Service Description:
Atlas Advanced Package

1. Overview

eSentire's Atlas Advanced Package (the "**Package**") is a managed detection and response ("**MDR**") solution that leverages the eSentire Atlas Platform to provide cybersecurity insights, along with threat prevention, detection, mitigation, response, and remediation. eSentire uses Client Data from various sources within the Client Environment to provide a comprehensive MDR solution. Specific elements of the Package are described herein, and the Package is scoped using the total number of Client-nominated servers, laptops, and desktop devices with supported operating systems ("**Endpoints**"). The number of Endpoints included in the Client Package are detailed on the Order Form and subject to Overages.

2. Service Definitions

In addition to the below, any capitalized terms contained in this service description are as defined herein:

- "**Atlas Platform**" means eSentire XDR platform which consolidates all data and drives workflow for all eSentire MDR services, including those in this Package. All data on the Atlas Platform, related to the delivery of the Package for Client, is retained for the Term, and deleted upon Package expiration.
- "**Client Data**" means, unless otherwise defined in the underlying terms and conditions referenced in the Order Form, (a) data, records, files of Client including e-mail sent or received by personnel of Client, and (b) all reports generated for or by Client as a result of the provision or use of the services included in the Package, except to the extent such reports contain intellectual property of eSentire.
- "**Indicators of Compromise (IOCs)**" means distinctive elements of data used to detect potential security breaches or malicious actions.
- "**Insight Portal**" means the Client interface into the Atlas Platform, where eSentire provides Client service overview, detailed threat case reporting and/or event summaries.
- "**MDR Services**" means the Endpoint Services, Log Services, and Network Services (if selected) included in this Package.
- "**Order Form**" means an ordering document, executed by the parties, that specifies services ordered by Client, including any amendments and supplements thereto.
- "**Threat Research & Intelligence Briefing**" means a curated monthly brief provided to Client on known and emerging cyber threats (i.e., malware, phishing campaigns, ransomware attacks, and other malicious activities) interspersed with time-sensitive updates about significant developments in the threat landscape.
- "**Term**" is defined on the Order Form during which time eSentire will deliver the Package described herein.

3. Package Elements

The Package consists of the following elements:

- collection of Client Data (including endpoint data, log data, and network data (if selected)) from Client systems (referred to herein as the "**Client Environment**") based on total Endpoints;
  - Limited to not more than 5,000 total Endpoints (actual quantity ordered detailed on Order Form);
- threat prevention and detection;
- security investigation of alerts detected via the Atlas Platform by eSentire security analysts;
- threat incident handling, reporting, hunting, and response (as required);
- access to Threat Research and Intelligence Briefings;
- support from the eSentire Cyber Resilience Team; and
- access to eSentire Insight Portal for access to reporting, and package features.

Client-specific selections for the Package are identified on the Order Form.

4. Access and Onboarding

Following receipt of a fully executed Order Form, a member of the eSentire Cyber Resilience Team (see **section 6** below) will work with Client to begin Package onboarding activities, which will include:

- assigning an eSentire onboarding manager and scheduling the initial onboarding call;
- establishing the onboarding project plan;
- deploying network or scanning appliances (ordered separately if applicable);
- connecting telemetry sources (including logs, enrichment and other data sources); and
- configuring integrations to Client applications.

Client will also be provided with access to the Insight Portal, which provides visibility over all subscribed eSentire services. The Insight Portal acts as a central hub for managing and monitoring security services, allowing Client to configure, integrate, and view eSentire Package elements in real-time. The Insight Portal includes self-service features such as:

- telemetry integration;
- collector configuration; and
- service setup.

Telemetry sources are further detailed below, and if appliances/sensors provided by eSentire ("**eSentire Equipment**") are required as part of Client Data collection, such eSentire Equipment will be listed on the Order Form. Client will be required to assist with accessing telemetry, installing applicable licensed software tools, or installing required eSentire Equipment. Telemetry sources include:

4.1. Endpoint (referred to on the Order Form within the Package as "**Endpoint Services**")

eSentire will collect in-scope Client endpoint data. Client may choose to (i) utilize a fully managed endpoint solution leveraging either the eSentire Agent or CrowdStrike licensed tools (eSentire is the license holder; each such fully managed solution an "**MSSP**" solution), or (ii) provide eSentire with access to its Client-licensed and eSentire-approved endpoint tools (referred to as an "**Managed-Only**" solution) already deployed in the Client environment (supportable endpoint tools include those offered by CrowdStrike, Microsoft, or SentinelOne, and each a "**Product Publisher**"). If Client selects the eSentire Agent as the MSSP solution, the eSentire Agent will collect endpoint telemetry and will generate endpoint detection and response ("**EDR**") alerts. Agent EDR alerts are stored in the Atlas Platform for the Term. Agent raw telemetry is stored on the Atlas Platform for 15 days. EDR alerts from supported Product Publisher technologies are stored in the Atlas platform for the Term, while raw telemetry collected by the applicable Product Publisher technologies will be stored on the cloud platform of the applicable Product Publisher for 15 days (in the case of an MSSP solution) or as defined by the Client (in the case of a Managed-Only solution). Client will also have the option of co-deploying the eSentire Agent alongside CrowdStrike tools in the MSSP solution (note when eSentire Agent is co-deployed, Agent EDR alerts are not collected or stored, Agent raw telemetry is stored on the Atlas Platform for 15 days). License requirements for solution types are described below.

4.2. Log (referred to on the Order Form within the Package as "**Log Services**")

eSentire will leverage Client log data and will perform real-time analytics on up to 10 approved log sources, to be identified by eSentire during onboarding. The Package includes unlimited log collection from those Client security controls, systems and applications deemed relevant by eSentire to its delivery of the Package. Log and audit data is stored in the SIEM/log module of the Atlas Platform and is retained for 365 days (or until the Package expires, whichever is first). Client may order additional online log storage retention for up to five years (or until the Package expires, whichever is first), and if requested will be listed on the Order Form in a separate section outside of the Package fees, and service table. The Package includes an MSSP log solution.

4.3. Network (referred to on the Order Form within the Package as "**Network Services**" or "**Threat Intelligence**")

In the standard Package configuration, eSentire will access the Client Environment in order to provide real-time capture and monitoring of network traffic, leveraging an MSSP network solution. Client will be required to install eSentire network sensors to capture a TAP or SPAN of network traffic. Network sensors capture network packets and metadata, which are stored on the network sensor inside the network environment where each sensor is deployed (physical appliance or virtual machine). Each network sensor will generate network alerts, which are stored in the Atlas Platform for the Term. Such sensors are eSentire Equipment and will be either physical or virtual appliances located at select locations in the Client Environment (generally co-located with Client firewalls), and if required/requested will be listed on the Order Form in a separate section outside of the Package fees, and service table.

Alternatively, if Client elects not to provide network telemetry, Client may receive eSentire's Threat Intelligence feed in a standardized format. Client may then ingest such feed into Client's security tools such as a TIP, firewall, email server, or endpoint technology, to enhance such tools with high value and up-to-date IOCs.

Client selections are detailed on the Order Form.

5. Package Deliverables

The following will be delivered to Client as part of the Package:

5.1. eSentire SOC and Security Analysts. An eSentire security analyst operating in an eSentire Security Operations Center ("**SOC**") will utilize the telemetry gathered from the sources described in **section 4** above to perform detailed security investigations of alerts detected via the Atlas Platform. Security analysts provide 24x7x365 monitoring and reaction to identify, investigate, and (where appropriate) prevent or contain potential Client threats. eSentire technical support is also available for Client assistance with the technologies directly linked and supporting the delivery of Packaged services. Such technical support is available 8am x 5pm EST, with the availability of support outside of these defined hours.

5.2. Unlimited Incident Handling. eSentire security analysts will perform incident handling for all security incidents. Incident handling includes detecting, analyzing, containing, and assisting in the recovery from security incidents, and may involve attempted isolation of compromised assets, disruption of attacker activities, termination of malicious processes, and severing of command-and-control connections. Security analysts also provide remediation guidance, investigate the initial access vector, and check for potential data exfiltration. Core objectives include:

- suppressing and containing threats before further damage occurs;
- investigating and neutralizing threats to prevent their continued operation;
- utilizing the deployed MDR Services to conduct investigations; and
- identifying root causes where possible.

In addition, eSentire also provides containment and remediation recommendations and, when necessary, defers to eSentire or third-party digital forensics/incident response ("**DFIR**") services (not included in the Package) when an incident cannot be fully contained through MDR alone or has other complicating factors (e.g., litigation, visibility, forensics, etc.).

5.2.1. Incident Handling Process:

When the Atlas Platform generates an indicator of a potential threat eSentire begins an investigation. An investigation includes validating the presence of a threat via Client telemetry and evidence data, threat intelligence, and other data and information sources within the Atlas Platform. Using this information and the automation capabilities of the Atlas Platform, a security analyst then determines the nature and extent of any compromise that may have occurred. Depending on the nature of the potential threat, activities conducted during the incident handling process may include:

- Threat analysis:
  - Assessment of the malicious nature of a threat and its potential impact.
  - Categorization according to industry essential practice frameworks including MITRE ATT&CK.
  - Contextualisation of validated threats based on factors such as industry vertical and geopolitical context.
- Threat hunting across Client's telemetry data which has been ingested into the Atlas Platform.
- Threat response actions taken per Client's previously configured response protocols.

- Recommendation to Client of a suggested response covering suggested next steps, and remediation activities as required.

After remediation, a summary of findings will be provided to Client, detailing evidence, and timelines. Throughout the process, corrective action tracking will be maintained. Upon completion of the incident handling processes, should Client defer to eSentire DFIR services or engage a third-party DFIR firm, eSentire will provide the Advanced findings of its investigation, including acquired forensic artifacts (if possible).

6. Cyber Resilience Team Support

As part of the Package, Client will receive ongoing service support and technical and commercial relationship management by eSentire's Cyber Resilience Team, which will assist Client with maximizing the benefits of the Package ("**Support**"). The Support deliverables provided as part of the Package will include:

6.1. Onboarding Support: eSentire's Cyber Resilience Team will provide guidance and a personalized setup of the Package elements ordered. This Support will assist Client with the deployment, integration of Package services into Client's existing infrastructure, establish meeting cadences, and set clear expectations. See **section 4** above for additional details.

6.2. Reporting and Reviews: In addition to eSentire's Threat Research and Intelligence Briefings, Client will receive regular reporting provided by the Cyber Resilience Team through:

- automated reports available via the Insight Portal;
- support from a pooled relationship manager; and
- quarterly review meetings which will include:
  - Operational Assessment
    - Current Package services utilization
    - Alert analysis and significant security incident review
    - Verification of contact information and escalation procedures
  - Security Updates
    - Threat Intelligence briefing on emerging threats
    - Relevant security advisories
  - Service Management
    - Performance metrics review
    - Service improvement recommendations
    - Client feedback collection

7. License Requirements

For Packaged services being provided in a MSSP capacity: where applicable, eSentire will procure all required licensing directly with the Product Publisher; eSentire will be the licensee of record with each Product Publisher; and eSentire will manage any such licensed solutions provided by Product Publisher. As the license holder, eSentire may grant Client enhanced access into eSentire's licensed environment. In the event such access is granted: Client acknowledges and agrees that any changes made by Client in the licensed environment could impair eSentire's ability to deliver the Package; Client accepts responsibility for such changes; and Client releases eSentire from its obligations to deliver the Package to the extent of such impairment.

For Endpoint Services being provided in a Managed-Only capacity, eSentire will manage Client's endpoint licensing. Client is responsible to procure and maintain its endpoint licensing directly with an approved Product Publisher (options listed below) during the entire Term, and to coordinate proper licensing permissions with such Product Publisher to allow eSentire full administrative access and credentials into Client's licensed environment. Client must purchase the following applicable licenses in order for eSentire to support Client in a Managed-Only capacity:

- CrowdStrike Managed-Only - requires Falcon Insight XDR + CrowdStrike Falcon Prevent + Threat Graph Standard
- Microsoft Managed-Only - requires Microsoft Defender for Endpoint Plan 2
- SentinelOne Managed-Only - requires Singularity Advanced (also recommended at least 14 Days retention ("**Deep Visibility**") to enable threat hunting)

8. Package Services General Information

The following information applies to this Package:

8.1. Client Responsibilities. General Client responsibilities for Packages are listed below. Client must comply with Client responsibilities in order for eSentire to meet its obligations and deliver services. Client Responsibilities are as follows:

- Client is responsible for all Client provided third-party equipment, software services, support, or vendors not under the control of eSentire.
- Client should respond to alerts and inquiries from eSentire in a timely fashion.
- Client should identify prior issues with Client's network to the eSentire team prior to Packaged services commencing (including any incidents, problems, errors, or other events subject to an open support ticket from a legacy or other third-party service provider).
- Client is responsible for implementing any recommendations or remediation advice provided by eSentire related to Client incidents, however, Client's decision to not implement any remediation recommendations may adversely impact eSentire's ability to deliver the Package.
- Client should communicate and coordinate any required changes to the Client network or other component required for the Packaged services to be delivered, prior to making any changes.
- Client may be provided with a level of administrative access to Packaged services for Client and its affiliates, professional advisors, service providers and agents (collectively, "**Representatives**"). Such administrative access may include, by way of example, access to portals or dashboards used to access Client Data or configure and control the Packaged services. Client acknowledges that, in addition to actions Client takes with respect to its own systems, actions that Client or its Representatives take utilizing such administrative access to Packaged services may impair eSentire's ability to provide the Package. In such case and to the extent of any such impairment, Client assumes full responsibility for such actions and releases eSentire from any (i) obligations to provide the impaired Packaged services or (ii) liability for the failure to provide such Packaged services.

8.2. MDR Service Level Objectives ("**SLOs**"). eSentire measures a set of internal objectives that apply to MDR Services. For each SLO, a minimum of 20 Threat Cases must be processed during the month for the SLO to apply. These eSentire standards are further described below. Defined terms for this **section 8.2** are as follows:

- "**Work Item**" means a collection of one or more events and alerts collected by the Atlas Platform requiring analysis by eSentire SOC Analysts.
- "**Actionable**" means a Work Item analysis has concluded that an alert or containment action is required, based on criteria established by eSentire and reviewed with Client.
- "**Threat Case**" means an Actionable Work Item, which results in a notification or action required.
- "**SOC Dashboard**" means the eSentire SOC interface into the Atlas Platform

8.2.1. Time to Engage ("**TTE**") – Work Item – SLO target 60 minutes:
The Service Level Indicator ("**SLI**") time starts when a Work Item is created in the SOC Dashboard and ends when an eSentire SOC Analyst changes the state of the Work Item in the SOC Dashboard to "under review". A Work Item is marked "under review" in the SOC Dashboard, when analysis of the Work Item by an eSentire SOC Analyst has commenced. The analysis includes collecting evidence and creating assessment notes against the Work Item. The outcome or duration of the analysis does not impact the TTE SLO target.

8.2.2. Time to Respond ("**TTR**") – Actionable Work Item – SLO Target based on Priority Level (Table 1):
As a result of the Work Item analysis described above, eSentire will determine if a Work Item is Actionable, and if so, will create a Threat Case. eSentire will then notify Client via the Insight Portal, and email, of any Threat Case. The SLI starts when a Threat Case has been created in the SOC Dashboard and ends when an eSentire SOC Analyst notifies the Client and provides the Client defined response remediation actions.

Table 1.

Priority Level	TTR SLO Target[1]
P1	10 minutes
P2	20 minutes
P3	40 minutes
P4	60 minutes
[1]SLO Target is measured as a monthly aggregate by priority level, taking into consideration all actionable Threat Cases from the previous month.	

The Priority Levels listed above are defined below (see Table 2).

Table 2.

Priority Level	Description
P4 (Low)	Minor activity recorded but not alerted, and the presence of likely unwanted activity - for example, adware.
P3 (Medium)	Suspicious activity that might not be deemed malicious by itself, and malicious activity not known to be targeted.
P2 (High)	Malware event, tactics, techniques, and procedure events, or events indicating targeted attack with potential for widespread impact.
P1 (Critical)	Malware infection(s), virus infection(s), and lateral movement, or indications of targeted attack with a high potential to cause grave damage to critical assets.

eSentire objectives listed above may be impacted by short periods due to scheduled maintenance where updates, patches, are installed and configured (i.e., maintenance windows), or when hardware deployment or replacements are required.

8.3. Add-on's. Client may order from eSentire additional licensed offerings outside of those included in or required or supported by the Packaged services ("**Add-Ons**"). Any such Add-Ons will be provided for Client use, but other than as described below, do not include any eSentire support or configuration assistance. Such Add-On's are only available to Client, when Client is being supported in an MSSP support model, eSentire is considered the licensee of such Add-Ons (referred to on the Order Form as an "**MSSP Add-on**" or "**Add-on**") and eSentire will provide access and documentation to Client. Client can request assistance with such MSSP Add-ons from eSentire, and eSentire will open a ticket with Product Publisher. Add-on's will be listed on the Order Form in a separate section outside of the Package fees, and service table.

8.4. eSentire Equipment. If Client is provisioned with eSentire Equipment, eSentire shall maintain the hardware and software for all eSentire-provided devices including any sensor. eSentire will ship replacements of failed components and receipt of replacements or failed components is subject to local custom or similar procedures. This maintenance policy does not apply to hardware provided by Client's organization. Shipping of replacement parts or systems for eSentire provided devices is included with the existing sensor fees. This replacement policy does not apply if the eSentire-provided hardware is damaged or lost through fire, theft or misuse. In the event of loss of eSentire-provided hardware through fire, theft or misuse, Client is responsible for the cost and shipping of the replacement. When eSentire Equipment is required to facilitate access to certain telemetry, such eSentire Equipment will be listed on the Order Form in a separate section outside of the Package fees, and service table.

8.5. eSentire Support. Client may contact the eSentire SOC related to eSentire services at any time by any of the following methods:

Method	Contact Information
Phone (North America)	+1-844-552-5837(Toll Free)
Phone (Direct-to-SOC Toll Outside of North America)	+353 21 4757102 (toll)
Phone (United Kingdom)	0800-044-3242 (Toll Free)
Email (Worldwide)	esoc@esentire.com
Mobile Application	per downloaded mobile application and associated instructions

Issue Tracking. eSentire maintains a ticketing system to handle all incoming contact from Clients. As such, eSentire keeps a log of all support calls and emails received from Client. Information to be included in this log include the name and location of the Client employee or contractor, eSentire security analyst involved, the date and time of the contact, the time to resolve the logged issue and details of the issue. This process is audited each year by eSentire's external auditors for SOC2 compliance.

8.6. Package Overages. Packages are scoped/sold using Endpoint totals, and the quantity is detailed on the Order Form. Should Client's number of Endpoints active as a daily average exceed 10% of the purchased value (measured on an average over one calendar month), notwithstanding any security event (the "**Overage**"), then Client will either (i) take steps to remove Endpoints within 30 Days of such Overage, or (ii) move to the next Package tier, and associated fees, to accommodate its usage for the remainder of the Term.

8.7. Product Publisher Flow Down Terms. If Client has ordered Services to be delivered as an MSSP solution, eSentire owns the licensing directly with the Product Publisher, and eSentire has an obligation to ensure Client agrees to flow down provisions applicable to the licensing. These flow down provisions are not negotiable and are required by the Product Publisher as written. In such case, Client agrees to the following Product Publisher flow down provisions:

8.7.1 Product Publisher – CrowdStrike, Inc. flow down provisions (if selected as the Endpoint Service solution):

8.7.1.1 Access & Use Rights. Client has a non-exclusive, non-transferable, non-sublicensable license to access and use the Product in accordance with any applicable Documentation solely for Client's Internal Use. Furthermore, if Client purchases a subscription to a Product with a downloadable object-code component ("**Software Component**"), Client may install and run multiple copies of the Software Components solely for Client's Internal Use. Client's access and use is limited to the purchased quantity and the period of time during which Client is authorized to access and use the Product or Product-Related Service.

8.7.1.2 Restrictions. The access and use rights do not include any rights to, and Client will not, with respect to any Offering (or any portion thereof): (i) employ or authorize any third party (other than eSentire) to use or view the Offering or Documentation, or to provide management, hosting, or support for an Offering; (ii) alter, publicly display, translate, create derivative works of or otherwise modify an Offering; (iii) sublicense, distribute or otherwise transfer an Offering to any third party (except as expressly provided in the Section entitled Assignment); (iv) allow third parties to access or use an Offering (except for eSentire as expressly permitted herein); (v) create public Internet "links" to an Offering or "frame" or "mirror" any Offering content on any other server or wireless or Internet-based device; (vi) reverse engineer, decompile, disassemble or otherwise attempt to derive the source code (if any) for an Offering (except to the extent that such prohibition is expressly precluded by applicable law), circumvent its functions, or attempt to gain unauthorized access to an Offering or its related systems or networks; (vii) use an Offering to circumvent the security of another party's network/information, develop malware, unauthorized surreptitious surveillance, data modification, data exfiltration, data ransom or data destruction; (viii) remove or alter any notice of proprietary right appearing on an Offering; (ix) conduct any stress tests, competitive benchmarking or analysis on, or publish any performance data of, an Offering (provided, that this does not prevent Client from comparing the Products to other products for Client's Internal Use); (x) use any feature of Product Publisher APIs for any purpose other than in the performance of, and in accordance with, these terms and conditions; or (xi) cause, encourage or assist any third party to do any of the foregoing. Client agrees to use an Offering in accordance with laws, rules and regulations directly applicable to Client and acknowledges that Client is solely responsible for determining whether a particular use of an Offering is compliant with such laws.

8.7.1.3 Third Party Software. Product Publisher uses certain third-party software in its Products, including what is commonly referred to as open-source software. Under some of these third-party licenses, Product Publisher is required to provide Client with notice of the license terms and attribution to the third party. See the licensing terms and attributions for such third-party software that Product Publisher uses at: https://falcon.crowdstrike.com/opensource.

8.7.1.4 Installation and User Accounts. Product Publisher is not responsible for installing Products. For those Products requiring user accounts, only the single individual user assigned to a user account may access or use the Product. Client is liable and responsible for all actions and omissions occurring under Client's user accounts for Offerings.

8.7.1.5 Malware Samples. If Product Publisher makes malware samples available to Client in connection with an evaluation or use of the Product ("**Malware Samples**"), Client acknowledges and agrees that: (i) Client's access to and use of Malware Samples is at Client's own risk, and (ii) Client should not download or access any Malware Samples on or through its own production systems and networks and that doing so can infect and damage Client's systems, networks, and data. Client shall use the Malware Samples solely for Internal Use and not for any malicious or unlawful purpose. Product Publisher will not be liable for any loss or damage caused by any Malware Sample that may infect Client's computer equipment, computer programs, data, or other proprietary material due to Client's access to or use of the Malware Samples.

8.7.1.6 Ownership & Feedback. The Offerings are made available for use or licensed, not sold. Product Publisher owns and retains all right, title and interest (including all intellectual property rights) in and to the Offerings. Any feedback or suggestions that Client provides to Product Publisher regarding its Offerings (e.g., bug fixes and features requests) is non-confidential and may be used by Product Publisher for any purpose without acknowledgement or compensation; provided, Client will not be identified publicly as the source of the feedback or suggestion.

8.7.1.7 Disclaimer. ESENTIRE, AND NOT PRODUCT PUBLISHER, IS RESPONSIBLE FOR ANY WARRANTIES, REPRESENTATIONS, GUARANTEES, OR OBLIGATIONS TO CLIENT, INCLUDING REGARDING THE PRODUCT PUBLISHER OFFERINGS. CLIENT ACKNOWLEDGES, UNDERSTANDS, AND AGREES THAT PRODUCT PUBLISHER DOES NOT GUARANTEE OR WARRANT THAT IT WILL FIND, LOCATE, OR DISCOVER ALL OF CLIENT'S OR ITS AFFILIATES' SYSTEM THREATS, VULNERABILITIES, MALWARE, AND MALICIOUS SOFTWARE, AND CLIENT AND ITS AFFILIATES WILL NOT HOLD PRODUCT PUBLISHER RESPONSIBLE THEREFOR. PRODUCT PUBLISHER AND ITS AFFILIATES DISCLAIM ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, PRODUCT PUBLISHER AND ITS AFFILIATES AND SUPPLIERS SPECIFICALLY DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT WITH RESPECT TO THE OFFERINGS. THERE IS NO WARRANTY THAT THE OFFERINGS WILL BE ERROR FREE, OR THAT THEY WILL OPERATE WITHOUT INTERRUPTION OR WILL FULFILL ANY OF CLIENT'S PARTICULAR PURPOSES OR NEEDS. THE OFFERINGS ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THE OFFERINGS ARE NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY, OR PROPERTY DAMAGE. CLIENT AGREES THAT IT IS CLIENT'S RESPONSIBILITY TO ENSURE SAFE USE OF AN OFFERING IN SUCH APPLICATIONS AND INSTALLATIONS. PRODUCT PUBLISHER DOES NOT WARRANT ANY THIRD-PARTY PRODUCTS OR SERVICES.

8.7.1.8 Client Obligations. Client, along with its Affiliates, represents and warrants that: (i) it owns or has a right of use from a third party, and controls, directly or indirectly, all of the software, hardware and computer systems (collectively, "**Systems**") where the Products will be installed or that will be the subject of, or investigated during, the Offerings, (ii) to the extent required under any federal, state, or local U.S. or non-US laws (e.g., Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq., Title III, 18 U.S.C. 2510 et seq., and the Electronic Communications Privacy Act, 18 U.S.C. § 2701 et seq.) it has authorized Product Publisher, through the Offerings, to access the Systems and process and transmit data through the Offerings in accordance with these terms and conditions, and as necessary to provide and perform the Offerings, (iii) it has a lawful basis in having Product Publisher investigate the Systems, process the Client Data and the Personal Data; (iv) that it is and will at all relevant times remain duly and effectively authorized to instruct Product Publisher to carry out the Offerings, and (v) it has made all necessary disclosures, obtained all necessary consents and government authorizations required under applicable law to permit the processing and international transfer of Client Data and Client Personal Data from each Client and Client Affiliate, to Product Publisher.

8.7.1.9 Falcon Platform. The 'Falcon EPP Platform' uses a crowd-sourced environment, for the benefit of all customers, to help customers protect themselves against suspicious and potentially destructive activities. Product Publisher's Products are designed to detect, prevent, respond to, and identify intrusions by collecting and analyzing data, including machine event data, executed scripts, code, system files, log files, dll files, login data, binary files, tasks, resource information, commands, protocol identifiers, URLs, network data, and/or other executable code and metadata. Client, rather than Product Publisher, determines which types of data, whether Personal Data or not, exist on its systems. Accordingly, Client's endpoint environment is unique in configurations and naming conventions and the machine event data could potentially include Personal Data. Product Publisher uses the data to: (i) analyze, characterize, attribute, warn of, and/or respond to threats against Client and other customers, (ii) analyze trends and performance, (iii) improve the functionality of, and develop, Product Publisher's products and services, and enhance cybersecurity; and (iv) permit Client to leverage other applications that use the data, but for all of the foregoing, in a way that does not identify Client or Client's Personal Data to other customers. Neither Execution Profile/Metric Data nor Threat Actor Data are Client's Confidential Information or Client Data.

8.7.1.10 Processing Personal Data. Personal Data may be collected and used during the provisioning and use of the Offerings to deliver, support and improve the Offerings, administer the licensing and further the business relationship, comply with law, act in accordance with Client's written instructions, or otherwise in accordance with these terms and conditions. Client authorizes Product Publisher to collect, use, store, and transfer the Personal Data that Client provides to Product Publisher as contemplated by these terms and conditions. While using certain Product Publisher Offerings Client may have the option to upload (by submission, configuration, and/or retrieval) files and other information related to the files for security analysis and response or, when submitting crash reports, to make the product more reliable and/or improve Product Publisher's products and services or enhance cyber-security. These potentially suspicious or unknown files may be transmitted and analyzed to determine functionality and their potential to cause instability or damage to Client's endpoints and systems. In some instances, these files could contain Personal Data for which Client is responsible.

8.7.1.11 Compliance with Laws. Client agrees to comply with all U.S. federal, state, local and non-U.S. laws directly applicable to it, in the exercise of its rights and performance of its obligations hereunder, including but not limited to, applicable export and import, anti-corruption and employment laws. Client acknowledges and agrees the Offerings shall not be used, transferred, or otherwise exported or re-exported to regions that the United States and/or the European Union maintains an embargo or comprehensive sanctions (collectively, "**Embargoed Countries**"), or to or by a national or resident thereof, or any person or entity subject to individual prohibitions (e.g., parties listed on the U.S. Department of Treasury's List of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders) (collectively, "**Designated Nationals**"), without first obtaining all required authorizations from the U.S. government and any other applicable government. Client represents and warrants that Client is not located in, or is under the control of, or a national or resident of, an Embargoed Country or Designated National.

8.7.1.12 Definitions (solely for the purposes of this **section 8.7.1**):

- "**Product Publisher Data**" shall mean the data generated by the Product Publisher Offerings, including but not limited to, correlative and/or contextual data, and/or detections. For the avoidance of doubt, Product Publisher Data does not include Client Data.
- "**Client Data**" means the data generated by the Client's Endpoint and collected by the Products.
- "**Documentation**" means Product Publisher's end-user technical documentation included in the applicable Offering.
- "**Endpoint**" means any physical or virtual device, such as, a computer, server, laptop, desktop computer, mobile, cellular, container or virtual machine image.
- "**Execution Profile/Metric Data**" means any machine-generated data, such as metadata derived from tasks, file execution, commands, resources, network telemetry, executable binary files, macros, scripts, and processes, that: (i) Client provides to Product Publisher in connection with this Package and the

Endpoint Services or (ii) is collected or discovered during the course of Product Publisher providing Offerings, excluding any such information or data that identifies Client or to the extent it includes Personal Data.

- "**Internal Use**" means access or use solely for Client's own internal information security purposes. By way of example and not limitation, Internal Use does not include access or use: (i) for the benefit of any person or entity other than Client, or (ii) in any event, for the development of any product or service. Internal Use is limited to access and use by Client's employees and ESentire solely on Client's behalf and for Client's benefit.
- "**Offerings**" means, collectively, any Products or Product-Related Services.
- "**Personal Data**" means information provided by Client to Product Publisher or collected by Product Publisher from Client used to distinguish or trace a natural person's identity, either alone or when combined with other personal or identifying information that is linked or linkable by Product Publisher to a specific natural person. Personal Data also includes such other information about a specific natural person to the extent that the data protection laws applicable in the jurisdictions in which such person resides define such information as Personal Data.
- "**Product**" means any of Product Publisher's cloud-based software or other products ordered by Client through eSentire, the available accompanying API's, the Product Publisher Data, any Documentation.
- "**Product-Related Services**" means, collectively, (i) Falcon OverWatch, (ii) Falcon Complete Team, (iii) the technical support services for certain Products provided by Product Publisher, (iv) training, and (v) any other Product Publisher services provided or sold with Products.
- "**Threat Actor Data**" means any malware, spyware, virus, worm, Trojan horse, or other potentially malicious or harmful code or files, URLs, DNS data, network telemetry, commands, processes or techniques, metadata, or other information or data, in each case that is potentially related to unauthorized third parties associated therewith and that: (i) Client provides to Product Publisher in connection with the Package and the Endpoint Services, or (ii) is collected or discovered during the course of Product Publisher providing Offerings, excluding any such information or data that identifies Client or to the extent that it includes Personal Data.

8.7.1.13 US Government End Users. If Client is a US Government entity the following shall also apply:

- Commercial Items. The following applies to all acquisitions by or for the U.S. government or by any U.S Government prime contractor or subcontractor at any tier ("**Government Users**") under any U.S. Government contract, grant, other transaction, or other funding agreement. The Products and Documentation are "commercial items," as that term is defined in Federal Acquisition Regulation ("**FAR**") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in FAR 12.211 and 12.212. In addition, Department of Defense FAR Supplement ("**DFARS**") 252.227-7015 (Technical Data – Commercial Items) applies to technical data acquired by Department of Defense agencies. Consistent with FAR 12.211 and 12.212 and DFARS (48 C.F.R.) 227.7202-1 through 227.7202-4, the Products and Documentation are being licensed to Government Users pursuant to the terms of this license(s) customarily provided to the public as forth in this section 8.7.1, unless such terms are inconsistent with United States federal law ("**Federal Law**").
- Disputes with the U.S. Government. If this section 8.7.1 fails to meet the Government's needs or is inconsistent in any way with Federal Law and the parties cannot reach a mutual agreement on terms of this section 8.7.1, the Government agrees to terminate its use of the Offerings. In the event of any disputes with the U.S. Government in connection with the Endpoint Services and the terms of this section 8.7.1, the rights and duties of the parties arising from such terms, shall be governed by, construed, and enforced in accordance with Federal Procurement Law and any such disputes shall be resolved pursuant to the Contract Disputes Act of 1978, as amended (41 U.S.C. 7101-7109), as implemented by the Disputes Clause, FAR 52.233-1.

- Precedence. This U.S. Government rights in this Section are in lieu of, and supersedes, any other FAR, DFARS, or other clause, provision, or supplemental regulation that addresses Government rights in the Offerings, computer software or technical data hereunder.

8.7.2 Product Publisher for Log Services – Sumo Logic, Inc. flow down provisions (newly defined terms in **section 8.7.2** shall only apply to this section):

8.7.2.1 Client will not, directly or indirectly, and will not permit or enable any third party to: (i) input, upload, transmit or otherwise provide to or through the software any information or materials that are unlawful or injurious or contain, transmit or activate any malicious code; (ii) damage, destroy, disrupt, disable, impair, interfere with or otherwise impede in any manner the software, in whole or in part; (iii) access or use the software for purposes of competitive analysis of the Log Services, the development, provision or use of a competing software service or product or any other purpose that is to the Product Publisher's detriment or commercial disadvantage; or (iv) use the software other than in accordance with this Service Description.

8.7.2.2 Client hereby grants to the Product Publisher: (A) a non-exclusive, royalty-free, worldwide, transferrable, sub-licensable license and right to use, copy, modify, create derivative works of, and disclose data, information or other material provided, uploaded or submitted by Client in the course of receiving the Log Services for internal purposes and for purposes of providing the Log Services; and (B) a non-exclusive, irrevocable, perpetual, royalty-free, full paid-up, worldwide, transferable, sub-licensable license and right to generate anonymized data for any business purposes (including, without limitation, for purposes of eSentire or its Product Publisher, improving, testing, operating, promoting and marketing products and services). Client shall retain all right, title and interest in and to the any data, information or other material provided, uploaded, or submitted by Client in the course of using the Log Services including all intellectual property rights therein.

8.7.2.3 Client acknowledges and agrees that the Product Publisher, may anonymize and use Client's Anonymized Data, share Anonymized Data with third parties for business and analytic purposes, combine Client's Anonymized Data with data from other sources to an aggregate dataset, use the resulting information for business and analytic purposes. Anonymized Data means data that has had all Client and Personally Identifiable Information ("**PII**") removed. Client's Anonymized Data will not be disclosed in any manner that would identify Client as the source of the data. The aggregate Anonymized Data will be separated from Client's data.

8.7.2.4 If required, Client will cooperate with Product Publisher in connection with the performance of the Log Services by making available such personnel and information as may be reasonably required and taking such other actions as Product Publisher may reasonably request. Client will also cooperate with Product Publisher in establishing a password or other procedures for verifying that only designated employees of Client have access to any administrative functions relating to the Log Services.

8.7.2.5 Unless otherwise specified by the Product Publisher, Client will use Product Publisher's then-current names, marks, logos, and other identifiers for the Log Services and Software ("**Trademarks**") and Product Publisher designated intellectual property related notices provided that Client will: (a) only use Trademarks in the form and manner, and in accordance with the quality standards and usage guidelines that Product Publisher specifically prescribes and only in connection with the Log Services; and (b) upon termination of these terms and conditions for any reason, immediately cease all use of the Trademarks. None of Client or any affiliate will (a) otherwise brand the Log Services or(b) otherwise use or register (or make any filing with respect to) any trademark, name or other designation relevant to the subject matter of this section 8.7.2 anywhere in the world, whether during or after the Term or (c) contest anywhere in the world the use by or authorized by the Product Publisher of any trademark, name or other designation relevant to the subject matter of this section 8.7.2 or any application or registration therefore, whether during or after the Term.

8.7.2.6 Client acknowledges and agrees that the Log Services operate on or with or using application programming interfaces (APIs) and/or other services operated or provided by third parties ("**Third- Party Services**"). For purposes of clarification, these Third-Party Services include applications and the like that are not incorporated into the Log Services directly and consist of applications such as third-party collection devices and the like. Product Publisher is not responsible for the operation of any third-party services nor the availability or operation of the Log Services to the extent such availability and operation is dependent upon Third-Party Services. Client is solely responsible for procuring any and all rights necessary for it and its customers to access Third Party Services and for complying with any applicable terms or conditions thereof. Product Publisher does not make any representations or warranties with respect to Third-Party Services or any third-party providers. Any exchange of data or other interaction between Client and a third-party provider is solely between Client and such third-party provider and is governed by such third party's terms and conditions.

8.7.2.7 Client agrees that it shall not make, or cause to be made, any untrue statement or communicate any untrue information (whether oral or written) that disparages or reflects negatively on the Log Services, Product Publisher or its management or employees. This paragraph shall not, however, prohibit the Client from testifying truthfully as a witness in any court proceeding or governmental investigation.

8.7.2.8 During the Term, the Client agrees that it shall not embed or utilize with the Log Services-related software in any service substantially similar in functionality to or identical in functionality to the Log Services.