SYMANTEC MANAGED SECURITY SERVICES
MSS SERVICE ATTRIBUTES

Revision Date: January 1, 2015

THIS MANAGED SECURITY SERVICES ATTRIBUTES DOCUMENT ("MSS Service Attributes") is made a part of and wholly incorporated into the Agreement, as defined in the Symantec order confirmation certificate referencing these MSS Service Attributes ("**Certificate**"), and apply to the Symantec Managed Security Services (individually a "**Service**" or collectively "**Service(s)**") set forth on the initial page(s) of such Certificate. As used herein, the term "**Symantec**" means Symantec Corporation and/or its subsidiaries and "**Customer**" means the customer identified on the initial page(s) of the Certificate, each a "**Party**" and together, the "Parties." Any capitalized terms not defined herein shall have the same meaning as in the Certificate or in the Managed Security Services Operation Manual ("**Ops Manual**").

For those Service(s) purchased prior to July 12, 2011, in addition to the terms contained herein, Customer acknowledges and agrees to continue compliance with sub-sections 3, 6, 7, 8, 9, 12, and 13 of Section 1 of the Managed Security Services Attributes dated May 27, 2010 (20100527) ("MSSA"). A copy of the MSSA is available at www.symantec.com/docs/TECH131855 or upon request from Symantec by emailing DL-MSS-BusinessOperations@symantec.com.

This MSS Service Attributes document is made up of the following sections:

- **Section 1**: Managed Security Services - General Terms and Conditions;
- **Section 2**: Managed Security Services - Service Descriptions;
- **Section 3**: Managed Security Services - Service Level Warranties; and
- **Section 4:** Managed Security Services - Service(s) Offerings Chart.

SECTION 1
MANAGED SECURITY SERVICES
GENERAL TERMS AND CONDITIONS

The Parties acknowledge and agree that the following terms and conditions apply to the Service(s):

1. **Service(s) Use Model:** Use of the Service(s) is subject to the limitations set forth below, as applicable to the Service(s) identified on the face of the Certificate:

1.1 **Enterprise Wide Model.**

a) **End User(s); Nodes.** For Service(s) identified on the initial page(s) of the Certificate 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 in Section 1.1(c) below and each such Device conforming to the version requirements stated in the Symantec Supported Product List ("SPL") available on the SII. 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, Essential, or Advanced), Customer shall receive the highest supported level of Service indicated on the SPL, not to exceed the level purchased.

b) **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 the Customer outsourced services.

c) **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.

1.2 **Per Unit Model:** For Service(s) not identified on the initial page(s) of the Certificate 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 on the initial page(s) of the Certificate.

2. **Customer Obligations / Responsibilities:** Customer acknowledges and agrees that Symantec's ability to perform the Service(s) during the Term may be subject to Customer meeting all of its obligations and Customer responsibilities as described in the Agreement during the Term. Customer acknowledges and agrees that Symantec will have no liability whatsoever for any failure to perform the Services(s) if such failure arises out of Customer's act or omission inconsistent with Customer's obligations described in the Agreement which impede Symantec's ability to perform the Service(s). Without prejudice to the foregoing, any such failure to perform the Service(s) by Symantec due to the foregoing shall not postpone or delay the Term nor be deemed a breach of the Agreement.

2.1 The following list of Customer responsibilities is the minimum required to ensure Symantec's ability to perform the Service(s). At a minimum, Customer is responsible for the following:

2.1.1 Providing 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 Service(s) Offerings Chart referenced in Section 4 of these MSS Service Attributes ("**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).

2.1.2 For monitoring Service(s) (as further described in the Service(s) Offerings Chart referenced in Section 4 of these MSS Service Attributes ("**Monitoring Service(s)**"), 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 Device(s) log data and transport such log data back to the SOC. 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 Ops 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 Device(s) log data 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 Device(s) configuration, as described by SOC personnel, to conform with the supported format.

2.1.3 For Management Service(s), providing a permanent, dedicated analog telephone line to support the Out-of-Band Management Solution (as defined in Section 2D of these MSS Services Attributes) if Symantec provides an Out-of-Band Management Solution to Customer. Customer is responsible for maintaining the functionality of this dedicated line. Details on the Out-of-Band Management Solution are contained in the Services Description section of this MSS Service Attributes and in the Ops Manual.

2.1.4 Providing 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 SII.

2.1.5 Providing the name, email, landline, mobile, and pager numbers for all shipping, installation and security points of contact.

2.1.6 Notifying Symantec at least twelve (12) hours in advance of any scheduled maintenance, network, or system administration activity that would affect Symantec's ability to perform the Service(s).

2.1.7 Reviewing the Daily Service Summary (as defined in the Ops Manual) to understand the current status of Service(s) delivered and actively work with the SOC to resolve any tickets requiring Customer input or action.

2.1.8 Sole responsibility for maintaining current maintenance and technical support contracts with Customer's software and hardware vendors for any Device(s) affected by Service(s).

2.1.9 Ensuring any Device(s) receiving Service(s) conform to the version requirements stated in the SPL.

2.1.10 Intentionally Omitted.

2.1.11 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 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.

2.1.12 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 will charge additional fees (Help Desk Tokens) in the event that Customer requires Symantec's assistance for remediation or resolution activities.

3. Intentionally Omitted.

4. **LCP License and Use Rights.** As part of certain Service(s), Symantec will provide to Customer certain software, in object code form, including any Documentation (as defined below), which will function as an LCP ("Licensed Software"). Upon installation on Customer's network, the Licensed Software will extract Device(s) logs and transport the data back to the SOC. Customer acknowledges and agrees to the terms contained in this clause 4 will control the use of the Licensed Software, and, unless otherwise stated below, will supersede the software license agreement displayed upon Licensed Software installation ("LCP EULA").

4.1 During the Term, Symantec grants to Customer a non-exclusive, non-transferable right to use the functionality of the Licensed Software that collects and/or stores logs from a log source and forwards those logs to Symantec for retention and/or security analysis ("Log Collection Functionality"), and the right to make a single uninstalled copy of the Licensed Software for archival purposes which Customer may use and install for disaster-recovery purposes (i.e. where the primary installation of the Licensed Software becomes unavailable for use). For the sake of clarity, Customer is not authorized to use any functionality of the Licensed Software other than the Log Collection Functionality.

4.2 Customer may not, without Symantec's prior written consent, conduct, cause or permit the: (i) use, copying, modification, rental, lease, sublease, sublicense, or transfer of the Licensed Software; (ii) creation of any derivative works based on the Licensed Software; (iii) reverse engineering, disassembly, or decompiling of the Licensed Software; (iv) use of the Licensed Software in connection with any service bureau, facility management, timeshare, service provider or like activity whereby Customer operates or uses the Licensed Software for the benefit of a third party; (v) use of the Licensed Software by any party other than Customer or its authorized agents in association with the Service(s); or (vi) use of a later version of the Licensed Software other than the version provided by Symantec unless Customer has separately acquired the right to use such later version through a separate license agreement.

4.3 The Licensed Software is the proprietary property of Symantec or its licensors and is protected by copyright law. Symantec and its licensors retain any and all rights, title and interest in and to the Licensed Software, including in all copies, improvements, enhancements, modifications and derivative works of the Licensed Software. Customer's rights to use the Licensed Software shall be limited to those expressly granted in this clause 4. All rights not expressly granted to Customer are retained by Symantec and/or its licensors.

4.4 Customer must use the Licensed Software with a dedicated physical or virtual system that meets the minimum system requirements for running the Licensed Software ("Dedicated System"), as indicated in the user documentation Symantec provides with the Licensed Software ("Documentation"). The Dedicated System must solely be dedicated to running only the Licensed Software. Customer may only use the Dedicated System with third party software that is expressly specified in the Documentation and provided by Symantec for Customer's use with the Licensed

Software and/or Dedicated System. Otherwise, Customer may not install and use any third party software with the Licensed Software or Dedicated System.

4.5 Upon installation of the Licensed Software on the Dedicated System, Customer must provide the administrative credentials to the SOC personnel to manage the Licensed Software on Customer's behalf.

4.6 Customer may make and use copies of the Licensed Software as authorized by Symantec solely for use with the Service(s).

4.7 Any updates to the Licensed Software that are generally made available to customers receiving Service(s) will be provided to Customer, which may include updates automatically uploaded to the Licensed Software at Symantec's discretion.

4.8 The Licensed Software may contain third party software programs ("Third Party Programs") that are available under open source or free software licenses. Nothing in the Agreement will alter any rights or obligations Customer may have under those open source or free software licenses. Notwithstanding anything to the contrary contained in such licenses, the disclaimer of warranties and the limitation of liability provisions in the Agreement shall apply to such Third Party Programs. Specifically, the Licensed Software includes Red Hat Enterprise Linux 6, which is provided by Red Hat, Inc. Customer's use of the Red Hat Enterprise Linux 6 component, including updates thereto, is subject to the terms of the Red Hat, Inc. "END USER LICENSE AGREEMENT RED HAT® ENTERPRISE LINUX® AND RED HAT® APPLICATIONS", contained in the LCP EULA.

4.9 Customer acknowledges that the Licensed Software and related technical data and services (collectively "Controlled Technology") are subject to the import and export laws of the United States, specifically the U.S. Export Administration Regulations (EAR), and the laws of any country where Controlled Technology is imported or re-exported. Customer agrees to comply with all relevant laws and will not export any Controlled Technology in contravention to U.S. law nor to any prohibited country, entity, or person for which an export license or other governmental approval is required. All Symantec products, including the Controlled Technology are prohibited for export or re-export to Cuba, North Korea, Iran, Syria and Sudan and to any country subject to relevant trade sanctions. Customer hereby agrees that Customer will not export or sell any Controlled Technology for use in connection with chemical, biological, or nuclear weapons, or missiles, drones or space launch vehicles capable of delivering such weapons.

4.10 The license rights granted to Customer to the Licensed Software will terminate upon the earlier of Customer's breach of any term contained herein 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 Licensed Software.

4.11 NOTWITHSTANDING ANYTHING CONTAINED IN THE LCP EULA, THOSE WARRANTIES AND DISCLAIMER OF DAMAGES AGREED UPON BY THE PARTIES FOR THE SERVICE(S) IN THE AGREEMENT WILL GOVERN AND CONTROL THE USE OF THE LICENSED SOFTWARE.

SECTION 2
MANAGED SECURITY SERVICES
SERVICES DESCRIPTIONS

A. **SERVICE FEATURES.** The Managed Security Service(s) Offerings Chart, contained in Section 4 of these MSS Service Attributes (“**Service(s) 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):

1. **Secure Internet Interface.** Each of the Service(s) includes access to and use of the web portal (“**Secure Internet Interface**” or “**SII**”), which is made available to Customer for use during the Term. References to the “**MSS Customer Portal**” in the Ops Manual shall be deemed to refer to the Secure Internet Interface.

2. **Managed Security Services Operations Manual.** The Ops Manual, which is available on the SII, 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 SII of any material change to the Ops Manual.

3. **Security Operations Centers.** All Service(s) are performed remotely from Security Operations Centers (“**SOC(s)**”).

4. **Scheduled Maintenance Outages**. Symantec will, from time to time, schedule regular maintenance on the SOC Infrastructure or on Device(s) receiving Management Service(s), requiring a maintenance outage. The protocol for any such maintenance outage is described in the Ops Manual.

B. **TECHNICAL SERVICE COORDINATOR**. Customer may optionally purchase the services of a Technical Service 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. Common tasks that a TSC can perform are identified in the Ops Manual.

C. **HOSTED MANAGEMENT CONSOLES.** Customer may purchase the use of Hosted Management Consoles (as described in the Ops Manual) 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.

D. **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.

E. ADDITIONAL / OUT OF SCOPE SERVICE(S); HELP DESK TOKENS.

1. Additional Service(s), features, or options described in the Service(s) Offerings Chart may be ordered through the submission of a purchase order.

2. Hour-long telephone technical support sessions (each, a "**Help Desk Token**") provided from the SOC Help Desk are available for purchase by Customer by submitting a purchase order. A Help Desk Token may only be used for services that fall outside of the scope of Service(s) ordered. The scope of such support is further described in the Ops Manual. Help Desk Tokens are only valid for one (1) year from the date of order acceptance by Symantec.

SECTION 3
MANAGED SECURITY SERVICES
SERVICE LEVEL WARRANTIES

A. SERVICE LEVEL WARRANTIES & SERVICE CREDITS.

The SLWs listed below will apply to those Service(s) listed in the Service(s) Offerings Chart (as further described in Section 4 of these MSS Service Attributes). The Service(s) 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 ("**Service Credit(s)**").

1. **Device Registration Warranty**.

   a. The Customer Responsibilities set forth in Section 1, clause 2.1.1, 2.1.2, and 2.1.9 must be met for Device(s) prior to Device Registration ("**Registration Requirements**").

   b. Symantec will register each Device(s) upon the later occurrence of the following: (i) fifteen (15) business days after completion of the Registration Requirements, (ii) upon the Start Date identified on the initial page(s) of the Certificate, or (iii) 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).

   c. 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:

      i) for Enterprise Wide Service(s), one (1) Service Credit for each day the deadline is missed;

      ii) 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

      iii) for all other Per Unit Service(s), one (1) Service Credit for each day the deadline is missed for each Device.

2. **Severe Event Notification Warranty**. For Essential and Advanced Monitoring Service(s), (as further described in the Service(s) Offerings Chart referenced in Section 4 of these MSS Service Attributes), Symantec will initiate contact to notify Customer of Emergency and Critical Events (as defined in the Ops Manual) within the specified Severe Event Notification Time identified in the Service(s) Offerings Chart, once the determination that an Emergency and Critical Event has occurred (as specified in the Ops 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 Event is deemed to be a Runaway Device, as defined in the Ops Manual.

3. **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 Service(s) Offerings Chart, of each calendar month during the Term (excluding Scheduled Outages, Maintenance, Hardware/Software Failures, Failures, as such terms are defined in the Ops Manual, resulting from changes made by the Customer, and circumstances beyond SOC control). 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).

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

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

6. **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 Service(s) Offerings Chart. If Symantec does not meet this SLW, and the Customer has not exceeded their contracted Emergency Change or Assistance Requests for the month as specified in Service(s) Offerings Chart, Symantec will credit Client's account with one (1) Service Credit.

7. **SOC Infrastructure Up-Time Warranty**. Symantec warrants that the SOC data storage, SOC log analysis processing, any Hosted Management Consoles (as described in the Ops Manual), the SII, and SOC customer communication methods (phone, email, SII) (together, the "**SOC Infrastructure**") shall be available in accordance with the SOC Infrastructure Up-time Percentage identified in the Service(s) Offerings Chart, for each calendar month during the Term (excluding scheduled maintenance). 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.

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

B. SERVICE CREDITS; LIMITATION OF SERVICE CREDIT LIABILILTY.

1. **Service Credits.** The process for requesting a Service Credit for an SLW failure is set forth in the Ops 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:

   a. For Enterprise Wide Service(s): A Service Credit shall be calculated as 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).

   b. 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 Help Desk Tokens and any one-time fees).

   c. 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.

2. **Limitation of Service Credit Obligation.** Notwithstanding anything to the contrary in the Agreement, 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 the Agreement will be limited to the issuance of Service Credit(s).

SECTION 4
MANAGED SECURITY SERVICES
SERVICE(S) OFFERINGS CHARTS

Feature	**SYMANTEC MSS SECURITY MONITORING SERVICES**		
	Log Retention Service	**Essential Security Monitoring Service[6]**	**Advanced Security Monitoring Service**
Service Use Model[5]	Per Unit or Enterprise Wide	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	10 minutes
SOC Infrastructure Up-Time Percentage	99.90%	99.90%	99.90%
Monthly Reporting Time	by 5th business day	by 5th business day	by 5th business day
Hosted Log Retention (duration @ SOC during Services Term only):			
Online Raw Log Retention	3 months (92 days)[3]	3 months (92 days)[3]	3 months (92 days)[3]
Additional 1 year Online Raw Log Retention	optional, 12 month increments	optional, 12 month increments	optional, 12 month increments
Offline (removeable media) Raw Log Retention[4]	12 months	12 months	12 months
Online Incident Data Retention	Service Term	Service Term	Service Term
Security Incident Analysis			
Log/Alert data collection, aggregation, and normalization	X	X	X
Logs available for SOC Analyst inspection	X[1]	X	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 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	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[7] (automatic correlation of networking and endpoint events with Symantec GIN to assist in detection of malicious activity)	N/A	N/A	X
Vulnerability Data Correlation Integration	N/A	X	X
Validate, Assess and Prioritize impact of Incident to Enterprise	X	X	X

Feature	SYMANTEC MSS SECURITY MONITORING SERVICES		
	Log Retention Service	**Essential Security Monitoring Service[6]**	**Advanced Security Monitoring Service**
Incident Escalation			
Method of Notification of Security Incidents:			
Voice (as defined in the Manual), SII, Email (per Incident or Digest)	N/A	X	X
Method of Notification of Outage Incidents[2]:			
Voice (as defined in the Manual), SII, Email (per Incident or Digest)	N/A	X	X
General Service Features			
Detection and response updated for emerging threats	N/A	X	X
Daily Service Summary delivered by e-mail	N/A	X	X
Log/device unavailability alerting and notification[2]	X	X	X
Online logs may be queried by customer via the SII	X	X	X
Compliance reporting available on the SII	X	X	X
Access to the Secure Internet Interface	X	X	X

[1] Log Retention alone performs no security analysis. However, the retained log data is automatically associated with security incidents generated by other devices under Essential or Advanced Security Monitoring service(s) and is available for SOC analyst inspection.

[2] 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.

[3] Subject to run away device limits per the Manual.

[4] Restoral fees apply - customer must purchase Help Desk Tokens commensurate with level of effort for data restoration.

[5] 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.

[6] As of January 1, 2015, the following MSS Essential Security Monitoring Service offerings will be delivered at the corresponding Advanced Security Monitoring Service level: Essential Security Monitoring Service Endpoint Block, Essential Security Monitoring Service Firewall or Unified Threat Management, Essential Security Monitoring Service Host Intrusion Detection System or Intrusion Protection System, Essential Security Monitoring Service Network Intrusion Detection System or Intrusion Protection System or Behavioral Analysis Device, Essential Security Monitoring Service Web Proxy or Advanced Persistent Threat.
Essential Security Monitoring Service Applications or Operating Systems, Essential Security Monitoring Service Router or Switch or Virtual Private Network Concentrator and Essential Security Monitoring Service Web Application Firewall will remain at the Essential Security Monitoring Service level.

[7] Refer to SPL to determine which technologies are required for Advanced Threat Protection – Detect.

	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 SII 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 SII 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
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					

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**
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
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 SII		Available on the SII		Available on the SII
Visibility into current tickets, Device status, Log Outage alerts	Available on the SII		Available on the SII		Available on the SII
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 MSS.

[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 after September 3, 2013 (end of sale). Existing customers with an active subscription for these Services may purchase additional entitlements to support incremental expansion (co-termed to the End Date of Customer's term of Service).