SERVICE DESCRIPTION

MailMarshal Integrated Cloud

Overview

Trustwave's MailMarshal Integrated Cloud ("**Service**" or "**Product**") is a cloud-based, email protection solution. The Service scans inbound, outbound and internal email and helps provide protection against viruses, malware, phishing, and spam. It further provides data loss prevention and acceptable use functionality. The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Form between Trustwave and Client.

Trustwave disclaims all liability if Client loses access to its email as a result of modifying the rules and connectors provisioned by Trustwave.

Service Features

The Service is available in two service tiers: Essentials or Advanced. Client may choose to have the Service provisioned on one of three available instances (US, EU, or Australia).

Essentials Service Features

MailMarshal Cloud Essentials includes the following service features:

- **Marshal Core Protection** – includes anti-spam detection, anti-malware detection, anti-virus detection, anti-phishing detection, anti-spoofing detection, business email compromise, fraud protection, insider threats, data loss prevention, attachment controls, size and bandwidth controls, acceptable use enforcement, blended threat module, and a robust policy engine
    - **Anti-spam Detection** – provides detection of spam, fraud, and phishing email messages using multiple technologies. As part of the anti-spam detection feature, Trustwave updates detection algorithms regularly. In addition, the SpamProfiler feature, which is included in anti-spam detection, delivers signature-based detection at the message level with very frequent updates.
    - **Blended Threat Module** – provides advanced protection against malicious links in emails through the application of a ruleset that allows messages to be scanned in real-time (time of click)
    - **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
    - **Anti-virus Detection** – scans for viruses in inbound, outbound, and internal emails

    - **User Matching** – matches specific email policies to specific user types.
- **Standard Support** – see Additional Information below

Advanced Service Features

MailMarshal Integrated Cloud Advanced includes the Essentials 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

Additional Information

Standard & Premium Support

The Service includes standard support and maintenance ("**Standard Support**"). Client has the option to upgrade the support level to premium support and maintenance ("**Premium Support**"), and the upgrade will be reflected in the applicable Order Form or SOW. Standard Support includes:

- Clarification of the functions and features of the Service
- Clarification of the documentation accompanying the Service
- Guidance to operate 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

The hours of operation for Standard Support are Monday through Friday, local business hours for the Trustwave team. Premium Support includes the features listed above with different hours of operation. The 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 Trustwave Support Services Guide). 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 Trustwave Support Services Guide and the Trustwave Service Levels – MailMarshal Cloud document.

Service Management

Client Obligations

For Trustwave to perform the Service, Client will

- configure appropriate settings as documented;
- enable or disable applicable components through the Client Console (as defined below);
- comply with MailMarshal Cloud Service Limits as published by Trustwave from time to time in the MailMarshal Cloud Knowledgebase available at https://support.trustwave.com/MailMarshalCloud/kb/item.asp?id=21041; and
- report false positives and false negatives to Trustwave as needed through documented methods, such as email forwarding or plug-ins within Client's email viewing software (e.g., Microsoft Outlook).

Trustwave Obligations

As part of the Service, Trustwave will

- provide Client with an account to enable the Service;
- use reasonable efforts to maintain proprietary detection technologies such as anti-spam, anti-malware, anti-phishing; and
- provide break-fix support, configuration changes, and updates as Trustwave deems appropriate.

Client Console

The Service includes a web-based interface ("**Client Console**") where Client may configure, monitor, and report on email content security. Trustwave will provide Client with initial user credentials, and Client may create additional credentialed users. Client's credentialed users may log in to the Client Console using a web browser. MailMarshal Integrated Cloud will authenticate such logins against a SAML SSO Identity Provider or against accounts created locally on the web application server. Once logged in, credentialed users are authorized to use MailMarshal Integrated Cloud according to the privileges associated with their accounts.

The Service includes the following additional components:

- **Dashboard** – shows a graphical summary of email processing statistics, licensed product features, and system information
- **Messages** – allows comprehensive searching for email content in Client's 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 retry messages per queue.
- **Rules** – displays a summary of Client's configured email policies and allows Client to apply policies selectively
- **Spam Quarantine Management**– Allows Client to grant review of quarantined emails to internal recipients or senders

Available processing rules and features are subject to change at Trustwave's discretion. Trustwave will notify Client of any changes through the notifications feature in the Client Console. The latest information is always available on the product documentation page, which is linked from the Client Console.

Using the Client Console, Client may

- generate predefined reports relating to email flow, email 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;
- view and configure general features of the Service interface;
- review Client Console activity and changes to the 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 information and basic setting information;
- set access accounts and permissions for the Client Console;

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

Provisioning and Implementation

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

Service Configuration

Trustwave and Client will cooperate to verify the Service is functionally configured by confirming that

- Client has access to the Client Console;
- the default configuration of Client's selected policy packages is functional;
- the configuration of Client's email infrastructure is functional; and
- Client is receiving notifications from the Client Console

Client Obligations

For Trustwave to provide the Service, Client will

- accurately complete a provisioning questionnaire. Client acknowledges that Trustwave is not responsible for delays in provisioning the Service if Client's responses to the questionnaire are inaccurate or delayed;
- ensure that Client's contact information is kept up to date;
- respond to Trustwave's requests in a timely manner;
- enable, disable, or establish email security policies through the Client Console;
- establish a base policy ruleset;
- configure permissions for administrators and users to manage quarantined messages;
- configure permissions for administrators to manage user groups used for the user matching feature of the Service; and
- report false positives and false negatives to Trustwave as needed through the Client Console or plug-ins within Client's email viewing software.

Trustwave Obligations

Trustwave will

- request the provisioning questionnaire information from Client;
- lead a welcome meeting to review and capture information on Client's existing information technology infrastructure and operating environment; and
- provide applicable user guides to assist Client in using the Service and applicable support processes and procedures.

Steady-State Operations

Trustwave may provide steady-state operations, maintenance, and change management functions for the Service.

Client Obligations

For Trustwave to provide the Service, Client will

- respond to notifications regarding operational issues in a timely manner;

- upon Trustwave's request, assist Trustwave with issue analysis;
- inform Trustwave of all Client environment maintenance activity and changes that may affect the provision of the Service;
- raise changes in accordance with the change management process below;
- provide Trustwave with technician access to the Client Console for management and maintenance purposes as requested by Trustwave;
- maintain the required connectivity from Client email infrastructure to the location where the Service is hosted;
- access the Client Console to maintain Client's desired email security policies; and
- access the Client Console to perform and maintain email user administration related to quarantined messages, enabling and disabling processing rules, and managing user groups for the user matching feature of the Service.

Trustwave Obligations

Trustwave will

- perform operational monitoring of the Service, including monitoring for performance and capacity;
- implement third-party software version updates (e.g., new releases, patches, hotfixes) as Trustwave deems necessary;
- implement break-fix support and configuration of the Service;
- create and update support tickets with relevant information as appropriate; and
- run reports at its discretion to determine whether Client is exceeding the agreed-upon number of users or licenses. If Trustwave determines that Client is exceeding the agreed-upon number of users or licenses, (i) Client will rectify the excess use within a timeframe established by Trustwave, or (ii) Trustwave will bill Client for the excess use.

Change Management

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

Trustwave will assess and implement change requests submitted by Client to Trustwave. Trustwave evaluates all requests to verify they are aligned with the features included with the Service and may confirm such changes will not detrimentally impact the security of Client's environment. Typical change requests for the Service include

- configuration changes to the Service as requested by Client; and
- change reversals as requested by Client.

Client Obligations

For Trustwave to provide the Service, Client will

- submit change requests using the Trustwave Fusion platform;
- submit a change request to change the incident priority when Client does not agree with an incident priority;
- provide Trustwave with requested information in a reasonable timeframe and review the risk assessment related to the requested changes;

- review, assess, and notify Trustwave of approval or non-approval of a proposed change request in a timely manner; and
- request that Trustwave roll back or reverse a change request if necessary;
    - Client will submit reversal requests by using the Trustwave Fusion platform, emailing Trustwave, or calling the Trustwave support team; and
    - Client will provide resources to execute joint testing of the change reversal, confirm the change reversal is aligned with Client's submitted request, and confirm completion of the rollback change request.

Trustwave Obligations

Trustwave will

- allow Client to submit change requests through the Trustwave Fusion platform as needed;
- perform change management activities when requested if in compliance with Trustwave policies;
- determine whether Client's change request is within the scope of the Service;
- source additional information as needed to support the implementation of Client's change request;
- assess the potential risk of implementation of Client's change request and advise Client of the outcome of the assessment;
- confirm Client's approval to implement the change request after reviewing risk assessment results with Client. Client is ultimately responsible for any resulting risks associated with the change request;
- confirm Client's acceptance of the 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 the change reversal activities;
    - execute joint testing with Client to check if the rollback is aligned to Client's change request; and
    - update the change request with information related to the rollback changes;
- notify Client when a change request is outside of 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/, the License Agreement between Trustwave and Client, or in the applicable SOW or Order Form between Trustwave and Client.