Endpoint Services – Microsoft

The Service name was updated by eSentire from “esENDPOINT for Microsoft Corporation Services”, to “Endpoint Services - Microsoft”. All other content remains the same.

Definitions

Endpoint Agent or Agent means the endpoint software agent utilized in providing the Endpoint services and as further described below.
Alert means an event that eSentire will escalate to the Client.
Emergency Incident Response means 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 means 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 means 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 means any litigation support, including but not limited to expert and fact witness testimony.
Disaster recovery and business continuity planning means 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 means any quantification of the reputational, operational, compliance or financial impact to the customer’s business.

Service Capabilities

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 Services 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 Customer. 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 Services.

Subscription Types

The Client can subscribe to two different types Endpoint subscriptions: Endpoint Prevent subscription and

Endpoint Detect and Respond subscription, both of which are available to ensure complete endpoint coverage.

Endpoint Prevent Subscription

- eSentire SOC will monitor detection and prevention events
- Machine Learning (ML) and Artificial Intelligence (AI) are used to detect known and unknown malware and ransomware
- Behavior-based indicators of attack (IOAs) prevent sophisticated file-less and malware-free attacks
- Exploit blocking stops the execution and spread of threats via unpatched vulnerabilities
- Threat Intelligence prevention blocks activities known to be malicious

Endpoint Detect and Respond Subscription

- eSentire SOC will investigate and respond to detections
- Continuous raw event recording provides full spectrum visibility at the endpoint
- Enables threat hunting—proactive and managed—with full endpoint activity details
- Enables entire attack life cycle visibility with context and threat intelligence data
- Delivers situational awareness on the current threat level of the organization, and how its changing over time

	Threat hunting	**Automated prevention**	**Host isolation**	**Enhanced ML capabilities**
Endpoint Prevent		X		
Endpoint Detect and Respond	X		X	X

Response Actions for Identified Threats

If Client is subscribed to Endpoint Prevent, once moved to a product-ready state, the Endpoint 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
- Detect and prevent known/unknown bad software (quarantine)

If Client is subscribed to Endpoint Detect and Respond, following the successful identification of a confirmed threat targeting a Client environment, the eSentire SOC will utilize the Endpoint Services to execute one of the following actions:

- Endpoint isolation
- Initiate interactive session on endpoint
- Download files to endpoint
- Delete files on endpoint
- Gather files and memory for host

If Client is subscribed to multiple eSentire services, response may be implemented at multiple enforcement points, including but not limited to network, endpoint, and cloud isolation.

Unless the Client opts-out, as part of the Endpoint Detect and Respond, eSentire will isolate potentially compromised machines. eSentire will isolate the machine using the Endpoint Detect and Respond

subscription 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 Endpoint Detect and Respond Agents are considered authorized for isolation unless otherwise communicated by the Client.
- eSentire will escalate all Alerts that require isolation to Client for their 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.

Client's subscribed to Endpoint Detect and Respond 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. eSentire is limited to endpoint response actions through the agents powered by the Endpoint Detect and Respond subscription.

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 the Customer. All Alerts are available within the eSentire Portal for Client review. All reporting is delivered through the eSentire Portal.

Deployment

eSentire is responsible for providing Client 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. An overview of the two subscriptions types are below:

- Endpoint Prevent - relates to the implementation of Next-Gen AV (NGAV) capabilities such as policy and configuration-based prevention mechanisms within the Endpoint service. This includes but is not limited to the ability to block, kill, or quarantine attempted malicious code execution and malicious running processes.
- Endpoint Detect and Respond - relates to 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 Customer's endpoint. This component of the service gives eSentire full spectrum visibility into the endpoint and allows for hunting for specific threats.

Both Endpoint Prevent and Endpoint Detect and Respond deployment methodologies can take up to thirty (30) days to fully tune. The deployment engineer, working with the Client, requires that eighty percent (80%) of the contracted Agents are 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 Endpoint 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 Endpoint Services
- Detailed summary of activities investigated during deployment

Tuning and Configuration

eSentire is responsible for configuring and tuning both the Endpoint Prevent and Endpoint Detect and Respond capabilities. Endpoint Prevent requires a special configuration and tuning process due to the automated blocking/killing capabilities. Detections through the Endpoint Prevent capability are handled by the deployment engineer during the tuning and configuration period(s). All detections via the Endpoint Detect and Respond capability are handled by the eSentire SOC immediately upon agent install.

Endpoint Prevent Subscription:

- The configuration of the Prevention service is a phased approach to increase the security of the Prevention component
- Requires eighty percent (80%) of the Agents to be deployed to the infrastructure before configuration and tuning begins
- Upon successful installation to 80% of the infrastructure a deployment engineer resource will be assigned to the engagement
- Weekly meetings to take the Client through configuration and tuning will happen over a four (4) week period
- Once the Client is in a hardened state the service is transitioned into production monitoring by the eSentire SOC
- Supported configuration modules
- Exploit Protection
- Network Protection
- Application Isolation
- Next Gen A/V

Endpoint Detect and Respond Subscription:

- 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 (4) weeks begins once 80% of agents are installed
- Supported configuration modules
- Microsoft Defender EDR

Client Responsibilities

Client will perform the obligations listed below and acknowledges that the ability for eSentire to deliver the Endpoint Services is dependent upon the 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 Services or suspension of service levels.

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 (30 days)

- granting access to all data and systems required for the successful delivery of the Endpoint Services
- ensuring that 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 Endpoint management server
- ensuring there is sufficient network bandwidth and access to perform the Endpoint Services
- assisting eSentire with troubleshooting related to the installation of Endpoint Agents
- notifying eSentire of newly added machines to the Endpoint service

Tuning and Configuration

Client is responsible for:

- making themselves available for weekly meetings to discuss detections identified during tuning
- ensuring that authorized contacts remain current, including approved access and all associated information

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
- validating and responding to the SOC for escalated Alerts
- providing information and assistance promptly during investigations conducted by eSentire when additional information is required

Service Level Objectives

The ability for 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 IT environment. The service levels below are only applicable to hosts that are licensed as part of the service and are actively communicating with the Endpoint service.

eSentire will monitor the Endpoint 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 the Client may be needed depending on the information available to the analyst at the time of the investigation.

Severity Priority	Description	Notification/Escalation
Low (P4)	Minor activity recorded but not alerted, and the presence of likely unwanted activity, for example, adware.	None (included within QSR Reporting)
Medium (P3)	Suspicious activity that might not be deemed malicious by itself, and malicious activity not known to be targeted.	Alert (via email) within 60 minutes of determination of the Security Event
High (P2)	Malware event, tactics, techniques, and procedure events, or events indicating targeted attack with potential for widespread impact.	Alert (via email) and response by containment (if not blocked by prevention mechanism) by eSentire within 40 minutes of determination of a Security Event, followed by a phone call to Client per defined escalation procedure in the configuration worksheet.

Critical (P1)	Malware infection(s), virus infection(s), and lateral movement, or indications of targeted attack with a high potential to cause grave damage to critical assets.	Alert (via email) and response by containment (if not blocked by prevention mechanism) by eSentire within 20 minutes of determination of a Security Event, followed by a phone call to Client per defined escalation procedure in the configuration worksheet.

Exclusions

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.