eSENTIRE

Service Description:
Endpoint Services – CrowdStrike

1. Service Overview

eSentire's Managed Detection Response for Endpoint Services - CrowdStrike (the "**Service**") is a managed service providing endpoint-level visibility and control to support threat prevention, threat detection, investigation, and response leveraging the CrowdStrike Falcon® agent/license ("**Agent**") installed on servers, laptops, and desktop devices with supported operating systems within Client's environment (the "**Client Environment**").

The eSentire Atlas Platform will capture telemetry from in-scope endpoints, enrich signals from other sources, analyze for suspicious or threatening behavior and support eSentire's Security Operations Center ("**SOC**") in delivering prevention, appropriate investigations, response, and remediation (as appliable, pursuant to the ordered subscription type). The Prevent subscription allows for automated identification, prevention, and remediation of threats via the Agent. The Detect and Respond subscription allows for full endpoint telemetry visibility to give the SOC analysts the ability to identify and investigate potential threats or suspicious activity. The Overwatch subscription leverages CrowdStrike's threat intelligence to enhance alerts and increase detection capabilities for novel threats. Client also has the option to add on Identity services (as further described below). Any subscription level selected by Client is supported by eSentire's SOC on a 24x7x365 basis.

2. Service Definitions

In addition to the above, 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

3.1. Investigation, Analysis and Response. eSentire is responsible for security event analysis and investigation to determine if a security event is real and warrants an escalation to Client and potential response action (isolation). If an event is deemed Actionable, due to its behavior and the type of detection, it will be escalated to Client as an Alert. Malicious activity will be contained (isolated) immediately by eSentire once identified. The SOC will perform event triage, assign criticality, and include all supporting information within the Alert and, if necessary, initiate escalation to Client.

eSentire will investigate all security events identified during the Service and escalate Actionable Alerts as appropriate. Once investigated, events are classified, alerted, and escalated to Client if there is an action required. eSentire will utilize an escalation process mutually agreed upon between Client and eSentire during the on-boarding process, to contact and relay information to Client. It is eSentire's responsibility to classify the criticality of the Alerts derived from individual events as part of the Service.

4. Subscription Types

4.1. Subscriptions. Client can subscribe to any of the following Endpoint Service - CrowdStrike subscriptions all available to ensure complete endpoint coverage ("**Subscription**"), and are further described below:

4.1.1 Prevent Subscription:

This Subscription relates to the implementation of Next-Gen AV (NGAV) capabilities such as policy and configuration-based prevention mechanisms within the Endpoint service. This includes but is not limited to the ability to block, kill, or quarantine attempted malicious code execution and malicious running processes. This Subscription option includes:

- 24/7 monitoring of prevented activity by the eSentire SOC;
- known and unknown malware and ransomware detected by using machine learning (ML) and artificial intelligence (AI);
- behavior-based indicators of attack (IOA) prevent sophisticated file-less and malware-free attacks;
- the execution and spread of threats via unpatched vulnerabilities stopped by exploit blocking; and
- activities known to be malicious blocked by threat intelligence prevention.

4.1.2 Detect and Respond Subscription:

This Subscription relates to the implementation of threat detection on data such as file monitoring, process command-line parameters, process monitoring, process use of network, loaded DLLs, API monitoring, binary metadata, windows registry monitoring from Client's endpoint. This component of the Service gives eSentire full spectrum visibility into the endpoint and allows for hunting for specific threats. This Subscription option includes:

- 24/7 monitoring, investigation, and response of detections by eSentire SOC;
- full spectrum visibility at the endpoint provided by continuous raw event recording;
- enabled threat hunting—proactive and managed—with full endpoint activity details;
- enabled entire attack life cycle visibility with context and threat intelligence data; and
- situational awareness of the current threat level of the organization, and how it is changing over time.

4.1.3 Prevent, Detect & Respond Subscription:

This Subscription bundles above subscriptions and provides all features noted (see 4.1.1 and 4.1.2).

4.1.4 Overwatch Subscription:

Client may choose to subscribe to this subscription option along with the Prevent, Detect & Respond subscription. This Subscription option includes:

- enhanced detection technology enriched with contextual details and global insights;

- 24/7 monitoring, investigation, and response of Overwatch detections by eSentire SOC; and
- access to threat hunting reports with always-current knowledge of tradecraft from more than 130 adversaries.

4.2. Identity Subscription. Client may also choose to subscribe to identity services leveraging a license to CrowdStrike's Falcon Identity ("**Identity Services**") for all in scope entities. The Identity Service will collect information in the Client Environment via Agents installed on applicable Domain Controllers.

If Client orders Identity Services as part of the Endpoint Service, it will:

- provide the eSentire SOC additional visibility, and the ability to monitor and investigate the scope and the impact of access privileges for identities across Client's Active Directory ("**AD**") and Azure AD;
- deliver AD security posture overview by analyzing user behavior and risk changes over time, including increases in account lockouts, high-risk endpoints, and duplicate/compromised passwords to get an overview of the attack surface of the organization;
- streamline identity verification and conditional access policies, leveraging adaptive analysis based on authentication patterns and behavior baselines; and
- extend multi-factor authentication to legacy systems and tools, reducing attack vectors.

The Identity Service is only offered in conjunction with the following Endpoint Services – CrowdStrike Subscriptions (at a minimum):

- Prevent, Detect & Respond

4.3 eSentire Atlas Agent. In providing the Service, eSentire may deploy eSentire's Atlas Agent on certain endpoints in addition to the CrowdStrike Falcon® Agent. The additional functionality provided by eSentire's Atlas Agent is described in the description which can be found on this webpage under "Additional Offerings": https://www.esentire.com/legal/documents.

4.4 Third Party License Requirements. Client may request each Service Subscription to be provided by eSentire in one of the following ways: a) as a managed service with bundled licensing ("**MSSP**"), b) as a managed service with resold licensing ("**Enterprise**") or c) in a managed only capacity ("**Managed Only**"). This selection will be detailed on the Order Form. Licensing requirements for each are detailed below:

4.4.1 MSSP Licensing requirements:
In this Service option, eSentire will procure all required licensing directly from CrowdStrike, will be the licensee of record with CrowdStrike, and provide management. As part of this license, eSentire will have access to 15 Days of Client data retention on the licenced instance, which can be used by eSentire in an investigation. As the Licensee, eSentire may grant Client enhanced access into eSentire's license instance, and if so granted, Client acknowledges and agrees that any changes made by Client in the licensed environment could negatively impact eSentire's ability to deliver the Services.

4.4.2 Enterprise Licensing requirements:
In this Service option, eSentire will procure and resell CrowdStrike licenses to Client. Client will be the licensee of record with CrowdStrike for the Service Term, and eSentire shall manage the licensing for Client. As part of this license, Client and eSentire will have access to seven Days of Client data retention on the licenced instance[3 (see table)], which can be used by Client or eSentire in

an investigation. Client has the option to purchase additional days of data retention on their license at an additional fee, and such additional purchase if requested will be detailed on the Order Form. As the License holder Client must provide eSentire full access to Clients CrowdStrike licensed environment. The licenses included with an Enterprise Service sale will include entitlements to the following:

Description	Product SKU	Quantity[2]
Falcon Endpoint Protection Enterprise Flexible Bundle	CS.EPPENT.SOLN	endpoints[1]
Prevent	CS.PREVENT.SOLN	endpoints[1]
Insight	CS.INSIGHT.SOLN	endpoints[1]
Threat Graph Extended 15 days[3]	CS.TG.EXT	endpoints[1]
Overwatch	CS.OW.SVC	endpoints[1]
Essential Support	RR.HOS.ENT.ESTL	1 unit
[1]Quantities will match the number of endpoint quantities identified on the Order Form. [2] Fees for the quantities above will be included in the total Annual Fees for the Endpoint Services, summarized in the associated Order Form(s). [3] Clients who sign an Order Form for this Service after August 2024 for full Prevent, Detect and Respond with Overwatch (Enterprise), by default will have Threat Graph Extended 15 days, otherwise 7 days of data retention applies (unless otherwise stated on the Order Form).		

4.4.3 Managed Only Licensing requirements:

In this Service option, eSentire will manage Client's CrowdStrike endpoint licensing, which has been procured by Client. Client must procure and maintain its endpoint licensing ("License") with CrowdStrike, during the entire Service Term, and coordinate proper licensing permissions with CrowdStrike, Inc. to allow eSentire full administrative access and credentials into Client's License instance. Client must purchase the following applicable licenses, in order to receive Endpoint Services in a Managed Only capacity from eSentire:

- CrowdStrike Falcon Insight XDR
- Threat Graph Standard
- CrowdStrike Falcon Prevent

4.4.4 Other CrowdStrike Licensed 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.

4.4.4.1 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.

4.4.4.2 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 troubleshoot such components directly with CrowdStrike, Inc. 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.

For any Service option detailed above, Client acknowledges and agrees that any changes made by Client in the licensed environment could negatively impact eSentire's ability to deliver the Services. In addition, Client acknowledges and agrees that any changes made by Client 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. Response Actions for Identified Threats

If Client has ordered the Prevent Subscription, once moved to a service-ready state, the Agent will be configured to execute any of the following actions on detection of confirmed malicious threat:

- process or file denylisting on the endpoint;
- block and kill malicious processes; or
- detect and prevent known/unknown bad software (quarantine).

If Client has ordered Identity Services, once moved to a service-ready state, the platform will be configured to execute any of the following actions:

- enforce Multi-Factor Authentication on users based on Client-approved conditional access policies; or
- restrict user access based on Client-approved conditional access policies.

If Client has ordered the Detect and Respond Subscription, following the successful identification of a confirmed threat targeting Client's Environment, the eSentire SOC will utilize the Service to execute one of the following actions:

- endpoint isolation;
- initiate interactive session on endpoint;
- download files to endpoint;
- delete files on endpoint; or
- gather files and memory for host.

If Client has purchased other eSentire services, response may be implemented at multiple enforcement points, including but not limited to network, endpoint, and cloud (if applicable).

Unless Client opts-out, as part of the Endpoint Services – CrowdStrike - Detect & Respond subscription option, eSentire will isolate potentially compromised machines. eSentire will isolate the machine using this Subscription and notify Client of the isolation via the agreed upon escalation procedure including evidence to support the action. The machines will remain in isolation until the threat has been remediated or Client has accepted the risk and has requested the eSentire SOC to remove the host from isolation.

- All endpoint Detect and Respond Agents are considered authorized for isolation unless otherwise communicated by Client.
- eSentire will escalate all Alerts that require isolation to Client for visibility and active feedback on the Alert. Client commits to identifying critical assets that are NOT to be isolated unless Client has given written authorization.
- eSentire commits to isolating machines that are NOT on the unauthorized list only to prevent the spread of malicious code and lateral movement by suspected attackers.

Clients subscribed to Endpoint Services – CrowdStrike - Detect and Respond subscription are hereby advised that the eSentire SOC has the functionality to isolate machines on Clients' network, the ability to

use this function to protect the network, and that the isolated machines will lose all connectivity to all other devices or resources on the network. eSentire is limited to endpoint response actions through the Agents powered by this Detect and Respond Subscription.

6. Incident Alerts and Reporting

eSentire sends Alerts via email for medium, high, and critical severity events followed by escalation(s) for high and critical severity events, as necessary, based on agreed upon escalation procedure in the configuration worksheet. A member of the eSentire customer success team will be assigned to review the overall Alerts with Client. All Alerts are available within the Insight Portal for Client review. All reporting is delivered through the Insight Portal.

7. Deployment

eSentire is responsible for providing Clients with the required installation documentation for the Agent. eSentire will provide an expert deployment engineer resource during deployment of the Service to assist with questions around how to deploy and the requirements for the Service.

For each of the Service Subscription options deployment methodologies can take up to 30 days to fully tune. eSentire, working with Client, requires that at least 80% of Client contracted endpoint quantities have Agents installed and/or deployed to be able to complete the tuning process and move to production-ready state. Once tuning has been completed it is transitioned to the SOC for real-time monitoring, and the Service is considered fully deployed and in-production.

Once the Service is moved to an active state, eSentire will provide the following documents:

- complete list of machines that are active within the Service; and
- detailed summary of activities investigated during deployment.

8. Tuning and Configuration

eSentire is responsible for configuring and tuning the Services. Endpoint Services – CrowdStrike – Prevent subscription, requires a special configuration and tuning process due to the automated blocking/killing capabilities. Detections through the Prevent Subscription capability are handled by an eSentire's deployment engineer during the tuning and configuration period(s). All detections via the Endpoint Services – CrowdStrike – Detect and Respond subscription capability are handled by the eSentire SOC immediately upon Agent install. There are not any additional considerations to what has been detailed below, related to the Overwatch Subscription.

8.1 Endpoint Services – CrowdStrike - Prevent Subscription. Summary of the tuning and configuration for this subscription option is as follows:

- The configuration of the Prevent Subscription is a phased approach to increase the security of the prevention component.
- Requires 80% of the Agents to be deployed to the infrastructure before configuration and tuning begins.
- Upon successful installation to 80% of the infrastructure an eSentire deployment engineer will be assigned.
- Weekly meetings to take Client through configuration and tuning will happen over a four week period.
- Once Client is in a hardened state, the Service is transitioned into production monitoring by the eSentire SOC.

8.2 Endpoint Services – CrowdStrike - Detect and Respond Subscription. Summary of the tuning and configuration for this subscription option is as follows:

- Data required for detection begins streaming immediately after installation of the Agent.
- eSentire SOC begins monitoring detection events immediately after installation.
- A baseline period of four weeks begins once 80% of Agents are installed.

8.3 Endpoint Services – CrowdStrike – Identity. Summary of the tuning and configuration for this subscription option is as follows:

- The configuration of the Identity Service is a phased approach meant to harden the security posture of an environment.
- Network Traffic Authentication Inspection must be enabled.
- Required 100% of the Agents to be deployed to the domain controllers before the baseline period (30 days) ends.
- After the baseline period, eSentire will work with Client to identify any misconfigurations and perform a review of domain security posture.
- Once Client is in a hardened state the service is transitioned into production monitoring by the eSentire SOC.

9. Client Responsibilities

Client will perform the obligations listed below and acknowledges that the ability for eSentire to deliver the Service is dependent upon Client's compliance with the obligations hereunder, including meeting the service levels below. Non-compliance with these obligations may result in suspension of the Endpoint service or suspension of service levels. The responsibilities of each party are also summarized in the responsibilities matrix which can be found in Appendix A.

9.1 Deployment. Client is responsible for:

- pushing out the Agent to its infrastructure and working with eSentire to confirm it is successfully installed within a reasonable timeframe (no more than 30 days);
- granting access to all data and systems required for the successful delivery of the Services;
- ensure no firewall rules or other blocking exists, as well as any other measure taken by Client, does not prevent the communication from endpoints to the Service management server;
- ensuring there is sufficient network bandwidth and access to perform the Service;
- assisting eSentire with troubleshooting related to the installation of the Agents; and
- notifying eSentire of newly added machines to the Service.

9.2 Tuning and Configuration. Client is responsible for:

- making themselves available for weekly meetings to discuss detections identified during tuning; and
- ensuring that authorized contacts remain current, including approved access and all associated information.

9.3 Investigation, Analysis and Response. Client is responsible for:

- responding to the escalated Alerts and validating the legitimacy of the content contained within the Alert;
- updating eSentire of any changes that would change the agreed upon escalation procedures;
- validate and respond to the eSentire SOC for escalated Alerts; and
- providing information and assistance during investigations conducted by eSentire when additional information is required.

10. Service Level Objectives

The ability for eSentire SOC to perform an investigation and assess whether a threat is malicious is dependent on a supported Agent being installed on a licensed host in Client's Environment. The service levels contained on the MDR General Information document are only applicable to hosts that are licensed as part of the Service and are actively communicating with the Service.

eSentire will monitor the Service 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 Client may be needed depending on the information available to the analyst at the time of the investigation.

11. Product Publisher – Flow Down Provisions

Unless other terms have been negotiated and attached or referenced on the Client's Order Form, the following terms are required by CrowdStrike, Inc. ("**Product Publisher**") to be agreed to by Client, for Services described herein, and as further detailed below:

11.1 Enterprise support model. If Client has ordered Services to be delivered in an Enterprise fashion, Client accepts and agrees to the full Product Publisher EULA which applies to the licenses. The Product Publisher's EULA can be found here: www.crowdstrike.com/terms.

11.2 MSSP support model. If Client has ordered Services to be delivered in an MSSP fashion, eSentire owns the licensing directly with the Product Publisher, and as an MSSP eSentire has an obligation to ensure Client agrees to flow down provisions applicable to the licensing. In such case, Client agrees to the following Product Publisher required flow down provisions:

11.2.1 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.

11.2.2 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, this Agreement; 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.

11.2.3 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.

11.2.4 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.

11.2.5 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.

11.2.6 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.

11.2.7 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.

11.2.8 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 this Agreement 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.

11.2.9 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.

11.2.10 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 Agreement and further the business relationship, comply with law, act in accordance with Client's written instructions, or otherwise in accordance with this Agreement. Client authorizes Product Publisher to collect, use, store, and transfer the Personal Data that Client provides to Product Publisher as contemplated in this Agreement. 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.

11.2.11 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 performance of this Agreement, 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.

11.2.12 Definitions (solely for the purposes of this section 11.2):

- "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 Agreement 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 this Agreement, 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.

10.2.13 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 Agreement, unless such terms are inconsistent with United States federal law ("Federal Law").
- Disputes with the U.S. Government. If this Agreement 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 for this Agreement, the Government agrees to terminate its use of the Offerings. In the event of any disputes with the U.S. Government in connection with this Agreement, the rights and duties of the parties arising from this Agreement, 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 under this Agreement.

Appendix A: Responsibilities Matrix

Function	Client	eSentire
Security – Detection monitoring, analysis	I	RAC
Security – Investigation	-	RAC
Security – Notification	I	RAC
Security – Detection resolution	-	RAC
Security – Threat Intelligence integrations	-	RAC
Security – Ad hoc threat sweeps for IOCs	-	RAC
Security – Custom IOAs, IOCs or workflows	RA	C
System – Custom alerts, dashboards, or workflows	RA	-
System – Initial product walkthroughs and/or guides	A	R
System – Deploying initial endpoints	R	ACI
System – Initial policy and environment configurations	AI	RAC
System – Post-deployment installation or host group management	RA	CI
System – User account management and administration	RA	CI
System – End user training*	R	C
Health – Data ingestion, uptime monitoring and tuning	-	RA
Health – Managing sensor updates	RA	C
Health – Performance or troubleshooting issues - MSSP	RA	RC
Health – Performance or troubleshooting issues - Managed	RA	C

R = Responsible; responsible for action and implementation. Responsibility can be shared.
A = Accountable; ultimately answerable for the activity or decision. This includes “yes” or “no” authority and veto power.
C = Consulted; typically, the subject matter experts, to be consulted prior to a final decision or action.
I = Informed; needs to be informed after a decision or action is taken.
*= Self service