrusion Protection • Content Filtering • Configuration for High Availability[6] • Site-to-site VPNs	• Firewalling • Network address translation (NAT) • Anti-virus • Intrusion Protection • Content Filtering • Configuration for High Availability[6] • Site-to-site VPNs • Cluster Architectures • Remote Access VPN	• Database Configuration • Database Replication • Manager Administration • Anti-virus/Desktop or System Firewall /IPS /Application Control/ Device Control/Host Integrity policy change assistance	• Database Configuration • Database Replication • Manager Administration • Group/Location Administration • Installation Packages • Anti-virus/Desktop or System Firewall /IPS /Application Control/ Device Control/Host Integrity policy management	• Policy management • Signature update • In-line configuration support • Configuration for High Availability[6]
Rule / VPN limits (per Device):					
Maximum Rules in Firewall/UTM Policy	Unlimited Rules		N/A		N/A
Maximum VPN Policy (site-to-site VPNs)	Unlimited VPNs (restricted to connections to other SOC Managed Firewalls)	Unlimited VPNs (no connection restrictions)	N/A	N/A	N/A

Feature	SYMANTEC MSS SECURITY MANAGEMENT SERVICES				
	Essential Management Firewall or UTM[7]	**Advanced Management Firewall or UTM[7]**	**Essential Management Endpoint Protection[7]**	**Advanced Management Endpoint Protection[7]**	**Advanced Management IDS or IPS**
Incident / Fault Management:					
Monitor Managed Device for accessibility by SOC	X	X	X	X	X
Monitor Managed Device for detected fault messages[3]	X	X	X	X	X
Monitor for content update failure messages[3]	X	X	X	X	X
Respond to and troubleshoot Managed Device issues	X	X	For Manager/Management Console only. Troubleshooting issues affecting Endpoint agent software is not included in scope of service(s).[4]		X
Lifecycle Management - Maintenance Notification:					
Standard Maintenance	24 hours' notice		24 hours' notice		24 hours' notice
Emergency Maintenance	1 hour's notice		1 hour's notice		1 hour's notice
Reporting:					
Monthly Service Report	Available on the Portal		Available on the Portal		Available on the Portal
Visibility into current tickets, Device status, Log Outage alerts	Available on the Portal		Available on the Portal		Available on the Portal
Access to the Secure Internet Interface	X	X	X	X	X

[1] Additional available with purchase of Help Desk Service Tokens.
[2] For Endpoints, User Administration for the Management Console always performed by Symantec “ter.
[3] Subject to the technology support of features.
[4] For Symantec products, SOC will facilitate escalation to Symantec Product Support (Customer should work directly with product support as applicable for resolution).
[5] For Enterprise Wide Advanced Management IDS/IPS purchased prior to July 2, 2012, these same features and SLW's apply.
[6] Support of the HA feature refers explicitly to configuring that component on a Device for which the Management Service has been purchased. For avoidance of doubt, Customer must purchase the Management Service for each Device they require to be managed, regardless of whether or not the Device is configured as part of a high availability pair.
[7] No new customers may purchase these Services. These Services were placed in an end-of-sale status on September 3, 2013. Existing customers with an active subscription for these Services may purchase additional entitlements to support incremental expansion (co-termed to the last day of Customer's Term).

	SYMNANTEC MANAGED ENDPOINT DETECTION AND RESPONSE SERVICE[4]	
Features	**Add-on to SEP+ATP or SEP+SEDR**	**Add-on to MSS Advanced Security Monitoring Service**
Service Usage Model	MEDR Model	
Managed Endpoint Detection and Response Investigation ("**MEDR Investigation**")	• An incident triage investigation is initiated when suspicious activities are detected by MEDR to determine if the activity is a threat and if the severity of suspicious activity is correct. • Performed by MSS security analysts remotely connecting to Symantec's proprietary MEDR tool and investigating host traffic.[5] • Based on the nature and type of the suspicious activity, Such MEDR Investigation may include the following activities performed using the MEDR tool: ○ Investigate host forensic data (memory, disk and system), network traffic and logs ("**Customer Data**") ○ Correlate collected findings and indicators of compromise with the Symantec Global Intelligence Network ○ Other remote investigation as deemed necessary by Symantec ○ Perform automated threat hunting using Symantec's MEDR tool • Contain known malware on individual endpoints that are discovered as part of an alert created by MEDR ○ If using SEDR, for Symantec to perform containment, SEDR must be on premise or hybrid (on premise and in the cloud).	
Service Level Warranty		
	Limited to the following: • SOC Infrastructure Up-Time Percentage: **99.90%**	See the Offering Chart for the MSS Advanced Security Monitoring Service
Hosted Log Retention		
	Not included	See the Offering Chart for the MSS Advanced Security Monitoring Service
Security Incident Analysis		
	Limited to the following: • Validate, Assess and Prioritize impact of Incident to Enterprise	See the Offering Chart for the MSS Advanced Security Monitoring Service

[4] **Out of Scope**. Anything not specifically described in this Service Description is out of scope and is not included in the Service. Customer acknowledges, understands and agrees that Symantec does not guarantee or otherwise warrant that the Service, or Symantec's recommendations and plans made by Symantec as a result of that Service, will result in the identification, detection, containment, eradication of, or recovery from all of Customer's system threats, vulnerabilities, malware, malicious software, or other malicious threats. Customer agrees not to represent to anyone that Symantec has provided such a guarantee or warranty.

[5] **Offsite Investigation**. MEDR Investigation is performed remotely. Customer authorizes Symantec to perform any MEDR Investigation of Customer Data necessary for the Service. Accordingly, Customer acknowledges and agrees that Symantec gathers Customer Data from Customer's computer network using Symantec's MEDR tool, as well as ATP, SEDR and SEP (as applicable). Customer explicitly consents to Symantec collecting such Customer Data from Customer's computer network and Customer assumes all risk and liability in this regard and Symantec shall have no liability in this regard whatsoever.

	SYMNANTEC MANAGED ENDPOINT DETECTION AND RESPONSE SERVICE[4]	
Security Incident Escalation		
	Limited to the following: • Method of Notification of Security Incidents: Voice (as defined in the Operations Manual), Portal, Email (per Incident or Digest) • Method of Notification of Outage Incidents: Voice (as defined in the Operations Manual), Portal, Email (per Incident or Digest)	See the Offering Chart for the MSS Advanced Security Monitoring Service
General Service Features		
	Limited to the following: • Detection and response updated for emerging threats • Log/device unavailability alerting and notification	See the Offering Chart for the MSS Advanced Security Monitoring Service
Additional Service Terms and Conditions		
Implementation of MEDR Tool	Customer must work with Symantec to deploy and implement the MEDR tool* in the environment that will be part of the MEDR Service. * The MEDR tool must be installed on a server running Windows 7 through Windows server 2016. The MEDR tool includes, without limitation, Dissolvable Agent Server (DAS). DAS must be a supported version as specified in the SPL.	
Implementation of LCPs	Customer must work with Symantec to deploy and implement appropriate LCPs.	N/A
Remote Access	• Customer must provide remote access to (1) Customer's implementations of the MEDR tool, ATP, SEDR and SEP (as applicable) and (2) necessary administrative credentials to enable Symantec to perform the MEDR Service. • Customer acknowledges, understands and agrees that an unauthorized intrusion into hosts and network access points may be prohibited by applicable local law. Customer is: (i) explicitly confirming to Symantec that it has obtained all applicable consents and authority for Symantec to deliver the Service; and (ii) giving Symantec explicit permission to perform the Service and to access and process any and all Customer Data related to the Service, including without limitation, consent to analyze host forensics including but not limited to, memory, disk, logs, data, network traffic in real time to detect evidence of known malicious communication patterns and traffic containing unrecognized malicious code (malware), connect to Customer's computer network, archive and retain all host forensics data including but not limited to, memory, disk, logs, data, network traffic captured as part of Services (including to store any malware and metadata supplied by Customer, or anyone else working with or for Customer), and (iii) representing that such access and processing by Symantec does not violate any applicable law or any obligation Customer owes to a third party; and (iv) accepting sole responsibility and liability with respect to engagement of such Service. Accordingly, Customer warrants and represents that it is the owner or licensee of any network, systems, IP addresses software, appliances, code, templates, tools, policies,	

	SYMNANTEC MANAGED ENDPOINT DETECTION AND RESPONSE SERVICE[4]
	records, working papers, data and/or computers upon which Symantec performs the Service ("**Customer Systems**"), which may be visible as Customer Data through Symantec's MEDR tool, as well as ATP, SEDR and SEP (as applicable), and that Customer is authorized to instruct Symantec to perform the Service on such Customer Systems. Customer shall fully indemnify and hold harmless Symantec for any claims by any third parties with respect to the Service.
Customer Security Testing	• Customer must provide Symantec at least twelve (12) hours in advance of any scheduled security testing including but not limited to penetration testing, application testing, vulnerability assessments to prevent false alarms.
Reporting	• Customer acknowledges and agrees that in the course of delivering the Service, Symantec may become aware of issues such as data breaches, network intrusions, or the presence of malware, and that such issues may give rise to regulatory reporting obligations which Customer is subject to in one of more territories in which Customer operates. Accordingly, Customer shall remain solely responsible for all such reporting requirements and Symantec shall have no liability in this regard whatsoever.
Litigation Support Services	• The following services ("**Litigation Support Services**") are **explicitly excluded** from the MEDR Service: o Depositions, fact witness testimony, expert witness testimony, affidavits, declarations, expert reports; o Responding to discovery requests, subpoenas; o eDiscovery services; or o Other forms of litigation support or participation in any legal proceeding relating to the subject matter of the engagement (including those involving a governmental entity). • Although the parties acknowledge that the Service may be sought by Customer at the direction of Customer's legal counsel, it is neither Symantec's nor Customer's intention for Symantec to perform Litigation Support Services. If, however, Symantec is later compelled to perform any Litigation Support Services, Customer and Symantec agree the following would apply to those Litigation Support Services regardless of whether such Litigation Support Services are sought directly by Customer or by a third party, and notwithstanding any conflict with other terms: o The then-current hourly rate would apply for all Symantec personnel who perform Litigation Support Services. Litigation Support Services are provided on a time and materials basis, since the actual time required to complete Litigation Support Services may vary. o The parties will work in good faith to document the terms in this "*Litigation Support Services*" section as well as any additional necessary terms and conditions in a separate agreement at such time as the need for Litigation Support Services should occur. o *Indemnification*. Customer will fully indemnify and reimburse Symantec for all losses, damages, liabilities, expenses, costs, and fees (including reasonable attorney's fees) and for Symantec personnel time (at the hourly rate listed above for Litigation Support Services) incurred in connection with any allegation, claim, demand, subpoena, or legal proceeding (including those involving a governmental entity) arising from any incident for which Customer has engaged Symantec to provide the Service, regardless of fault. o This "*Litigation Support Services*" Section will survive termination or expiration of the Agreement.

ATTACHMENT 2

MANAGED NETWORK FORENSICS SERVICE

SERVICE FEATURES.

*Managed Network Forensics Investigation ("**MNF Investigation**")*

Symantec's MSS security analysts will initiate an incident forensic investigation when a suspicious activity is detected by MSS in an effort to determine if the activity is a threat. MNF Investigation is performed by MSS security analysts remotely connecting to Customer-owned Network Forensics Investigation Devices and investigating network traffic to aid Customer in determining if the severity of suspicious activity is correctly identified.

Based on the nature and type of the suspicious activity, Symantec will attempt to perform the MNF Investigation.

Such MNF Investigation may include the following activities:

- Monitoring hostile activity
- Investigating network packet capture data and network traffic logs ("**Customer Data**")
- Correlating collected findings and indicators of compromise with the Symantec Global Intelligence Network
- Other remote investigation as deemed necessary by Symantec

CUSTOMER RESPONSIBILITIES

Customer acknowledges and agrees that Symantec can only perform the applicable Service if Customer provides required information or performs required actions as set forth in the Agreement or as reasonably requested by Symantec. Accordingly, and without limitation, if Customer does not meet the following responsibilities, Symantec's performance of the applicable Service may be delayed, impaired or prevented, as noted below and further defined in the Managed Network Forensics Operations Manual:

- *Network Forensics Investigation Devices ("**NFID**"):*
  - The List of Symantec Approved NFIDs are found in the Supported Product List available on the MSS Portal (requires login).
  - NFIDs to be covered by the Service must be appropriately deployed and configured according to the standards defined by MSS security analysts.
  - NFIDs must be online and available for MNF Investigation for Symantec to perform the Service. Customer must maintain and keep the approved NFIDs properly running and functioning. Failure to do so does not constitute a failure to deliver the Service on Symantec's part.

- *Adequate Customer Personnel*: Customer must provide adequate personnel to assist Symantec in delivery of the Service, upon reasonable request by Symantec.

- *Reasonable Assistance*: Customer must provide reasonable assistance to Symantec, including, but not limited to, providing Symantec remote access to the managed device(s) and necessary administrative credentials to enable Symantec to perform the Service.

- *Accurate Information*: Customer must provide Symantec with accurate and up-to-date information, including, the name, email, landline, mobile, and pager numbers for all designated, authorized points of contact. Customer must provide the name, email, and phone numbers for all shipping, installation and security points of contact.

- *Customer's Outage*: Customer must provide Symantec at least twelve (12) hours in advance of any scheduled outage (maintenance), network, or system administration activity that would affect Symantec's ability to perform the Service.

- *Customer Security Testing:* Customer must provide Symantec at least twelve (12) hours in advance of any scheduled security testing including but not limited to penetration testing, application testing, vulnerability assessments to prevent false alarms.

- *Customer Software and Hardware*: It is Customer's sole responsibility to maintain current maintenance and technical support contracts with Customer's software and hardware vendors for any NFID(s) affected by the Service. It is Customer's responsibility to ensure that the NFID(s) are scoped and implemented in accordance with manufacturer's suggested standards. Customer is responsible for remediation and resolution of changes to NFID(s) which negatively impact the Service or the functionality, health, stability, or performance of NFID(s).

SERVICE-SPECIFIC TERMS SERVICE CONDITIONS

- *Out of Scope*. Anything not specifically described in this Service Description is out of scope and is not included in the Service. Customer acknowledges, understands and agrees that Symantec does not guarantee or otherwise warrant that the Service, or Symantec's recommendations and plans made by Symantec as a result of that Service, will result in the identification, detection, containment, eradication of, or recovery from all of Customer's system threats, vulnerabilities, malware, malicious software, or other malicious threats. Customer agrees not to represent to anyone that Symantec has provided such a guarantee or warranty.

- *Offsite Investigation*. MNF Investigation is performed remotely. Customer authorizes Symantec to perform any MNF Investigation of Customer Data necessary for the Service. Accordingly, Customer acknowledges and agrees that Symantec may be required to connect its computers and equipment to Customer's computer network. Customer explicitly consents to Symantec connecting its computers and equipment to Customer's computer network and Customer assumes all risk and liability in this regard and Symantec shall have no liability in this regard whatsoever.

- *Exclusions*. The following services ("**Litigation Support Services**") are explicitly excluded from the Services:
  - ✓ Depositions, fact witness testimony, expert witness testimony, affidavits, declarations, expert reports;
  - ✓ Responding to discovery requests, subpoenas;
  - ✓ eDiscovery services; or
  - ✓ Other forms of litigation support or participation in any legal proceeding relating to the subject matter of the engagement (including those involving a governmental entity).

  - *Litigation Support Services*. Although the parties acknowledge that the Service may be sought by Customer at the direction of Customer's legal counsel, it is neither Symantec's nor Customer's intention for Symantec to perform Litigation Support Services. If, however, Symantec is later compelled to perform any Litigation Support Services, Customer and Symantec agree the following would apply to those Litigation Support Services regardless of whether

such Litigation Support Services are sought directly by Customer or by a third party, and notwithstanding any conflict with other terms:

- The then-current hourly rate would apply for all Symantec personnel who perform Litigation Support Services. Litigation Support Services are provided on a time and materials basis, since the actual time required to complete Litigation Support Services may vary.
- The parties will work in good faith to document the terms in this "Litigation Support Services" section as well as any additional necessary terms and conditions in a separate agreement at such time as the need for Litigation Support Services should occur.
- *Indemnification*. Customer will fully indemnify and reimburse Symantec for all losses, damages, liabilities, expenses, costs, and fees (including reasonable attorney's fees) and for Symantec personnel time (at the hourly rate listed above for Litigation Support Services) incurred in connection with any allegation, claim, demand, subpoena, or legal proceeding (including those involving a governmental entity) arising from any incident for which Customer has engaged Symantec to provide the Service, regardless of fault.
- This "Litigation Support Services" Section will survive termination or expiration of the Agreement.

- *Reporting*. Customer acknowledges and agrees that in the course of delivering the Service, Symantec may become aware of issues such as data breaches, network intrusions, or the presence of malware, and that such issues may give rise to regulatory reporting obligations which Customer is subject to in one of more territories in which Customer operates. Accordingly, Customer shall remain solely responsible for all such reporting requirements and Symantec shall have no liability in this regard whatsoever.

- *Personnel*. Symantec reserves the right to assign any suitable skilled resource(s) available to provide Services. Symantec is not obligated to provide a specific Symantec resource or third-party resource.

- *Access Rights*. Customer will ensure that Symantec has access to all NFIDs necessary to complete the Service at all times. Where applicable, such access shall include appropriate user accounts to perform remote investigation of Customer Data collected by NFIDs. Customer acknowledges, understands and agrees that an unauthorized intrusion into network access points may be prohibited by applicable local law. By agreeing to this Agreement, Customer is: (i) explicitly confirming to Symantec that it has obtained all applicable consents and authority for Symantec to deliver the Service; and (ii) giving Symantec explicit permission to perform the Service and to access and process any and all Customer Data related to the Service, including without limitation, consent to analyze network traffic in real time to detect evidence of known malicious communication patterns and traffic containing unrecognized malicious code (malware), connect to Customer's computer network, archive and retain all network traffic captured as part of Services (including to store any malware and metadata supplied by Customer, or anyone else working with or for Customer), and (iii) representing that such access and processing by Symantec does not violate any applicable law or any obligation Customer owes to a third party; and (iv) accepting sole responsibility and liability with respect to engagement of such Service. Accordingly, Customer warrants and represents that it is the owner or licensee of any network, systems, IP addresses software, appliances, code, templates, tools, policies, records, working papers, data and/or computers upon which Symantec performs the Service ("**Customer Systems**"), which may be visible through MNFIDs as Customer Data, and that Customer is authorized to instruct Symantec to perform the Service on such Customer Systems. Customer shall fully indemnify and hold harmless Symantec for any claims by any third parties with respect to the Service.

- *Service Limitation*. Applicable law or regulation(s) of the country in which the Service, including without limitation MNF Investigation, will be performed may limit or alter the scope of the Service.