Managed Detection and Response Service Terms

1. DEFINITIONS

"**Alert Logic**" refers to Alert Logic, Inc., Sungard AS' designated third-party provider of the Managed Detection and Response Services.

"**Designated Contacts**" refers to Customer-nominated support contacts whose details will be registered with Alert Logic, a copy of which may be provided to Sungard AS by Alert Logic.

"**Downtime**" refers to the minutes during the month that the MDR — Professional Service or Managed WAF Service is not available (including Excluded Downtime).

"**Excluded Downtime**" shall have the meaning as set forth in the Service Levels section below.

"**Total Minutes**" refers to the number of minutes in a calendar month.

2. MANAGED DETECTION AND RESPONSE — PROFESSIONAL

2.1. Features

The Managed Detection and Response (MDR) — Professional Service delivers 24x7 threat detection and incident management. MDR — Professional Service includes:

- **Network Monitoring**: A significant source of threat data is obtained through monitoring the network traffic between systems. This data is collected using a direct connection to switches (via a port mirror or span port) or via the Alert Logic agent and processed by the network appliance.
- **Log Data Monitoring**: Alert Logic provides services and systems to ingest, parse and store logs from Customer's systems to help support Customer compliance and analysis requirements, and to help support Alert Logic's threat detection and compliance services. Log data monitoring includes 100MB/day/node of log data analysis and storage for log data and log retention for one (1) year.
- **Cloud Security Service Integration**: Alert Logic is integrated with Amazon Web Services (AWS) and Microsoft Azure using log and application programming interface (API) methods.
- **Cloud Change Monitoring**: By analyzing changes to cloud environments through the ingestion of logs, configuration changes can generate incidents that are escalated to Customer.
- **User Behavior Monitoring**: User behavior anomaly detection (UBAD) helps to detect and alert for suspicious user activity in enterprise environments. Machine-learning determines baselines in AWS, Azure and Office 365.
- **File Integrity Monitoring**: By analyzing changes to files in Customer's environments, file integrity monitoring can identify anomalies or threats that may attach to existing OS files.
- **MDR — Essential Service**: Alert Logic monitors Customer's Windows and Mac endpoints using a dedicated agent that employs machine-learning and behavioral analytics to monitor and isolate endpoint attacks at the earliest opportunity, including so-called "zero-day" threats.

2.2. Service Levels

Monthly Uptime Percentage of Availability	Service Credit Percentage of Monthly Fees Attributable to the MDR — Professional Service
<99.5%	3.50%
<98.5%	7.00%
<97.5%	10.50%
<96.5%	14.00%
<95.5%	17.50%

Table 1. Reliability for Hosted Services

$$\textbf{Availability} = 100 \text{ X } \frac{\text{Total Minutes-Downtime}}{\text{Total Minutes-Excluded Downtime}}$$

"**Excluded Downtime**" includes:

- Planned downtime minutes for the month
- Any period for which Alert Logic provides at least three (3) days of advance notice that the Service will be unavailable
- Any unavailability caused by circumstances beyond Sungard AS' or Alert Logic's reasonable control, including, without limitation:

  i. Force majeure
  ii. Computer or telecommunications failures or delays involving hardware or software not within Sungard AS' possession or reasonable control
  iii. Network intrusions or denial-of-service attacks
  iv. Customer-supplied hardware, software or materials
  v. Any acts or omissions of Customer or its agents, including, without limitation, failure to provide up-to-date Secure Sockets Layer (SSL) certifications and keys

Monthly Failures	Service Credit Percentage of Monthly Fees Attributable to the MDR — Professional Service
Fewer than 5	7.00%
5 or more	17.50%

Table 2. MDR — Professional 15-Minute Escalation Commitment

Alert Logic will escalate detected security incidents within 15 minutes of detection. The 15-minute time period consists of the time between system detection of a security incident and the time the security incident is escalated to Customer via automated system log or phone call.

Monthly Failures	Service Credit Percentage of Monthly Fees Attributable to the MDR — Professional Service
Fewer than 5	7.00%
5 or more	17.50%

Table 3. Review Services 24-Hour Reporting Commitment

MDR Professional and MDR Enterprise include a review of logs at least once during every 24-hour period. Alert Logic will escalate any potential security incidents that are detected during the review process. Review activity will be accessible online by Customer.

Monthly Failures	Service Credit Percentage of Monthly Fees Attributable to the MDR — Professional Service
Fewer than 5	0.70%
5 or more	1.40%

Table 4. Submitted Service Request 2-Hour Email Response Commitment

Alert Logic will respond to support requests submitted by Customer via web portal or telephone within two (2) hours of receipt and will resolve or escalate properly submitted service requests within 24 hours of receipt.

Monthly Failures	Service Credit Percentage of Monthly Fees Attributable to the MDR — Professional Service
Fewer than 5 occurrences	7.00%

Monthly Failures	Service Credit Percentage of Monthly Fees Attributable to the MDR — Professional Service
5 or more occurrences	17.50%

Table 5. Inline Device Service 15-Minute Commitment

3. MANAGED DETECTION AND RESPONSE — ESSENTIAL

3.1. Features

Managed Detection and Response (MDR) — Essential Services provides 24x7 platform support with troubleshooting deployments, user interface and general product queries such as console support, agent installation, the configuration of alerts, appliance management, vulnerability scanning configuration and output. MDR — Essential includes:

- **Endpoint Detection**: Alert Logic monitors Customer Windows and Mac endpoints using a dedicated agent that employs machine-learning and behavioral analytics to monitor and isolate endpoint attacks at the earliest opportunity, including so-called “zero-day” threats.
- **Internal and External Vulnerability Scanning**: Alert Logic uses vulnerability scanning information to identify vulnerable customers for proactive notification of increased risks based on threat intelligence and emerging threats.
- **PCI Scanning**: Alert Logic provides technology and services that enable Customer to meet the Payment Card Industry Data Security Standard (PCI DSS) 3.2 compliance mandate, including scanning.
- **Cloud Configuration Checks**: Alert Logic performs security remediation when issues related to the configuration of cloud services have been identified during a scan, from cloud logs or via cloud APIs.
- **Cloud CIS Benchmarks**: Alert Logic provides real-time reporting based on industry-standard Center for Internet Security (CIS) benchmarks for AWS and Microsoft Azure.

4. MANAGED DETECTION AND RESPONSE — ENTERPRISE

4.1. Features

The Managed Detection and Response (MDR) — Enterprise Service is an optional enhancement to the MDR — Professional Service that, if selected by Customer, must be separately contracted for in an Order. MDR Enterprise Service provides access to a security analyst who helps ensure Customer’s threat response is aligned with Customer’s environment and expectations. The security analyst also will carry out several on-request and proactive activities to enhance the MDR — Professional Service. These on-request and proactive activities include:

- **Continuous Threat Hunting**: Alert Logic will conduct periodic threat hunting activities and, after significant security events, generate additional customer value through the identification of new or emerging threats, or identify potential threats that cannot be identified by automation alone.
- **Proactive Tuning and Sensor Optimization**: A security analyst will review recent incidents, intrusion detection system (IDS) events and logs in any known context of Customer’s environment and look to identify any trends or high-volume activity that could be considered “noisy” to Customer.
- **Extended Security Investigations**: Upon identification or suspicion of a threat or attack against its infrastructure, Customer may request assistance from Alert Logic’s security analyst to analyze data from the affected environment to ascertain and report upon the legitimacy of the suspected threat and/or its impact.
- **Weekly Security Review**: A weekly call with Customer to discuss the findings of the data acquired that relate to its current security posture. Additional topics from a consultative standpoint also will be discussed.

- **Annual Onsite**: The designated security analyst will visit Customer sites once per year, or as otherwise agreed to by the Parties, to hold in-depth meetings, meet key stakeholders and build relationships to foster a collaborative approach to protecting Customer's systems.

4.2. Service Levels

Monthly Failures	Service Credit Percentage of Monthly Fees Attributable to the MDR — Enterprise Service
Fewer than 5	7.00%
5 or more	17.50%

Table 6. Review Services 24-Hour Reporting Commitment

MDR — Enterprise includes review of logs at least once during every 24-hour period. Alert Logic will escalate any potential security incidents that are detected during the review process. Review activity will be accessible online by Customer.

Monthly Failures	Service Credit Percentage of Monthly Fees Attributable to the MDR — Enterprise Service
Fewer than 5	0.70%
5 or more	1.40%

Table 7. Submitted Service Request 2-Hour Email Response Commitment

5. MANAGED WEB APPLICATION FIREWALL SERVICE

5.1. Features

The Managed Web Application Firewall (WAF) Service ("Managed WAF Service") is a managed security service that provides inline web application protection by detecting and blocking potential threats from reaching Customer's web applications.

The Managed WAF Service includes:

- ActiveWatch™ Services that leverage ActiveIntelligence, web application security experts:
  - ActiveIntelligence consists of security researchers and threat intelligence analysts who work together to create and manage security content. This content enables the Service to identify incidents that require review by the ActiveWatch™ team while filtering out irrelevant security events.
  - ActiveWatch™ is the human component to monitoring and investigating incoming events based on the service provided (i.e., log analytics, intrusion detection system (IDS) and Managed WAF)
- Access to a security analyst to provide Customer with application policy configuration, tuning, guidance and assistance with analysis of potential web application security issues.

5.2. Service Levels

Monthly Uptime Percentage of Availability	Service Credit Percentage of Monthly Fees Associated with the Managed WAF Service
<99.5%	3.00%
<98.5%	7.50%

Monthly Uptime Percentage of Availability	Service Credit Percentage of Monthly Fees Associated with the Managed WAF Service
<97.5%	10.50%
<96.5%	14.00%
<95.5%	17.50%

Table 8. Reliability for Hosted Services

For purposes of the above service levels detailed in the table, Monthly Fees refer to the month in which the Service failed to perform in accordance with a service level as set forth below.

$$\textbf{Availability} = 100 \text{ X } \frac{\text{Total Minutes-Downtime}}{\text{Total Minutes-Excluded Downtime}}$$

Monthly Failures	Service Credit Percentage of Monthly Fees Associated with the Managed WAF Service
Fewer than 5	0.70%
5 or more	1.40%

Table 9. Submitted Service Request 2-Hour Email Response Commitment

Alert Logic will respond to support requests submitted by Customer via web portal or telephone within 2 hours of receipt and will resolve or escalate properly submitted service requests within 24 hours of receipt.

Monthly Failures	Service Credit Percentage of Monthly Fees Associated with the Managed WAF Service
Fewer than 5 occurrences	7.00%
5 or more occurrences	17.50%

Table 10. Inline Device Service 15-Minute Commitment

Alert Logic will respond to support requests for inline devices submitted by Customer via web portal or telephone within 15 minutes of receipt. The inline devices must be online and accessible to Alert Logic for support to be provided. For support requests related to potential block events, Customer must provide Alert Logic with the Request ID found on the blocking page of each managed website within Web Security Managers configuration and management interface. This can be accessed through the Alert Logic Portal.

6. ADDITIONAL TERMS

6.1. General

6.1.1. Overages

In the event Customer contracts for the MDR — Professional Service and uses Services in excess of the entitled amount identified on the Order by more than twenty percent (20%), Sungard AS may notify Customer of the excess usage and request that usage is reduced to align with entitlement. If after sixty (60) days, usage remains above entitlement, Sungard AS may commence billing Customer for excess usage at the same fee as is charged under the current Order or, at Sungard AS' sole discretion, at a higher or different tier of service. Charges for over-usage will apply from the date of notification through the end of the Initial Term or Renewal Term. Overage fees will be invoiced separately on the first invoice subsequent to the fees being incurred.

6.1.2. EULA

The Services under this Order are provided by Alert Logic and are subject to Alert Logic's end-user license agreement (EULA) available at https://www.alertlogic.com/docs/alert-logic-end-user-license-agreement.pdf. By entering into the Order, Customer agrees to be bound by the EULA's terms and conditions.

6.1.3. Restricted Rights

If Customer uses the Services and documentation by or for any unit or agency of the US Government, the Services and any related documentation are provided with Restricted Rights. Use, duplication or disclosure by the US Government is subject to the restrictions set forth in FAR 12.212 and DFAR 227.7202.

6.1.4. Noncontrolled Networks

Customer recognizes that the Internet consists of multiple participating networks that are separately owned and, therefore, are not subject to the control of Alert Logic (such networks being "Noncontrolled Networks"). Malfunction or cessation of Internet services by Internet service providers or of any of the networks that form the Internet may make the services temporarily or permanently unavailable. Customer agrees that Sungard AS shall not have any liability whatsoever when the services are temporarily or permanently unavailable due to non-availability of Noncontrolled Networks, including due to malfunction or cessation of Internet services by network(s) or Internet service providers not subject to the control of Alert Logic, or due to any accident or misuse by Customer. These limitations shall apply notwithstanding the failure of the essential purpose of any limited remedy.

6.1.5. Limitation on Liability

Notwithstanding anything to the contrary, Sungard AS' liability for a breach of its obligations relating to confidential information, information security or personal data (including, but not limited to, compliance with applicable data protection laws such as General Data Protection Regulation — GDPR) for the MDR Services shall be limited in the aggregate to a maximum liability cap five (5) times the fees paid by Customer to Sungard AS for the MDR Services in the 12 months prior to the time the cause of action accrued.

6.1.6. Use of Contact Information

Sungard AS may share certain limited contact information (e.g., customer name and contact information, including name, phone number and email address) with Alert Logic to deliver the MDR Services. By entering into this Order, Customer consents to Sungard AS' collection, use and disclosure of such contact information.

6.2. Service Levels: General

Alert Logic will provide Customer with reasonable advance notice of any planned maintenance occurring outside of the scheduled maintenance window. Alert Logic will provide Customer with advance notice of unplanned maintenance, if possible.

6.3. Service Levels: Exclusions

Notwithstanding anything to the contrary, including the terms set forth in the General Service Terms, Service levels will not apply to the following circumstances:

- During any trial periods, periods of planned maintenance, periods of non-availability due to a force majeure, or periods of suspension of Service by Alert Logic in accordance with the Agreement.
- Customer is not in compliance with the Agreement, including these Service Terms.
- A denial-of-service attack from a third party or one that is perpetuated by or through Customer which causes a denial-of-service attack to occur on Alert Logic's systems or networks (or any similar event).
- Customer is unable to access the Internet due to circumstances outside of Sungard AS' or Alert Logic's reasonable control.
- Customer's environment (as applicable) is not properly configured or where Customer or Customer's agent has disabled one or more sensors.
- Customer has not provided up-to-date SSL certificates and keys for Alert Logic to tune or configure Web Security Manager and Threat Manager products for monitoring and protection of HTTPS traffic. Sungard AS is not responsible if Customer fails to provide up-to-date certificates and keys.
- Performance delays or failure of the Services caused by:
    - Equipment, software, systems, services or data not provided by Sungard AS or Alert Logic
    - Acts or omissions of Customer or Customer's agent that violate the terms of the Agreement
- For MDR — Professional and MDR — Enterprise instances deployed on Customer's or a third party's hardware, Sungard AS will not be responsible for any hardware-related issues and, if not deployed on the most-current minimum recommended hardware specifications, Sungard AS will not be responsible for supporting degradation of performance.
- Sungard AS or Alert Logic's delay in providing or inability to provide support due to Customer's failure to maintain accurate and complete information regarding the Designated Contacts.

6.4. Service Levels: Remedy

In the event that Alert Logic fails to provide a Service at the level required by the service levels above, the sole and exclusive remedy for Customer, and Sungard AS' sole and exclusive liability, are as set forth herein (the "Remedy"). The Remedy is not cumulative with any other obligation that Sungard AS may have under the Agreement.

For Services purchased as part of a suite or bundle, the service credit will be based on the pro-rata portion of the cost of the applicable Service which did not meet the service-level requirement, as determined by Sungard AS in its reasonable discretion. If fees are paid annually or quarterly, the service credit will be pro-rated to the monthly value. Service credits will be applied to Customer's next Sungard AS invoice.

In addition to any service credits owed to Customer hereunder, the Remedy includes the right for Customer to terminate the Order in the event that Alert Logic fails to meet any stated service levels for five (5) consecutive months.

The aggregate maximum service credit for any and all failures to provide Services at the level required that occur in a single calendar month shall not exceed one calendar month of service credit. If Customer is late in making any undisputed payments owing pursuant to the Agreement at the time of the occurrence which would otherwise entitle Customer to a Remedy, no such Remedy shall be available to Customer.

Customer must notify Sungard AS within 30 days from the Service failure to be eligible for the Remedy. Failure to comply with this requirement will forfeit Customer's right to receive such Remedy.

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.