Cloud Services – CrowdStrike

1. Service Overview

eSentire's Cloud-Native Application Protection Platform ("**CNAPP**") Services - CrowdStrike (the "**Service**") provides analysis, investigation and alerting based on threats identified in Client's cloud infrastructure and workloads. The Service leverages a cloud security technology powered by CrowdStrike ("**Product Publisher**"), combined with the eSentire Atlas Platform to provide cybersecurity insights, along with threat prevention, detection, mitigation, and response. This Service is scoped using the number of Client identified virtual machine(s) ("**VM(s)**") and/or containerized workloads, that represent cloud servers and resources ("**Cloud Resources**") in the Client environment, as detailed on the Order Form. The Service only supports Cloud Resources hosted within the following cloud infrastructure providers: Amazon Web Services, Google Cloud Platform, or Microsoft Azure.

2. Service Definitions

Any capitalized terms contained in this Service Description are as defined herein, or as defined in the "Managed Detection Response ("MDR") Services - General Information" document (referred to herein as the "**MDR General Information**" document) which can be found under the "Managed Detection and Response ("MDR") Services" section found on this webpage: https://www.esentire.com/legal/documents. The MDR General Information document contains information applicable to all MDR services, including this Service.

3. Service Capabilities

The Service collects information from all in-scope Cloud Resources (collectively the "**Cloud Environment**") and monitors and analyzes the data for potential threats, unusual behavior, or other indicators of compromise. Suspicious activity detected is monitored by eSentire's Security Operations Center ("**SOC**") on a 24x7x365 basis, initiating investigations and Client notification as required. The Service includes the following:

3.1 Deployment. For a new deployment, eSentire will begin by collecting the required information for onboarding. Following data collection/validation, eSentire will provision access to the Atlas Platform, schedule a kickoff call with Client, and coordinate deployment for the applicable number of in-scope Cloud Resources. A Client contact with administrator access to the Client's Cloud Environment is required to complete integration. eSentire will review the configuration worksheet with the Client during this initial deployment of the Service to confirm Client has included key areas of its Cloud Environment to maximize coverage and visibility. Following initial deployment, eSentire will provide ongoing hardening guidance as the Cloud Environment changes.

3.2 Incubation and Tuning Phases. After deployment is completed, the Service will enter an incubation phase to fine tune the security Alerts. eSentire will work through the incubation and tuning phases with Client and work to move them into a production state. Until incubation and tuning are complete, events generated by the Cloud Environment will not be monitored by the eSentire SOC. Additional details for this phase are:

- **Phase 1 - Facilitate normalization of tooling**. The solution leverages both rule-based detection and anomaly-based detection; the latter needs time to baseline the Cloud Environment configured so that Alerts can be triggered if the baseline is exceeded.

- **Phase 2 - Prevention of Alert flooding after onboarding**. Depending upon the Client Cloud Environment configuration, after the initial deployment, there is potential for a flood of Alerts. During the incubation and tuning phase, all alerting will be turned off, and neither Client nor the eSentire SOC will receive notifications. After initial deployment, to optimize the Alerts based on severity and relevance to Client, eSentire will manually review Alerts with Client. When this phase closes, Alerts will flow into the eSentire SOC.
- **Phase 3 - Identification of false positives**. eSentire will review the Service with the Client, including the Atlas Platform, as well as any other applicable user interface ("**UI**"), and/or features. eSentire will also review the alerting, specifically the workflow for managing false positives. During this time, eSentire will provide Client an incubation phase report outlining all Alerts starting from Phase 1 and 2 above. After review, Client and eSentire will identify false positives contained in the report and agree on which Alerts should no longer be reported. eSentire will apply Client changes, and dismiss Alerts for the specific policy, on the specific Cloud Resource, ensuring that subsequent Alerts for that policy do not fire for the specific Cloud Resource. Of note, in the event a Cloud Resource is configured to be compliant with a policy but is subsequently modified to be non-compliant, an Alert may report again. Alerts from the incubation report which Client indicates are legitimate Alerts, will be passed on to the production service phase. The incubation report will include instructions to assist Client with remediation of these specific Alerts.

3.3 Service Production. Once the Service moves into the production phase, Client's Cloud Environment will be monitored in real-time against Service policies which define the criteria to send an Alert. The SOC will monitor the Cloud Environment 24x7x365, and will investigate and escalate identified critical severity events to Client. The Service tools will also be tuned to send automated notifications directly to Client for non-critical events that still require remediation. New threat detections (as applicable) are consistently being added to the Service and applied to the Client Cloud Environment, at no additional charge.

During production, eSentire will monitor Cloud Resources in the Cloud Environment for items such as:

- misconfiguration of Cloud Resources;
- threats present in VM and container-based workloads;
- communication to/from IP addresses on eSentire's proprietary threat blacklist;
- anomalies in typical user and entity behavior analytics;
- identity issues stemming from over-permissioning and / or unused accounts;
- threats discovered in audit logs;
- anomalous activity, including deviations from baseline behavior correlating changes to cloud API interactions, user privileges, group policies, access keys, and other configurations;
- critical service exposures;
- misconfigurations in cloud automation tooling;
- illicit activity attempting to leverage the Cloud Environment to mine cryptocurrencies such as Bitcoin and Ethereum;
- potential account hijacking attempts by monitoring for unusual login activities such as concurrent attempts, peculiar geo-locations, and unknown browsers or operating systems; and
- sensitive modifications to the Cloud Environment.

The Service policies contain two classifications of Alerts, and depending on the classification, eSentire will handle Alerts as follows:

- **Alerts that are non-remediable by eSentire, investigable by eSentire.** Such Alerts are mainly the result of policies which identify potentially malicious behavior. These Alerts will be identified as requiring investigation by the eSentire SOC, and eSentire will investigate and attempt to identify information related to such Alert such as (as applicable):
  - user account which made a potentially sensitive configuration change to a Cloud Resource;
  - unusual user activity, which occurred at the same time as a potentially sensitive configuration change (identification of potential account compromise);
  - identification of abnormal cloud resource utilization, as a result of malicious activity such as crypto mining;
  - identification of false positive Alerts, filtering these out from Alerts reported to Client; and/or
  - determine the threat actor, impacted Cloud Resources, and severity of threat.

  Once the SOC has completed collecting information related to the Alert, if required, eSentire will send Client the Alert summary along with recommended remediation activities. This information will be sent to the Client via email and also posted to the Atlas Platform for Client action. eSentire will escalate based on priority level, and defined actions, described in the MDR Service Level Objectives (link provided in section 3 below).

- **Alerts that are non-remediable by eSentire, non-investigable by eSentire.** Such Alerts are mainly mis-configuration items that will be sent to Client directly by eSentire, via email and also posted to the Atlas Platform for Client action. These types of Alerts can only be corrected by Client as they require account configuration changes and/or review. The details included in the Alert sent to Client will include information on the policy criteria that caused the Alert, details on the violating Cloud Resource and specific steps to remediate the condition.

  The Alerts that are sent to Client, and identified for Client action on the Atlas Platform, will remain unresolved until Client either performs the recommended remediation steps, or advises eSentire that the Alert was a false positive and should be suppressed.

4. Subscription Types and Responsibilities

4.1 Subscription Types. Client can subscribe to one or more of the follow Service subscriptions (each a "**Subscription**"):

4.1.1 Cloud Services – CrowdStrike - CNAPP Proactive
- Monitoring of cloud environment for misconfigurations and adherence to industry standard compliance frameworks.
- Evaluation of cloud platform API logs for identification of known-bad and anomalous events.
- Scoped via the number of VMs in the covered Client Environment.

4.1.2 Cloud Services – CrowdStrike - CNAPP VM
- The capabilities of "CrowdStrike CNAPP – Proactive"
- Runtime monitoring of VM workloads via agent installation.
- Does not cover VMs running containers.
- Scoped via the number of sensors deployed to cloud VMs
- Requires subscription to: Endpoint Services - CrowdStrike

4.1.3 Cloud Services – CrowdStrike - CNAPP Container

- The capabilities of "CrowdStrike CNAPP – Proactive"
- Runtime monitoring of containerized workloads via Helm or Daemonset agent deployment.
    - Does not cover VMs or managed containers like ECS/EKS Fargate, Azure Container Instances, or Google Cloud Run.
- Scoped via the number of sensors deployed to hosts running containers
- Requires subscription to: Endpoint Services - CrowdStrike

4.1.4 Cloud Services – CrowdStrike - CNAPP Managed Container

- The capabilities of "CrowdStrike CNAPP – Proactive"
- Runtime monitoring of managed containers like ECS/EKS Fargate, Azure Container Instances, or Google Cloud Run.
    - Does not cover VMs or traditional containerized hosts.
- Scoped via the average number of monitored managed containers
- Requires subscription to: Endpoint Services - CrowdStrike

Client may request the Service to be provided by eSentire in one of the following ways: a) as a co-managed service with bundled licensing ("**MSSP**"), b) in a managed only capacity ("**Managed Only**"), or c) in an enterprise licensing agreement ("**Enterprise**"). This selection will be detailed on the Order Form. Licensing details and requirements for each are detailed below:

4.2 MSSP Licensing Requirements. In this Service option, eSentire will procure all required licensing directly from Product Publisher; eSentire will be the licensee of record with Product Publisher and provide management. As the Licensee, eSentire may grant Client enhanced access into eSentire's license instance.

4.3 Managed Only Licensing requirements. In this Service option, eSentire will manage Client's Product Publisher licensing, which has been procured by Client. Client must procure and maintain its cloud licensing ("**License**") with Product Publisher, during the entire Term of the Service, and coordinate proper licensing permissions with the Product Publisher to allow eSentire full administrative access and credentials into Client's License instance. Client must purchase the following applicable licenses (or their successors/replacements, subject to eSentire approval), in order to receive the Service in a Managed Only capacity from eSentire:

- **Cloud Services – CrowdStrike – CNAPP Proactive – Managed Only**, the following licenses must be procured:
    - CS.FCS.PRO.SOLN – Falcon Cloud Security – Proactive ("Proactive")
- **Cloud Services – CrowdStrike – CNAPP VM – Managed Only**, the following licenses must be procured:
    - CS.FCS.RP1 – Falcon Cloud Security – CNAPP – VM ("CNAPP – VM")
- **Cloud Services – CrowdStrike – CNAPP Container – Managed Only**, the following licenses must be procured:
    - CS.FCSC.RP1 – Falcon Cloud Security – CNAPP – Container ("CNAPP – Container")
- **Cloud Services – CrowdStrike – CNAPP Managed Container – Managed Only**, the following licenses must be procured:
    - CS.FMC.RP1 – Falcon Cloud Security – CNAPP – Managed Container ("CNAPP – Managed Container")

4.4 Enterprise Licensing requirements. In this Service option, eSentire will procure and resell Product Publisher licenses to Client. Client will be the licensee of record with Product Publisher for the Service Term, and eSentire shall manage the licensing for Client. As the License holder Client must provide eSentire full access to Clients CrowdStrike licensed environment.

4.5 Responsibilities

Responsibilities of each Party are as described below:

Function	Client	eSentire
Grant eSentire permission to reparent Client CrowdStrike CID for management purposes (Only applies to "Managed Only" model)	X	
Grant required permissions within Client Cloud Resources to enable the Service.	X	
Provide required information to support Service onboarding of Cloud Resources.		X
Complete configuration of Cloud Resources in the Cloud Environment as required.	X	
Install agents/sensors on hosts or containers as required by service level.	X	
Preparation of the incubation period report.		X
Return incubation period report to eSentire, complete with input on each Alert.	X	
Perform Service tuning based on input from Client via the incubation period report.		X
Perform monitoring of the Cloud Environment included in the Service, 24x7x365.		X
Provide detailed information regarding misconfiguration of Cloud Resources, enabling Client to perform required configuration changes within the Cloud Environment.		X
Where applicable, perform investigations into the cause of an Alert and provide investigation details to Client.		X
When requested, provide contextual information to aid in the investigation of an Alert.	X	
Answer Client questions about the Service, Alerts, configuration, or other items.		X
Provide Client with the opportunity to review Service status including items such as: • Alerts • Number of Alerts triggered for reporting period • License utilization • Cloud Resources under protection		X

4.6 Other CrowdStrike Licenses Offerings:

Client may order from eSentire additional CrowdStrike licensed offerings outside of those included in or required or supported by the Service ("**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.

4.6.1 MSSP Support Model - When Client orders the Service from eSentire 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.

4.6.2 Enterprise Support Model or Resale - When Client orders the Service from eSentire in an Enterprise support model, Client is considered the licensee of such Add-Ons (referred to on the Order Form as an "**Enterprise Resale**" or "**Resale**") and Client will need to troubleshoot such components directly with the Product Publisher.

eSentire does not warrant or guarantee the successful operation of Add-Ons. Add-Ons are made available by eSentire to Client on an "as-is" basis and eSentire specifically disclaims all representations and warranties with respect to Add-Ons, express or implied, including the implied warranties of merchantability, operability, and fitness for a particular purpose. Use of any such Add-Ons is subject to Client's acceptance of and compliance with the full Product Publisher EULA which applies to the Add-Ons,

which can be found here: www.crowdstrike.com/terms. A list of available CrowdStrike License Add-Ons and descriptions can be found on this webpage under "Additional Offerings": https://www.esentire.com/legal/documents.

4.7 Client Acknowledgement. For any Service option or licensing model detailed in this section, Client acknowledges and agrees that any changes made by Client in the licensed environment but not authorized by eSentire could negatively impact eSentire's ability to deliver the Services. In addition, Client acknowledges and agrees that any changes made by Client in the licensed environment during the term of this Service should be reviewed with eSentire, otherwise eSentire shall be released from any and all obligations to effectively provide the Services as contemplated herein. Throughout the Service Term, Client must provide and eSentire must maintain administrator or equivalent access which enables eSentire staff and systems to execute the tasks included in this service description. Access will only be provided to select, authorized eSentire employees and will be audited.

5. Service Level Objectives

The ability for eSentire SOC to perform an investigation and assess whether a threat is malicious is dependent on an active CrowdStrike Falcon Cloud license from Product Publisher being integrated and in production in the Client Cloud Environment. The service levels set out in the MDR General Information, are only applicable to hosts that are licensed as part of the Service and are actively communicating with the Service.

eSentire will monitor the in-scope Client Cloud Resources for potential threats and respond accordingly. When potentially malicious activity is identified, eSentire will perform an investigation and will respond according to the identified threat. Additional confirmation from the Client may be needed depending on the information available to eSentire at the time of the investigation.

6. Service Terms and Information

6.1 Service Overages. The Services are scoped/sold using Cloud Resource totals, and the quantity is detailed on the Order Form. Should Client's number of Cloud Resources active as a daily average exceed 10% of the contracted value (measured on an average over one calendar month), notwithstanding any security event (the "**Overage**"), then Client will either (i) take steps to reduce Cloud Resources to the contracted level within 30 Days of such Overage, or (ii) move to the next Service level, and associated fees, to accommodate its usage for the remainder of the Term.

6.2 Product Publisher Flow Down Terms. If Client has ordered Services to be delivered in an MSSP fashion, eSentire has an obligation to ensure Client agrees to flow down provisions required by the Product Publisher applicable to the licensing. These flow down provisions are not negotiable. In such case, Client agrees to the following Product Publisher required flow down provisions:

6.2.1 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.

6.2.2 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.

6.2.3 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.

6.2.4 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.

6.2.5 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.

6.2.6 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.

6.2.7 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.

6.2.8 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.

6.2.9 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.

6.2.10 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.

6.2.11 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.

6.2.12 Definitions (solely for the purposes of this **section 6.2**)

- "**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.

6.2.13 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.