Trustwave®

SERVICE DESCRIPTION

MailMarshal Service Provider Edition

Overview

Trustwave's MailMarshal Service Provider Edition ("**Service**") is a software-based, multi-tenant, email protection solution that allows Trustwave customers (each a "**Service Provider**") to offer an email filtering service to their customers. The Service provides web-based configuration and allows Service Provider to manage the Service for Service Provider and Service Provider's customers. The Service implements the Trustwave MailMarshal email filtering solution 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.

Service Features

The Service is available as software, which Service Provider will manage for third-party customers and their end-users ("**Service Provider Edition**"). The Service is available in two service tiers: Essentials or Advanced.

Essentials Service Features

MailMarshal SPE Essentials includes the following service features:

- **Service Provider Interfaces** – includes a web-based management shell for administrative management of customers and policy, delegated customer management of policy and email messages, delegated end-user spam management, and a connector agent for customer and end-user synchronization
- **Marshal Core Protection** – includes anti-spam detection, anti-malware detection, anti-virus detection, anti-phishing detection, anti-spoofing detection, business email compromise fraud protection, data loss prevention, attachment controls, size and bandwidth controls, acceptable use enforcement, unlimited custom rules, 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, Trustwave updates detection algorithms regularly. In addition, the SpamProfiler feature, which is included in the anti-spam detection, delivers signature-based detection at the message level with very frequent updates.
    - **Data Loss Prevention –** performs content inspection and contextual analysis of data before an email is sent out to help block unauthorized transfers of data

  - **Acceptable Use Enforcement** – filters for explicit, adult images and inappropriate language in email through the application of specific rulesets
  - **Blended Threat Module** – provides advanced protection against malicious links in emails through the application of a ruleset that allows email messages to be scanned in real time (time of click).
- **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
- **Standard Support** – see Additional Information below

Service Provider Obligations

For Trustwave to provide the Service, Service Provider will

- provide the necessary infrastructure (including hardware, software, and storage and networking services) to install and run the software;
- manage and maintain the necessary infrastructure;
- install the MailMarshal and MailMarshal SPE software in accordance with the documentation;
- configure automatic updates to anti-spam, anti-virus, and product modules;
- configure policy offerings;
- configure Service Provider's customer records and instruct Service Provider's customers on the settings required to access the Service;
- manage the system and support Service Provider's customers on a daily basis;
- upgrade the software to a currently supported version as required;
- report false positives and false negatives to Trustwave as needed through documented methods, such as email forwarding or plug-ins within Service Provider's email viewing software (e.g., Microsoft Outlook); and
- report usage to Trustwave on a regular basis.

Trustwave Obligations

As part of the Service, Trustwave will

- provide Service Provider with access to download the software and automatic updates to the software;
- provide Service Provider with credentials to enable the Service;
- provide Service Provider with sample rules and policies;
- provide Service Provider with frequent updates to anti-spam, anti-virus, and anti-malware detection abilities; and
- provide break-fix support, configuration changes, and any additional updates as Trustwave deems appropriate.

Optional Service Features

The Service may include the following optional service features.

Secure Email Encryption

This optional service 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. Secure email encryption is offered in two service tiers: Essentials and Advanced.

The Essentials level of secure email encryption provides secure, web-based delivery of content.

The Advanced level of secure email encryption provides additional delivery options, branding of the encryption portal, two factor authentication, and message composition.

Service Provider Obligations

For Trustwave to provide this optional service feature, Service Provider will

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

Trustwave Obligations

For this optional service feature, Trustwave will

- collect relevant information to configure the service feature;
- connect Service Provider's account and Service Provider's customers' accounts to the encryption feature;
- provide break-fix support; and
- update and configure the service feature as appropriate.

Secure Email Archiving

This optional feature delivers copies of messages to a cloud-based, forensic quality archive. The rules define the parameters for triggering email archiving based on the user matching component included in the Service.

This optional service feature includes a web portal where

- Service Provider's customer administrators can manage permissions for other users in the organization; and
- Service Provider's customer users can search for and work with messages depending on permissions granted.

Service Provider Obligations

For Trustwave to provide this optional service feature, Service Provider will

- create and document rules to forward messages for archiving; and
- provide information to Trustwave as required by Trustwave.

Trustwave Obligations

For this optional service feature, Trustwave will

- collect relevant information to configure the feature;
- connect Service Provider's account to the archiving feature;
- provide break-fix support; and
- update and configure the feature as appropriate.

Third-Party Anti-Virus Add-on

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

Service Provider Obligations

For Trustwave to provide this optional service feature, Service Provider will install the additional anti-virus software and allow automatic updates as described in the applicable documentation.

Trustwave Obligations

For this optional service feature, Trustwave will

- add the applicable anti-virus engine to Service Provider's account;
- provide break-fix support for the applicable anti-virus engine; and
- update or configure the applicable anti-virus engine as Trustwave deems necessary.

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, which is 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 Trustwave Support Services Guide.

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 SOW or Order Form between Trustwave and Client.