Service Description:
Endpoint Services– eSentire Agent

1. Service Overview

eSentire MDR for Endpoint – eSentire Agent (the "**Service**") is a managed service providing endpoint-level visibility and control to support threat prevention, threat detection, investigation, and response ("the Service") through software agents (the "**eSentire Agent**" or "**Agent**") installed on servers, laptops, and desktop devices with supported operating systems within a client environment (the "**Client Environment**"). The eSentire Agent is integrated with the Atlas Platform and 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 appropriate prevention, investigation, response, and remediation.

The Service will collect information from endpoints in the Client Environment. Each eSentire Agent only collects data from the endpoint on which it is installed. Suspicious activity detected is monitored by eSentire's SOC on a 24x7x365 basis, initiating investigations, enabling response, and notifying Client as required.

2. Service Definitions

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 (https://www.esentire.com/legal/documents?Service=MDR, referred to herein as the "**MDR Landing Page**").

3. Service Capabilities

3.1. Description. eSentire Agents will be installed on all in-scope endpoints in the Client Environment and the Service will capture telemetry, retain this collected data in the Atlas Platform, automatically prevent threats, enable SOC investigations of known threats and suspicious activity, facilitate threat hunting, create Alerts for Client, and allow the SOC to respond and remediate where appropriate. Client will have access to documentation and limited self-management of Agents through the Insight Portal, which will also consolidate threat Alerts with investigation details from eSentire SOC analysts. The Service includes the following:

- **Self-Service Install**. Client will access the Insight Portal to download binaries and installation instructions to deploy eSentire Agents to its in-scope endpoints.
- **Data Capture**. From in-scope endpoints, the Agent will collect system information such as IP addresses, logged in users, running processes and other data points critical to threat detection, investigation, and response activity. Such telemetry data will be securely transported to and stored on the Atlas Platform to be used by eSentire in threat detection, analysis, and investigations.
- **Data Retention**. Telemetry data gathered will be retained for 13 months, during the Service Term, for use by the SOC in the delivery of the Services. All data transported to the Atlas Platform for analysis and review are stored in the Atlas Platform and are subject to eSentire's administrative, physical, and technical safeguards. Client Data is encrypted in transit and at rest. The Atlas Platform is a multi-tenant platform, and all Client Data is logically separated from the data of other clients. Exports of subsets of collected data are available to the Client by contacting eSentire support. Upon

termination of the Service, Client Data in the eSentire environment is securely destroyed or allowed to expire per standard retention policies while remaining under standard safeguards.

- **Detection and Analysis**. Collected Client Data will be analyzed by eSentire systems and human analysts, identifying potentially threatening or suspicious activity.
- **Prevention.** A deep learning static and behavioral analysis engine is used to prevent known and unknown malware, zero-day exploits, ransomware, and common script-based attacks by blocking download, write to disk and/or execution. eSentire will monitor prevention events and provide tuning assistance and exception configuration as required. This Prevention Module is included in the Service; however, Client may order a Service subscription option which disables the Prevention Module if required (I.e., when other anti-malware agents exist in the Client Environment and may conflict) which will be detailed on the Order Form if applicable.
- **SOC Capabilities - Alerting, Response and Remediation**. Work Items for potential threats are processed, enriched, and delivered to eSentire's SOC. eSentire uses the data from eSentire Agents within the provision of its broader MDR services by including other signals, threat intelligence, and investigations to determine the nature and severity of the security event and will notify Client according to defined escalation procedures and service levels. The SOC will respond and remediate Work Items where appropriate and previously agreed between eSentire and Client. eSentire is responsible for threat prevention (if included in Client's order), detection, analysis, investigation, escalation. Response is a shared responsibility between eSentire and Client. eSentire is responsible for Work Item analysis and investigation to determine if it is Actionable and warrants an Alert escalation to Client for potential response action..
- **Automated notification.** Selected Work Items may result in automated notifications directly to Client, bypassing SOC investigation.
- **Threat Sweeps and Threat Hunts.** Security analysts will periodically perform deep forensic investigations aggregating and correlating data from the Client Environment and other sources to identify elusive threats. Sweeps and hunts are not performed in real time, are not subject to any service level agreements and are initiated purely from observed activity, threat research or hypotheses.
- **Insight Portal Access.** The Insight Portal is the primary Client interface to access the outcomes of all eSentire MDR services, including the Service. The Insight Portal provides an overview of Client's security posture and provides details on Threat Cases, support tickets, ongoing investigations, service status, and other information. Client can access more detailed information about the installed Agents through the Agent dashboard. Client will also have the ability to perform some self-service actions as further detailed in section 8 below.

3.2. <u>Response Actions.</u> At Service inception, an eSentire Onboarding Manager will meet with Client to develop the specific response protocols. Any developed protocols will be extensions beyond the base Threat Case and notification actions covered in standard service levels.

3.3. <u>Remediation Actions.</u> eSentire does not take direct remediation actions, however, email notifications may contain remediation advice to be executed by Client. Examples of recommended remediation actions may include actions such as:

- restoring one or more endpoints from backup
- persistence removal
- pursue security awareness training
- etc.

4. Subscription Options

eSentire is leveraging technology developed by Deep Instinct, LLC, to provide the Prevention Module. Deep Instinct's technology is licensed by eSentire and included in the eSentire Agent as part of the Service. The Service includes two subscription options as detailed below:

4.1 eSentire Agent. This is the standard service offering and includes Agent installations on in-scope endpoints to capture telemetry data, identify possible threats, enable SOC investigations, facilitate threat hunting, and create Alerts. The eSentire SOC will respond and remediate where appropriate. This Service subscription option also offers endpoint prevention and will be used to automatically prevent known and unknown malware, zero-day exploits, ransomware, and common script-based attacks by blocking download, write to disk and/or execution.

4.2 eSentire Agent – Prevention Module Excluded. In the case where the Prevention Module functionality conflicts with existing anti-virus/endpoint protection platforms, Client may order this subscription option in which the Prevention Module can be disabled from the Service. This subscription option of the Service includes Agent installations on in-scope endpoints to capture telemetry data, identify possible threats, enable SOC investigations, facilitate threat hunting, create Alerts, and allow the SOC to respond and remediate where appropriate.

5. Deployment

The number of licenses ordered are summarized on the Order Form. Eligible target systems for the Service, include Client owned laptops, desktops, workstations, and servers running supported Windows, MacOS or Linux operating systems. See Agent documentation for supported operating systems. Following receipt of a signed order from Client, eSentire will send Client an email with instructions on how to access required installation documentation and installation package for the eSentire Agent via the Insight Portal. Client is responsible for installation of the Agents on their in-scope endpoints. eSentire will provide Client access to an eSentire onboarding manager for additional assistance and guidance during the deployment process.

Client will be responsible for validating all Service-related information available on the Insight Portal and the deployment of the Agent to at least 80% of the in-scope endpoints. Once 80% of total Agents ordered are installed, monitoring of collected telemetry data by the SOC will begin and all Service features described herein will be available, subject to tuning of the Prevention Module, which (unless disabled by Client) will commence at this time (see section 6 below).

6. Configuration and Tuning

eSentire is responsible for configuration and tuning of the Agent. The Prevention Module requires a configuration and tuning process due to the automated blocking/killing capabilities, which requires approximately four weeks. Threats detected by the Prevention Module are handled by the eSentire deployment engineer during the configuration and tuning period. All other detections are handled by the eSentire SOC immediately following successful installation of the Agent. Handover of Prevention Module detections to the SOC will occur at the end of the tuning phase.

Additional details related to configuration and tuning include:

- Weekly meetings to take Client through configuration and tuning will happen over a four-week period.
- Once the Service is in a tuned state, the Service is transitioned into full production monitoring by the eSentire SOC.

- Periodically, eSentire will review and make any necessary amendments to tuning – yearly, or more frequently as required due to material changes in software/service capability, in the Client Environment, in service scope, or in the threat landscape.

7. Maintenance and Support

eSentire will be responsible for providing updates to the eSentire Agent as well as maintenance of services residing within the Atlas Platform. Notification of updates will be sent out at least two weeks prior to Agent updates being pushed out to endpoints the Client Environment. Installation of patches to Agents in the Client Environment will be the responsibility of eSentire; Client will be consulted and informed. Updates requiring reboot or other disruptions to the host endpoint will be scheduled with Client. Updates to Prevention Module tuning, such as allowlisting specific processes are available by contacting the SOC (email (esoc@esentire.com), creating a ticket in the Insight Portal, or phone call to 1-866-579-2200).

8. Co-Management

Client will be provided limited management of its installed instances of eSentire Agent though the Insight Portal. This management includes self-service access to:

- Agent health status
- Up-to-date installation files, installation instructions and documentation
- Endpoint isolation/remove isolation
- Uninstall Agent on Endpoints

9. Service Level Objectives

The ability of the eSentire SOC to perform an investigation and assess a threat is dependent on a licensed Agent being installed on an endpoint in Client's environment. The service level objectives found on the MDR Landing Page are only applicable to Agents that are licensed as part of the Service and are actively communicating with the eSentire SOC.

10. Responsibilities

The responsibilities of each party are summarized below and in the responsibilities matrix which can be found in Appendix A.

10.1 Client Responsibilities: To maximize the effectiveness of the Service, Client is responsible for performing the obligations listed below. Client acknowledges that non-compliance with these obligations may interfere with eSentire's ability to deliver the Service in accordance with the applicable service levels agreed to, and result in suspension of the Service. Client's obligations include:

- Working with eSentire to implement the proper security protections to limit attack vectors and increase security posture.
- Ensuring any changes to access into the Client Environment are communicated to eSentire.
- Providing the necessary resources, information, documentation and access to personnel, equipment, and systems, as reasonably required by eSentire, to allow eSentire to perform the Service.
- Deploying eSentire Agents to Client endpoints and working with eSentire to confirm they have been successfully installed within a reasonable timeframe (not to exceed 30 days).
- Granting access to all data and systems required for the successful delivery of the Service.
- Ensuring that no firewall rules or other network blocking exists that would negatively impact communication by the eSentire Agent between endpoints and the eSentire SOC.

- Ensuring that all required exceptions for existing security tools are in place before installation of the eSentire Agent.

In the event Client fails to perform its obligations in the time and manner specified or contemplated above, or should any assumption set out herein with respect to the Service fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages.

10.2 eSentire Responsibilities: eSentire's obligations include:

10.2.1 Detection Monitoring, Analysis & Resolution.

- Ensuring all telemetry data from the eSentire Agent are ingested into the Atlas Platform.
- Processing, enrichment, and continuous tuning to identify patterns, flag anomalous activity and reduce false positives.

10.2.2 Investigation, Remediation and Notification.

- Providing 24/7 human-led investigation of Alerts, utilizing all available tools and information.
- Supporting notification requirements as outlined in any service level agreements.
- Performing immediate host isolation for all confirmed Actionable Work Items.
- Performing deep-dive analysis and root cause analysis upon acknowledgement of critical Alerts or upon request for non-critical Alerts.
- Providing Threat Case summary on the Insight Portal.

10.2.3 Threat Intelligence.

- Performing ad hoc threat sweeps for indicators of compromise ("**IOCs**") based on eSentire's threat intelligence research and intelligence feeds.

10.2.4 Policy and Environment Configurations and Consulting.

- Hosting weekly configuration and tuning meetings until the Service is in a ready state.
- Providing post-deployment policy tuning and support.
- Providing updates to Agent instances operating on Client's endpoints.

11. Service Availability

SOC monitoring, investigation, response, and notification is a 24X7X365 service. Technical support for the eSentire Agent is available 8am-6pm EST, Monday-Friday excluding Canadian statutory holidays. After-hours support for high severity issues is available by contacting the SOC.

12. Service Turndown

When Client discontinues the Service, an email will be sent two to three days prior to decommissioning to provide Client with instructions to uninstall the Agent. Upon termination of the Service, all collected data in the eSentire environment is securely destroyed or allowed to expire per standard policies while remaining under standard safeguards.

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
Security – Ad hoc threat sweeps for IOCs	-	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	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– Monitoring of agent health	RA	I
Health – Managing sensor updates	I	RA
Health – Adding and removing hosts from isolation	RAI	RAI
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