Managed Endpoint Defense

eSentire will provide best practice guidance through the Client's installation of endpoint defense agents (CB Defense) and direct assistance in establishing initial monitoring policies for endpoint defense. After Client installation and over a period of no more than six (6) weeks, eSentire analysts then assists the definition of standard blocking policies and consults with named Client representatives during scheduled sessions during regular business hours (Eastern timezone) to achieve a hardened policy state based on said Client's previously defined risk profile. At this hardened policy state, the endpoint defense agents are considered actively operational and delivering optimal Client endpoint defense agent value. The EPP Agents communicate events, perform blocking actions based on endpoint protection platform policy and update status to a corresponding third-party-provided cloud service. This third-party-provided cloud-hosted service is provided by the endpoint technology vendor and enables the co-management of endpoint protection platform policy management directly by the Client and by eSentire analysts (via GUI) and systems (via APIs) for the delivery of Endpoint Managed Defense Services. eSentire then provides support for ongoing policy amendment recommendations at the scheduled initiation of the Client and periodically and proactively monitors Client policy and main changes made by Client to said policies through the endpoint agent self-management portal. Requests for analyst consultation through Managed Endpoint Defense Service are maintained through telephone and email accessible 24 hours a day, 7 days per week and all interactions by or with eSentire analysts are during business hours (Eastern timezone). eSentire analysts provide periodic advice based on Client policy changes and unfolding global security circumstances and provides this directly on an as-needed basis and/or in scheduled quarterly business reviews.

Definitions

"Endpoint Protection Platform Agent" or "EPP Agent" means the specific piece of software deployed on the endpoint devices for the purpose of enabling or effecting the functions of an Endpoint Protection Platform.

"Endpoint Protection Platform" or "EPP" means all or part of a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

"Endpoint Protection Platform Cloud Service" refers to the centralized, cloud-based portion of the endpoint protection platform used for the management of multiple Client-deployed agents. This is the centralized co-management location used by both Client representatives and eSentire analysts and also is the data collection point for the eSentire data pipeline for further Managed Endpoint Defense analysis Services.

"eSentire Data Pipeline" is a universal method for the ingestion of signals from external sources like the Endpoint Protection Platform Cloud Service ultimately for the purpose of monitoring, auditing, detecting threats and anomalies, finding patterns and trends, applying deterministic and/or statistical and/or machine learning algorithms to assist or optimize the aforementioned as well as to generate Client-facing reporting and dashboards.

i. Powered by Leading Endpoint Technology – The Managed Endpoint Defense Service depends on and uses a leading endpoint protection platform including third-party provided endpoint agents and a corresponding third-party provided cloud service (both from same vendor of endpoint protection platform) to block identified malware and provide insight into potential endpoint threats at the client site and globally across the eSentire client base. The endpoint policy hardening recommendations during the activation and onboarding process along with the ongoing analysis, threat notifications and policy refinements of the Managed Endpoint Defense Service are based on the endpoint protection platform

(in toto, agents and cloud service) and include access to the third-party provided cloud service by deployed third-party provided endpoint agents and APIs from eSentire systems to this Endpoint Protection Platform via cloud portion of service.

ii. **Guided Endpoint Policy Deployment and Onboarding** -- eSentire provides best practice guidance through the Client's installation of endpoint protection platform agents and direct assistance in establishing initial monitoring policies for endpoint protection platform. After Client installation and over a period of no more than six (6) weeks, eSentire analysts then assists the definition of standard blocking policies and consults with named Client representatives during scheduled sessions during regular business hours (Eastern time zone) to achieve a hardened policy state based on said Client's previously defined risk profile. At this hardened policy state, the EPP Agents are considered actively operational and delivering ongoing Client endpoint protection platform functions.

iii. **Co-Managed Endpoint Protection Platform** -- eSentire will provide Client with secure access to third-party provided Endpoint Protection Platform Cloud Service access. This access allows both the Client and eSentire analysts to manage the Endpoint Protection Platform and serves as the source of truth for deployed policy.

iv. **Endpoint Protection Platform Event Collection** -- in addition to the co-managed access to the third-party provided Endpoint Protection Platform Cloud Service, eSentire will establish an event data pipeline from the third-party provided Endpoint Protection Platform Cloud Service in order to monitor and identify anomalies within the Client installation.

v. **Periodic policy recommendations to Client** – eSentire periodically and proactively monitors Client policy and main changes made by Client to said policies through EPP Agent self-management cloud service. eSentire analysts also provide periodic advice based on Client policy changes and unfolding global security circumstances and provides this directly on an as-needed basis and/or in scheduled quarterly business reviews. Additionally, eSentire will provide best practice recommendation and policy updates to the Endpoint Protection Platform based on industry information and through the monitoring of global eSentire endpoint protection platform deployment base.

vi. **Client-initiated policy consultation requests** –eSentire provides support for ongoing policy amendments recommendations of the Endpoint Protection Platform at the scheduled initiation of the Client. Requests for analyst consultation through the Managed Endpoint Defense Service are maintained through telephone and email, accessible 24x7x365, and all interactions by or with eSentire analysts will be scheduled in advance and occur during business hours in the North American Eastern time zone.

vii. **Client-provided Endpoint Protection Platform Agent licenses** may be supported as part of the Managed Endpoint Defense Service only using eSentire approved vendor EPP Agents and vendor EPP Agent version.

Client Responsibilities. Client is responsible for:

i. Granting access to any and all data and systems for receipt of the Managed Endpoint Defense Services;
ii. Installation of endpoint Agent software on workstations/endpoints, including any changes or updates to the endpoint which would have removed the Agent software;
iii. Ensuring no firewall rules or other blocking exists that would prevent the communication from endpoints to the Endpoint Protection Platform Cloud Service;
iv. Providing the necessary resources, information, documentation and access to personnel, equipment and systems, as reasonably required by eSentire, to allow eSentire to perform the Managed Endpoint Defense Services; and
v. Complying with all applicable local, state, provincial, federal and foreign laws in using the Managed Endpoint Defense Services.