Symantec™ Incident Response Retainer Services

Service Description

November 2019

SERVICE OVERVIEW

This Service Description, with any attachments included by reference, is part of any agreement which incorporates this Service Description by reference (collectively, the "Agreement"), for the Services described in this Service Description and are provided by Symantec, now a part of Broadcom, Inc. This Service Description shall apply to Services purchased by Customer on or after October 5, 2015. For Services purchased by Customer prior to October 5, 2015, the Service Description dated April 6, 2015 or June 3, 2015 shall apply based on Customer's purchase date, a copy of which is available at http://go.symantec.com/proserveterms or upon request to Symantec.

Symantec™ Incident Response Retainer Services allow Customer to maintain access to critical capabilities needed to effectively respond to one or more security incidents. Symantec™ Incident Response Retainer Services comprise one or more of the following services (each a "**Service**" or collectively, "**Services**"), depending on the offering purchased by Customer as indicated in the Subscription Instrument and as further described in this Service Description:

1. **Retainer Services*:** *Standard*, *Enterprise* and *Advanced Enterprise* retainer bundles comprise our recommended number of pre-purchased Service Days and SLA options, and are available for a term of either **12**, **24**, or **36** months (each a "**Retainer Service**").
2. **Custom Retainer Options*:** Customized retainers that include either a **24-hour** or **48-hour** SLA and a number of Service Days in a combination not provided by one of the Retainer Services ("**Custom Retainer Options**"). Custom Retainer Options may be purchased individually as an individual service option or to augment Customer's existing Retainer Service. Custom Retainer Options may be purchased for a term of either **12**, **24** or **36** months. **IN THE EVENT A CUSTOM RETAINER OPTION IS PURCHASED TO AUGMENT CUSTOMER'S EXISTING RETAINER SERVICE, THE CUSTOM RETAINER OPTION SHALL CO-TERMINATE WITH SUCH RETAINER SERVICE**.
3. **Additional Service Days and Responders***: Customers of a Retainer Service or Custom Retainer Option may pre-purchase additional Services Days in advance and/or purchase Additional Responder(s) as needed during an Incident Investigation.

* All Services **must** be delivered by Symantec within the **Region(s)** for which fees have been paid as set forth in the Subscription Instrument.

TABLE OF CONTENTS

TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES

SERVICE FEATURES. The following table illustrates the Service features associated with incident response retainer services.

SERVICE FEATURE	SERVICE FEATURE DESCRIPTION
SERVICE MANAGEMENT	Customer will be assigned a Symantec Service Manager based on Customer's market segment or location, and Customer security maturity.
24x7 PHONE AND EMAIL ACCESS	Customer will have access to a 24x7 phone number to contact Symantec's Incident Response delivery team to request incident response assistance ("**Incident Response Assistance Call**"). Customer may also contact the Incident Response delivery team 24x7 by email.
CALL-BACK SLA	Symantec's Incident Response delivery team will return Customer's Incident Response Assistance Call within 3 hours following receipt of such call by Symantec. In the event Customer's Incident Response Assistance Call is not returned within the applicable timeframe, Symantec agrees to credit Customer's account with 1 Service Credit.
EMERGING THREAT REPORTS	Symantec will periodically provide Customer with Emerging Threat Reports published by Symantec via email on emerging threats that may impact Customer's security posture. Emerging Threat Reports may contain the following: (i) Executive Summary; (ii) Technical Threat Details; (iii) Attack Vector; (iv) Detection Capabilities and Indicators; (v) Mitigation Strategy and Recommendations; and/or (vi) References to additional resources.
REMOTE SLA	Symantec will commence remote service within 12 Normal Business Hours following Symantec Receipt (as defined in **Remote Service** below). In the event Symantec does not commence a Remote Assessment within the applicable timeframe, Symantec agrees to credit Customer's account with 1 Service Credit for each Normal Work Day of delay.
INCIDENT INVESTIGATION	Details of what Symantec may perform during an Incident Investigation are provided below under "**INCIDENT INVESTIGATION**". An Incident Investigation shall be performed at Customer's location, which must be within the Region(s) for which fees have been paid as set forth in the Subscription Instrument.
SERVICE DAYS	▪ **Standard** includes **10**, **20** or **30** Service Days for a 12, 24 or 36 month Term respectively. ▪ **Enterprise** includes **30**, **60** or **90** Service Days for a 12, 24 or 36 month Term respectively. ▪ **Advanced Enterprise** includes **60**, **120** or **180** Service Days for a 12, 24 or 36 month Term respectively. ▪ **Custom Retainer Options** includes additional quantities of **5**, **10** or **15** Service Days for a **12**, **24** or **36** month Term respectively.

SERVICE FEATURE	RETAINER SERVICES			Custom Retainer Options*	SERVICE FEATURE DESCRIPTION
	STANDARD	ENTERPRISE	ADVANCED ENTERPRISE		
FLY TO SITE SLA	Priority Scheduling	48 Hours	24 Hours	48 or 24 Hours (as purchased by Customer)	An Incident Investigation responder(s) will be "in transit" to Customer's location for an Incident Investigation within the applicable timeframe following Incident Investigation Registration. The term "in transit" means the Incident Investigation responder(s) will have commenced travel to Customer's location, which **must** be within the **Region(s)** for which fees have been paid as set forth in the Subscription Instrument. In the event that the Incident Investigation responder(s) is not "in transit" within the applicable timeframe, Symantec agrees to credit Customer's account with 1 Service Credit for each Normal Work Day of delay. With respect to "**Priority Scheduling**", Symantec will use reasonable efforts only to have an Incident Investigation responder(s) 'in transit' promptly following Incident Investigation Registration.

*In the event a Custom Retainer Option is purchased to augment Customer's existing Retainer Service, the Custom Retainer Option shall co-terminate with such Retainer Service.

In addition to a Retainer Service or a Custom Retainer Option, Customer may purchase the following:

SERVICE FEATURE	SERVICE FEATURE DESCRIPTION
ADDITIONAL SERVICE DAYS	If Customer desires to increase Service Days included in Customer's Retainer Service or Custom Retainer Option (as applicable), Customer may pre-purchase additional Service Days prior to a security incident occurring in increments of **5**, **30** or **60** Service Days. Customer's location must be within the Region(s) for which fees have been paid as set forth in the Subscription Instrument. Pre-purchased additional Service Days will co-terminate with the Term of Customer's Retainer Service or Custom Retainer Option (as applicable).
ADDITIONAL RESPONDERS	If Symantec determines that additional Incident Investigation responder(s) ("**Additional Responder(s)**") are recommended during an Incident Investigation, Customer may choose to purchase such Additional Responder(s). A purchase of 1 Additional Responder entitles Customer to 1 Additional Responder for the Incident Investigation during **5** Service Days and will be reflected in a Work Authorization Form. **Any Additional Responder(s) must be used and delivered within 30 days following the purchase date.**

INCIDENT INVESTIGATION

Requesting Incident Investigation. Customer shall contact Symantec to request an Incident Investigation. Based on the nature and type of security incident, Symantec and Customer will mutually agree on an appropriate number and type of responders and Service Days required. Symantec will then provide Customer with a corresponding Work Authorization Form or "WAF" describing these decisions, and Customer must sign and return the WAF to Symantec ("**Incident Investigation Registration**"). Incident Investigation Registration is the date of receipt by Symantec of the signed WAF. Following Incident Investigation Registration, Symantec will commence travel to Customer's location and/or coordinate remote efforts to conduct an Incident Investigation in accordance with the Service Level Agreement (*where applicable*). Further details of what Symantec may perform during an Incident Investigation are provided below.

Customer acknowledges and agrees that an on-site Incident Investigation involving travel will require at least 3 Service Days. If Customer determines more time is needed than originally requested, Customer may request additional Service Days. Following Customer's request, Symantec will then provide Customer with a corresponding WAF, which Customer must sign and return to

Symantec. For the avoidance of doubt, where applicable additional Service Days requested by Customer will first be deducted from Customer's available Service Days; or if Customer has no Service Days available, Customer may purchase the additional Service Days required by Customer.

Incident Investigation Features. Subject always to the nature of Customer's security incident, logistics with respect to Symantec's delivery of the Services, and the number of Service Days available and requested by Customer, Symantec may perform certain of the activities described below, as coordinated with Customer's Project Manager, solely to the extent Symantec can reasonably complete such activities based on the Service Days requested by Customer:

Information Gathering and Project Coordination:

- Working with Customer to identify required Customer Incident response team resources including, without limitation, a Customer Project Manager.
- Reviewing Customer's networking diagrams to determine the design of the existing network infrastructure.
- Conducting onsite interviews with Customer's representatives and designated Customer personnel responsible for:
  - Managing servers, clients, and remote systems to determine connectivity and management processes;
  - Internet gateway security to determine availability of solutions to provide information security protection, monitoring and mitigation;
  - Email security to determine availability of solutions to provide information security protection, monitoring and mitigation managing the endpoint security solutions to identify monitoring capabilities.
- Establishing procedures for documentation of actions taken and the handling of findings.
- Scheduling the necessary resources and establishing meeting cadence in coordination with Customer's Project Manager.

Detection, Data Collection and Analysis:

Conducting an assessment of Customer's compromised information systems assets which may include the following tasks:

- Monitor hostile activity.
- Network packet capture and analysis.
- Log collection & analysis.
- Live system artifact collection.
- Physical system memory analysis.
- Disk analysis.
- Malware sample collection
- Advanced Malware Analysis (Reverse Engineering Services)
- Cross-reference collected findings and indicators of compromise with Symantec analysts and with the Symantec Global Intelligence Network (GIN) to potentially identify links to campaigns and adversaries.
- Identify data extraction techniques.
- Other analysis as deemed necessary by Symantec.

Malware Outbreak:

Depending on the Symantec technologies deployed by Customer, Symantec may also provide the following:

- Analyze and correlate indicators of compromise within and between the following products: Symantec Endpoint Protection Manager, Symantec Data Loss Prevention, Symantec Critical Systems Protection, and Symantec Management Platform.
- Review log data from anti-malware defense capabilities to determine current threat information leading to recommendations to Customer for containment and eradication.
- Review policy and configuration within the Symantec Endpoint Protection Manager:
  - Antivirus and Antispyware configuration options.
  - Virus event detection, scanning, remediation, and mitigation settings.
  - Advanced Threat Detection Configuration.
  - Application & Device Control.
  - Network Threat Protection firewall.
  - Intrusion protection system (IPS) configuration options – Network and Browser.

  - Network Access Control host integrity checks and remediation actions configuration options.
  - Network Access Control integration configuration of network devices and network services with enforcement components (if applicable).
  - Client Content Update (Live Update) Settings.
- Other analysis as deemed necessary by Symantec.

Containment:

Review and analyze compromised information systems assets and provide a written analysis of the threat and short-term containment plan recommendations to assist with the following:

- Monitor and/or stop hostile activity.
- Isolate affected resources.
- Guide Customer through execution of the recommended containment plan.

Eradication and Recovery:

Review and analyze compromised information systems assets and provide a written strategy and recommendations for threat eradication and recovery.

Remote Services:

Symantec may perform certain remote services during an Incident Investigation ("**Remote Service**") on Customer data, including, without limitation, hardware, software, images, memory, network, logs ("**Customer Data**"). Customer acknowledges and agrees that any such Remote Service performed by Symantec shall be subject to the following: (a) Remote Service of Customer Data shall be scheduled by Customer via the Incident Response delivery team; (b) Customer shall, at its sole cost and expense, be solely responsible for the delivery of Customer Data (on a medium to be mutually agreed with Symantec) to Symantec and the return of such Customer Data to Customer following conclusion of Remote Service; (c) Customer Data shall be delivered to Symantec at a location mutually agreed between Customer and the Incident Response delivery team, in a tamper-evident container (where applicable). Where applicable, Customer shall provide Symantec with the applicable delivery tracking number and shall ensure that Symantec's physical acknowledgement of receipt is required upon delivery. For the purposes of a Remote Services, "**Symantec Receipt**" shall be the date of receipt of Customer Data by Symantec; (d) all Remote Services performed by Symantec shall be during Normal Business Hours only; (e) Symantec shall have no responsibility whatsoever with respect to Customer Data, including, without limitation, to any Customer Data that may remain within any Customer hardware (whether accessible, readable or not).

Advanced Malware Analysis and Reverse Engineering:

Reverse Malware Analysis is a specialized type of Remote Service. Advanced analysis of malware submitted by Customer may include both static and dynamic malware analysis techniques. Static analysis may include the dissection of the different resources of the submitted file or files and studying each component. The file or files can also be disassembled (reverse engineered) using a disassembler to gain an understanding of what the program is supposed to perform. Dynamic Malware Analysis may also be performed whereby Symantec observes the behavior of the malware while running on an emulated host using either virtual machines and/or sandbox environments to observe the behavior of the malware step by step while its instructions are being processed by the CPU and the live effects on file system and memory. Malware analysis concludes with a written report detailing the attributes and behaviors of the submitted malware sample or samples and potential impacts to Customer's environment and recommended defensive actions to remediate current infections and to protect against further infection or propagation.

Written Report and Presentation:

Upon completion of this engagement Symantec will deliver a set of documents containing the following types of components:

- **Executive Summary**
  - Background
  - Initial findings
  - Initial Attack Narrative
  - Scope of Compromise

- Malicious Code
- Involved High Profile Systems
- Containment Strategy
- Summary of Recommendations

- **Conclusions**
- **Detailed Findings**
  - Technical Findings
  - Attack Timeline
  - Attack Taxonomy
  - Identified Vectors
  - Analysis of Identified Threats
- **Recommendations**
  - Incident Specific Remediation/Mitigation steps
  - General Recommendations
- **List of tools used in Analysis**
- **Lists of Systems Analyzed**

Upon request, Symantec may also provide a presentation summarizing the contents of the written report outlined above, intended to be adaptable for Customer's use in briefing Customer's board of directors or senior executive staff.

READINESS SERVICES

Customers who purchase 10 or more Service Days may, during the applicable Term, exchange 5 or more included Service Days allocated to that annual period for any of the Readiness Services set forth below.

Delivery of a Readiness Service is subject to Symantec resource availability. Readiness Services must be scheduled by Customer via the Symantec's Incident Response delivery team at least 30 days in advance. Symantec will provide Customer with a corresponding WAF describing the Readiness Service, and Customer must sign and return the WAF to Symantec. If exchanging Service Days for a Readiness Service, the total number of Service Days required for each Readiness Service will vary as scoped by Symantec, but will require a minimum of at least 5 Service Days. No fraction of Service Days is permitted, and no credit is owed to Customer. The Service Level Agreement shall not apply to any Readiness Service.

- **Incident Response Readiness Assessment**. Symantec will assess Customer's ability to detect and respond to security incidents by conducting an onsite workshop to understand Customer's current definition of roles and responsibilities during a security incident. The Incident Response Readiness Assessment will provide Symantec with critical insights needed to help deliver an Incident Investigation based on Customer's unique environment, and enable Symantec to provide recommendations to assist Customer in improving its response times and effectiveness during an Incident Investigation.

- **Incident Response Plan Assessment**. An Incident Response Plan Assessment comprises in-depth assessment of Customer's information security incident response plan. Symantec will work with Customer to determine current and future needs and examine how the incident response plan currently operates from a strategic, operational and tactical viewpoint. This approach allows Symantec to provide a holistic review of Customer's incident response plan. Dependencies between Customer's incident response team, other internal teams and third parties will also be reviewed to determine the effectiveness and efficiency of these arrangements. An incident response plan assessment is performed using a series of questionnaires, workshops and interviews, typically over a 3-4 week period, and a 3-4 day onsite review. Symantec will provide an assessment snapshot with recommended actions presented at the end of the onsite visit.

- **Incident Response Plan Development**. An incident response plan helps minimize the impact of security incidents and shortens the timeframe between incident identification and incident resolution. Accordingly, an Incident Response Plan should foster a continuous improvement process that leverages lessons learned from past incidents to improve overall security effectiveness. An Incident Response Plan documents the processes and procedures, roles and responsibilities of various stakeholders, and

communications flows and notifications procedures that are critical in timely recovery from security incidents. Symantec will leverage its experience in responding to incidents throughout the globe combined with industry best practices to produce an Incident Response Plan tailored to Customer's organizational needs and unique requirements.

- **Incident Response Tabletop Exercises**. Symantec will use a table top exercise ("**TTX**") to test and refine Customer's existing Incident Response Plan or process. The TTX is performed in a conference room where Customer's key stakeholders talk through the Incident Response Plan or process and their response to a particular incident without the need to actually deploy Customer equipment or resources. During the TTX gaps and weaknesses in the Incident Response Plan or process may be identified. After the TTX, a debriefing will occur to review findings and create a plan for improving the Incident Response process.

- **Incident Response Training**. Symantec will scope Customer's needs, develop Incident Response training based on the scoping, and provide Incident Response training to assist Customer in the initial identification and containment of security incidents. Incident Response training may be tailored to specific Customer requests, internal team composition and specific security Incident Response handling requirements. Incident Response training topics may include security awareness, current security trends, data handling, volatile data collection, or other relevant areas.

- **Advanced Threat Hunting**. Symantec will search Customer's network to attempt to uncover the presence of compromises (a compromise assessment) and threat activity previously unidentified in Customer's environment ("**Advanced Threat Hunting**"). Symantec uses proprietary hunting methodology and technologies to search networks and identify the presence of possible threats ranging from undetected malware to full advanced persistent threat activity. Advanced Threat Hunting uses Symantec's vast intelligence resources that include indicators from the Symantec Global Intelligence Network, and research from Symantec analysts. Symantec will provide Customer with a better understanding of any potential exposure that may have been uncovered during the exercise and provide recommendations for containment and eradication.

TRAVEL AND EXPENSES ("T&E")

The Annual Subscription Charge does not include any travel and expenses ("**T&E**") that may be required to deliver Services. Customer will pay, if applicable, reasonable T&E incurred in the course of performance of the Services. T&E up to **USD $5,000** (or the local currency equivalent for non-U.S. expenditures) per resource for every 3 Service Days of Service, or **USD $10,000** if intercontinental travel is involved shall not require Customer's prior approval. Any T&E that Symantec incurs above the applicable amount must be pre-approved by Customer in writing to be reimbursed. All T&E will be invoiced by Symantec at actual cost in accordance with Symantec's standard business practices.

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:

- **Project Manager**. Customer will nominate a "Project Manager" to assist Symantec in coordinating Customer resources in a timely manner and to act as the focal point for resolution of Service related issues. Customer's Project Manager shall also have the necessary technical and business knowledge and authority to make decisions concerning the Service. In addition, Customer shall assign an appropriate number of suitable skilled personnel to assist and cooperate with Symantec consistent with the Service described in this Service Description. Customer will further provide escalation/contact information for required resources. Customer must identify and provide the names for Customer's Incident Response resources.

- **Facilities**. Customer will provide Symantec with all necessary cooperation, information and support that may reasonably be required by Symantec for the performance of the Service including, without limitation, arranging and/or obtaining appropriate travel documentation (including work permits, visas, etc.), access to suitably configured computers, unrestricted network physical connectivity, technical support resources for installing network monitoring hardware, software products and applicable passwords, at such times as Symantec requests. In addition, Customer will provide Symantec personnel with access to all buildings, phone systems, internet access, server rooms, and workstations, and will provide all necessary passes for access to

such areas if work is required by Customer outside of a Normal Business Hours. Customer will also provide access to a suitable conference room facility for meetings, interviews, and facilitated sessions during any on-site components of the Services and provide technical support resources for installing network monitoring hardware, where applicable.

- **Information**. Customer will ensure that Symantec has access to the following at all times: (i) materials and resources related to Customer's business and technical environment; (ii) software design documentation, current design diagrams, and other information required to deliver the Service; (iii) access to all operating systems and network and computing environments necessary to complete the Service. Where applicable, such access shall include various user accounts for relevant applications, as needed, to perform for example, a penetration assessment, including, a list of relevant IP addresses, URLs and user authentication.

SERVICE-SPECIFIC TERMS

SERVICE CONDITIONS

- **No Refund**. The Service(s) are non-cancellable and payments for the Service(s) are non-refundable.
- **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.
- **Service Days Expiration**. All Services and Service Days expire if not used and delivered during the Term (including without limitation any applicable Incident Investigations) and no credit or refund will be due Customer for any expired or unused Services.
- **Offsite Analysis**. Customer authorizes Symantec to perform any offsite analysis of Customer Data necessary for the Service. Accordingly, Customer acknowledges and agrees that Symantec may be required to connect its computers and equipment directly to Customer's computer network. Customer explicitly consents to Symantec connecting its computers and equipment directly 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.
- **Service Hours**. Except for Customer's 24/7 access to request assistance (as described in the Service features), all Services will be performed during Normal Business Hours. However, it is understood that an Incident Investigation is provided on an urgent basis, and that flexibility may be requested and accommodated, subject to local labor laws and the free choice of the individual resources delivering the Incident Investigation.
- **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;
  - 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 Services 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.
- This "Litigation Support Services" Section will survive termination or expiration of the Agreement.

Privilege. If Customer has listed General Counsel contact information in the Required Contact Information Form or has otherwise entered into a separate agreement confirming that the engagement is being conducted at the request of, and at the direction of, Customer's legal counsel, Symantec will work with all reasonable requests from Customer's legal counsel to preserve any attorney-client, attorney work product, or other applicable privileges. Symantec will treat all findings, reports and documentation it provides to Customer as part of the Services as Confidential Information.

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 Services, regardless of fault.

- **Reporting**. Customer acknowledges and agrees that in the course of delivering the Services, 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 acknowledges, understands and agrees that an unauthorized intrusion into wireless 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 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**"), 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 Services, including without limitation an Incident Investigation, will be performed may limit or alter the scope of the Services.

SERVICE LEVEL AGREEMENT

- A Service Credit shall equal 2.5% of the Annual Subscription Charge for the applicable Service. Service Credit(s) granted hereunder will first be applied toward Customer's next invoice due for the applicable Service after submission of a Service Credit Request, or if no additional invoice is due for the applicable Service, as a payment. Notwithstanding anything to the contrary in the Agreement, in no event shall Symantec be required to credit Customer more than 7.5% of the Annual Subscription Charge payable by Customer for the affected Service in any calendar month and Symantec's maximum cumulative liability to issue Service Credits for an annual period of the Term shall not exceed the Annual Subscription Charge. Symantec's sole and exclusive obligation and Customer's sole and exclusive remedy for this Service Level Agreement shall be limited to the issuance of Service Credits.

- With respect to a Custom Retainer Option or additional Service Days with the Term shorter than 1 year due to co-termination, fees paid for purchasing such Custom Retainer Option, to the extent they are subject to a Service Credit, will be included in the calculation of the Annual Subscription Charge on a prorated basis.
- If Customer believes it is entitled to a remedy in accordance with the Service Level Agreement, Customer must submit a Service Credit Request within 10 Normal Work Days of the end of the calendar month in which the suspected Service Level Agreement non-compliance occurred.
- All Service Credit Requests will be subject to verification by Symantec.
- Symantec shall not be responsible for its inability to perform Services (including meeting the Service Level Agreement) in whole or in part: (i) due to unforeseen circumstances or to causes beyond Symantec's reasonable control including but not limited to war, strike, riot, crime, acts of God, or shortages of resources ; (ii) legal prohibition, including but not limited to, passing of a statute, decree, regulation or order; (iii) during any period of suspension of Service by Symantec in accordance with the terms of the Agreement; (iv) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (v) Symantec resources are required to obtain visas prior to performing work in Customer's country.
- The remedies set out in the Service Level Agreement shall be Customer's sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise, with respect to the Service Level Agreement.

DEFINITIONS

Capitalized terms used in this Service Description shall have the meaning given below. Any capitalized terms not defined in this Service Description shall have the same meaning as in the Subscription Instrument.

"Annual Subscription Charge" shall mean the annual charge Customer has paid for the Service that Customer has subscribed to in the Subscription Instrument.

"Incident Investigation" shall mean an incident investigation conducted by Symantec based on the nature and type of a particular security incident as further described in this Service Description.

"Normal Work Day" shall mean a day that comprises the Normal Business Hours.

"**Normal Business Hours**" shall mean the normal working hours, typically between 8.00 a.m. and 5.30 p.m. local time, exclusive of any applicable statutory rest periods, weekends and public holidays, as observed in the country in which Services are performed.

"Remote Assessment" shall mean a remote assessment conducted by Symantec during an Incident Investigation as further described in this Service Description.

"Region" shall mean either: (i) the Americas, (ii) EMEA, or (iii) APJ, as applicable.

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

"Service Credit Request" shall mean the notification which Customer must submit to Symantec by email to Customer's Service Manager.

"**Service Day**" shall mean 1 Symantec resource working 1 Normal Work Day.

"**SLA**" or "**Service Level Agreement**" shall mean the applicable service level set forth in the Service Description.

"**Subscription Instrument**" shall mean one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a Symantec certificate or a similar document issued by Symantec, or a written agreement between Customer and Symantec, that accompanies, precedes or follows the Service.

"**Symantec**" shall mean: (i) **Symantec Corporation**, with a place of business located at 350 Ellis Street, Mountain View, CA 94043, USA, for Services delivered by Symantec in the Americas, where "**Americas**" shall mean all countries in the North, Central or South America or the Caribbean area; (ii) **Symantec Asia Pacific Pte Limited**, with a place of business located at 6 Temasek Boulevard, #11-01 Suntec Tower 4, Singapore 038986, for Services delivered by Symantec in Asia Pacific, where "**APJ**" shall mean the Pacific Island region, including Australia and New Zealand or a country in the continent of Asia (except Kazakhstan, Kyrgyzstan, Russia,

Turkmenistan, Uzbekistan and the Middle East); or (iii) **Symantec Limited**, with a place of business located at Ballycoolin Business Park, Blanchardstown, Dublin 15, Ireland, for Services delivered by Symantec in EMEA, where "**EMEA**" shall mean, any country of the World other than Americas and APJ.

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

"**WAF**" or "**Work Authorization Form**" shall mean the form Symantec provides to Customer pursuant to which Customer authorizes and acknowledges the location, contact information, T&E, Additional Responders, Readiness Service(s), and/or Service Day(s) for Incident Investigation(s).

END OF SERVICE DESCRIPTION