Service Description:
Endpoint Services – Prevent, Detect & Respond – Managed Only

1. Service Overview

eSentire's Endpoint Services – Prevent, Detect & Respond - Managed Only (the "**Services**") provides Client with endpoint-level visibility, threat prevention, detection, investigation, response, and remediation as defined herein, delivered by the eSentire SOC using the endpoint agent chosen and licensed by Client. eSentire will leverage Client owned licensing (see section 4.2) which will be integrated with eSentire's platform in order for eSentire to provide the Service.

2. Service Definitions

"**Endpoint Agent**" or "**Agent**" means the endpoint software agent utilized in providing the Services as further described below.

In addition to the above, any capitalized terms contained in this Service Description are as defined herein, or as defined on the Managed Detection and Response ("**MDR**") Services landing page (which can be found under Service Descriptions at: https://www.esentire.com/legal/documents).

3. Service Capabilities

3.1 Description

eSentire will leverage Client's licensing to obtain email, user identity, application control, and visibility, which will enable the eSentire SOC to identify and investigate potential threats or suspicious activity within Client's environment. The Service is supported by eSentire's SOC on a 24x7x365 basis and will result in human-led investigations of suspicious activity and alerting.

During the Term of the Service, eSentire will provide threat detection, analysis, investigation, escalation, response, and limited remediation (as described below). In addition, eSentire is responsible for security event analysis and investigation to determine if a security event is considered a legitimate threat and warrants an escalation to Client and a potential response action. If an event is deemed Actionable, due to its behavior and the type of detection, it will be escalated to Client as an Alert. The SOC will perform event triage, assign criticality, and include supporting information and analysis within the Alert and, if necessary, initiate escalation to Client. Malicious or suspicious activity will be identified and resolved by eSentire, utilizing response playbooks. Client will receive access to the eSentire Insight Portal, which will consolidate threat alert reports and investigation details from eSentire SOC analysts. Threat Cases will be visible to Client on their Insight Portal dashboard; however, it is eSentire's responsibility to classify the criticality of Alerts derived from individual events. The following support is included as part of the Services:

- Threat Detection:
  - Curation and tuning of agent detections, rules, policies to generate Actionable Alerts.
  - Collection of detections, metadata and selected raw telemetry to aid in investigation, threat hunting and response activity.
  - Enriching collected Client data with context – such as geolocation of IPs, Client-specific context, and threat intelligence.
- Analysis:

- ○ Analysis of Alerts generated by Clients Licensed platform either through automation in the eSentire XDR platform and/or by eSentire (SOC, incident handlers and/or threat hunters)

eSentire may filter traffic based on volume to optimize service delivery. Once investigated, events are classified, alerted, and escalated to Client if an action required. eSentire will utilize the escalation process, agreed upon during the on-boarding process, to contact and relay information to the Client. The defined escalation process is a mutually agreed upon process between the Client and eSentire.

If Client is subscribed to multiple eSentire services, response may be implemented at multiple enforcement points, including but not limited to network, endpoint, and cloud.

3.2 Response Actions

At the conclusion of a review of a Work Item, eSentire will classify the item as either a threat or non-threat. The classification of an event as a "threat" will generate a Threat Case and be further evaluated and marked by severity level (Low, Moderate, High, or Critical), which are further defined within the Service Level Objectives (see section 7). A list of classifications, severity levels, and the associated actions/alerts and follow up expected is as defined in table 1 below:

Table 1:

Classification	Severity Level	Action	Alert	Disposition	Follow Up
Threat	Low/Medium	No Client Action Needed	No Alert	True Positive	Automated remediation actions (SOC can assist with further actions upon request)
		Client Action Needed	Alert with description and relevant data	True Positive	Underlying telemetry and associated data will be available Clients Insight Portal dashboard Subscription to Prevent, Detect, & Respond will result in automated remediation actions (SOC can assist with further actions upon request)
	High/Critical	Client Action Needed	Alert with description and relevant data eSentire threat response • host isolation • identity isolation • remediation actions Escalation procedure (email/phone call with acknowledgement expected)	True Positive	Underlying telemetry and associated data will be available on Insight Portal Subscription to Prevent, Detect, & Respond will result in automated remediation actions (SOC can assist with further actions upon request)
Non-Threat (False Positive / Benign)	N/A	No Client Action Needed	No Alert	False Positive	Recurrences of identical activity will be logged as ignored

3.3 Remediation Actions

eSentire can assist the Client with remediation activities for high or critical threats from active hands-on keyboard attackers, on the endpoint itself, upon alerting Client. The types of remediation support actions that can be provided by eSentire, in coordination with Client are as follows:

- Process or file denylisting on an endpoint
- Block and kill malicious processes.

- Detect and prevent known/unknown bad software (quarantine malicious files)
- Downloading files to an endpoint.
- Isolate an endpoint.
- Initiate a remote shell interactive session ("**Real Time Response**") on the endpoint to perform a deeper investigation or remediation actions, which can (at our discretion) include:
    - Stop/remove services and registry keys.
    - Perform system reboots to remove malware from volatile memory.
    - Gather files and memory for host.
    - Terminate processes.
    - Delete files on an endpoint.

4. Subscription Options

The Service contains one service delivery option which is Endpoint Services – Prevent, Detect and Respond – Managed Only. The Service requires that Client secures appropriate endpoint licensing with one of the product publishers listed in section 4.2 below. A brief summary of the elements of the subscription are as follows (and as summarized in Table 2 below):

4.1 Endpoint Prevent, Detect and Respond – Managed Only ("Prevent, Detect, and Respond")

- Prevent: eSentire will assist with configuration of next-generation antivirus ("**NGAV**") functions to enable automated prevention of threats.
- Detect: Detection events and alerts from both the NGAV and endpoint, detect, and response ("**EDR**") modules will be monitored by eSentire and analyzed and investigated by automated processes and SOC Analysts. Detections will include those provided by the product publisher and eSentire developed detections.
- Respond: eSentire SOC Analysts will initiate response actions using the product publisher technology.

Table 2:

Endpoint Subscription	Threat Hunting	Automated Prevention	Host Isolation
Prevent		X	
Detect & Respond	X		X

4.2 Third-Party Licensing Requirements

Client must procure and maintain endpoint licensing ("**License**") with any of the listed product publishers (each a "**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 the Client's License instance. Client must purchase at least one of the following licenses:

- CrowdStrike Falcon Insight XDR + CrowdStrike Falcon Prevent + Threat Graph Standard
- VMware Carbon Black Cloud Endpoint Enterprise
- VMware Carbon Black Cloud Workload Enterprise
- Microsoft M365 E5, Microsoft M365 E5 Security Add-On, Microsoft Business Premium (plus x1 Azure AD P2 license), or Microsoft Defender for Endpoint Plan 2 standalone (plus x1 Azure AD P2 license).

Client will retain ownership of the License and will continue to have all access to utilize their License. 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 Term of the Service, 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. Deployment

Client is responsible for Agent deployment related to the Clients Product Publisher Licensing. eSentire will provide Clients with the required installation documentation for the Endpoint Agent.

6. Tuning and Configuration

eSentire is responsible for configuring and tuning the Service capabilities leveraging Clients Licensing. Service deployment methodologies can take up to 30 days to fully tune. This requires a special configuration and tuning process due to the automated blocking/killing capabilities that will need to be established. eSentire requires that Client has 80% of the contracted Agents deployed prior to completing the eSentire tuning process and moving the Service into a production-ready state. Detections utilizing Clients Licensing capability are handled by the eSentire (Prevent) during the tuning and configuration period(s). All detections provided pursuant to the Detect and Respond portion of the Service are handled by the eSentire SOC immediately upon Agent install, however, all Service activities related to the Prevent portion of the Service require tuning before sent to the SOC for real time. Once tuning has been completed, the Service will be live and transitioned to the SOC for real-time monitoring at which time the Service is considered fully deployed and in-production. Additional details related to tuning and configuration are as follows:

- Data required for detection begins streaming immediately after Client has installed the Agents.
- eSentire begins monitoring detection events immediately after an end-to-end verification test is successfully completed.
- The configuration of the Prevent portion of the Service is a phased approach.
- A tuning period of four weeks for tuning the Prevent portion of the Service begins once 80% of Agents are installed. Weekly meetings to take Client through configuration and tuning will happen over the four-week period.
- Once the tuning period is completed, Prevent with necessary exclusions will be fully active.
- Hosts must remain under eSentire's configured prevention policies to ensure compatibility and continued Service support.

7. Service Level Objectives

The ability for eSentire SOC to perform an investigation and assess whether a threat is malicious is dependent on Licensing from Product Publisher being integrated and in production in Client's applicable environment. The service levels contained on the Managed Detection and Response ("MDR") Services general description found here (https://www.esentire.com/legal/documents), are only applicable to Clients environment in scope that are licensed as part of the Service, and are actively communicating with the Service.

8. 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 above. In the event Client fails to perform its obligations herein, in the time and manner specified or contemplated below, or should any obligation set out herein with respect to the Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages. Notifying eSentire of newly added machines to the Service during the Service Term. Should the ingestion usage on a monthly average basis be more than 10% of the daily ingestion limit (identified on the Order Form), notwithstanding any security event, for more than two consecutive months, Client will move to the next ingestion level to accommodate its usage for the remainder of the Service Term.

Non-compliance with these obligations may result in suspension of the Service or suspension of service levels. A responsibilities matrix is located in Appendix A below.

8.1 Client Responsibilities

Client obligations include:

- Deployment and Endpoint Maintenance including:
  - installing Agents on endpoints in scope of the Service and working with eSentire to confirm Agents are operational;
  - granting eSentire access to all data and systems required for the Service;
  - ensuring there are no firewall rules, network configurations or other infrastructure issues that prevent communication from Agents to the Product Publisher's management server;
  - ensuring there is sufficient network bandwidth and access to perform the Service;
  - troubleshooting Agent configuration issues with Product Publisher; and
  - notifying eSentire of newly added Endpoints or additional Agents (not originally included in the scoping).

- Tuning, Configuration and User Management including:
  - being available for weekly meetings to discuss detections identified during tuning;
  - ensuring Client authorized contacts remain current, including approved access and all associated information (note: Clients authorized contacts are provided to eSentire by Client during Service inception and can be maintained through contact with the SOC or Client's CSM. Authorized contacts are individuals allowed to approve changes to services, configurations and to respond to escalated alerts); and
  - administering and maintaining user access within Client's Licensed instance.

- Investigation, Analysis and Response including:
  - responding to the escalated alerts and validating the legitimacy of the content contained within the Threat Case;
  - updating eSentire of any changes altering agreed upon escalation procedures; and
  - promptly providing information and assistance during SOC investigations conducted by eSentire when additional information is required.

8.2 eSentire Responsibilities:

- Detection Monitoring, Analysis & Resolution including:
  - ensuring all detections from Product Publisher are ingested into eSentire's XDR platform;
  - processing, enrichment and continuous tuning of raw telemetry and asset data to identify, patterns, flag anomalous activity and reduce false positives; and
  - automatic writebacks to resolve ingested alerts.

- Investigation, Remediation and Notification including:
  - 24/7 human-led investigation of tuned Alerts, utilizing all available tools and information to determine outcome of Alerts;
  - e-mail notifications, including recommendations, upon determination of an actionable security event, with escalated alerts by phone for high and critical severity notifications;
  - immediate host isolation for all confirmed high or critical threats, interrupting any active attacks;
  - deep-dive analysis and root cause analysis upon acknowledgement of critical alerts or upon request for non-critical alerts;
  - remediation actions (section 3.3), including taken upon determination of a critical incident by eSentire incident handlers; and
  - threat case summary for all notifications available on the Insight Portal.

- Threat Intelligence including:
  - integrations built and managed by our threat teams to cross-reference multiple subscriptions (network, log, or cloud), providing analysts with greater context for investigations; and
  - ad-hoc threat sweeps for indicators of compromise ("IOC's") based on eSentire's threat intelligence research and feeds.

- Policy and Environment Configurations and Consulting including:
  - introductory walkthrough and professional support;
  - blue team, endpoint consulting to implement eSentire recommended configurations, based on industry and Product Publisher essential practices;
  - weekly tuning and configuration meetings until service is in a ready state; and
  - post-deployment policy tuning and support.

9. Service Terms.

9.1 Exclusions

The Services do not provide Emergency Incident Response including but not limited to deep Forensic Investigation, recovery support, Litigation Support, Disaster Recovery and Business Continuity Planning, and/or the quantification of the Business Impact, with respect to all Client assets, whether currently under embedded Incident Response or not.

Services are limited to in-scope Endpoints and do not extend to any Product Publisher license add-on, module, or feature unless mentioned in the above description. eSentire operationalizes the Anti-virus (Prevent) and EDR (Detect and Respond) modules/features of the Product Publishers Agent technology for the purposes of preventing, responding to, or remediating threats. Examples of out-of-scope modules include, but are not limited to, Device Control, Firewall Control, Workloads, Identity, or other optional services that may be available to Client.

Appendix A: Responsibilities Matrix

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

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