eSENTIRE

Service Description:
Endpoint Services – SentinelOne

1. Service Overview

eSentire's Managed Detection Response for Endpoint Services - SentinelOne (the "**Service**") is a managed service providing endpoint-level visibility and control to support threat prevention, threat detection, investigation, and response leveraging the SentinelOne 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 Prevent, 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. Either subscription level selected by Client is supported by eSentire's SOC on a 24x7x365 basis.

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

3.1. Investigation, Analysis and Response. eSentire is responsible for threat detection, analysis, investigation, escalation, and isolation. eSentire is responsible for security event analysis and investigation to determine if a security event is real and warrants an escalation to the Client and potential response action (isolation). If an event is deemed as actionable, due to its behavior and the type of detection, it will be escalated to the 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 the Client.

eSentire will investigate all security events identified through the Endpoint service and escalate actionable alerts as appropriate in accordance with the Service Level Objectives (SLOs). Once investigated, events are classified, alerted, and escalated to the Client if there is 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.

It is eSentire's responsibility to classify the criticality of the Alerts derived from individual events as part of the Endpoint Service.

4. Subscription Types

4.1. Subscriptions. Client has the ability to subscribe any of the following Endpoint Service - SentinelOne 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 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 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 Prevent, Detect and Respond Subscription:
In addition to what is summarized in 4.1.1. above, this Subscription option includes 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 a Client's Endpoint. This component of the service gives eSentire full spectrum visibility into the endpoint and allows for hunting for specific threats, isolating endpoints and performing other response actions as needed in the platform. In addition to the above, 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.

4.2 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:

4.2.1 MSSP Licensing requirements:
In this Service option, eSentire will procure all required licensing directly from SentinelOne, will be the licensee of record with SentinelOne, and provide management. As part of this license, if Client has ordered the Prevent, Detect and Respond Subscription - eSentire will have access to 30 Days of Client data retention ("Deep Visibility") 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.

4.2.2 Enterprise Licensing requirements:

In this Service option, eSentire will procure and resell SentinelOne licenses to Client. Client will be the licensee of record with SentinelOne for the term of the Services, and eSentire shall manage the licensing for Client. As part of this license, Client and eSentire will have access to at least 14 days Client data retention ("Deep Visibility") on the licenced instance, 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 SentinelOne licensed environment. The licenses included with an Enterprise Service sale will include entitlements to the following:

Description	Quantity[2]
Complete Protection Platform and Enterprise Support (Per Workstation)	endpoints[1]
Platform Pro (Per endpoint)	endpoints[1]
Deep Visibility (14 Days)	endpoints[1]
[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).	

4.2.3 Managed Only Licensing requirements:

In this Service option, eSentire will manage Client's SentinelOne endpoint licensing, which has been procured by Client. Client must procure and maintain its endpoint licensing ("License") with SentinelOne, during the entire Term of the Service, and coordinate proper licensing permissions with SentinelOne, 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:

- SentinelOne Singularity Control (required for Prevent Subscription)
- SentinelOne Singularity Complete (required for Prevent, Detect, and Respond Subscription)
    - Also recommended at least 14 days retention ("Deep Visibility") to enable threat hunting.

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 product-ready state, the Agent will be configured to execute one 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 the Prevent, Detect and Respond Subscription, in addition to the above, 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 the Client opts-out, eSentire will isolate potentially compromised machines. eSentire will isolate the machine and notify the 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 Agents are considered authorized for isolation unless otherwise communicated by the 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 the 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 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.

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.

eSentire is responsible for providing Clients with the required installation documentation for the Endpoint Agent. eSentire will provide an expert deployment engineer resource during deployment of the Endpoint service to assist with questions around how to deploy and the requirements for the service. There are two key components to the service which will dictate the deployment services required for the engagement.

8. Tuning and Configuration

eSentire is responsible for configuring and the Services. The Prevent Subscription option requires a special configuration and tuning process due to the automated blocking/killing capabilities, and detections through the Prevent capability are handled by an eSentire security consultant during the tuning and configuration period(s). All detections via the Endpoint Prevent, Detect and Respond capability are handled by the eSentire SOC immediately upon Agent install.

8.1. Endpoint Services – SentinelOne - Prevent Subscription. A 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 the 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 – SentinelOne – Prevent, Detect and Respond Subscription. In addition to the summary in section 8.1, a summary of the tuning and configuration for the detect and respond portion of 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.

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 promptly 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 SentinelOne, 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 applicable terms applicable to use of the licensing contained in the SentinelOne Master Subscription Agreement ("MSA") (found here: www.sentinelone.com/legal/master-subscription-agreement), which are required by the Product Publisher.

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. Definitions (solely for the purposes of this section 11):
- "Product" means any of Product Publisher's cloud-based Product or other products ordered by Client through eSentire, the available accompanying API's, the Product Publisher data, and any related documentation.

11.2.2. Access and Use Rights. Subject to the terms and conditions of this Agreement, during the Term of this Agreement, Client has a non-transferable, non-sublicensable, non-exclusive license to access

and use the Product delivered with the Endpoint Services in accordance with any applicable Product documentation, and solely for Client's internal use.

11.2.3. Acknowledgements: Client acknowledges that: (i) the Agreement is solely between eSentire and Client; (ii) eSentire is solely responsible to the Client for the Endpoint Services; (iii) Endpoint Product Publisher has no liability directly to Client, and Client will seek any remedies to which it may be entitled under the Agreement solely against eSentire, and any provisions of the Agreement regarding the limitation of Endpoint Product Publisher's liability shall survive expiration or termination of the Agreement indefinitely; (iv) the Client may not, and may not help or assist others, to modify, disclose, alter, translate or create derivative works of the Product used in delivering the Endpoint Services, sublicense, resell, distribute, lease, rent, lend, transfer, assign or otherwise dispose of the Product used in delivering the Endpoint Services, or use the Endpoint Services other than as expressly permitted by the Order Form.

11.2.4. Restrictions: Client may not use of the Product delivered as part of the Endpoint Services to (i) store, transmit or test for any viruses, Product routines or other code designed to permit unauthorized access, disable, erase or otherwise harm Product, hardware or data, or to perform any other harmful actions; (ii) probe, scan or test the efficacy or vulnerability of the Product, or take any action in an effort to circumvent or undermine the Product, except for the legitimate testing of the Product in coordination with Product Publisher; (iii) attempt or actually disassemble, decompile or reverse engineer, copy, frame or mirror any part or content of the Product; (h) access, test, and/or use the Endpoint Services or Product in any way to build a competitive product or service, or copy any features or functions of the Endpoint Services or Product; (i) interfere with or disrupt the integrity or performance of the Product; (j) attempt to gain unauthorized access to the Endpoint Services or their related systems or networks; or (k) disclose to any third party or publish in any media any performance information or analysis relating to the Endpoint Services or Product.

11.2.5. Compliance with Laws: 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, including, without limitation to store or transmit infringing, libelous or otherwise unlawful or tortious material, or material in violation of third-party property, personal or privacy rights

11.2.6. Warranty: eSentire is solely responsible for any product warranties, whether express or implied by law, and for all liability from and to Client arising out of eSentire's implementation and use of the Endpoint Services.

11.2.7. Expiration or Termination: Promptly upon expiration or termination of the Order Form, the Client will delete all copies of the Endpoint related Product and all related materials, and at Endpoint Product Publishers' request (via eSentire), the Client must agree to certify the destruction and return of the Product used in delivering the Endpoint Services and related materials.

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 STAR Rules, IOCs or implementations	RA	C
System – Custom alerts, dashboards, or reports	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