Network Services

The Service name was updated by eSentire from “esNETWORK Services”, to “Network Services”. All other content remains the same.

Definitions

Cloud Services – The collective cloud-based service offerings, including all services related to Network Services.
Alert - An event or set of events that eSentire will escalate to the Customer.
Emergency Incident Response - The rapid mobilization and deployment activities aimed at quickly securing Client systems and networks, providing incident response services beyond what MDR provides. Covers the full lifecycle of an incident - containing the full extent of the attack (across all attack surfaces).
Embedded Incident Response - MDR will identify and contain the attacker (within the visibility and scope of the MDR service) and provide remediation guidance to the customer.
Forensic investigation – Salvaging as much information as possible from the Client’s systems and networks deemed in scope and regression analyzing that information to conclusively determine the full extent of compromised assets.
Litigation support – Any litigation support, including but not limited to expert and fact witness testimony.
Disaster recovery and business continuity planning – Assessment, execution and/or building of disaster recovery and continuity planning processes and techniques. Used to help an organization recover from a disaster and continue or resume routine business operations.
Business impact – Any quantification of the reputational, operational, compliance or financial impact to the customer’s business.

Service Description

eSentire's Network Service is a managed service that provides 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 the 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 Security Operations Center (SOC) 24x7x365, initiating investigations, issuing response actions to disrupt traffic and notifying the Client as required. 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.

Service Features

Packet Capture

Network Sensors are positioned in the client 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.

Metadata Capture

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

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.

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

Executioner

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

Asset Manager Protect (AMP) Threat Intelligence

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

Country Killer

Geolocation is used to detect connection attempts to nation states on a Client-configurable blocklist.

SSL Decryption

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

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 the Client's security posture and details on escalated alerts, ongoing investigations, service status and other information.

Network Sensors

Upon the Parties executing an Order Form for the Network Services, eSentire will provide at least one (1) 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. Small Office Home Office ("SOHO") Sensors will be restricted to internal network traffic only.

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.).
- For SOHO Sensor Only: Home network user traffic should be segregated from business user traffic. Non-business users should not have access to the eSentire SOHO solution.

- For SOHO Sensor Only: Sensor deployment on the local network must support Ethernet (IEEE 802.3x) standards and throughputs. WAN/Internet (site-site VPN) must support typical consumer broadband services available from major network operations (e.g. Cable, DSL, FTTx, WiMax, 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. The Client may choose from a set of available maintenance windows to receive updates.

Service Level Objectives

Severity Priority	Alert Category	Notification/Escalation
Low (P4)	Minor activity is recorded but not alerted.	None. Accessible on demand through Insight portal.
Medium (P3)	Acceptable Use Policy violations.	Automated email notification within 120 minutes of reception of the policy violation event on the eSentire platform.
High (P2)	Potential threat activity that does not require immediate attention but if left unchecked may lead to more severe security incidents.	Email notification within 40 minutes of determination of the security event by the SOC.
Critical (P1)	Threat activity that requires immediate attention. These items may indicate that a severe security incident is underway or is imminent. This category also includes issues that indicate a disruption in eSentire service.	Email notification within 20 minutes of the determination of a security event followed by phone call to the Client per defined escalation procedures.

Client Responsibilities

Client is responsible for:

- any and 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 the 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 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.

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. In the event that Client fails to notify eSentire of network changes as contemplated above, then eSentire shall be released from any and all obligations to monitor the Client's network until Client has notified eSentire of such change.

Reports and Confidentiality

Except for the purpose of fulfilling eSentire's obligation under this Agreement, eSentire shall not disclose the information derived to any party for any purpose without express written consent from the Client and all Client information is bound by the Confidentiality provisions set out in the Terms and Conditions.

Exclusions

The Network Services exclude the following:

- the design, creation, maintenance and enforcement of a security policy for Client;
- eSentire attempting to access Client's servers without Client's express written or verbal consent; and
- eSentire is not responsible to provide network hardware required to SPAN networks (such as switches, hubs, or network taps) and has no liability or responsibility in the event of inability to SPAN any interface.

The MDR service does not provide emergency incident response (as defined above) 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.