Service Description:

Atlas Email Security with Sublime

1. Service Overview

eSentire's Atlas Email Security (the "**Service**") is a co-managed email threat detection and response service within the "**Atlas Platform**", the eSentire security operations platform which consolidates all data and drives workflow for all eSentire managed detection and response services, including those in the Service. It uses a Sublime Security, Inc. (the "**Product Publisher**") email security tenant, deployed and configured by eSentire, to detect malicious email in Client's Microsoft 365 or Google Workspace environment.

The Service is co-managed. eSentire deploys the tenant, applies a standard configuration, tunes it with Client during onboarding, maintains eSentire threat detection rules, and is Client's first point of contact for support. Client receives co-administrator access to the tenant and is responsible for day-to-day runtime administration. eSentire does not administer Client's mail systems.

The Service investigates Product Publisher alerts created by threat detection rules alongside Client's other telemetry. Response actions run from the Atlas Platform through the Product Publisher's APIs; eSentire personnel do not connect directly to Client email systems.

The Service is licensed per user, as detailed on the Order Form. Number of mailboxes associated with these users is subject to Fair Use provisions.

2. Service Capabilities

The Service protects mailboxes through the Product Publisher's API-based platform. No mail routing or MX record changes are required, and the Service can run alongside Client's native Microsoft or Google controls or an existing secure email gateway.

2.1 Supported Email Platforms. Microsoft 365 (Exchange Online) and Google Workspace (Gmail), connected through their APIs.

2.2 Threat Detection. Every message is analyzed by the Product Publisher's detection engine, which combines natural-language and intent analysis, sender and behavioral analysis, deep inspection of attachments, URLs, images and QR codes, and campaign grouping. Each flagged message carries an Attack Score and the detection logic that produced it. Coverage includes credential phishing, business email compromise, malware and ransomware delivery, callback phishing, QR-code phishing, calendar (ICS) phishing, and email bombing.

2.3 Automated Response at Delivery. Product Publisher evaluates mail as it is received and processed and applies the automated actions defined in the standard configuration, such as quarantine, move to spam, trash, or a warning banner. Detection and action are automatic and do not require SOC or Client involvement.

2.4 User-Reported Phishing Triage. A "Report Phishing" button or abuse mailbox can feed the Atlas Platform. The Atlas Platform triages reported messages and provides a verdict with reasoning.

Copyright © 2026 eSentire, Inc. All Rights Reserved.

2.5 Post-Delivery Response from Atlas. After delivery, eSentire can remove or quarantine malicious messages by calling the Product Publisher's APIs from the Atlas Platform, according to the Client's configured response orchestration.

2.6 Detection Content. The Product Publisher and eSentire's Threat Response Unit ("**TRU**") maintain detection rules for the Client systems from which Client Data is collected for the delivery of the Service (the "**Client Environment**"). Custom content is not supported, but TRU will collaborate with Clients.

2.7 Atlas Integration and Investigation. Alerts are ingested into the Atlas Platform, enriched, correlated with endpoint, identity, network and cloud telemetry, and made available in the user interface of the Atlas Platform (the "**Atlas UI**"). During an investigation, the Atlas Platform may query the Product Publisher tenant for additional data, such as message metadata, message groups, and link-click activity.

2.8 Client Self-Service. Client co-administrators can use the Product Publisher tenant directly for message search, review queues, allow and block lists, exclusions, quarantine release, reports, and Product Publisher training resources.

3. Data Storage and Portability

The Atlas Platform collects data from the Client Environment, including email security telemetry from the Product Publisher tenant (all such collected Client Data, "**Raw Data**"). Raw Data is processed and analyzed to generate "**Signals**," which are further processed, correlated, and investigated by the Atlas Platform and the Atlas agentic AI framework, designed to enrich and investigate alerts in the Atlas Platform to produce "**Findings**." Metadata of, excerpts of, or entire copies of Raw Data and Signals may be attached to Findings as evidence. A Finding may give rise to a "**Ticket**," which tracks the lifecycle of that Finding; Tickets are also created to track technical support requests and other work performed under the Service.

The Product Publisher tenant is a third-party technology instance. Raw Data collected by the tenant, including email message content and message data, is retained within the tenant, subject to the retention terms of the Product Publisher and the tenant's retention settings, and is not stored on the Atlas Platform. Raw Data export from the tenant is determined by the capabilities of the Product Publisher. Upon expiration or termination of the Service, the tenant will, at Client's election, either be decommissioned or transferred to Client's full control (see Section 8.4 below).

Signals, Findings and Ticket data held on the Atlas Platform are retained for the shorter of 13 months or to the end of the Service term.

During the term, Client may export Signals, Findings, and Ticket data at any time using the Atlas UI's export functions, Atlas Platform API access, or Atlas Platform model context protocol (MCP) access.

Upon expiration or termination of the Service, all Client Data held on the Atlas Platform (including Signals, Findings, and Ticket data) is deleted. Prior to the end of the Service term and data deletion, Client may request the return of Client Data as follows:

- Full Findings and Ticket data may be exported in compressed CSV format and transferred to a Client-controlled AWS S3 bucket or Azure storage account.

Copyright © 2026 eSentire, Inc. All Rights Reserved.

- Bulk Raw Data held on the Atlas Platform, if any, is not available through standard export functions at termination and can only be provided upon Client's request. Bulk extraction may be subject to an additional fee based on the volume of data extracted.

4. Deployment, Onboarding and Support

4.1 Deployment. eSentire provisions and licenses one Product Publisher tenant for Client, connects it to Client's Microsoft 365 or Google Workspace tenant with Client-granted API permissions, and applies eSentire's standard configuration (baseline detection rules, automations, actions, integration with the Atlas Platform, and audit logging). eSentire is the licensee of record with the Product Publisher.

4.2 Onboarding and Tuning. During onboarding, eSentire works with Client to review mail flow and protected groups, populate lists such as executives and VIPs, set exclusions and allow lists, choose which detections trigger automatic action, configure the user-reporting path, and tune for false positives. eSentire directs Client administrators to the Product Publisher's training modules to learn runtime administration. Typical onboarding is 2 weeks; onboarding effort is 16 hours.

4.3 Co-Administration. Client receives co-administrator access to the tenant to perform runtime maintenance. eSentire manages the tenant's integrations, eSentire content, and connection to the Atlas Platform. Activity in the tenant is audited and monitored by eSentire. Changes made by Client in the tenant can affect eSentire's ability to deliver the Service; see Section 8 below.

4.4 Support. eSentire is Client's first point of contact for support, by email, telephone and the Atlas UI, for both security and system issues related to the Service. eSentire escalates to the Product Publisher where required. Client does not contact the Product Publisher directly for support unless directed to do so by eSentire.

4.5 Maintenance. eSentire maintains the tenant configuration it owns and applies eSentire and Product Publisher rule updates.

5. Detection Content and Response Actions

5.1 Detection Rules. eSentire maintains the standard rule set in the tenant, drawn from the Product Publisher's rule feeds and eSentire's own detections, and creates additional eSentire rules. eSentire's TRU reviews and approves eSentire content.

5.2 Client-Created Rules. Client may create custom rules and automations in the tenant. Client-created rules are Client's responsibility and are not monitored or investigated by eSentire unless TRU has reviewed and approved them.

5.3 Response Actions. Actions are performed in one of two ways:

Mode	Triggered by	Examples	Performed by
Automated, at delivery	Tenant rules, Attack Score, verdicts	Quarantine, move to spam, trash, warning banner, alert to Slack, webhook or email	Product Publisher, under the configuration agreed at onboarding
Post-delivery, from Atlas Platform	SOC investigation or Client request	Quarantine or trash a message or a whole campaign, calendar event removal, link-click lookup	Atlas Platform, through Product Publisher APIs

Copyright © 2026 eSentire, Inc. All Rights Reserved.

Each action is subject to the permissions Client has granted to the tenant. Removing messages from mailboxes is executed by API only; eSentire staff do not log in to Client's email systems. Quarantined and trashed messages remain recoverable by Client according to Microsoft and Google retention behavior. Actions taken by the SOC are recorded in the Finding.

5.4 Approval. Post-delivery actions are performed in accordance with the Client's response orchestration configurations. These can be modified at any time.

6. Fair Use

Fair Use policies will be in effect to enforce reasonable usage of the Service. “Reasonable usage” means, as applicable, the range of endpoint agents, cloud workloads, collected data, alert volumes, monitored mailboxes, penetration test targets, vulnerability scan targets, and retests will fall within 4x the average for customers of similar scope. Entitlement averages are posted and updated regularly in Atlas UI and are available in consultation with Client’s technical account manager. Averages are measured on 30 day rolling averages. In the event volumes of usage are outside expected bounds, eSentire will work with the Client to investigate and recommend alternate configurations or other service packages. Service will not be interrupted. Alerts, investigations and other security monitoring and assistance is not capped.

7. Responsibilities Matrix (RACI)

R = Responsible; performs the work (can be shared). A = Accountable; ultimately answerable, with approval and veto authority. C = Consulted before a decision or action. I = Informed after. Product Publisher is shown for reference; Client interacts only with eSentire, and Product Publisher’s obligations run to eSentire.

Function	Client	eSentire	Product Publisher
Onboarding			
Provision and license Product Publisher tenant	I	RA	R
Grant Microsoft 365 / Google Workspace API permissions	RA	C	-
Standard configuration (rules, automations, actions)	I	RA	C
Atlas Platform integration and alert forwarding	I	RA	C
Identify VIPs, protected groups, mail flow, exclusions	RA	C	-
Tuning to Client needs during onboarding	RA	RA	-
Configure user-report button / abuse mailbox	RA	C	-
Client admin training (self-directed)	RA	C	R
Detection			
Maintain Product Publisher core detection content and feeds	I	I	RA
eSentire rule research, creation and maintenance	I	RA	C
TRU approval of Client-created rules	C	RA	-
Create and manage custom Client rules	RA	C	-
Monitor and investigate alerts from Client-created rules (not TRU-approved)	RA	-	-
Ongoing tuning: allow lists, exclusions, thresholds	RA	C	-
Response and SOC			

Copyright © 2026 eSentire, Inc. All Rights Reserved.

Automated actions at delivery (per agreed configuration)	I	RA	R
Alert monitoring and investigation (eSentire-managed content)	I	RA	-
Notification and escalation per response orchestration	I	RA	-
Post-delivery removal via Atlas Platform API	A	R	-
Review of user-reported phishing	A	RC	-
Release of false-positive quarantined messages	RA	C	-
Remediation outside email (password reset, endpoint isolation)	RA	C	-
System and Health			
Tenant platform uptime and patching	I	RA	R
Tenant integrations and Atlas Platform connection health	I	RA	C
Co-admin user and role management	RA	C	-
Audit and monitoring of tenant activity	I	RA	C
First-line support	I	RA	C
Escalation and product defects	I	RA	R
Client Environment			
Notify eSentire of email system changes (routing, gateways, domains, migrations)	RA	I	-
Notify eSentire of major tenant changes made via co-admin access	RA	I	-
Health of Microsoft 365 / Google Workspace and its API access	RA	C	-
Turndown			
Decision to take over tenant	RA	C	I
Sever tenant from eSentire and transfer ownership	I	RA	R

8. Client Responsibilities, Exclusions and Turndown

8.1 Client is responsible for:

- granting and maintaining the Microsoft 365 or Google Workspace permissions the Product Publisher tenant needs, and keeping API access functional;
- informing eSentire of changes to its email systems (for example gateways, mail routing, domains, tenant migrations) and of major changes it makes in the Product Publisher tenant through co-administrator access, and reviewing significant changes with eSentire in advance; eSentire is released from service level obligations affected by changes it was not told about;
- runtime administration of the tenant, including allow lists, exclusions, quarantine release, and the review queue;
- managing its custom rules and automations, which are not monitored by eSentire unless approved by TRU;
- designating a primary contact and co-administrators, and managing their accounts;
- configuring the user-report path and communicating it to end users;
- remediation outside the email platform, such as account recovery, endpoint actions and user follow-up, unless separately covered by other eSentire services;
- complying with its own legal, privacy and retention requirements for email data; and

Copyright © 2026 eSentire, Inc. All Rights Reserved.

- providing the information, access and personnel reasonably required by eSentire.

8.2 Exclusions. The Service excludes: operation or administration of Client's mail platform; secure email gateway replacement or mail routing; outbound or internal email DLP; email archiving and encryption; security awareness training and phishing simulation; domain authentication (SPF, DKIM, DMARC) management; monitoring of Client-created rules not approved by TRU; and direct eSentire access to Client mailboxes.

8.3 Service Levels. For more information on our Service Level Agreement, please refer to the MDR SLA description in the Legal Catalogue.

8.4 Service Turndown. At the end of the Term, Client may choose to take over the Product Publisher tenant. Client must establish a licensing relationship with the Product Publisher sufficient to carry the tenant. eSentire will then remove eSentire-proprietary configuration and eSentire user access, disable the Atlas connection, sever the tenant from eSentire, and transfer ownership to Client. If Client does not take over the tenant, it is decommissioned, and the data and configuration in it are destroyed. Client Data held on the Atlas Platform is deleted at expiration or termination, and Client may request its prior return as described in Section 3.

Copyright © 2026 eSentire, Inc. All Rights Reserved.