Cloud Services – Wiz

1. Service Overview

eSentire's Cloud Services - Wiz (the "**Service**") provides analysis, investigation and alerting based on threats identified in Client's cloud infrastructure and workloads. The Service leverages a cloud security technology powered by Wiz ("**Product Publisher**"), combined with the eSentire Atlas Platform to provide cybersecurity insights, along with threat prevention, detection, mitigation, and response. This Service is scoped using a number of Client identified Wiz Essential or Wiz Advanced billable units and, if leveraged, the number of Client identified Wiz Defend and or Wiz Runtime Sensor billable units (collectively, "**Billable Units**"), that represent resources ("**Cloud Resources**") in the Client environment as detailed on the Order Form. The Service only supports a Cloud Environment (as defined below) hosted within the following cloud infrastructure providers: Amazon Web Services, Google Cloud Platform, or Microsoft Azure.

2. Definitions

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.

3. Service Capabilities

The Service collects information from all in-scope Cloud Resources (collectively the "**Cloud Environment**") and monitors and analyzes the data for potential threats, unusual behavior, or other indicators of compromise. Suspicious activity detected is monitored by eSentire's Security Operations Center ("**SOC**") on a 24x7x365 basis, initiating investigations and Client notification as required.

Client's Cloud Environment will be monitored in real-time against Service policies which define the criteria to send an Alert. The SOC will monitor the Cloud Environment 24x7x365 and will investigate and escalate identified critical severity alerts to Client. The Service tools will also be tuned to send automated notifications directly to Client for non-critical events that still require remediation. New threat detections (as applicable) are consistently being added to the Service and applied to the Client Cloud Environment, at no additional charge.

During service delivery, eSentire will monitor Cloud Resources in the Cloud Environment for items such as:

- misconfiguration of Cloud Resources;
- threats present in VM and container-based workloads;
- communication to/from IP addresses on eSentire's proprietary threat blacklist;
- anomalies in typical user and entity behavior analytics;
- identity issues stemming from over-permissioning and / or unused accounts;
- threats discovered in audit logs;
- anomalous activity, including deviations from baseline behavior correlating changes to cloud API interactions, user privileges, group policies, access keys, and other configurations;
- critical service exposures;
- misconfigurations in cloud automation tooling;
- illicit activity attempting to leverage the Cloud Environment to mine cryptocurrencies such as Bitcoin and Ethereum;
- potential account hijacking attempts by monitoring for unusual login activities such as concurrent attempts, peculiar geo-locations, and unknown browsers or operating systems; and
- sensitive modifications to the Cloud Environment.

The Service policies contain two classifications of Alerts, and depending on the classification, eSentire will handle Alerts as follows:

- Alerts that are non-remediable by eSentire, investigable by eSentire. Such Alerts are mainly the result of policies which identify potentially malicious behavior. These Alerts will be identified as requiring investigation by the eSentire SOC, and eSentire will investigate and attempt to identify information related to such Alert such as (as applicable):
    - user account which made a potentially sensitive configuration change to a Cloud Resource;
    - unusual user activity, which occurred at the same time as a potentially sensitive configuration change (identification of potential account compromise);
    - identification of abnormal cloud resource utilization, as a result of malicious activity such as crypto mining;
    - identification of false positive Alerts, filtering these out from Alerts reported to Client; and/or
    - determine the threat actor, impacted Cloud Resources, and severity of threat.

  Once the SOC has completed collecting information related to the Alert, if required, eSentire will send Client the Alert summary along with recommended remediation activities. This information will be sent to the Client via email and also posted to the Atlas Platform for Client action. eSentire will escalate based on priority level, and defined actions, described in the MDR service level objectives described in section 7 below.

- Alerts that are non-remediable by eSentire, non-investigable by eSentire. Such Alerts are mainly mis-configuration items that will be sent to Client directly by eSentire, via email and posted to the Atlas Platform for Client action. These types of Alerts can only be corrected by Client as they require

account configuration changes and/or review. The details included in the Alert sent to Client will include information on the policy criteria that caused the Alert, details on the violating Cloud Resource and specific steps to remediate the condition.

The Alerts that are sent to Client, and identified for Client action on the Atlas Platform, will remain unresolved until Client either performs the recommended remediation steps, or advises eSentire that the Alert was a false positive and should be suppressed.

4. Subscription Options

4.1 Subscription Types. Client can subscribe to one or more of the follow Service subscriptions (each a "**Subscription**"):

4.1.1 Cloud Services – Wiz Cloud – Managed Only

- Monitoring of cloud environment for misconfigurations and adherence to industry standard compliance frameworks.
- Scoped via the number of Wiz Essential or Wiz Advanced billable units in the Cloud Environment.

4.1.2 Cloud Services – Wiz Defend - Managed Only

- Requires subscription to "Cloud Services – Wiz Cloud – Managed Only"
- Runtime monitoring of VM and containerized workloads (Wiz Sensor)
- Analysis of cloud platform API logs and other logs ingested to Wiz Defend.
- Scoped via the number of Wiz Defend or Wiz Sensor billable units in the Cloud Environment

The Service is provided by eSentire in a managed only capacity ("**Managed Only**"). This will be detailed on the Order Form. Licensing details and requirements are detailed in Section 8.

5. Deployment

For a new deployment, eSentire will initiate the onboarding process by collecting and validating the required Client environment and contact information. Once validated, eSentire will provision Client access to the Atlas Platform and provide detailed instructions for integrating the Client's Wiz environment with eSentire Atlas.

A Client-designated contact with administrator-level access to the Wiz tenant is required to complete the integration steps. Following successful deployment and initial data ingestion, eSentire will conduct a service overview session with the Client to review the operational workflow, escalation procedures, and ongoing service expectations.

6. Maintenance & Support

Client is responsible for procuring, licensing, and maintaining all vendor software and hardware required for eSentire service delivery, including ongoing vendor support entitlements. eSentire does not provide support for the underlying vendor product, and any issues related to vendor licensing, product defects, or vendor-directed maintenance activities remain the Client's responsibility.

eSentire provides full support and maintenance for the managed service layer and the Atlas platform, including service configuration, policy management, platform availability, and ongoing operational support. Clients may contact eSentire Support for any issues related to the delivery of the managed service or access to the Atlas portal.

7. Service Level Objectives

The ability for eSentire SOC to perform an investigation and assess whether a threat is malicious is dependent on an active Wiz Essential, Wiz Advanced, Wiz Defend and or Wiz Sensor license from Product Publisher being integrated and in production in the Client Cloud Environment. The service level objectives set out in the MDR General Information, are only applicable to hosts that are licensed as part of the Service and are actively communicating with the Service.

eSentire will monitor the in-scope Client Cloud Resources 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 eSentire at the time of the investigation.

8. Responsibilities

8.1 Client Obligations

- Procure and maintain all required Wiz licenses for the entire Term of the Service.
- Maintain vendor support entitlements and handle all vendor licensing, product defect, and vendor-directed maintenance issues.
- Coordinate licensing permissions with Wiz to grant eSentire full administrative access via API credentials.
- Designate a contact with administrator-level access to the Wiz tenant to complete integration.
- Grant required permissions within Cloud Resources to enable the Service.
- Complete configuration of Cloud Resources in the Cloud Environment as required.
- Perform recommended remediation steps or advise eSentire of false positives for alerts identified on the Atlas Platform.

- Provide contextual information when requested to aid in alert investigations.
- Ensure Billable Units do not exceed 10% of contracted value (monthly average); reduce usage or upgrade the Service level within 30 days if an overage occurs.
- Review any environment changes with eSentire; unauthorized changes may release eSentire from service obligations.

8.2 eSentire Obligations

- Initiate onboarding by collecting and validating Client environment and contact information.
- Provision Client access to the Atlas Platform and provide integration instructions.
- Conduct a service overview session following successful deployment.
- Monitor the Client's Cloud Environment 24x7x365 for threats, misconfigurations, and anomalous activity.
- Investigate critical severity alerts and escalate to the Client with recommended remediation steps.
- Send automated notifications to the Client for non-critical alerts requiring remediation.
- Continuously add new threat detection capabilities to the Service at no additional charge.
- Provide full support and maintenance for the managed service layer and the Atlas Platform (configuration, policy management, platform availability, operational support).
- Provide detailed information on Cloud Resource misconfigurations to enable Client remediation.
- Answer Client questions about the Service, alerts, configuration, and related items.
- Provide service status reporting (alerts, alert volumes, protected Cloud Resources).

8.3 Required 3rd Party Licenses

In this Managed Only Service, eSentire will manage Client's Product Publisher licensing, which has been procured by Client. Client must procure and maintain its cloud licensing ("License") with Product Publisher, during the entire Term of the Service, and coordinate proper licensing permissions with the Product Publisher to allow eSentire full administrative access via API credentials into Client's License instance.

Client must purchase the following applicable licenses (or their successors/replacements, subject to eSentire approval), in order to receive the Service in a Managed Only capacity from eSentire:

- Cloud Services – Wiz Cloud– Managed Only, one of the following licenses must be procured:
    - Wiz Essential

- Wiz Advanced

- **Cloud Services – Wiz Defend – Managed Only**, one or more of the following licenses must be procured:
  - Wiz Defend
  - Wiz Sensor

9. Service Availability

The Service is delivered by eSentire's SOC on a 24x7x365 basis, providing continuous monitoring, investigation, and escalation of threats identified within the Client's Cloud Environment. Service notifications, alerts, and investigation summaries are delivered to the Client via email and the Atlas Platform. General service inquiries, configuration requests, and non-emergency support are handled by eSentire during standard business hours (Monday through Friday, 8:00 AM to 8:00 PM Eastern Time), excluding eSentire-observed holidays. Critical security escalations are handled around the clock regardless of business hours.

10. Service Turndown

Upon expiration or termination of the Service, eSentire will initiate a service turndown process to ensure an orderly transition. eSentire will remove Client Wiz managed configurations and integrations from the Client's Atlas environment. Client access to the Atlas Platform, including historical alerts, investigation records, and reporting data, will be discontinued at the end of the turndown period. As the Client retains ownership of all vendor licensing under the Managed Only model, the Client's Wiz environment and associated data will remain intact and accessible to the Client following turndown. eSentire will coordinate with the Client to establish a mutually agreed-upon turndown timeline and ensure continuity of the Client's security posture throughout the transition.

11. Terms & Conditions

11.1 Service Overages. The Services are scoped/sold using Billable Unit totals, and the quantity is detailed on the Order Form. Should Client's number of Billable Units active as a daily average exceed 10% of the contracted value (measured on an average over one calendar month), notwithstanding any security event (the "**Overage**"), then Client will either (i) take steps to reduce Billable Units to the contracted level within 30 Days of such Overage, or (ii) move to the next Service level, and associated fees, to accommodate its usage for the remainder of the Term.

11.2 Client Acknowledgement. For any Service option or licensing model detailed in this section, Client acknowledges and agrees that any changes made by Client in the licensed environment but not authorized by eSentire could negatively impact eSentire's ability to deliver the Services. In addition, Client

acknowledges and agrees that any changes made by Client in the licensed environment during the term of this Service should be reviewed with eSentire, otherwise eSentire shall be released from any and all obligations to effectively provide the Services as contemplated herein.

12. Appendix

12.1 RACI Chart

Function	Client	eSentire
Grant required permissions within Client Cloud Resources to enable the Service.	X	
Provide required information to support Service onboarding of Wiz to the eSentire Atlas Platform.		X
Complete configuration of Cloud Resources in the Cloud Environment as required.	X	
Perform monitoring of the Cloud Environment included in the Service, 24x7x365.		X
Provide detailed information regarding misconfiguration of Cloud Resources, enabling Client to perform required configuration changes within the Cloud Environment.		X
Where applicable, perform investigations into the cause of an Alert and provide investigation details to Client.		X
When requested, provide contextual information to aid in the investigation of an Alert.	X	
Answer Client questions about the Service, Alerts, configuration, or other items.		X
Provide Client with the opportunity to review Service status including items such as: • Alerts • Number of Alerts triggered for reporting period • Cloud Resources under protection		X