Security Services (North America) Service Terms

1. MONITORING SERVICES

Monitoring Services (except for Monitoring Services: Web Server with Transactions) are conducted at 5-minute intervals. Customer notification is triggered by two consecutive negative polling responses.

Monitoring Services detect only positive or negative Internet Control Message Protocol/Simple Network Management Protocol (ICMP/SNMP) responses from direct Network Interface Card (NIC) polling and do not detect SNMP traps. Monitored devices may generate false-positive alerts due to network congestion or application activity.

Customer will enable connectivity to Sungard Availability Services' (Sungard AS') monitoring infrastructure and provide a dedicated NIC. Monitoring Services may require a monitoring agent be installed on the device. Customer will install the agent and perform any vendor-required upgrades or updates, unless the device OS is managed by Sungard AS.

If more than one instance or partition of an OS or application is running on a monitored device, the Sungard AS monitoring "unit" is per instance instead of per device or server.

1.1. Features

Sungard AS will perform the following for the number of devices identified in the Order:

(a) Monitor the ability of the device NIC to respond to ICMP and SNMP requests.
(b) Monitor device power availability and fan status.
(c) Monitor the CPU, memory, temperature and WAN interface thresholds identified in the completed customer design requirements (CDR) form
(d) Notify Customer if the Monitoring Services detect non-responsiveness or exceeded thresholds.

2. NETWORK SERVICES

2.1. LAN Services and WAN Services

2.1.1. Features

Sungard AS will provide the following for the number of network termination devices identified in the Order in accordance with the completed CDR form:

(a) Maintenance of the network equipment software configuration backup.
(b) Exclusive control of administrator security passwords and IDs (Customer may request a copy of device configuration data).
(c) Monitor critical patch alerts and provide Customer notification of such patches.
(d) If identified in the Order, provision the network termination devices.
(e) Coordination of third-party equipment vendor maintenance and detected equipment problem resolution.
(f) Hardware Installation Services (if the equipment is located in the Designated Sungard AS Facility).
(g) Equipment Management Services.
(h) Monitoring Services: Device.

2.1.2. General

For all Customer-provided hardware receiving Managed Network Equipment Services, Customer will:

(a) Provide verification of licenses and the necessary license keys applicable to Customer-provided software.
(b) Provide Sungard AS with administrative- and root-level access.

(c) Obtain and maintain 24x7 maintenance agreements with the equipment vendor with 4-hour response time and notify the vendor of Sungard AS' authorization to act as Customer's agent under the maintenance agreements.
(d) For equipment located at a Customer premises, Customer will provide physical and logical access as reasonably required by Sungard AS to perform the Services.

Sungard AS is not responsible for resolution of failures associated with:

(a) Hardware or software that is end of life or not otherwise supported by the vendor.
(b) Customer written or other software not supported by Sungard AS.

3. SECURITY SERVICES

Customer administrative access to Sungard AS devices used to provide Security Services is not permitted. Customer may request a copy of device configuration data.

Sungard AS does not guarantee device failure time to fix. Sungard AS will maintain spare device inventory or engage and manage maintenance vendors in accordance with the terms of the underlying maintenance Agreement. Sungard AS is not responsible for vendor failure to deliver parts or repairs within maintenance agreement timelines.

3.1. Managed Firewall & VPN Services

3.1.1. Features

Sungard AS will provide the following for the number of firewalls identified in the Order:

(a) Firewall configuration and firewall policy changes in accordance with the completed CDR form.
(b) Resolution of detected firewall problems.
(c) Retention of firewall logs for 90 days.
(d) Creation of backup and restore firewall rules.
(e) ICMP/SNMP monitoring.
(f) Monitoring Services: Device throughput and virtual private network (VPN) outage.
(g) Customer-notification and coordination of critical patch alerts.
(h) Equipment Management Services.
(i) Installation of Sungard-AS-provided solution.
(j) LAN Equipment Services for a Sungard-AS-provided production switch.

3.1.2. General

Customer is responsible for software management and configuration of Customer managed VPN endpoint(s).

Sungard AS does not monitor VPN persistence.

3.2. Managed Host Intrusion Protection Service ("IPS")

3.2.1. Features

Sungard AS will provide the following for the number of servers identified in the Order:

(a) Installation (only if the applicable Customer server receives OS Management Services) and configuration of intrusion detection and intrusion prevention software in accordance with the completed CDR form.
(b) Configuration of intrusion detection and intrusion prevention rules, including fine tuning of rules during the 30-day period following the initial configuration and implementation of Customer-requested changes to intrusion detection and intrusion prevention rules.
(c) 24x7x365 intrusion monitoring and notification to Customer of detected alerts based on manufacturer- and Customer-approved settings.

(d) If identified on the completed CDR form, detection and prevention of attempted intrusions and server misuse consisting of traffic abnormalities and/or pre-defined known attack signatures.
(e) If identified on the completed CDR form, automatic implementation of new attack signatures as made available by the vendor.
(f) Retention of IPS logs for 90 days.

3.2.2. General

Intrusion prevention features block attacks based on pre-selected criteria. Otherwise, traffic meeting the customized attack criteria will be dropped.

Customer will install the IPS software unless Customer contracts for OS Management Services for the server on which the software is installed.

3.3. Managed Network Intrusion Protection Service ("NIPS")

3.3.1. Features

Sungard AS will provide the following for the number of IPS appliances identified in the Order:

(a) Installation and configuration of intrusion detection and intrusion prevention appliances in accordance with the completed CDR form.
(b) Configuration of intrusion detection and intrusion prevention rules, including fine tuning of rules during the 30-day period following the initial configuration and implementation of Customer-requested changes to intrusion detection and intrusion prevention rules.
(c) 24x7x365 intrusion monitoring and notification to Customer of detected alerts based on manufacturer- and Customer-approved settings.
(d) If identified on the completed CDR form, detection and prevention of attempted intrusions and server misuse consisting of traffic abnormalities and/or pre-defined known attack signatures.
(e) If identified on the completed CDR form, automatic implementation of new attack signatures as made available by the vendor.
(f) Retention of IPS logs for 90 days.
(g) Managed Vulnerability Protection Service.
(h) Monitoring Services: Device.
(i) Equipment Management Services.
(j) Hardware Installation Services.

For NIPS, the Service will decrypt and inspect Secure-Sockets-Layer-encrypted (SSL-encrypted) network traffic to identify potential security threats (if identified on the completed CDR form).

3.3.2. General

Intrusion prevention features block attacks based on pre-selected criteria. Otherwise, traffic meeting the customized attack criteria will be dropped.

Customer will provide one Ethernet port connection for each network segment covered by the Network IPS services.

Network IPS does not inspect or prevent encrypted traffic.

3.4. Threat Manager Services

3.4.1. Features

Sungard AS will provide the following in accordance with the completed CDR form for the number of Customer-specified nodes identified on the Order:

(a) Monitoring, analysis and logging of security events using a Sungard-AS-provided hardened security appliance.

(b) Sensor tuning and optimization.
(c) Threat and vulnerability signature updates.
(d) Asset identification and criticality ranking.
(e) Vulnerability assessments and related reporting.
(f) Web portal access.
(g) Additional operational configuration and monitoring as indicated in the completed CDR form if Sungard AS is managing other appliances in the Customer environment.
(h) Customer-selected notification of detected threats via email or Web page as identified in the completed CDR form.

If identified on the Order, Sungard AS will provide the Threat Manager — SSL Decryption Service, which enables the Threat Manager Service to decrypt and inspect SSL-encrypted network traffic to identify potential security threats.

If identified on the Order, Sungard AS will provide the Threat Manager — ActiveWatch Service, which provides access to SANS Global Information Assurance Certification (GIAC) certified intrusion detection analysts who analyze the data generated through Sungard AS' Threat Manager Service. Customer will be alerted when valid hostile traffic is identified and will be advised on potential remediation steps. Security analysts monitor the network on a 24x7x365 basis.

3.5. Log Manager Services

3.5.1. Features

Sungard AS will provide the following for the number of Customer-specified log sources identified in the Order:

(a) Collection, storage, reporting and correlation of log data using a Sungard-AS-provided device up to the quantity of GBs specified in Part 1 of the Order, if any.
(b) Storage of log data for the lesser of the period of time stated in the Order or the Term of the Order.
(c) Web portal access.

If identified on the Order, Sungard AS will provide the Log Manager — Log Review Service, which provides analyst review of the previous day's log data that was collected and stored by the Log Manager Service. This review is performed to identify and notify Customer of potential security incidents as well as to document such incidents and the taken related actions.

3.6. Threat Manager Services and Log Manager Services

3.6.1. General

The Log Manager Service is provided using a third-party subcontractor.

The Threat Manager and Log Manager Services security appliances can be installed within a Designated Sungard AS Facility or at a Customer facility. In the event the Services are provided for appliances installed in a Customer facility, Sungard AS will ship the appliances to the Customer-specified facility and Customer will:

(a) Provide, monitor and manage all installation, power, network, physical and logical infrastructure, and security requirements necessary to support the appliances.
(b) Upon termination of the Services, Customer will uninstall, pack and return the security appliances in the same condition as received (normal wear and tear excepted) to Sungard AS pursuant to Sungard AS' reasonable instructions.

3.7. Unified Threat Management Managed SSL VPN Services, Unified Threat Management Managed IPsec VPN Services, and Managed Client VPN Services

3.7.1. Features

Sungard AS will provide the following for the number of VPNs or users identified on the Order:

(a) Remote SSL or IPsec-protected access to Customer's systems, networks, and/or applications.
(b) Implementation of the initial network configuration in accordance with the completed CDR form.
(c) Retention and control of passwords and IDs.
(d) Implementation of Customer-requested VPN policy changes.
(e) Monitoring of critical patch alerts.
(f) Monitoring Services: Device for the device(s) providing the VPN Services.

3.7.2. General

Customer will provide:

(a) An IPsec- or SSL-compliant device or subscribe to a Sungard-AS-supported multi-protocol label switching service to terminate the IPsec or SSL connections.
(b) SSL licensing for Customer-provided equipment.

3.8. Managed Two-Factor Authentication Services

3.8.1. Features

Sungard AS will provide the following for the number of users identified in the Order:

(a) Implementation of the initial network configuration in accordance with the completed CDR form.
(b) Licensing of required clients (solely with respect to Sungard-AS-provided equipment used to provide the Service).
(c) Retention and control of passwords and IDs.
(d) Support and administration of token authentication for access control.
(e) Implementation of Customer-requested additions, changes and deletions of Customer user identification.
(f) Monitoring of critical patch alerts and Customer notification of such patches.

3.8.2. General

Two-Factor Authentication Services are available either as a Hard Token (key fob) or Soft Token (software) using the industry-standard, advanced encryption standard algorithm.

3.9. Managed Vulnerability Protection Services

3.9.1. Features

Sungard AS will provide the following for the number of IP addresses identified in the Order:

(a) Customization of recurring vulnerability scanning of the internal and external network, application and remote access devices in accordance with the completed CDR form.
(b) Configuration of scans, including fine tuning of scans during 30-day period following the initial configuration and implementation of Customer-requested changes to scans.
(c) Scans at the frequencies specified by Customer.
(d) Scan reports identifying device-type (access gateways, routers or other types of equipment), machine-type, name and OS, and detected vulnerabilities.

3.10. Managed Digital Certificate Services

3.10.1. Features

Sungard AS will provide the following for the number of 128-bit digital certificates identified in the Order:

(a) Installation (if the SSL device receives Equipment Management Services), provisioning of 12-month-valid certificates for SSL-enabled equipment in accordance with the completed CDR form.
(b) Issuance of replacement certificates upon the expiration of each 12-month period or upon Customer request.
(c) Maintenance of the certificate revocation list.

3.10.2. General

Customer will:

(a) Generate the required digital key pair and device certificate signing request.
(b) Install the SSL certificate unless Customer contracts for Equipment Management Services for the SSL-enabled device.

Customer requests for replacement certificates, except due to expiration, may be charged at Sungard AS' then-current rates.

3.11. Unified Threat Management Standard and High Availability Services

3.11.1. Features

Sungard AS will provide the following for the number of instanced identified in the Order:

(a) One device or virtual machine (VM) for Standard Service or two devices or VMs for High Availability Service.
(b) Firewall configuration and firewall policy changes in accordance with the completed CDR form.
(c) Resolution of detected firewall problems.
(d) Retention of firewall logs for 90 days.
(e) Creation of backup and restore firewall rules.
(f) ICMP/SNMP monitoring.
(g) Monitoring, Customer-notification and coordination of critical patch alerts.
(h) Equipment Management Services.
(i) Hardware Installation Services.
(j) LAN Services for a Sungard-AS-provided production switch.

3.11.2. General

Customer is responsible for software management and configuration of Customer-managed VPN endpoint(s).

Sungard AS does not monitor VPN persistence.

3.12. Unified Threat Management (IDS IPS option)

3.12.1. Features

Sungard AS will provide the following for the number of Intrusion Detection System / Intrusion Prevention System (IDS/IPS) instances and network segments identified in the Order:

(a) Installation (only if the applicable Customer server receives OS Management Services) and configuration of IDS/IPS software in accordance with the completed CDR form.
(b) Configuration of IDS/IPS rules, including fine tuning of rules during 30-day period following initial configuration and implementation of Customer-requested changes to IDS/IPS rules.
(c) Automatic implementation of new attack signatures as made available by the vendor.

(d) 24x7x365 intrusion monitoring and notification to Customer of detected alerts based on manufacturer- and Customer-approved settings.
(e) If identified on the completed CDR form, detection and prevention of attempted intrusions and server misuse consisting of traffic abnormalities and/or pre-defined known attack signatures.
(f) If identified on the completed CDR form, automatic implementation of new attack signatures as made available by the vendor.
(g) Retention of related security logs for 90 days.
(h) ICMP/SNMP monitoring.

3.12.2. General

If multiple network segments are monitored, the Customer network architecture must support VLAN tagging or one Ethernet interface per monitored network segment.

Intrusion Prevention Services block attacks based on pre-selected criteria. Otherwise, traffic meeting the customized attack criteria will be dropped.

3.13. Unified Threat Management Application Control and URL Filtering

3.13.1. Features

Sungard AS will provide the following for the number of instances identified in the Order:

(a) Implementation of Customer-defined policies identifying, blocking or limiting access to, and usage of Customer-identified applications, URLs and vendor-defined content types.
(b) Execution of up to 10 policy changes (i.e., adds, moves or changes) per month.

3.13.2. General

Content identification and categorization is limited to and managed solely through a centralized database provided by the equipment vendor.

3.14. Web Application Firewall Service

3.14.1. Features

Sungard AS will provide the following Web application firewall (WAF) functionality in conjunction with the third-party delivered Service via download to the required hardware:

(a) HTTP monitoring to determine whether the monitored site(s) are available and responding to regular requests.
(b) HTTPS monitoring to determine whether the monitored site(s) are available and responding to regular requests.
(c) Inspection of and responses to all incoming Web traffic based on the applicable Customer-defined security policy.
(d) SSL client authentication, authorization and certificate forwarding to the back-end support.
(e) Threat and vulnerability signature updates.
(f) HTTPS termination and optional re-encryption of requests before being sent to the Web system.
(g) Customer-selected notification of detected threats (only if identified on the Order as ActiveWatch).
(h) Hosting of logs and policy configuration in Sungard AS' third-party service provider's data center.
(i) Access to the third-party Web portal for Service-related reports.
(j) Monitoring of Service availability.
(k) Hardware provision if identified on the Order.

3.14.2. General

Customer will:

(a) Report all operational and environment changes that may affect the performance of the Service, including, but not limited to, changes to network topology, network hardware, firewall rules and configuration and HTTP/HTTPS site code.
(b) Open specified ports on the Customer network to ensure that Sungard AS' third-party service provider has the connectivity required to deliver the Service.
(c) Provide necessary hardware that meets Sungard-AS-supported specifications, unless provided by Sungard AS as identified on the Order.
(d) Unless provided by Sungard AS under a separate Service, Customer will ensure that all physical connections and network configurations enable Sungard AS to monitor, maintain and administer the Web Application Firewall Service.

The Web Application Firewall Service security appliances can be installed within a Designated Sungard AS Facility or at a Customer facility. If the Services are provided for appliances installed in a Customer facility, Sungard AS will ship the appliances to the Customer specified facility and Customer will:

(a) Provide, monitor and manage all installation, power, network, physical and logical infrastructure, and security requirements necessary to support the appliances.
(b) Upon termination of the Service, Customer will uninstall, pack and return the security appliances in the same condition as received (normal wear and tear excepted) to Sungard AS pursuant to Sungard AS' reasonable instructions.

The Web Application Firewall Service is provided using a third-party Sungard AS subcontractor.

3.15. Security Information and Event Management ("SIEM") Services

3.15.1. Features

Sungard AS will provide the following for the number of events per second ("EPS") identified in Part 1 of the Order:

(a) Installation and configuration of the Security Information and Event Management (SIEM) solution in accordance with the completed CDR form.
(b) Configuration of SIEM correlation rules, including fine tuning of rules during the 30-day period following the initial configuration and implementation of Customer-requested changes to correlation rules.
(c) 24x7x365 security event monitoring and notification to Customer of detected alerts based on manufacturer- and customer-approved settings.
(d) Collection, retention, reporting (including agreed-upon custom reporting), and correlation of logs up to the quantity of GBs or TBs specified in Part 1 of the Order and available to Customer Portal.
(e) Storage of log data for the time period specified in Part 1 of the Order.

3.15.2. General

The SIEM security appliances can be installed within a Designated Sungard AS Facility or at a Customer facility. If the Services are provided for appliances installed in a Customer facility, Sungard AS will ship the appliances to the Customer-specified facility and Customer will:

(f) Provide, monitor and manage all installation, power, network, physical and logical infrastructure, and security requirements necessary to support the appliances.
(g) Upon termination of the Service, Customer will uninstall, pack and return the security appliances in the same condition as received (normal wear and tear excepted) to Sungard AS pursuant to Sungard AS' reasonable instructions.

4. SUPPORT SERVICES

4.1. Hardware Installation Services

4.1.1. Features

Sungard AS will perform the following for the number of original-equipment-manufacturer-supported (OEM-supported) hardware devices identified in the Order:

(a) Receiving, unpacking and installation of the hardware into computer racks or cabinets in accordance with the completed CDR form.
(b) Installation of network cables and cross-connects.

4.1.2. General

Customer will provide a hardware list and installation requirements (e.g., shelf location, special power requirements, etc.) and schedule prepaid delivery of hardware to the appropriate Designated Sungard AS Facility.

Sungard AS will notify Customer of receipt of Customer-shipped hardware. If Customer does not verify the equipment identified in Sungard AS' notice within 3 business days of receipt, Sungard AS may return the hardware to Customer at Customer's expense.

4.2. Equipment Management Services

4.2.1. Features

Sungard AS will perform the following for each piece of equipment identified in the Order:

(a) Engage maintenance vendors in the resolution of detected equipment failures.
(b) Coordinate vendor-provided preventative maintenance.
(c) Install vendor-provided firmware upgrades.

4.2.2. General

For all Customer-provided equipment and software, Customer will:

(a) Obtain and maintain 24x7 maintenance agreements for Customer-provided hardware (with 4-hour response time for hardware) and software that receives Equipment Management Services.
(b) Obtain the consent of the maintenance vendor allowing Sungard AS to act as Customer's agent.
(c) Provide Sungard AS with root or administrative security passwords, IDs and access.

Equipment Management Services do not include the resolution of disputes with maintenance vendors regarding the maintenance vendors' services.

5. SECURITY SERVICES SERVICE-LEVEL AGREEMENTS

5.1. Firewall, IDS and IPS Log Retention Service-Level Agreement (SLA)

Agreement: Sungard AS will provide Customer with online access to security logs in connection with the Service it has purchased (i.e., Firewall, IDS and/or IPS Services) for 90 days after the date of creation.

Remedy: If Sungard AS fails to meet the Firewall, IDS and IPS Log Retention SLA, Customer is entitled to a credit equal to 10% of the Order's Monthly Fee for each month in which the failure occurred.

5.2. IDS and IPS Security Alert

Agreement: Sungard AS will notify Customer of security events based on manufacturer- and Customer-approved settings within 15 minutes of Sungard AS' detection and identification of the major event.

Remedy: If Sungard AS fails to meet the Security Alert SLA, Customer is entitled to a credit equal to10% of the Order's Monthly Fee for each month in which the failure occurred.

5.3. Threat Manager and Log Manager Availability

Agreement: The Threat Manager and Log Manager Service will be available to monitor, analyze and log security events (each as applicable) 99.9% of the time measured on a monthly basis.

Remedy: If Sungard AS fails to meet the Threat Manager and Log Manager Availability SLA, Customer is entitled to a credit equal to 10% of the Order's Monthly Fee for each month in which the failure occurred.

5.4. Threat Manager ActiveWatch Escalation SLA

Agreement: Escalation to an IDS analyst will take place within 30 minutes of an attack or vulnerability being detected by the Threat Manager Service.

Remedy: If Sungard AS fails to meet the Threat Manager ActiveWatch SLA, Customer is entitled to a credit equal to 10% of the Order's Monthly Fee for each month in which the failure occurred.

5.5. Security Services: Web Application Firewall Services Availability

Agreement: The Web Application Firewall Service will be available 99.9% of the time measured on a monthly basis.

Remedy: If Sungard AS fails to meet the Web Application Firewall Services Availability SLA, Customer is entitled to a credit equal to 10% of the Order's Monthly Fee for each month in which the failure occurred.

6. NOTIFICATION SERVICE-LEVEL AGREEMENT

6.1. Services — Notification

Agreement: Sungard AS will notify Customer, in the manner requested by Customer in the Customer Portal, within 15 minutes after Sungard AS has conducted reasonable preliminary investigation verifying that the Services or Customer equipment monitored by the Services are unavailable.

Remedy: If Sungard AS fails to meet the Notification SLA, Customer is entitled to a credit equal to 3% of the Order's Monthly Fee for each failure in that month. In the event that Customer notifies Sungard AS, within the 15-minute period, regarding unavailability of equipment or Services, this remedy is not operational.

7. GENERAL SERVICE TERMS

These Services are also subject to the General Service Terms at https://www.sungardas.com/hubfs/_multimedia/document-file/sungardas-general-service-terms.pdf.