eSENTIRE

# Service Description: Network Services

## 1. Service Overview

eSentire's Network Services are managed services that provide real-time capture and monitoring of network traffic to detect and respond to potential threats to Client systems (the "**Network Services**"). Network Services leverage physical or virtual network devices ("**Network Sensors**") in Client's physical and virtual networks and cloud environments (the "**Client Environment**") working in conjunction with the eSentire Atlas platform to monitor, store and analyze captured network traffic for potential threats, unusual behavior, or other indicators of compromise. Suspicious activity is monitored by eSentire's SOC 24x7x365, initiating investigations, issuing response actions to disrupt traffic, and notifying Client as required. The Network Services can also be configured to proactively and automatically disrupt known bad or threatening traffic. The Network Services can also be configured to proactively and automatically disrupt known bad or threatening traffic. The Network Services are fully managed and available on a subscription basis. Client may order the Network Services to be provided on physical and virtual networks, or cloud environments utilizing using quantities detailed on an Order Form (i.e. Workloads, Users, or units as defined below).

## 2. Service Definitions

In addition to the below, 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.

"**Users**" means the quantity of knowledge workers in Client network environment. When Client requests Network Services for its physical and VMware networks (also referred to as "**On-prem**"), the Order Form will detail the number of Users for such On-prem environments, physical sensors, and/or VMware virtual sensor(s).

"**Workloads**" means the number of AWS EC2 virtual machines, or host container systems in Client's network environment. When Client requests Network Services for Amazon Web Services ("**AWS**") virtual networks, the Order Form will detail the number of AWS Workloads and AWS virtual sensor(s).

## 2. Service Capabilities

2.1. Packet Capture. Network Sensors are positioned in Client's environment and utilize SPAN or TAP ports to collect and store packet data. Captured data is stored locally on the sensor and is leveraged for analysis by detection systems and by eSentire SOC Analysts and Threat Hunters in investigations.

2.2. Metadata Capture. Network metadata is captured to be used in investigations and threat hunts.

2.3. Traffic Disruption. Connections suspected to be malicious or undesired as detected by various detection features are interrupted by the Network Sensor through configurable automated action, or through manual intervention by an eSentire SOC Analyst. This interruption will be executed through actions taken by the Network sensor, through integration to Client firewall(s), or both, as appropriate.

2.4. Deep Packet Inspection and Intrusion Detection. Captured packets are inspected using rule, signature- and ML-based detections to identify potential threats and issue alerts to the eSentire

SOC and/or Client. This feature may also identify policy/acceptable use violations per Client configuration and create informational notifications.

2.5. Executioner. Downloads of executable programs are detected and can result in notation of the event for reporting, automated notification to Client and/or disruption of the download.

2.6. Threat Intelligence. eSentire's Threat Intelligence (TI) library is used to detect connections to and from known bad actors. The TI database is comprised of eSentire proprietary research, other open-source and subscription sources of intelligence and the real-time results of SOC investigations.

2.7. Country Killer. Geolocation can be used to detect and block connection attempts to and from nation states on a Client-configurable blocklist.

2.8. SSL Decryption. For encrypted networks, the Network sensor can operate with select network visibility devices to access a decrypted span for full visibility.

2.9. Data Access and Reporting. The eSentire Insight portal is the primary Client interface to access the outcomes of MDR services, including Network. Insight portal provides an overview of Client's security posture and details on escalated alerts, ongoing investigations, service status and other information.

2.10. Network Sensors. Upon the Parties executing an Order Form for the Network Services, eSentire will provide at least one physical and/or virtual Network Sensor for each location that is to receive the Network Services as detailed on the applicable Order Form. Sensors will be sized according to traffic volumes and storage requirements and identified on the applicable Order Form. Network Sensor(s) will be deployed with one or more SPAN or TAPs to analyze network traffic flows of the following types:

- External Network (Internet) to Internal Network.
- Internal Network to External Network (Internet).
- Other data segments as required and depending on the volume of data to be monitored and capacity of the Sensor (VPN, DMZ, VoIP, Market Data, etc.).

eSentire will configure and remotely manage the Sensor and its embedded software as part of the Network Services. Client may only access the configuration of such Sensor with eSentire's prior written authorization. eSentire shall only access the configuration of other network devices connected to the Sensor with Client's authorization and shall do so through an encrypted and secure means.

eSentire is responsible for software updates for the Network Sensor and will perform periodic vulnerability scans and other tests to maintain a secure solution. Client may choose from a set of available maintenance windows to receive updates.

## 3. Service Level Objectives

The ability for eSentire SOC to perform an investigation and assess whether a threat is malicious is dependent on a supported Network Sensor being installed on a licensed host in Client's IT environment. The service levels in the MDR General Information document are only applicable to hosts licensed as part of the service and actively communicating with the Network service.

eSentire will monitor the Network Services 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.

## 4. Client Responsibilities

Client will perform the obligations listed below and acknowledges that the ability for eSentire to deliver the Network 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 Network Service or suspension of service levels. Client is responsible for:

- all data and systems which Client grants access to for receipt of the Network Services;
- obtaining all necessary licenses, permissions, and consents to enable eSentire to access Client's network and servers in order to provide the Network Services;
- designating a Project Coordinator to work directly with and serve as the primary Client contact with eSentire for the duration of Client's receipt of the Network Services;
- providing eSentire with a complete copy of its security (including privacy) policies, as available. Client is solely responsible for creating, maintaining, and enforcing its security policies to protect the security of Client Data and Systems;
- its choice of equipment, systems, software and online content;
- providing the necessary resources, information, documentation and access to personnel, equipment, and systems, as reasonably required by eSentire, to allow eSentire to perform the Network Services;
- providing a current network topology diagram to ensure capturing the correct traffic and correct configuration of the Network Services;
- notifying eSentire in advance of any network changes that will affect Client's network topology and /configuration so that all relevant traffic is being captured within the Sensor; and
- communicating all network infrastructure changes to eSentire. Effective monitoring requires that ability to SPAN or TAP an interface on any applicable segment.
- The cost to run workloads in the cloud and transfer data in and out of the cloud is entirely the responsibility of Client, including all public cloud costs to run eSentire's software images.

In event Client fails to perform its obligations in the time and manner specified or contemplated above, or should any assumption outlined herein with respect to the Network Services fail to be valid or accurate, then eSentire will not be responsible for any related delay or damages. If Client fails to notify eSentire of network changes as contemplated above, then eSentire shall be released from all obligations to monitor Client's network until Client has notified eSentire of such change.

## 5. Exclusions

The MDR service does 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 customer assets, whether currently under Embedded Incident Response or not.

Firewall integration is an optional response mechanism limited to a defined set of supported firewall models.