Trustwave®

SERVICE DESCRIPTION

MailMarshal (On-Premises)

Overview

Trustwave's MailMarshal (On-Premises) ("**Service**") is a software-based, email protection solution. The Service scans both inbound and outbound 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.

Service Features

The Service is hosted by the Client on one or more Windows servers or virtual machines and uses a Microsoft SQL server in a traditional datacenter or cloud environment under Client's control. The Service is available in two service tiers: Essentials or Advanced. Additional service features are available with each tier.

Essentials Service Features

MailMarshal Essentials includes the following 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, 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.
    - **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)
- **Standard Support** – see Additional Information below

Advanced Service Features

MailMarshal 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

Client Obligations

For Trustwave to provide the Service, Client 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 software according to the procedures provided in the product user guide and release notes documentation;
- configure a minimum set of rules according to documented best practices;
- configure additional rules as required to meet Client's policy objectives;
- configure automatic updates to anti-spam, anti-virus, and product modules;
- keep the software updated to the currently supported version; 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

Trustwave will

- provide Client with access to download the software and automatic updates to the software;
- provide Client 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. Any purchased optional service features will be indicated in the applicable SOW or Order Form 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. Secure email encryption is available 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.

Client Obligations

For Trustwave to provide this optional service feature, Client will

- provide information to Trustwave as required by Trustwave;
- create rules to forward messages for encryption as described in the applicable documentation; and
- report processing errors to Trustwave's support team.

Trustwave Obligations

For this optional service feature, Trustwave will

- collect relevant information to configure the service feature;
- enable access to the encryption feature from Client's servers;
- provide break-fix support; and
- update and configure the service feature as appropriate.

Third-Party Anti-Virus Add-on

Sophos Anti-Virus engine is included in the Service. Client 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.

Client Obligations

For Trustwave to provide this optional service feature, Client 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 Client's account;
- provide break-fix support for the applicable anti-virus engine; and
- update or configure the service feature 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.