SERVICE DESCRIPTION

# Secure Email Gateway (SEG) Cloud

## Service Description Overview

Trustwave Secure Email Gateway (SEG) Cloud is a cloud-based email protection solution for secure Internet email. SEG Cloud scans both inbound and outbound email and helps provide protection against viruses and malware and targeted threats such as phishing and unwanted spam. Flexible email policy configuration assists with internal controls and compliance management. SEG Cloud also provides temporary message storage for a client's Internet email by queuing emails when the Client's internal email system is down and delivering them once the Client's internal email systems is back online.

## Base Features

### Client Console

The Client Console is a SEG Cloud Web interface for Clients (email administrators) to configure, monitor, and report on email content security for their organization. A number of views are provided to assist in daily administration of email traffic flow and status.

- **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. The Email logs are retained for 90 days and Content logs are available for delivered email for 7 days. Full content available for quarantined email for 14 days (permanently purged after this time)
- **Message Queues**-Shows the status of incoming and outgoing messages for each server and for each destination route (email domain or forwarding server). Messages may be deleted or manually retried per queue. Messages are retried up to 72 hours and then returned to sender.
- **Reports-**The Client can generate Predefined Reports relating to email flow, classification or blocking actions. The Client can use the Client Console to view reports or schedule email delivery of the reports.
- **Rules-** Displays a summary of the configured Client email policies. Package Policies-Displays a listing of available Policy Packages.
- **Policy Elements**-The Client can use the Client Console to view User Groups and Message Templates
- **User Groups** Create and maintain user groups to apply email policy to specific internal or external users.
- **Message Templates**-Create and maintain message templates to send customized email notifications based on the result of processing rules.

- **Administration-**Allows Client administrator access to view and configure the following general features of the SEG Cloud interface.
- **Audit History**-Review SEG Cloud console activity and changes to SEG Cloud configuration, for any period.
- **Connector Agent History**-Review SEG Cloud Connector Agent activity and changes to Connector Agent configuration.
- **Domains**-Review the email domains that SEG Cloud is managing.
- **Configuration**-View and edit Client contact and basic setting information.
- **Logins-**Set access accounts and permissions for the Client Console.
- **Message Digests**-Manage periodic notification to users of quarantined messages.
- **Spam Quarantine Management (SQM) Configuration**-Manage the end-user spam quarantine management module of SEG Cloud.

## Policy packages

Policy Packages consist of the standard protection policy package and the Optional Service Feature Policy Packages referred to in this service description.

After completion of the initial default configuration of the relevant Policy Package, the Client uses the Client Console to:

- Enable or disable the available email policy rules
- Apply User Matching to the available email policy rules

## Standard protection policy package

The SEG Cloud Service includes a standard protection policy package with the following predefined rulesets that helps provide protection against spam and viruses and malware, including malicious email attachments.

The standard protection policy package rulesets are:

### Outbound rulesets

- Malware Protection-Scan outgoing messages, at the time of sending, for malicious code and content, Blended Threats and suspicious attachments.
- Anti-Spam-Blocks outgoing spam messages using a variety of technologies
- Size and Bandwidth Control-Blocks outbound messages based on size
- Attachment Control-Blocks messages which contain common attachment types or those unknown to the SEG Cloud Service
- Message Content-Blocks messages which contain specific content
- Client Blacklist-Outbound blacklist management

### Inbound rulesets

- Invalid Recipient Handling-Blocks inbound emails to invalid (unknown) addresses.
- Anti-Spam-Blocks incoming spam messages, from the time of delivery, using a variety of technologies.
- Malware Protection-Scans inbound messages for malicious code and content, Blended Threats, and suspicious attachments.
- Size and Bandwidth Control-Blocks inbound messages based on size.
- Attachment Control-Blocks messages which contain common attachment types or those unknown to the SEG Cloud Service.
- Message Content-Blocks messages which contain specified content.
- Client Blacklist-Blacklist management.

### Dead letter handling ruleset

- Dead Letter/Spam-Quarantines undeliverable emails or emails that are malformed or emails which cannot be scanned.

# Provisioning and Implementation

## Implementation

The provisioning team is the Client's first point of interaction with Trustwave after the contract is executed. This team is responsible for working with Client to Review and analyze the Client Provisioning Questionnaire and Provision and implement the SEG Cloud Service scanning of the Clients inbound and outbound email traffic.

The SEG Cloud Service is deemed to be delivered and operational when:

- The Client has access to the Client Console.
- The Client's email infrastructure is communicating with and is visible to the Trustwave Platform.
- The SEG Cloud Service is scanning the Clients inbound and outbound email traffic.

## Service introductions and information gathering

Trustwave provisioning, assurance and delivery teams are assigned to assist Client in implementing the successful configuration and rollout of the Client's SEG Cloud Service, which includes the following actions:

- Send an introduction email to the Client providing guidance on how to provide the necessary Client Provisioning Questionnaire prior to a remote kick-off meeting
- Contact the Client to establish and schedule the timing of the remote kick-off meeting
- Remotely create an instance for, and establish the Client within, the Client Console

## Service and environment assessment

Trustwave provisioning engineers work with clients to help ensure optimal service configuration, including:

- Assessment of the completeness of the Client Provisioning Questionnaire provided
- Assess that the Client's email policies and the Client's proposed configuration of, the standard protection policy package default rulesets and any selected Optional Service Feature Policy Package rulesets, are consistent with SEG Cloud Service capabilities
- Presentation and confirmation proposed default configuration of the Client's selected Policy Packages

## Service configuration

Trustwave provisioning will work with the Client to verify that SEG Cloud Service is brought into an operational state, confirming:

- Client access to the Customer Console
- Default configuration of the Client's selected Policy Packages
- Configuration of the Client's email infrastructure
- Notification to the Client's DNS administrator of the necessary changes to the Clients MX Records to point to the Trustwave Platform

## Welcome call

The Trustwave provisioning team will schedule a welcome call with the Client

- During the welcome call, TW will introduce the Client to the Client Console
- Review the client's usage and understanding of the Client Console, including the functionality to Review available reports; Modify permissions for other Client Console users as appropriate or available to the Client and review How to access and leverage applicable views within the Client Console.

### Trustwave Responsibilities

- Establish and maintain contact with Client and navigate Client through the provisioning process
- Request and collect provisioning questionnaire information from Client
- Initiate provisioning activities with Client by leading welcome meetings to review and capture information on the existing IT infrastructure and operating environment as necessary to fulfill the provisioning process
- Provision the Client account and the SEG Cloud Service to enable the standard protection policy package and any Client selected Optional Service Feature policy packages
- Provide applicable user guides to assist the client in using the Service and applicable support process and procedures
- Validate that the SEG Cloud Service is scanning the Client's inbound and outbound email traffic according to the service delivery design

### Client Responsibilities

- Accurately complete provisioning questionnaire
- Respond to requests in a timely manner from the provisioning team when establishing contact and collecting required provisioning information
- Notify the Client's DNS Administrator to redirect the Client's MX records to point to the Trustwave Platform
- Enable, disable and establish email security policies through the Client Console, the default Policy Package email policy rules as required, including email user administration for items such as quarantined messages, enabling and disabling processing rules and managing user groups for User Matching
- Report false positives (Not Spam) and/or false negatives (Spam) as needed through the Client Console
- Read and understand all provided user guides and documentation
- Participate in and confirm Client's understanding of materials explained during the Welcome call
- The Client acknowledges that Trustwave is not responsible for delays in provisioning due to delays or inaccurate Client Provisioning Questionnaire
- Trustwave is not responsible for providing the SEG Cloud Service as designed, until the service is deemed delivered and operational

## Service Management

Trustwave will provide ongoing 24x7 steady-state operations, maintenance and change management functions for Trustwave SEG Cloud Services' infrastructure.

### Trustwave Responsibilities

- Perform 24x7 operational monitoring of the SEG Cloud Service, including performance and capacity of the Trustwave Platform
- Implement third-party software version upgrades/updates (new releases and patches/hotfixes), break-fix support and configuration of the Trustwave Platform to accommodate the ongoing supply of the Client's SEG Cloud Service
- Create support tickets to manage support activities and Update tickets with relative information when providing support activities

### Client Responsibilities

- Respond to notifications raised by Trustwave 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 SEG Cloud Service
- Raise changes in accordance with the change management process
- Provide, when necessary to Trustwave, technician access to the Client Console to allow for any actions necessary for Trustwave to act on behalf of the Client for management and maintenance purpose
- Maintain the required connectivity from Client email infrastructure to the Trustwave Platform
- Access the Client Console to maintain the Client's desired email security policies and perform and maintain email user administration including for items such as quarantined messages, enabling and disabling processing rules and managing user groups for User Matching

### Reporting

The SEG Cloud Service includes access to Predefined Reports for selection by the Client, relating to messages which provide detailed data about the messages passing through SEG Cloud and a Summary which provides an overview of message traffic passing through SEG Cloud.

The Predefined Reports options can be viewed in the Customer Guide.

### Trustwave Responsibilities

- Provide Client access to the Predefined Reports
- Generate the Client-selected Predefined Reports and make them accessible through the Client Console and/or delivered via email
- Provide written notice to the Client of any changes to the report format

### Client Responsibilities

- View and download generated Predefined Reports through the Client Console
- Maintain correct contact information to help ensure successful email delivery of, and/or access to, the Predefined Reports

## 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 appropriate Client IT staff. Trustwave establishes an email address for each Client contact, to support communication with the Client personnel responsible for administration of the Client's environment.

Change Management will assess and implement change requests submitted by the Client to the Trustwave Security Operations Centers (SOC). All requests are evaluated to help ensure that they are aligned with the features included with the SEG Cloud Service and will not detrimentally impact the security of the Client's environment. Typical change requests for the SEG Cloud Service are:

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

### Trustwave Responsibilities

- Allow authorized Client personnel to submit Security Incidents through the TrustKeeper Client Portal, as needed. Perform change management activities when requested and in compliance with Trustwave policies.
- Validate that the request was submitted by an authorized Client contact, and notify Client if validation is not successful. Determine whether the request is in-scope with the terms of the Service. Source additional information as necessary to support the implementation of the change request.

- Assess the potential risk that will result 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.
- Confirm Client acceptance of implemented changes.
- When authorized Client personnel request that Trustwave 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 successful execution of change reversal activities.
    - Execute joint testing with Client to validate the rollback is aligned to Client's request, and gain Client confirmation of the same.
    - Update the change request with information on rollback changes.
- Notify Client where a change request is outside the scope of the service and/if additional charges will apply to a change request, subject to a separate quoted consultancy project.

### Client Responsibilities

- Submit change requests using the TrustKeeper Client Portal.
- Where the Client does not agree with a Security Incident priority, submit a change management request to change the priority of the relevant Security Incident.
- Provide Trustwave with requested information in a reasonable timeframe and Provide resources to review the risk assessment relating to requested changes. Review, assess and notify Trustwave of approval or non-approval to a proposed change request.
- When required, authorized Client personnel may request that Trustwave roll back or reverse a change request.
    - Submit reversal requests using the TrustKeeper Client Portal, emailing or phoning the Trustwave support team; 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.

The Client acknowledges that change requests that exceed two (2) man days of effort is deemed a project and is subject to acceptance by the Client of separately quoted additional charges.

## Optional Features

The following additional Client Packages are available as optional service features to the SEG Cloud Service:

### Data protection package

This policy package provides Data Loss Prevention (DLP) of inbound and outbound emails and attachments through application of the following ruleset.

### Sensitive material ruleset

This ruleset scans outbound messages for potentially sensitive content:

- **Block Credit Card Numbers**-This rule blocks messages that have indications of credit card numbers in the email message body or its attachments.
- **Block Social Security Numbers**-This rule blocks messages that have indications of US Social Security numbers in the email message body or its attachments
- **Copy Messages with HIPAA Content** -This rule archives messages that contain keywords which might fall under the US HIPAA act. The messages should be reviewed by the administrator to verify their content.
- **Copy Messages with SEC Content-**This rule blocks messages that contain keywords which might be a violation of US Securities and Exchange Commission regulations. The messages should be reviewed by the administrator to verify their content.

- **Copy Messages with Sarbanes-Oxley Content** -This rule blocks messages that contain keywords which might be a violation of the US Sarbanes-Oxley act. The messages should be reviewed by the administrator to verify their content.

## Trustwave Responsibilities

- Provision the Client account to enable this package
- Provide break-fix support and update/upgrade and configure the feature as required

## Client Responsibilities

- Enable or disable the sensitive material ruleset through the Client Console, as required
- Report false positives and/or false negatives as needed through support requests

## Advanced protection package

This package enables the Blended Threat Module (BTM) that helps provide advanced, real-time (time of click) protection against malicious links in emails through the application of the following ruleset.

## Blended Threat Module

- The **Blended Threat Module** includes a ruleset that allows messages to be scanned for Blended Threats and consists of the following features:
- **Blended Threats Scanner-** This rule performs two functions; Rewrites URLs in the body of incoming email messages and when the email recipient clicks the rewritten URL link, it submits the URL to the Trustwave Link Validator cloud service for real time scanning.
- **Blended Threats Exclusions-**Allows for the creation and maintenance of a list of domains that are excluded from being rewritten for Blended Threats scanning

## Trustwave Responsibilities

- Provision the Client account to enable this package
- Provide Trustwave Link Validator cloud service functionality
- Provide break-fix support and update/upgrade and configure the feature and services as required

## Client Responsibilities

- Enable or disable the Blended Threat scanner through the Client Console as required
- Enable or disable Blended Threat exclusion feature, and create and maintain the blended threat exclusion ruleset through the Client Console as required

## Acceptable use package

- This package filters explicit adult images and inappropriate language from email through the application of the following rulesets.

## Objectionable material outbound ruleset

- This ruleset scans outbound messages for objectionable content, such as offensive language (vulgarity), pornography, or hate speech.

## Image analyzer outbound ruleset and Image Scanner

- This ruleset performs deep image analysis to block outbound messages with attached images that are identified as potentially offensive (pornographic) by deep image analysis.

## Objectionable material inbound ruleset

- This ruleset scans inbound messages for objectionable content, such as offensive language, pornography, or hate speech.

## Image analyzer inbound ruleset and Image Scanner

- This ruleset performs deep image analysis to block inbound messages with attached images that are identified as potentially offensive (pornographic) by deep image analysis

## Trustwave Responsibilities

- Provision the Client account to enable this package.
- Provide break-fix support and update/upgrade and configure the feature as required.

## Client Responsibilities

- Enable or disable the objectionable material and image analyser rulesets through the Client Console, as required.
- Report false positives and/or false negatives as needed through support requests.

## Secure email encryption package

- This package provides email encryption capabilities to help protect sensitive data and support compliance requirements through the application of the following rulesets.

## Secure email encryption ruleset

- This ruleset provides rules for triggering email encryption via the Trustwave Secure Email Encryption service and encrypts messages based on User Matching.
- Routes messages to the Trustwave Secure Email Encryption service if specified users match. Note: User Matching MUST be configured before enabling this rule.
- Encrypts Messages using keyword
- Sends the message to the Trustwave Secure Email Encryption service if an encryption keyword (as specified in the rule description in the Client Console) is specified in the email subject.
- Encrypts Messages containing Credit Card Data and sends the message to Trustwave Secure Email Encryption service if it matches credit card information in the message.
- Encrypt messages containing SSN data and sends the message to the Trustwave Secure Email Encryption service if it matches US Social Security Number data.

## Trustwave Responsibilities

- Collect required information to configure the encryption service
- Provision the Client account to enable this package
- Provide break-fix support and update/upgrade and configure the feature as required

## Client Responsibilities

- Provide required information to Trustwave for provisioning of encryption service
- Enable or disable the secure email encryption ruleset through the Client Console, as required
- Report package rule processing errors as needed through support requests