BT Assure Threat Services – Annex to the General Service Schedule

BT Reference No. **-**** -*****

1 Definitions

The following definitions apply, in addition to those in the General Terms and Conditions and the General Services Schedule of the Agreement.

"**CEP**" means Customer Enrolment Package, a document in which the Customer records the configuration information required for delivery of the Service.

"**Messages**" means any data sent by a Sensor to a Sentry, either a log message, an alert, or an accept/deny notification from a firewall.

"**Sensor**" means a device, operating system, database or other software or hardware that the Customer owns or licenses that can generate log data and is configured by the Customer to send messages to the Sentry.

"**Sentry**" means a passive data receiver owned and used by BT to provide the Services.

"SOC" means the BT Security Operations Center and/or Socrates.

2 Service Overview

BT Assure Threat Services provide the Customer with a comprehensive view of network security activity and a defence against malicious attacks. The BT Assure Threat Services include the following services:

2.1 BT Assure Threat Monitoring (ATM)

2.1.1 ATM is used to monitor security and non-security devices (Sensors). BT will provide one or more hardware or virtual Sentries at a Site(s) to monitor log data from all the Sensors listed in the Order. The Sensor must be one listed in the "BT Supported Device List", a copy of which is available on request. The Sentry configuration will be determined based on the Customer provided information in the CEP.

An option is available to the Customers to retain threat monitoring data within the European Union borders instead of data being collected and stored in the US SOC location, This option is referred to as "EU Data Dominion". For this option BT will evaluate the Customer requirements and if eligible for the EU Data Dominion option, BT will agree in writing the scope of the Customer data that is restricted to the European Union.

The log data is used to monitor events such as access violations and policy violations on the devices. If the devices cannot forward log information in passive mode by using Syslog, SMTP or other passive/active modes, the Customer must load an agent-based log forwarder on to the Sensor.

Event rules ("filters") are deployed on the Sentry to enable real time threat detection and filtering of the messages received. The event rules used depend on the device type(s) and product versions.

Log data is categorised into three event types:

(a) Direct Security Relevant (DSR), which are generated by systems designed to identify known attack signatures such as IDS devices or an operating system with established security-related system messages provided by the manufacturer. These events are identified within the context of the Customer's environment and ISRs (see below).

(b) Indirect Security Relevant (ISR), which are log messages from a non-security platform (not an IDS, IPS, or firewall of any type) that generate message types with security relevance, such as authentication messages and administrative activity logs.

(c) Non-Security Relevant (NSR), in which filters added to the Service filter out non security relevant messages.

2.1.2 BT's event tracking, correlation, and problem ticket management system, "Socrates" consists of a number of tools and technologies used by BT's security analysts. All filtered messages from the Sentry are sent to Socrates which categorises and prioritises problem tickets, weeds out false

positives, stores the data for future audit, and presents information about critical tickets to the security analysts for review.

2.1.3 BT will provide 24x7x365 real time event response, in accordance with alert guidelines and the escalation and notification contact tree provided by the Customer in the CEP. Not all problem tickets require Customer contact but all are assigned a severity; Interesting, Relevant, Suspicious and Critical.

2.1.4 Sentry failures.

2.1.4.1 If the SOC detects a hardware failure in a BT supplied Sentry, a field engineer will be sent to the Site for further investigation. If it is determined that a hardware part replacement is required, BT will order the part and install it when it has arrived at the Site.

2.1.4.2 If a Virtual Sentry fails due to a problem with the Virtual Sentry image, BT will provide access to an updated image that the Customer will need to download and install on its virtual machine server. If a Virtual Sentry fails due to a hardware or OS issue, the Customer will be responsible for correcting the issue.2.1.5 The Customer will be given access to a portal where the Customer can access service information such as reporting, sensor information, and change requests.

2.1.6 BT will retain the Customer's Messages that are transmitted to BT's SOCs as follows:

(a) Fifteen (15) days of detailed information will be retained on-line in Socrates and the portal;

(b) Six (6) months of weekly reports will be retained on-line in the portal;

(c) One (1) year of online storage for monthly reports.

2.1.7 BT will retain the Customer's firewall Messages that are transmitted to BT's SOCs as follows.

(a) A daily summary will be computed for total bytes and connections and ninety (90) days of daily summary information will be retained online;

(b) No data detail or summary information will be retained offline for firewall traffic logs.

(c) Ticketed events from Firewall Threshold violations will be kept as per Section 2.1.6 above

2.1.8 Following termination of Service, BT will continue to store the Customer's data in its data backup complex and continue to safeguard such data at the same levels as existing customers. BT will use approved commercial services to destroy storage media at BT determined intervals or upon media failure.

2.2 BT Assure Vulnerability Scanning (AVS)

2.2.1 The AVS service enables management of Customer IP scans which can be scheduled weekly, monthly, quarterly or on-demand. BT uses scan technology from Qualys. The Customer has the following options:

(a) Assure Internal Vulnerability Scanning which scans the Customer's network assets using Scanner Appliance(s) and cross-references the data compiled during a scan against a continuously up-to-date inventory of network assets. BT will provide Scanner Appliance(s) that will scan the Customer's network as scheduled. BT will ship Scanner Appliance(s) to the Customer for installation by the Customer.

(b) Assure External Vulnerability Scanning which scans the Customer's IT environment from the public Internet and cross-references the data compiled during a scan against a continuously up-to-date inventory of network assets and the current state of operation.

(c) Assure Vulnerability Scanning PCI Compliance add-on to Assure Internal Vulnerability Scanning and/or Assure External Vulnerability Scanning in which BT will perform, once every three (3) Months, two scans of the same target networks: an initial Pre-Compliance Scan to confirm the list of target IP addresses and identify any vulnerabilities requiring remediation, and, following a remediation period of up to seven (7) days, a PCI Compliance Scan of the

target IPs identified during the preceding Discovery Scan. BT will provide the Customer with a PCI Scan Report, normally within three (3) Business Days of the scan to enable the Customer to take remedial actions to fix any identified vulnerabilities.

2.2.2 BT does not make any warranty that AVS will be error-free, free from interruption or failure, or secure from unauthorized access, or that it will detect every vulnerability in the Customer's network, or that the results generated by AVS will be error-free, accurate, or complete. AVS may become unavailable due to any number of factors including scheduled or unscheduled maintenance, technical failure of the software, telecommunications infrastructure, or the Internet.

2.2.3 Customer reporting information is stored by Qualys and available via a portal. PCI scan reports and related information will be stored for a period of two (2) years from the date of scanning.

2.2.4 BT reserves the right to restrict the number of scans to no more than one per week.

2.3 BT Assure Device Management (ADM)

BT will provide Assure Device Management Services, by remotely managing the Customer's systems in the form of software or appliance(s) provided by a 3rd party equipment manufacturer or software provider ("vendor") and owned by the Customer (or to which the Customer has license rights granted) or software or appliance(s) provided by BT and owned by BT.

2.3.1 The Customer can order any of the following options:

(a) Snort Managed Intrusion Detection Service ("BT Snort/MIDS").

(b) Managed Intrusion Detection Service ("MIDS").

(c) Managed Intrusion Prevention Service ("MIPS").

(d) Managed Firewall Service ("MFS").

For BT Snort/MIDS, BT is responsible for providing the managed IDS equipment, obtaining product/equipment support and maintenance, and management of its suppliers, including event and dispatch management.

For the other options, the Customer is responsible for providing the equipment, obtaining product/equipment support and maintenance and management of its suppliers, including event and dispatch management.

BT will review each Managed Device configuration before taking management responsibility and will provide best practice recommendations. In order to complete the review, the Customer must provide BT with remote access to the device with authority rights to retrieve the device configuration.

2.3.2 BT will provide, as necessary,

(a) maintenance updates to the Managed Device applications and underlying operating systems, and OS updates for appliance-type Devices. These include the installation and tuning of any signature updates, Managed Device application patches, and alerting configuration, within the administrative boundaries defined by the Managed Device application vendor's own management console interface. For the avoidance of doubt, this does not include comprehensive OS upgrades (such as from Windows XP to Windows 7)

(b) for administrative changes, maintenance updates and system upgrades to the Managed IPS, BT can release signatures in active mode, but recommends that all new signatures and automated event analysis blocking capability be deployed in passive mode for a period of time to test the effectiveness within the Customer's environment.

(c) additions, deletions, and modifications of rules, administrative changes, maintenance updates and system upgrades to the Managed Firewalls.

BT will make any changes it considers necessary to the Managed Devices to maintain the security of the Customer's environment and configuration changes to the Managed Devices to protect the Customer's network. These changes do NOT include any Customer requested changes, vendor changes, or changes

needed due to business changes of the Customer. BT will inform the Customer via email or phone, and via periodic reports, of the changes it has made.

2.3.3 BT will respond to any Customer requested changes, which must be made in writing via email, as below. On validation of change requests, BT will schedule changes with the Customer, and coordinate with the Customer to implement the changes. BT will provide:

2.3.3.1 For MIDS

(a) Up to five (5) changes per Month per Managed Device for Pattern changes and tuning (each change can include up to ten (10) configuration changes). Tuning changes are defined as "Modifying conditions under which an existing signature will generate an outbound alert from the IDS" such as changing included or excluded source/destination networks.

(b) two (2) changes per Month to pre-defined network ranges when available.

2.3.3.2 For MIPS and MFS

(a) Up to five (5) changes per Month. In most cases, BT will schedule changes with the Customer to occur within 24 hours of request, or at a predetermined date requested by Customer. Complex changes may require more preparation time. A change is defined as "Any modification of allowable ports and/or protocols, on either ingress or egress filtering, to add, delete, or change traffic flow through the IPS between any two points on either side of the interface such as changing a web server object to allow inbound and outbound tcp/443 traffic in addition to existing tcp/80 traffic."

(b) The Service supports devices with up to fifty (50) discrete policy rules defined on a single IPS. Network segment changes, defined as "Adding, changing, or deleting objects connected to the IPS' network segment interface", are supported by the service, with up to five (5) such changes allowed during any Month. BT will support up to two (2) expedited changes in which BT will schedule changes with Customer to occur within four (4) hours of request, or later as defined by Customer. In no case will BT support a number of discrete policy rules per IPS or Firewall in excess of the manufacturer's recommended limit for any installation, taking into account vendor make and model, amount of traffic throughput on the device, and any other specifics which may arise as a result of existing rules or policies which are unusually complex or CPU-intensive for the device to process.

(c) BT will provide written guidance to the Customer if a requested change falls outside these parameters, with a recommendation either to upgrade the device to one more capable, or to revise the existing rules to keep under the recommended ceiling.

For the avoidance of doubt, any unused changes cannot be carried over from one Month to the next.

BT will contact the Customer if the Managed Device hardware is suspected to have failed or needs physical maintenance.

2.4 BT Assure Log Retention (ALR)

The ALR Service collects logs from all supported connected data sources, including networking, servers and applications. The ALR Service allows access to compliance reporting and to all collected enterprise log data.

Managed Log Retention (MLR) appliances are provided, owned and managed by BT.

BT will provide the following information to the Customer as part of the ALR service:

(a) Log Collection. Log data will be collected from Syslog, SNMP and LEA for Checkpoint log sources.

(b) Real-Time Reporting. Log data will be normalised from a variety of log source devices. The Customer will be able to run reports and build searches on the normalised log data.

(c) Monitoring and Alerting. BT will provide health monitoring of the MLR appliance and service.

(d) Archiving. BT will provide facilities to configure MLR appliances to record the contents of their local archives to Customer-supplied backup mechanisms or shared network volumes.

(e) Management. BT will provide, as necessary, administrative changes, maintenance updates and OS upgrades to the MLR appliances.

BT will contact the Customer if the MLR appliances under management are suspected to have failed or if they need physical maintenance.

BT will provide 24x7x365 management of MLR appliances.

BT will evaluate typical inbound message rates and volumes periodically across BT's customer base to calculate normal levels for any given source device type, and alert the Customer if their particular measured rates are more than 50% higher than that average. In such circumstances BT reserves the right to require the Customer to add additional hardware (at the Customer's expense).

BT does not guarantee a Log Retention period beyond 90 days. Any longer period requested by the Customer will be chargeable and assessed in accordance with Clause 19.15 of the General Terms and Conditions.

3. Service Delivery

BT will remotely configure any Equipment used in the supply of Services and following installation of Equipment by BT except for equipment associated with the AVS service, conduct a set of standard tests to ensure that the configuration at a Site is functioning correctly.

The Operational Service Date (OSD) for a Site occurs as follows:

3.1 ATM - when the Sentry or Virtual Sentry, as applicable, is installed and configured allowing remote connectivity by the BT SOC.

3.2 ADM - For BT owned Snort/MIDS, when the MIDS device is installed and configured allowing remote connectivity by the BT SOC. A Sentry install is also required for monitoring. For third party IDS, IPS, or Firewall, when the BT SOC has remote connectivity and management access to the device.

3.3 ALR - when the MLR device is installed and configured allowing remote connectivity by the BT SOC.

3.4 AVS - when the Customer is provisioned by the BT SOC in the Qualys system.

BT will provide IP address range(s) of the gateways at the BT SOC that will be supporting the Customer.

4 BT Service Management Boundary (SMB)

4.1 For Sensors not managed by BT, the Customer will be responsible for configuring the devices to transmit messages to the Sentry(s) and work with BT to reconfigure and tune the devices to reduce the generation of false positives from the Customer's infrastructure.

4.2 For Sensors monitored and managed by BT, the Customer will be responsible for enabling remote connectivity and management access to the devices by the BT SOC.

4.3 If out of band ("OOB") access is required, BT will provide Secure OOB devices which will be connected to a Customer provided analog telephone line which terminates directly from the telephone service provider to the modem. This line shall not transit the Customer's PBX, and shall not be used other than to call BT. The Customer is responsible for all call charges. OOB management is only supported with third party managed devices not for the BT Snort/MIDS device.

4.4 For Virtual Sentry, the Customer will be responsible for the underlying equipment, the Operating System, and the Virtual Machine environment. BTs responsibility is for the Virtual Sentry image supplied as an OVF package and its Sentry functionality.

5 The Customer's Responsibilities

5.1 The Customer acknowledges and agrees that BT will not start its delivery processes until BT has received the completed CEP.

5.2 The Customer will promptly notify BT in writing of changes to information contained in the CEP.

5.3 The Customer shall not use the Services to monitor a third party's network or any devices or applications not expressly chosen by the Customer for its internal business purposes to be active on the Customer's network.

5.4 The Customer is responsible for ensuring that its monitored devices are sending log files to the BT Sentry device. If a period of tuning is required, the Customer acknowledges and agrees that BT will charge from the OSD as defined in section 3.

5.5 The Customer understands that it is ordering the Service for its network as currently assessed. Any Customer requested changes that require platform upgrades may result in limitations of the Service. The Customer may have the option to order upgrades to rectify this.

5.6 ATM, ALR, ADM

5.6.1 The Customer is responsible for providing KVM (keyboard, video, mouse) for any on-site maintenance or support of supplied CPE. If KVM is not available at the time of the site visit, the customer will be responsible for all associated costs as it will be treated as an aborted site visit.

5.6.2 On termination of the Service, the Customer shall allow BT to recover BT owned Equipment from its Site(s). The Customer will store the BT Equipment until it arranges for its recovery with BT's supplier.

5.6.3 The Customer is responsible for deinstallation of Qualys scanners and Out of Band Modems provided by BT and returning them to BT.

5.6.4 The Customer shall provide 24x7 access to its Site(s) for maintenance. If the Customer cannot do this, then the SLAs will not apply.

5.7 ATM

5.7.1 For Hardware Sentry installation, the Customer will allow BT to install Sentry(s) inside the Customer's network on a network segment where the Sensors being monitored can deliver Messages to the Sentry.

5.7.2 The Customer must provide an outgoing network path from server to public internet to enable remote access from the Sentry(s) to BT's Security Operations Centres via SSL (TCP port 443) and enable temporary inbound access via SSH on request from BT.

5.7.3 The Customer shall provide a three (3) hour maintenance window weekly.

5.7.4 The Customer's network will have a minimum outbound bandwidth equivalent of an E1/T1 circuit for the Sentry to use to maintain connectivity from the Customer site to a SOC.

5.7.5 For Virtual Sentry installation, the Customer must provide a suitable server and Virtual Machine environment for installation of the Virtual Sentry image. The Customer may use an Open Virtualization Format (OVF) supporting Virtual Machine vendor of its choice (e.g. VMware, Microsoft, Oracle, etc.), as the BT Virtual Sentry image is supplied as an OVF package. The Customer acknowledges that BT uses VMware VSphere versions 4 and 5 when testing and will only provide install instructions for VSphere versions 4 and 5. The Customer will be provided with recommended hardware/software specifications for the server Running the Virtual Sentry image.

5.7.6 The Customer must follow BT's instructions for download and installation of the Virtual Sentry image within 14 calendar days of receipt of the email from BT containing login, download, and installation instructions for the Virtual Sentry image.

5.7.7 On termination of the Service, the Customer must de-install the virtual sentry image within 30 calendar days.

5.8 AVS

5.8.1 The Customer is responsible for installing Scanner Appliance(s) on a Customer network segment where the security devices and sensors being scanned can be accessed from the Scanner Appliance.

5.8.2 The Customer shall enable remote access between the onsite Scanner Appliance(s) and BT's or its supplier's SOCs via SSL and SSH.

5.8.3 The Customer shall notify BT immediately in writing of any changes in, or increases in the number of, the IP address(es) and/or domain name(s) that are listed in its account with the BT.

5.8.4 The Customer represents and warrants that it has full right, power, and authority to consent to have the tests for vulnerabilities of the IP addresses and/or domain names which the Customer notifies BT in writing. The Customer agrees to indemnify and hold BT harmless from and against any and all liabilities, losses, damages, costs, and expenses (including legal fees) incurred by BT resulting from the Customer's breach of this section.

5.8.5 The Customer acknowledges and agrees that the AVS service and the results of the AVS service (excluding individual factual data gathered from its network) and all Intellectual Property Rights relating thereto are exclusively owned by BT or BT's third-party supplier. The Customer also acknowledges and agrees that it will not obtain any rights or interests thereto, except as expressly granted in this Service Annex.

5.8.6 The Customer acknowledges that scanning of IP addresses and/or domain names may in some circumstances result in the disruption of other services at its Site(s).

5.8.7 The Customer agrees that it is its responsibility to perform backups of data on all devices connected to its IP addresses and/or domain names before using AVS. The Customer further assumes the risk for all damages, losses, and expenses resulting from the use of AVS.

5.8.8 The Customer agrees not to

(a) use the Scanner Appliance, AVS Service, Reports, API or any data or information contained in any of the foregoing, except for the limited purpose of vulnerability management with regard to the IP addresses for which the Customer has ordered the Service;

(b) rent, lease, or loan the AVS Service, or any part thereof, or permit third parties to benefit from the use of the AVS Service via timesharing, service bureau arrangements, or otherwise;

(c) open, disassemble, or tamper with Scanner Appliance in any fashion;

(d) transfer possession of Scanner Appliance to any third party; or

5.8.9 The Customer shall keep any user name and password provided for access to the AVS Service confidential and will promptly notify BT if it learns of any unauthorized use of the user name or password.

5.8.10 The Customer acknowledges and agrees that all data and information contained within the AVS Service, Scan Data and Reports (excluding individual factual data gathered form the Customer's network IP addresses), and all information concerning or materially relating to the Scanner Appliance(s), are Confidential Information of BT's supplier. The Customer will not use any Confidential Information of BT's supplier for any purpose not expressly permitted by this Service Annex, and will disclose the Confidential Information of BT's supplier only to those employees who have a need to know such Confidential Information for purposes of this Service Annex, and who are under a duty of confidentiality no less restrictive than the Customer's duty hereunder. The Customer will protect BT's supplier's Confidential Information from unauthorised use, access, or disclosure in the same manner as the Customer protects its own confidential information of a similar nature, and with no less than reasonable care.

5.8.11 The Customer shall return the Scanner Appliance(s) to BT on termination of the AVS Service. BT reserves the right to charge the Customer the cost of replacing the devices if BT does not receive the Scanner Appliance(s) within forty five (45) days of termination Service.

5.8.12 AVS PCI Compliance

(a) The Customer acknowledges and agrees that BT is bound by the Payment Card Industry (PCI) Approved Scan Vendor Compliance Test agreement with the PCI Security Standards Council (SSC) and that, in order to assist the PCI SSC in ensuring the reliability and accuracy of BT's testing and assessment procedures for customers, BT may need to provide (within fifteen (15) days of written request) the Customer's testing and assessment results to any PCI Member, where the Customer is a Financial Institution of such PCI Member, Issuer of such PCI Member, Merchant authorised to accept such PCI Member's payment cards, Acquirer of accounts of Merchants authorised to accept such PCI Member's payment cards or Processor performing services for such PCI Member's Financial Institutions, Issuers, Merchants or Acquirers.

(b) The Customer acknowledges and agrees that BT is bound by the PCI Approved Scan Vendor Compliance Test agreement with the PCI SSC, which requires BT to disclose any data or other information obtained by BT from the Customer in the course of providing the PCI Scanning service to the PCI SSC and/or its PCI Members, as requested by the Customer. Further, each PCI Member of the PCI SSC may disclose such information on an as needed basis to its respective member Financial Institutions and Issuers and to relevant governmental, regulatory and law enforcement inspectors, regulators and agencies.

5.9 ADM

5.9.1 The Customer will allow BT to install BT Snort/MIDS device(s) inside the Customer's network on a network segment where the device can deliver Messages to the Sentry.

5.9.2 The Customer shall obtain and keep vendor (or applicable third-party provided) support and maintenance services for the 3rd Party Managed Devices for the duration of the Services.

5.9.3 The Customer shall provide BT with exclusive administrative access to the Managed Devices and the Customer will have no administrative rights to the managed system.

5.9.4 The Customer is responsible for OS installation and licensing. The Customer will provide system backup capabilities as directed by BT and access to storage resources if a backup/recovery is required. No other applications or services shall be installed without explicit written permission from BT.

5.9.5 The Customer shall provide the following conditions for all associated management applications of Managed Devices:

(a) Management application installed on a vendor approved hardware platform, on the then current recommended OS.

(b) Server hardware for software based Managed Devices that meets the Management Application vendor's minimum requirements, matching scope of deployment.

(d) Management application must run on dedicated hardware. No other applications or services other than those used by the management application will be run on the hardware without BT's written permission.

(e) BT will have sole administrative access to the OS and application, and the device shall not be joined to a network Domain or other logical unit which possesses higher-ranking access credentials which supersede any local restrictions specific to the OS and application.

(f) BT will harden/configure the OS consistent with the management application Vendor's best practices.

5.9.6 For third party MIDS the Customer shall perform all maintenance and administration of any underlying operating system or hardware on which the Managed IDS application runs if not appliance based. The Customer shall retain an administrative account, which provides access to these system-level parameters but shall not modify the operating parameters of the Managed IDS application under any circumstances.

5.9.7 The Customer shall respond to BT alerts regarding hardware, software and maintenance.

5.9.8 The Customer, at its cost, shall perform third party hardware upgrades, including replacement of hardware that cannot support new vendor software releases or cannot meet its performance demands as directed by BT.

5.9.9 The Customer shall enable remote access to Managed Devices from BT SOCs via SSL and SSH or IPSEC VPN or a combination of these as required by the vendor.

5.10 ALR

5.10.1 Customer shall work with BT to establish the optimal MLR appliance configuration before implementation of the MLR appliance.

5.10.2 The Customer will allow BT to install MLR device(s) inside the Customer's network on a network segment where the MLR can deliver Messages to the Sentry.

5.10.3 The Customer will work with BT's SOC to ensure that logs are collected from the Critical Assets defined in the CEP.

5.10.4 The Customer shall enable remote access to the agreed upon MLR appliances from BT's SOC.

6 Charges and Payment Terms

The Charges for the Service will comprise some or all of the following components, depending on the option selected on the Order:

Product	One-time Charge	Recurring Charge	Notes
ATM			
ATM Service Activation	Non-Recurring Charge		
ATM Site Provision	Non-Recurring Charge		Charge is per Site
ATM Service Management		Monthly Recurring Charge	Charge is based on the number and type(s) of monitored devices.
Sentry Install	Non-Recurring Charge		Charge per Sentry.
Sentry Appliance		Monthly Recurring Charge	Charge per single hardware or virtual Sentry configuration or HA Sentry configuration
ALR			
ALR Site Provision	Non-Recurring Charge		Charge is per Site
ALR Service Management		Monthly Recurring Charge	Charge is based on the number of log sources
MLR Install	Non-Recurring Charge		Charge per MLR device.
MLR Appliance		Monthly Recurring Charge	Charge per single MLR configuration or HA MLR configuration

ADM			
ADM Site Provision	Non-Recurring Charge		Charge is per Site.
ADM Service Management		Monthly Recurring Charge	Charge is based on the number and type of monitored/managed devices
BT Snort/MIDS Install	Non-Recurring Charge		Charge is per BT Snort/MIDS.
AVS			
AVS Site Provision	Non-Recurring Charge		Charge is per Site
AVS Service Management		Monthly Recurring Charge	Charge is based on the number of scanned IP addresses and type of scanning (internal/external and PCI)
Scanner Appliance		Monthly Recurring Charge	Charge per Internal Scanner.

7 Service Levels

Unless otherwise stated on the Order, the SLA Categories for Availability for each service are as follows:

Service	**SLA Category**
Assure Threat Monitoring, Single Sentry configuration	F
Assure Threat Monitoring, High Availability Sentry configuration	A
Assure Log Retention, Single MLR configuration	F
Assure Log Retention, High Availability MLR configuration	A
Assure Device Management, BT MIDS configuration	F
Assure Vulnerability Scanning, External Scanning MVS service	A