eSENTIRE

Description:
eSentire Atlas Agent

1. Overview

eSentire's Atlas Agent (the "**eSentire Atlas Agent**" or "**Agent**"), is proprietary software owned by eSentire which, when installed on servers, laptops, and desktop devices with supported operating systems within a client environment (the "**Client Environment**"), can provide additional endpoint-level visibility and control to support threat prevention, threat detection, investigation, response and incident response.

2. Description

eSentire Atlas Agents are installed on all in-scope endpoints in the Client Environment and will actively capture telemetry while installed. The data collected by the Agent will be retained in eSentire's XDR platform (the "**Atlas Platform**") which consolidates all data and drives workflow for all eSentire MDR services. Client will have access to the following features/capabilities:

2.1. Self-Service Install. eSentire will send Client an email with instructions on how to access required installation and deployment instructions documentation and the installation package for the eSentire Agent via the eSentire web interface (the "**Insight Portal**"). The number of Agent licenses ordered are set out on the Order Form and will align to the eSentire Endpoint Service endpoint quantities ordered by Client. Eligible target systems for Agents include Client-owned laptops, desktops, workstations, and servers running supported Windows operating systems (supported systems can be provided upon request). 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.

2.2. Data Capture. Agents will collect system information on each endpoint on which they are installed, such as IP addresses, logged in users, running processes and other data points critical to threat detection, investigation, and response activity ("**Client Data**"). Client Data will be securely transported to and stored on the Atlas Platform.

2.3. Data Retention. Client Data gathered by each Agent will be retained until the earlier of either the expiration of the Endpoint Service or 13 months from collection. All Client Data collected by the Agent and transported to the Atlas Platform is stored in the Atlas Platform and is 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. See section 6 for Agent Turndown activities.

2.4. Co-management. Client will be provided with limited management rights over Clients installed instances of eSentire Agent within the Insight Portal. This management includes Client self-service access to:

- view Agent health status;
- view installation instructions and documentation and access up-to-date installation files;
- implement or remove endpoint isolation;
- uninstall Agents from endpoints (note: in the event Client removes Agents from endpoints via the self-service capabilities – some features/capabilities of the Agent will not be available)

2.5 Endpoint Management. Agents are installed as an add-on to eSentire's Endpoint Service, and the Agent automatically deploys CrowdStrike Endpoint Licensing on in scope endpoints.

2.6 Incident Response Services ("IR Services") - Discounted Rate and One Hour Return Call. Client may engage eSentire for IR Services by contacting the eSentire SOC. Upon contacting the SOC, a support ticket will be opened, and the eSentire IR team will return Client's call within one-hour from receiving the support ticket. If an IR Service is required following the call, eSentire will provide Client with an IR Service order form which will reflect a discounted hourly rate. IR Services may include forensics analysis, malcode analysis, mergers and acquisitions assessments, human resource policy/corporate security/PII/or data exfiltration investigations, eDiscovery collection, post breach support, breach consulting, or other related technical investigation support services.

2.7 Threat Detection. Telemetry captured by Agents is automatically examined for threat indicators.

2.8 Asset Inventory. For each endpoint where an Agent is installed, additional asset details of the endpoint will be automatically sent to the Atlas platform.

2.9 Threat Sweeps and Threat Hunts. In addition to threat sweeps and threat hunts conducted as part of Client's Endpoint Service, eSentire will leverage Agents to periodically perform additional ad-hoc investigations to aggregate and correlate Client Data with data from 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 on the basis of observed activity, threat research or hypotheses – as an additional view into the Client Environment over and above that of the Endpoint Service activities.

3. Maintenance and Support

eSentire will be responsible for providing updates to the eSentire Agent. Notification of updates will be issued at least two weeks prior to Agent updates being pushed out to endpoints in the Client Environment. Installation cadence of updates may be selected by Client to include automatic updating or manual updating by Client. Updates requiring reboot or other disruptions to the host endpoint will be scheduled with Client.

4. Responsibilities

eSentire responsibilities include:

- Confirming telemetry data from installed Agents are ingested into the Atlas Platform;
- Processing, enriching, and continuously tuning to identify patterns, flag anomalous activity and reduce false positives; and
- Performing ad hoc threat sweeps for indicators of compromise ("IOCs") based on eSentire's threat intelligence research and intelligence feeds.

5. Agent Turndown

When Client's Endpoint Service expires, or Client requests the Agent be removed from Client endpoints, eSentire will send Client an email two to three days prior to decommissioning to provide Client with instructions to uninstall the Agent. All Client Data in the eSentire environment shall be securely destroyed or allowed to expire per standard policies while remaining under standard safeguards.