Trustwave®

SERVICE DESCRIPTION

MailMarshal

Overview

Trustwave's MailMarshal service ("**Service**") is a cloud-based or on-premises email protection solution. The Service scans for both inbound and outbound email and helps provide protection against viruses, malware, phishing, and spam. The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Confirmation between Trustwave and Client.

Service Features

The Service is available in three formats: (i) as an on-premises software install ("**MailMarshal**"), (ii) through a cloud-based portal ("**MailMarshal Cloud**"), or (iii) as software to be managed by Client for third-party end-users ("**Service Provider Edition**"). MailMarshal and MailMarshal Cloud are each available at two service tiers: Essentials or Advanced.

Essential Service Features

MailMarshal Essentials and MailMarshal Cloud Essentials includes the following features:

- **Blended Threat Module** – provides advanced, real-time (time of click) protection against malicious links in emails through the application of a ruleset that allows messages to be scanned in real-time (time of clock) against malicious links in email.
- **Acceptable Use Enforcement** – filters for explicit, adult images and inappropriate language in email through the application of specific rulesets.
- **Data Loss Prevention** – performs content inspection and contextual analysis of data before an email is sent out to help block unauthorized transfers of data.
- **User Matching** – matches specific email policies to specific user types.
- **Sophos Anti-Virus** – scans for viruses in both inbound and outbound emails.
- **Standard Support** – see Additional Information below.

Advanced Service Features

MailMarshal Advanced and MailMarshal Cloud Advanced includes the Essential Service Features listed above and the following additional features:

- **Sandboxing** – searches for malware by executing or detonating code in a simulated and isolated environment to observe that code's behavior and output activity.
- **Advanced Image Analysis** – performs image analysis to block inbound messages with attached images that are identified as potentially pornographic.

- **Premium Support** – see Additional Information below.

Client Obligations

For Trustwave to provide MailMarshal and MailMarshal Cloud, Client will

- enable or disable applicable components through the Client Console; and
- report false positives and false negatives to Trustwave as needed through support requests.

Trustwave Responsibilities

For MailMarshal and MailMarshal Cloud, Trustwave will

- provide Client with an account to enable the Service; and
- provide break-fix support, updates, and configuration changes as Trustwave deems appropriate.

MailMarshal Cloud

MailMarshal Cloud includes a web-based interface ("**Client Console**") where Client may configure, monitor, and report on email content security. Trustwave will provide Client with the agreed number user credentials (as provided in an applicable SOW or Order Confirmation). Client's credentialed users may log in to MailMarshal Cloud using a web browser. MailMarshal Cloud will authenticate such logins against a Windows domain or against accounts created locally on the web application server. Once logged in, credentialed users are authorized to use MailMarshal Cloud according to the privileges associated with their accounts.

The following additional components are included in MailMarshal Cloud:

- **Dashboard** – shows a graphical summary of email processing statistics and summaries of licensed product features and system information.
- **Messages** – allows comprehensive searching for email content in the system.
- **Message Queues** – shows the status of incoming and outgoing messages for each server and for each destination route (email domain or forwarding server). Client may delete or manually retire messages per queue.
- **Rules** – displays a summary of the configured email policies.

Using the Client Console, Client may

- generate predefined reports relating to email flow, classification, or blocking actions;
- view reports or schedule email delivery of the reports;
- view user groups and message templates;
- create and maintain user groups to apply email policy to specific internal or external users;
- create and maintain message templates to send customized email notifications based on the result of processing rules';
- view and configure general features of the Service interface;
- review Client Console activity and changes to Service configuration for any period;
- review connector agent activity and changes to connector agent configuration;
- review the email domains managed by the Service;
- view and edit Client contact and basic setting information;
- set access accounts and permissions for the Client Console;

- manage periodic notification to users of quarantined messages; and
- manage the end-user spam quarantine management module.

Service Provider Edition

Client may also purchase the Service in the Service Provider Edition, in which case Client is a reseller of the Service to its third-party end-users. This version of the Service is subject to the reseller agreement in place between Trustwave and Client (the reseller). The Service Provider Edition includes the Essential Service Features and the Advanced Service Features listed above (and subject to the same Client Obligations and Trustwave Responsibilities). Trustwave will provide the Service as a on-premises software install for Client's third-party end-users and Client will manage and customize the Service.

Client Obligations

For the Service Provider Edition, Client will use the IP address for the location of the relevant data center where the Service will be hosted to redirect the end-users' mail exchange records. Client will supply the IP address to the third-party end-users. Client is wholly responsible for the set-up, maintenance, and continuation of the Service to its third-party end-users. Client will pay for an additional license for each additional third-party end-user.

Optional Service Features

The Service may include the following optional service features. Any purchased optional service features will be indicated in the applicable SOW or Order Confirmation between Client and Trustwave.

Secure Email Encryption

This optional feature encrypts emails to help protect sensitive data and support compliance requirements through the application of a ruleset. The rules define the parameters for triggering email encryption based on the User Matching component included in the Service.

Client Responsibilities

For Trustwave to provide this optional feature, Client will

- provide information to and as required by Trustwave;
- enable or disable the secure email encryption ruleset through the Client Console, as required by Trustwave; and
- report package rule processing errors to Trustwave's support team.

Trustwave Responsibilities

For this optional feature, Trustwave will

- collect relevant information to configure the feature;
- connect Client's Service account to the encryption feature; and
- Provide break-fix support and update and configure the feature as appropriate.

Third-Party Anti-Virus Add-on

While Sophos Anti-Virus is included in the Service, Client may purchase additional email gateway anti-virus (AV) engines. The specific additional AV engine(s) will be enumerated in the applicable Order Confirmation or SOW between Client and Trustwave.

Client Responsibilities

For Trustwave to provide this optional feature, Client will report false positives and false negatives as applicable to Trustwave.

Trustwave Responsibilities

For this optional feature, Trustwave will

- add the applicable AV engine to Client's account; and
- provide break-fix support and update or configure the feature as Trustwave deems necessary.

Additional Information

Standard & Premium Support

Client may elect either standard support and maintenance ("**Standard Support**") or premium support and maintenance ("**Premium Support**") and the selection will be indicated in the applicable SOW or Order Confirmation. Both service tiers include the following support features:

- Clarification of functions and features of the Service
- Clarification of the documentation accompanying the Service
- Guidance in operation of the Service
- Assistance in identifying and verifying the causes of suspected errors in the Service
- Advice on remediating identified errors in the Service, if reasonably possible

Hours of operation for Standard Support are Monday through Friday, local business hours for the Trustwave team. Hours of operation for Premium Support are (i) Standard Support hours of operation and (ii) 24x7 on-call support for Priority 1 issues (as defined in the TAC Support Guide available online). If Client contacts Trustwave outside of the Standard Support hours of operation, Client must do so by telephone.

For detailed information on technical support deliverables, services, escalation process, priority definitions, SLAs, and other support items, please request a copy of the TAC Support Guide.

Provisioning and Implementation (MailMarshal Cloud Only)

Trustwave and Client will work together to gather relevant information and set up Client's access to MailMarshal Cloud. Upon completion of the provisioning and implementation process, Trustwave will begin MailMarshal Cloud.

Service Configuration

Trustwave and Client will cooperate to verify MailMarshal Cloud is functionally configured by confirming that

- Client has access to the Client Console;
- the default configuration of the Client's selected Policy Packages are functional;
- the configuration of the Client's email infrastructure is functional; and
- Client is receiving notifications from the Client Console based on mail exchange records.

Client Responsibilities

For Trustwave to provide this feature of MailMarshal Cloud, Client will

- accurately complete provisioning questionnaire. Client acknowledges that Trustwave is not responsible for delays in provisioning due to delays in completing or inaccurate responses to the provisioning questionnaire;
- respond to Trustwave's requests in a timely manner;
- enable, disable, or establish email security policies through the Client Console; and
- establish a base policy ruleset, including:
    - email policy rules
    - which administrators and users can manage quarantined messages
    - which administrators and users can manage user groups used for the User Matching component

Trustwave Responsibilities

For this feature, Trustwave will

- request and collect provisioning questionnaire information from Client;
- lead a welcome meeting to review and capture information on the existing IT infrastructure and operating environment;
- provide applicable user guides to assist Client in using MailMarshal Cloud and applicable support process and procedures; and
- report false positives (not spam) or false negatives (spam) as needed through the Client Console.

Service Management

Trustwave will use commercially reasonable efforts to provide steady-state operations, maintenance, and change management functions for MailMarshal Cloud only.

Client Responsibilities

For Trustwave to provide this feature, Client will

- respond to notifications regarding operational issues in a timely manner and, when requested, assist Trustwave with issue analysis;
- inform Trustwave of all Client environment maintenance activity and changes that may affect the supply of the Service;
- raise changes in accordance with the change management process below;
- provide, when necessary to Trustwave, technician access to the Client Console for management and maintenance purposes;
- maintain the required connectivity from Client email infrastructure to where the MailMarshal Cloud service is hosted; and
- access the Client Console to maintain the Client's desired email security policies and perform and maintain email user administration, including for quarantined messages, for enabling and disabling processing rules, and for managing user groups for the User Matching component.

Trustwave Responsibilities

For this feature, Trustwave will

- perform operational monitoring of MailMarshal Cloud, including for performance and capacity;
- implement (as Trustwave deems necessary) third-party software version updates (new releases and patches/hotfixes) and implement break-fix support and configuration of the Service; and
- create support tickets and update tickets with relevant information, as appropriate.

Change Management

Trustwave maintains an overall change control and configuration management procedure for its support infrastructure and associated services. Changes that could affect the operation of the Client's environment are coordinated with Client. Trustwave establishes an email address for each Client contact to support communication with the Client personnel responsible for administration of the Client's environment.

Trustwave will assess and implement change requests submitted by Client to the Trustwave security operations centers (SOC). Trustwave evaluates all requests to verify they are aligned with the features included with the MailMarshal Cloud and will use commercially reasonable efforts to confirm such changes will not detrimentally impact the security of the Client's environment. Typical change requests for the Service are:

- Configuration changes to the Service as requested by Client
- Change reversals as requested by Client

Client Responsibilities

For Trustwave to provide this feature, Client will

- submit change requests using the Trustwave Fusion platform;
- where the Client does not agree with an incident priority (see TAC Support Guide), submit a change management request to change the priority;
- provide Trustwave with requested information in a reasonable timeframe and review the risk assessment relating to requested changes;
- review, assess, and notify Trustwave of approval or non-approval to a proposed change request; and
- as needed, request that Trustwave roll back or reverse a change request;
    - submit reversal requests by using the Trustwave Fusion platform, emailing, or phoning the Trustwave support team; and
    - provide resources to execute joint testing and confirm the change reversal is aligned with the Client-submitted request and confirm completion of the change rollback request.

Client acknowledges that change requests that exceed sixteen (16) hours of Trustwave time are not included in the Service and will require purchase of additional Trustwave services.

Trustwave Responsibilities

For this feature, Trustwave will

- allow Client to submit security incidents through the Trustwave Fusion platform, as needed;
- perform change management activities when requested and if in compliance with Trustwave policies;

- determine whether the request is within the scope of the Service;
- source additional information as necessary to support the implementation of the change request;
- assess the potential risk from implementation of the change request and advise Client of the outcome;
- confirm Client approval to implement the change request after reviewing risk assessment results with Client. Client is ultimately responsible for any resultant risks;
- confirm Client acceptance of implemented changes;
- when authorized by Client to roll back or reverse a change request,
    - confirm receipt of Client's request for a change reversal and confirm completion of the change rollback upon execution of change reversal activities;
    - execute joint testing with Client to check if the rollback is aligned to Client's request; and
    - update the change request with information on rollback changes; and
- notify Client where a change request is outside the scope of the Service and if additional charges will apply to a change request.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in Trustwave's Master Terms and Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or in the applicable Statement of Work or Order Confirmation between Trustwave and Client.