Trustwave®

USER GUIDE

MailMarshal Cloud Integrated Mode Available Policy and Features

Table of Contents

About This Document

This document provides details of the policy and feature configuration available to MailMarshal Cloud customers for the M365 Integrated mode.

Use this listing along with the MailMarshal Cloud Customer Guide to understand the available features and functions of MailMarshal Cloud.

If you have a business need that you believe is not covered by the polices and features listed, contact Trustwave to discuss your requirements.

Notes:

- The policy and features for the Integrated mode offering differ from the policy and features in the Gateway mode (SMTP forwarding) mode. Gateway mode customers should refer to the document for that mode.
- Additional rules for Integrated mode are planned to be released shortly.
- For Integrated mode, bandwidth control and blocked/invalid senders and recipients are managed in M365.
- Folder move actions shown in the user interface have a clause “and categorize as…” A future update will populate details for this clause and provide reporting on this information.

1 Non-Rule Functionality

1.1 Disclaimers (Message Stamps)

Two configurable disclaimer texts are available, one for inbound messages and one for outbound messages. Disclaimers can be stamped at the top or bottom of messages. If a disclaimer is enabled, all messages for the direction will be stamped (User Matching and other conditions are not supported).

1.2 Keywords Detection

Customers can block (quarantine) messages that contain keywords or phrases. Keyword entries can be combined using Boolean and proximity operators. Separate keyword lists are available for inbound and outbound messages. For details, see the Customer Guide and Help.

1.3 Administrative Email Addresses

The Server address and Administrator address can be set for each configured domain. It is not possible to configure specific addresses for each notification.

1.4 Notifications

Notification templates and notification rules cannot be customized. Only the templates and notifications configured in existing rules can be used.

1.5 Digests

Default Digest Templates and Quarantine Digests are configured. Additional Digest Templates and Digests can be configured.

1.6 Blended Threats Exclusions

Customers using Blended Threats Protection can maintain a list of domains that will never be subject to Blended Threats scanning. URLs in these domains will not be rewritten by the Blended Threats functionality.

1.7 Executive Names List

Customers can provide a list of names and email addresses of company executives. This list is used to assist in prevention of email fraud, by identifying messages from external sources that may appear to come from trusted internal users.

1.8 Entra Groups

Customers can synchronize user and group information (for rule User Matching) to MailMarshal Cloud from Entra ID by importing Entra groups.

2 Processing Policies

- Unless otherwise noted, individual rules can be enabled or disabled.
- Where noted, User Matching can be applied to policy groups (rulesets) and rules. User Matching allows you to apply policy based on groups of email addresses, including wildcard entries. User Matching allows you to apply any combination of the following conditions:
    - Where Addressed To
    - Where Addressed From
    - Except Where Addressed To
    - Except Where Addressed From

2.1 Package: Standard Protection – Outbound Rules

2.1.1 Malware Protection (Outbound)

This ruleset scans outgoing messages for malicious code and content, blended threats, and suspicious attachments.

Rule: Block Malware - Email Threat Detection (Notify)

Cannot be disabled

This rule targets traits of malware-sending bots and suspicious attachments. The heuristic detection script is updated regularly to detect emerging threats.

When a message arrives
And the message is outgoing
Where message is categorized as 'Known Threats'
Then
Send a 'Malware Out' system notification message
  And write log message with 'Malware - Threats'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Malware - Suspect File Attachments

This rule scans messages for suspicious file attachments. These attachments are rarely transferred via email, and can harbor malicious content.

When a message arrives
And the message is outgoing
Where message contains attachment(s) named '*.bat' '*.chm' '*.cmd' '*.com' '*.pif' '*.hlp' '*.hta' '*.inf' '*.ins' '*.js' '*.jse' '*.lnk' '*.one' '*.reg' '*.scr' '*.sct' '*.shs' '*.url' '*.vb' '*.vbe' '*.vbs' '*.msc' '*.wsf' '*.wsh' '*.nws' '*.{*}' '*.cpl'
Then
Write log message with 'Malware - Suspect File Attachments'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Malware - Suspect File Attachments (Notify)

This rule scans messages for suspicious file attachments. These attachments are rarely transferred via email, and can harbor malicious content. The sender is notified about the message being blocked.

When a message arrives
And the message is incoming
Where message contains attachment(s) named '*.bat' '*.chm' '*.cmd' '*.com' '*.pif' '*.hlp' '*.hta' '*.inf' '*.ins' '*.js' '*.jse' '*.lnk' '*.one' '*.reg' '*.scr' '*.sct' '*.shs' '*.url' '*.vb' '*.vbe' '*.vbs' '*.msc' '*.wsf' '*.wsh' '*.nws' '*.{*}' '*.cpl'
Then
Send a 'File Extension Out' system notification message
  And write log message with 'Malware - Suspect File Attachments'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Malware - Signature Scanner

Cannot be disabled

This rule scans messages for malware using traditional, signature-based AV technology. It cannot be turned off or have exclusions applied to it.

When a message arrives
And the message is outgoing
Where the result of a virus scan , when scanning with all scanners, is 'Contains Virus'
Then
Write log message with 'Malware - Known Malware'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Malware - Signature Scanner Error

Cannot be disabled

This rule sends a notification to the system administrator if the AV scanner experiences an unexpected failure. It cannot be turned off or have exclusions applied to it.

When a message arrives
And the message is outgoing
  Except where addressed from 'TEMP XLS Senders'
Where the result of a virus scan , when scanning with all scanners, is 'Virus scanner signature is out of date' or 'Unexpected scanner error'
Then
Send a 'Malware - AV Scanner Error' notification message
  And write log message with 'Malware - AV Scanner Error'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Malware - Signature Scanner File Error

Cannot be disabled

This rule sends a notification to the system administrator if the AV scanner experiences a failure analyzing a file. It cannot be turned off or have exclusions applied to it.

When a message arrives
And the message is outgoing
  Except where addressed from 'TEMP XLS Senders'
Where the result of a virus scan , when scanning with all scanners, is 'File is corrupt' or 'Could not fully unpack or analyze file'
Then
Send a 'Malware - AV Scanner Error out (Sender)' notification message
  And write log message with 'Malware - AV Scanner Error'
  And move the message to 'Quarantine (Outgoing)' with release action “continue processing”

2.1.2 Anti-Spam (Outbound)

User Matching Allowed

This ruleset blocks outgoing spam messages using a variety of technologies.

Rule: Block Phishing

User Matching Allowed

This rule blocks suspected phishing messages. Messages blocked by this rule are monitored by the threat evaluation team. Trustwave strongly recommends you do not enable SQM management of the Spam – Phishing category.

When a message arrives
And the message is outgoing
Where message is categorized as 'Phishing'
Then
Write log message with 'Spam - Phishing'
  And move the message to 'Spam – General' with release action "continue processing"

Rule: Block Spam - Signatures and Behavior

User Matching Allowed

This rule blocks messages identified as spam by multiple technologies including signatures and botnet characteristics. These messages are identified as spam with high confidence. End user review is normally not required.

When a message arrives
And the message is outgoing
Where the message is detected as spam by SpamProfiler (Spam, Spam Bulk Mail, Confirmed (Malware), High (Probable Malware)) and SpamBotCensor
Then
Write log message with 'Spam - High Certainty'
  And move the message to 'Quarantine (Outgoing)' with release action “skip to the next policy group”

Rule: Block Spam - Signatures and Heuristics

User Matching Allowed

This rule blocks messages identified as spam by multiple technologies including signatures and heuristic analysis of content. These messages are identified as spam with high confidence. End user review is normally not required.

When a message arrives
And the message is outgoing
Where the message is detected as spam by SpamCensor and SpamProfiler (Spam, Spam Bulk Mail, Confirmed (Malware), High (Probable Malware))
Then
Write log message with 'Spam - High Certainty'
And move the message to ‘Quarantine (Outgoing)’ with release action “skip to the next policy group”

Rule: Block Suspect Spam - Signatures

User Matching Allowed

This rule blocks messages identified as spam by a signature based technology. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is outgoing
Where the message is detected as spam by SpamProfiler (Spam, Spam Bulk Mail, Confirmed (Malware), High (Probable Malware))
Then
Write log message with ‘Spam - General’
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Suspect Spam - Heuristics

User Matching Allowed

This rule blocks messages identified as spam by heuristic analysis of content. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is outgoing
Where the message is detected as spam by SpamCensor
Then
Write log message with ‘Spam - General’
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Suspect Spam - URL Block List

User Matching Allowed

This rule blocks messages identified as spam because they contain web links that are associated with spam. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is outgoing
Where message is categorized as 'URL Block List'
Then
Write log message with ‘Spam - General’
And move the message to ‘Quarantine (Outgoing)’ with release action “skip to the next policy group”

Rule: Block Suspect Spam - Keywords

User Matching Allowed

This rule blocks messages identified as spam because they contain keywords associated with spam (a list manually maintained by Trustwave). These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is outgoing
Where message triggers TextCensor script(s) 'ISP-Maintained Keyword List'
Then
Write log message with 'Spam - General'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block Suspect Spam - High Volume

User Matching Allowed

This rule blocks messages that have similar signatures and high volume. Please note it may trigger false positives if you have mass mailings originating from your system.

When a message arrives
And the message is outgoing
Where the message is detected as spam by SpamProfiler (Spam Bulk Mail, Suspected Spam, Confirmed (Malware), High (Probable Malware))
Then
Write log message with 'Spam - General'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Suspect Spam - Suspicious URLs in message

User Matching Allowed

This rule blocks messages that contain URLs identified as suspicious (phishing, malware, or spam) by the Trustwave URL Categorizer.

When a message arrives
And the message is outgoing
Where the message contains suspect URLs
Then
Write log message with 'Suspect URL - Trustwave URL Categorizer'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

2.1.3 Attachment Control (Outbound)

Rule: Block unknown attachments

User Matching Allowed

This rule blocks messages which contain attachments that cannot be identified by the scanning service. Unidentifiable attachments are uncommon, and these attachments may or may not be malicious.

When a message arrives
And the message is outgoing

Where message attachment is of type 'BIN'
Then
Write log message with 'Attachment Type - Unknown'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block unknown attachments (Notify)

User Matching Allowed

This rule blocks messages which contain attachments that cannot be identified by the scanning service. Unidentifiable attachments are uncommon, and these attachments may or may not be malicious. This rule notifies the sender of the message that it was blocked.

When a message arrives
And the message is outgoing
Where message attachment is of type 'BIN'
Then
Send a 'Attachment Type – Unrecognized (out)' notification message
And write log message with 'Attachment Type - Unknown'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block executable files

User Matching Allowed

This rule blocks messages which contain executable attachments. Files in this category include Win32 executables, Mac executables, Unix executables, and self-extracting archives.

When a message arrives
And the message is outgoing
Where message attachment is of type 'EXECUTABLE'
Then
Write log message with 'Attachment Type - Executable'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block executable files (Notify)

User Matching Allowed

This rule blocks messages which contain executable attachments. Files in this category include Win32 executables, Mac executables, Unix executables, and self-extracting archives. This rule notifies the sender of the message that it was blocked.

When a message arrives
And the message is outgoing
Where message attachment is of type 'EXECUTABLE'
Then
Send a 'Attachment Type - Executable' notification message
And write log message with 'Attachment Type – Executable (out)'
And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block executable files (unless in Archive File)

User Matching Allowed

This rule blocks messages which contain executable attachments. Files in this category include Win32 executables, Mac executables, Unix executables, and self-extracting archives. This rule notifies the sender of the message that it was blocked. Executable files inside standard archives, such as ZIP, RAR, or ARJ will not be blocked.

When a message arrives
And the message is outgoing
Where message attachment is of type 'EXECUTABLE'
  And where attachment parent type is not of type: ' ARCHIVE'
Then
Send a 'Attachment Type - Executable' notification message
  And write log message with 'Attachment Type - Executable'
  And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block Video files

User Matching Allowed

This rule blocks messages which contain video attachments. Files in this category include AVI, MP4, Flash, and Quicktime files.

When a message arrives
And the message is outgoing
Where message attachment is of type 'VIDEO'
Then
Write log message with 'Attachment Type - Video'
  And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block Video files (Notify)

User Matching Allowed

This rule blocks messages which contain video attachments. Files in this category include AVI, MP4, Flash, and Quicktime files. A notification is sent to the sender.

When a message arrives
And the message is outgoing
Where message attachment is of type 'VIDEO'
Then
Send a 'Video out' system notification message
  And write log message with 'Attachment Type - Video'
  And move the message to 'Quarantine (Outgoing)' with release action "skip to the next policy group"

Rule: Block Sound files

User Matching Allowed

This rule blocks messages which contain sound attachments. Files in this category include MP3, OGG, WAV, and Quicktime audio files.

When a message arrives
And the message is outgoing
Where message attachment is of type 'SOUND'
Then

Write log message with 'Attachment Type - Sound'
And move the message to ‘Quarantine (Outgoing)’ with release action “skip to the next policy group”

Rule: Block Sound files (Notify)

User Matching Allowed

This rule blocks messages which contain sound attachments. Files in this category include MP3, OGG, WAV, and Quicktime audio files. This rule notifies the sender of the message that it was blocked.

When a message arrives
And the message is outgoing
Where message attachment is of type 'SOUND’
Then
Send a 'Attachment Type - Sound out' notification message
And write log message with 'Attachment Type - Sound'
And move the message to ‘Quarantine (Outgoing)’ with release action “skip to the next policy group”

Rule: Block encrypted attachments

User Matching Allowed

This rule blocks messages which contain encrypted attachments. Files in this category include password-protected archives and encrypted PDF and Office documents.

When a message arrives
And the message is outgoing
Where message attachment is of type 'ENCRYPTED’
Then
Write log message with 'Attachment Type - Encrypted'
And move the message to ‘Quarantine (Outgoing)’ with release action “skip to the next policy group”

Rule: Block encrypted attachments (Notify)

User Matching Allowed

This rule blocks messages which contain encrypted attachments. Files in this category include password-protected archives and encrypted PDF and Office documents. This rule notifies the sender of the message that it was blocked.

When a message arrives
And the message is outgoing
Where message attachment is of type 'ENCRYPTED’
Then
Send a 'Attachment Type - Encrypted out' notification message
And write log message with 'Attachment Type - Encrypted'
And move the message to ‘Quarantine (Outgoing)’ with release action “skip to the next policy group”

Rule: Block Office Macro Documents

User Matching Allowed

This blocks messages that contain Office documents having macros included in them.

When a message arrives
And the message is outgoing
Where message is categorized as 'Office Document Macros'
Then
Write log message with 'Attachment Type – Office Macros'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Office Macro Documents (Notify)

User Matching Allowed

This blocks messages that contain Office documents having macros included in them. A notification is sent to the sender.

When a message arrives
And the message is outgoing
Where message is categorized as 'Office Document Macros'
Then
Send a 'Office Macro Document (Out)' system notification message
Write log message with 'Attachment Type – Office Macros'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

2.1.4 Message Content (Outbound)

Rule: Strip read receipts from messages

User Matching Allowed

This rule removes read receipt requests from messages. The messages content is otherwise unaffected.

When a message arrives
And the message is outgoing
Then
Write log message with 'Strip Read Receipt Headers'
And rewrite message headers using 'Strip Read Receipt Request'

Rule: Strip sensitive information from headers

User Matching Allowed

This rule strips information from a message's header which might leak information about your internal network environment. This includes information about the network hosts that handled the message during delivery, and the software package and version information that may be in use by your organization. The messages content is unaffected.

When a message arrives
And the message is outgoing
Then
Rewrite message headers using 'Remove selected Header fields'

Rule: Block Fragmented Messages

User Matching Allowed

Fragmented messages are messages that come in one or more parts, and are re-assembled at the delivery point to read the entire content. Fragmented messages are very rarely used for legitimate purposes today, and can be an indicator that an attacker is attempting to bypass content scanning filters..

When a message arrives
And the message is outgoing
Where message contains one or more headers 'Detect Fragmented Messages'
Then
Write log message with 'Message - Fragmented Message'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Encrypted Messages

User Matching Allowed

This rule prevents messages which contain S/MIME or PGP encrypted material from being sent to your organization. Internal employees may receive confidential information in encrypted form, to prevent detection by automated systems.

When a message arrives
And the message is outgoing
Where message attachment is of type 'P7M; PGP’
And where message spoofing analysis is based on anti-relay and where Sender ID evaluation fails with Moderate Settings
Then
Write log message with 'Message - Encrypted'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

2.1.5 Dead Letter Handling (Outbound)

Quarantines malformed or otherwise unscannable or undeliverable mails.

No customer configuration is allowed.

2.2 Package: Standard Protection – Inbound Rules

2.2.1 Malware Protection (Inbound)

This ruleset scans inbound messages for malicious code and content, blended threats, and suspicious attachments. Our Base offering will use the Sophos Anti-Malware engine, which will be included for all customers as part of the basic package.

Rule: Block Malware - Email Threat Detection

This rule targets traits of malware-sending bots and suspicious attachments. The heuristic detection script is updated regularly to detect emerging threats.

When a message arrives
And the message is incoming
Where message is categorized as ‘Known Threats'
Then
Write log message with 'Malware - Threats'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Malware - Suspect File Attachments

This rule scans messages for suspicious file attachments. These attachments are rarely transferred via email, and can harbor malicious content.

When a message arrives
And the message is incoming
Where message contains attachment(s) named '*.bat' '*.chm' '*.cmd' '*.com' '*.pif' '*.hlp' '*.hta' '*.inf' '*.ins' '*.js' '*.jse' '*.lnk' '*.one' '*.reg' '*.scr' '*.sct' '*.shs' '*.url' '*.vb' '*.vbe' '*.vbs' '*.msc' '*.wsf' '*.wsh' '*.nws' '*.{*}' '*.cpl'
Then
Write log message with 'Malware - Suspect File Attachments'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Malware - Signature Scanner

This rule scans messages for malware using traditional, signature-based AV technology. It cannot be turned off or have exclusions applied to it.

When a message arrives
And the message is incoming
Where the result of a virus scan , when scanning with all scanners, is 'Contains Virus'
Then
Write log message with 'Malware - Known Malware'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Malware - Signature Scanner Error

This rule sends a notification to the system administrator if the AV scanner experiences an unexpected failure. It cannot be turned off or have exclusions applied to it.

When a message arrives
And the message is incoming
Where the result of a virus scan , when scanning with all scanners, is 'Virus scanner signature is out of date' or 'Unexpected scanner error'
Then
Send a 'Malware - AV Scanner Error out' notification message
And write log message with 'Malware - AV Scanner Error'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Malware - Signature Scanner File Error

This rule sends a notification to the system administrator if the AV scanner experiences an unexpected failure. It cannot be turned off or have exclusions applied to it.

When a message arrives
And the message is incoming
Where the result of a virus scan , when scanning with all scanners, is 'File is corrupt' or 'Could not fully unpack or analyze file'
Then
Send a 'Malware - AV Scanner (recipient)' notification message
And write log message with 'Malware - AV Scanner Error'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Malware – Advanced Malware Exploit Detection

User Matching Allowed

This rule blocks messages that contain files that trigger the Trustwave SEG Advanced Malware Engine. A notification is sent to the recipient.

When a message arrives
And the message is incoming
Where message is identified as containing malware by Yara Analysis Engine AMAX
Then
Send a 'AMAX In' notification message
And write log message with 'Malware – Advanced Malware Detection'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Malware – Malformed PDF Detection

User Matching Allowed
Disabled by default. Trustwave recommends you enable this rule.

This rule blocks messages that contain PDF files that are malformed and cannot be opened and scanned. They could potentially be malicious. A notification is sent to the recipient. *(This rule may be subject to a small amount of false positives)*

When a message arrives
And the message is incoming
Where message is identified as containing malware by Yara Analysis Engine Malformed PDF
Then
Send a 'Malformed PDF In' notification message
And write log message with 'Malware – Suspect File Attachments'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.2.2 Anti-Spam (Inbound)

User Matching Allowed

This ruleset block incoming spam messages using a variety of technologies.

Rule: Allow users on Global Whitelist

Bypasses Spam check for trusted addresses (managed by Trustwave).

When a message arrives
And the message is incoming
Where addressed from 'Global Whitelist'

Then
Write log message with 'Info - Safe Sender'
And pass the message on to the next policy group

Rule: Allow Users on Safe Senders list

User Matching Allowed

Bypasses Spam check for trusted addresses (managed by each end user).

When a message arrives
And the message is incoming
Where the sender is in the recipient's safe senders list
Then
Write log message with 'Info - Safe Sender'
And pass the message on to the next policy group

Rule: Block Users on Blocked Senders list

User Matching Allowed

This rule blocks messages based on the recipient's Blocked Senders list (managed in the SQM console). Before using this rule, request enablement of the Blocked Senders feature. This option is intended to allow users to block material that is unwanted but not malicious, such as newsletters.

When a message arrives
And the message is incoming
Where the sender is in the recipient's blocked senders list
Then
Write log message with 'Spam – End user blacklist'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Phishing

User Matching Allowed

This rule blocks suspected phishing messages. Messages blocked by this rule are monitored by the threat evaluation team. Trustwave strongly recommends you do not enable SQM management of the Spam – Phishing category.

When a message arrives
And the message is incoming
Where message is categorized as 'Phishing'
Then
Write log message with 'Spam - Phishing'
And move the message to 'Spam - General' with release action "continue processing"

Rule: Block Spam - Signatures and Behavior

User Matching Allowed

This rule blocks messages identified as spam by multiple technologies including signatures and botnet characteristics. These messages are identified as spam with high confidence. End user review is normally not required.

When a message arrives
And the message is incoming
Where the message is detected as spam by SpamProfiler (Spam, Spam Bulk Mail, Confirmed (Malware), High (Probable Malware)) and SpamBotCensor
Then
Write log message with 'Spam - High Certainty'
And move the message to ‘Quarantine (Incoming)’ with release action “skip to the next policy group”

Rule: Block Spam - Signatures and Heuristics

User Matching Allowed

This rule blocks messages identified as spam by multiple technologies including signatures and heuristic analysis of content. These messages are identified as spam with high confidence. End user review is normally not required.

When a message arrives
And the message is incoming
Where the message is detected as spam by SpamCensor and SpamProfiler (Spam, Spam Bulk Mail, Confirmed (Malware), High (Probable Malware))
Then
Write log message with 'Spam - High Certainty'
And move the message to ‘Quarantine (Incoming)’ with release action “skip to the next policy group”

Rule: Block Suspect Spam - Signatures

User Matching Allowed

This rule blocks messages identified as spam by a signature based technology. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is incoming
Where the message is detected as spam by SpamProfiler (Spam, Spam Bulk Mail, Confirmed (Malware), High (Probable Malware))
Then
Write log message with ‘Spam - General’
And move the message to ‘Quarantine (Incoming)’ with release action “skip to the next policy group”

Rule: Block Suspect Spam - Behavior

User Matching Allowed

This rule blocks messages identified as spam due to characteristics typical of spambot origin. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is incoming
Where the message is detected as spam by SpamBotCensor
Then

Write log message with ‘Spam - General’
And move the message to ‘Quarantine (Incoming)’ with release action “skip to the next policy group”

Rule: Block Suspect Spam - Heuristics

User Matching Allowed

This rule blocks messages identified as spam by heuristic analysis of content. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is incoming
Where the message is detected as spam by SpamCensor
Then
Write log message with ‘Spam - General’
And move the message to ‘Quarantine (Incoming)’ with release action “skip to the next policy group”

Rule: Block Suspect Spam – Newly Registered Domain

User Matching Allowed

Blocks mail containing URLs referencing domains that were registered in the past 24 hours.

When a message arrives
And the message is incoming
Where message is categorized as 'Newly registered domain'
Then
Write log message with ‘Spam – Domain Age Detection’
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Suspect Spam - URL Block List

User Matching Allowed

This rule blocks messages identified as spam because they contain web links that are associated with spam. These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is incoming
Where message is categorized as 'URL Block List'
Then
Write log message with ‘Spam - General’
And move the message to ‘Quarantine (Incoming)’ with release action “skip to the next policy group”

Rule: Block Suspect Spam - Keywords

User Matching Allowed

This rule blocks messages identified as spam because they contain keywords associated with spam (a list manually maintained by Trustwave). These messages are identified as spam with moderate confidence. Enabling end user review (digest or SQM) is recommended.

When a message arrives
And the message is incoming
Where message triggers TextCensor script(s) 'ISP-Maintained Keyword List'
Then
Write log message with ‘Spam - General’
And move the message to ‘Quarantine (Incoming)’ with release action “skip to the next policy group”

Rule: Block Suspect Spam - Foreign Character Sets

User Matching Allowed

This rule blocks messages that use foreign character sets.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Suspect Character Sets'
Then
Write log message with 'Spam - Foreign Character Sets'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block Suspect Spam – Suspicious URLs in message

User Matching Allowed

This rule blocks messages that contain URLs identified as suspicious (phishing, malware, or spam) by the Trustwave URL Categorizer.

When a message arrives
And the message is incoming
Where message contains suspect URLs
Then
Write log message with ‘Suspect URL - Trustwave URL Categorizer’
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

2.2.3 Business Email Compromise (Inbound)

This ruleset helps detect and manage Business Email Compromise Fraud emails.

Rule: Block BEC - BEC Fraud Filter

User Matching Allowed

Trustwave strongly recommends you do not disable this rule

This rule blocks messages with multiple traits associated with BEC fraud.

When a message arrives
And the message is incoming
Where message is categorized as ‘BECFraud v8’
Then
Send a 'Business Email Compromise - In' system notification message
And write log message with "BEC - Filter'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block – Executive Name Match

User Matching Allowed

Blocks emails when a name in the From: header matches one of those configured in the Executive Names List.

When a message arrives
And the message is incoming
Where message is categorized as ‘Executive Name’
Then
Send a 'Business Email Compromise - In' system notification message
  And write log message with "BEC – Executive Name'
  And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Block – Domain Similarity Match

User Matching Allowed

Blocks emails where the domain in the From: header closely resembles one of your local domains.

When a message arrives
And the message is incoming
Where message is categorized as ‘Domain Similarity’
Then
Send a 'Business Email Compromise - In' system notification message
  And write log message with "BEC – Domain Similarity’
  And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Warn – From Reply-To Mismatch

User Matching Allowed

Adds a warning to the message where the From and Reply-To email addresses are mismatched.

When a message arrives
And the message is incoming
Where message is categorized as 'From Reply-To Mismatch'
Then
Write log message with "BEC – From Reply-To Mismatch'
And stamp message with "BEC – From Reply-To Mismatch'

Rule: Warn – External Email

User Matching Allowed

Adds a warning to the message indicating that the message was received from an external source.

When a message arrives
And the message is incoming
Then
Stamp message with "External Email Warning'

2.2.4 Attachment Control (Inbound)

Rule: Block unknown attachments

User Matching Allowed

This rule blocks messages which contain attachments that cannot be identified by the scanning service. Unidentifiable attachments are uncommon, and these attachments may or may not be malicious.

When a message arrives
And the message is incoming
Where message attachment is of type 'BIN'
Then
Write log message with 'Attachment Type - Unknown'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block unknown attachments (Notify)

User Matching Allowed

This rule blocks messages which contain attachments that cannot be identified by the scanning service. Unidentifiable attachments are uncommon, and these attachments may or may not be malicious. This rule notifies the recipient of the message that it was blocked.

When a message arrives
And the message is incoming
Where message attachment is of type 'BIN'
Then
Send a 'Attachment Type - Unrecognized' notification message
And write log message with 'Attachment Type - Unknown'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block executable files

User Matching Allowed

This rule blocks messages which contain executable attachments. Files in this category include Win32 executables, Mac executables, Unix executables, and self-extracting archives.

When a message arrives
And the message is incoming
Where message attachment is of type 'EXECUTABLE'
Then
Write log message with 'Attachment Type - Executable'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block executable files (Notify)

User Matching Allowed

This rule blocks messages which contain executable attachments. Files in this category include Win32 executables, Mac executables, Unix executables, and self-extracting archives. This rule notifies the recipient of the message that it was blocked.

When a message arrives
And the message is incoming
Where message attachment is of type 'EXECUTABLE'
Then
Send a 'Attachment Type - Executable' notification message
And write log message with 'Attachment Type - Executable'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block executable files (unless in Archive File)

User Matching Allowed

This rule blocks messages which contain executable attachments. Files in this category include Win32 executables, Mac executables, Unix executables, and self-extracting archives. Executable files inside standard archives, such as ZIP, RAR, or ARJ will not be blocked.

When a message arrives
And the message is incoming
Where message attachment is of type 'EXECUTABLE'
And where attachment parent type is not of type: ' ARCHIVE'
Then
Send a 'Attachment Type - Executable' notification message
And write log message with 'Attachment Type - Executable'
And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Video files

User Matching Allowed

This rule blocks messages which contain video attachments. Files in this category include AVI, MP4, Flash, and Quicktime files.

When a message arrives
And the message is incoming
Where message attachment is of type 'VIDEO'
Then
Write log message with 'Attachment Type - Video'
  And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Sound files

User Matching Allowed

This rule blocks messages which contain sound attachments. Files in this category include MP3, OGG, WAV, and Quicktime audio files.

When a message arrives
And the message is incoming
Where message attachment is of type 'SOUND'
Then
Write log message with 'Attachment Type - Sound'
  And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Sound files (Notify)

User Matching Allowed

This rule blocks messages which contain sound attachments. Files in this category include MP3, OGG, WAV, and Quicktime audio files. This rule notifies the recipient of the message that it was blocked.

When a message arrives
And the message is incoming
Where message attachment is of type 'SOUND'
Then
Send a 'Attachment Type - Sound' notification message
  And write log message with 'Attachment Type - Sound'
  And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block encrypted attachments

User Matching Allowed

This rule blocks messages which contain encrypted attachments. Files in this category include password-protected archives and encrypted PDF and Office documents.

When a message arrives
And the message is incoming
Where message attachment is of type 'ENCRYPTED'
Then
Write log message with 'Attachment Type - Encrypted'
  And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block encrypted attachments (Notify)

User Matching Allowed

This rule blocks messages which contain encrypted attachments. Files in this category include password-protected archives and encrypted PDF and Office documents. This rule notifies the recipient of the message that it was blocked.

When a message arrives
And the message is incoming
Where message attachment is of type 'ENCRYPTED'
Then
Send a 'Attachment Type - Encrypted' notification message
  And write log message with 'Attachment Type - Encrypted'
  And move the message to 'Quarantine (Incoming)' with release action "skip to the next policy group"

Rule: Block Archive attachments (Notify)

User Matching Allowed

This rule blocks messages which contain archived attachments. Files in this category include ZIP, ARJ, TAR and other formats. This rule notifies the recipient of the message that it was blocked.

When a message arrives
And the message is incoming
Where message attachment is of type 'ARCHIVE'
Then
Send a 'Archive in' system notification message
  And write log message with 'Attachment Type - Archive'
  And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Office Macro Documents

User Matching Allowed

This blocks messages that contain Office documents having macros included in them.

When a message arrives
And the message is incoming
Where message is categorized as 'Office Document Macros'
Then
Write log message with 'Attachment Type – Office Macros'
  And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Office Macro Documents (Notify)

User Matching Allowed

This blocks messages that contain Office documents having macros included in them. A notification is sent to the recipient.

When a message arrives
And the message is incoming
Where message is categorized as 'Office Document Macros'
Then
Send a 'Office Macro Document (In)' system notification message
  Write log message with 'Attachment Type – Office Macros'
  And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.2.5 Message Content (Inbound)

Rule: Strip read receipts from messages

User Matching Allowed

This rule removes read receipt requests from messages. The message content is otherwise unaffected.

When a message arrives
And the message is incoming
Then
Write log message with 'Strip Read Receipt Headers'
And rewrite message headers using 'Strip Read Receipt Request'

Rule: Block Fragmented Messages

User Matching Allowed

Fragmented messages are messages that come in one or more parts, and are re-assembled at the delivery point to read the entire content. Fragmented messages are very rarely used for legitimate purposes today, and can be an indicator that an attacker is attempting to bypass content scanning filters.

When a message arrives
And the message is incoming
Where message contains one or more headers 'Detect Fragmented Messages'
Then
Write log message with 'Message - Fragmented Message'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Encrypted Messages

User Matching Allowed

This rule prevents messages which contain S/MIME or PGP encrypted material from being sent to your organization. Internal employees may receive confidential information in encrypted form, to prevent detection by automated systems.

When a message arrives
And the message is incoming
Where message attachment is of type 'P7M; PGP'
And where message spoofing analysis is based on anti-relay and where Sender ID evaluation fails with Moderate Settings
Then
Write log message with 'Message - Encrypted'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.2.6 Dead Letter Handling (Inbound)

Quarantines malformed or otherwise unscannable or undeliverable mails.

No customer configuration is allowed.

2.3 Package: Blended Threats

Note: This package is optional and incurs an additional fee.

2.3.1 Blended Threats Protection (Inbound)

This ruleset allows you to check messages for Blended Threats, which are URL links that lead to malicious content on websites. Blended Threat checking includes two parts: rewriting of URLs by the included rule, and scanning by a cloud service when the URL link is clicked.

Rule: Bypass Rewrite for SMime Signed Messages

User Matching Allowed

This rule skips the Blended Threat URL rewriter when the message contains SMime signed data. Customers who need to maintain the check on signed mail at the internal server can choose to use this rule. CAUTION: URLs in the affected messages will not be scanned for malicious content at time of click. Recipients cannot be notified by a modification to affected messages because that would also prevent later validation of the signature. Set user matching to affect the minimum possible number of messages.

When a message arrives
And the message is incoming
Where message attachment is of type 'P7S'
Then
Pass the message on and skip the next rule

Rule: Blended Threats Scanner

User Matching Allowed

This rule rewrites URLs in the body of incoming email messages, so that the linked page will be submitted to a cloud service for scanning when the email recipient clicks the link.

When a message arrives
And the message is incoming
Then
Rewrite URLs in the message for Blended Threats scanning

2.4 Package: Data Protection

2.4.1 Sensitive Material (Outbound)

This ruleset scans outbound messages for potentially sensitive content, such as credit card numbers, US Social Security numbers or keywords for the financial/medical industry.

Rule: Block Credit Card Numbers – Extensive (with Notification)

User Matching Allowed

This rule looks for indications that credit card numbers are present in an email message or its attachments. The message recipient is notified. NOTE: This rule triggers on the presence of any string of

numbers that matches the format of a card number. It is likely to cause some false triggers on documents containing many numbers.

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Credit Card Number - Plain'
  And where message is categorized as 'CreditCard'
Then
Send a 'Policy Risk out' system notification message
  And write log message with 'Policy Breaches - Credit Card Numbers'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Credit Card Numbers – Keywords (with Notification)

User Matching Allowed

This rule looks for indications that credit card numbers are present in an email message or its attachments. To trigger, the rule also requires the presence of word(s) like "credit", "card" or "expiry" in the message. The message sender is notified.

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Credit Card Number - Keywords'
  And where message is categorized as 'CreditCard'
Then
Send a 'Policy Risk out' system notification message
  And write log message with 'Policy Breaches - Credit Card Numbers'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Social Security Numbers – Extensive (with Notification)

User Matching Allowed

This rule looks for indications that US Social Security numbers are embedded in an email message or its attachments. The message recipient is notified. NOTE: This rule triggers on the presence of any string of numbers that matches the format of a Social Security Number. It is likely to cause some false triggers on documents containing many numbers. The message sender is notified.

When a message arrives
And the message is outgoing
Where message is categorized as 'SocialSecurity'
Then
Send a 'Policy Risk out' system notification message
  And write log message with 'Policy Breaches - Social Security Numbers'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Social Security Numbers – Keywords (with Notification)

User Matching Allowed

This rule looks for indications that US Social Security numbers are present in an email message or its attachments. To trigger, the rule also requires the presence of related keyword(s) in the message. The message recipient is notified.

When a message arrives
And the message is outgoing
Where message triggers system text censor script(s) 'Social Security Number - Keywords'
  And where message is categorized as 'SocialSecurity'
Then
Send a 'Policy Risk out' system notification message
  And write log message with 'Policy Breaches - Social Security Numbers'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Copy Messages with HIPAA Content

User Matching Allowed

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. Sending a digest to the administrator is recommended.

When a message arrives
And the message is outgoing
Where message is categorized as 'HIPAA'
Then
Copy the message to 'Archive (Outgoing)' with release action "continue processing"
  And write log message with 'Policy Breaches - HIPAA Content'

Rule: Copy Messages with SEC Content

User Matching Allowed

This rule archives messages that contain keywords which might be a violation of the US Securities and Exchange Commission's regulations. The messages should be reviewed by the administrator to verify their content. Sending a digest to the administrator is recommended.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Keyword List - SEC'
Then
Copy the message to 'Archive (Outgoing)' with release action "continue processing"
  And write log message with 'Policy Breaches - SEC Content'

Rule: Copy Messages with Sarbanes-Oxley Content

User Matching Allowed

This rule archives 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. Sending a digest to the administrator is recommended.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Keyword List - SOX'
Then
Copy the message to 'Archive (Outgoing)' with release action "continue processing"
  And write log message with 'Policy Breaches - SOX Content'

2.4.2 Sensitive Material (Inbound)

This policy scans inbound messages for potentially sensitive content, such as credit card numbers, US Social Security numbers or keywords for the financial/medical industry.

Rule: Block Credit Card Numbers – Extensive (with Notification)

User Matching Allowed

This rule looks for indications that credit card numbers are present in an email message or its attachments. The message recipient is notified. NOTE: This rule triggers on the presence of any string of numbers that matches the format of a card number. It is likely to cause some false triggers on documents containing many numbers.

When a message arrives
And the message is incoming
Where message triggers system text censor script(s) 'Credit Card Number - Plain'
  And where message is categorized as 'CreditCard'
Then
Send a 'Policy Risk in' system notification message
  And write log message with 'Policy Breaches - Credit Card Numbers'
  And move the message to 'Quarantine (incoming)' with release action "continue processing"

Rule: Block Credit Card Numbers – Keywords (with Notification)

User Matching Allowed

This rule looks for indications that credit card numbers are present in an email message or its attachments. To trigger, the rule also requires the presence of word(s) like "credit", "card" or "expiry" in the message. The message recipient is notified.

When a message arrives
And the message is incoming
Where message triggers system text censor script(s) 'Credit Card Number - Keywords'
  And where message is categorized as 'CreditCard'
Then
Send a 'Policy Risk in' system notification message
  And write log message with 'Policy Breaches - Credit Card Numbers'
  And move the message to 'Quarantine (incoming)' with release action "continue processing"

Rule: Block Social Security Numbers – Keywords (with Notification)

User Matching Allowed

This rule looks for indications that US Social Security numbers are present in an email message or its attachments. To trigger, the rule also requires the presence of related keyword(s) in the message. The message recipient is notified.

When a message arrives
And the message is incoming
Where message triggers system text censor script(s) 'Social Security Number - Keywords'
  And where message is categorized as 'SocialSecurity'
Then
Send a 'Policy Risk in' system notification message

And write log message with 'Policy Breaches - Social Security Numbers'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.5 Package: Acceptable Use

2.5.1 Objectionable Material (Outbound)

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

Rule: Block Vulgarity

User Matching Allowed

This rule blocks messages containing common obscenities and vulgarities.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Language - Mild Profanity'
Then
Write log message with 'Policy Breaches - Vulgarity'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Racist and Hate Language

User Matching Allowed

This rule blocks messages containing especially offensive language, such as racist or hate speech.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Language - Racist and Hate'
Then
Write log message with 'Policy Breaches - Racist and Hate Language'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Pornographic Language

User Matching Allowed

This rule blocks messages containing sexually explicit or pornographic language.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Language - Pornographic'
Then
Write log message with 'Policy Breaches - Pornographic Language'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Block Pornographic Language (Notify)

User Matching Allowed

This rule blocks messages containing sexually explicit or pornographic language. The sender is notified about the message being blocked.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Language - Pornographic'
Then
Send a 'Language Out' system notification message
  And write log message with 'Policy Breaches - Pornographic Language'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Chain Letters

User Matching Allowed

This rule blocks messages which have the appearance of an Internet chain letter.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Generic Chain Letters'
Then
Write log message with 'Policy Breaches - Chain Letter'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Virus Hoaxes

User Matching Allowed

This rule blocks messages which have the appearance of a hoax virus warning chain letter.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Generic Virus Hoaxes'
Then
Write log message with 'Policy Breaches - Virus Hoax'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Block Script and Code

User Matching Allowed

This rule looks for indications that script and code in embedded in an email message, which could potentially be dangerous.

When a message arrives
And the message is outgoing
Where message triggers system TextCensor script(s) 'Script and Code'
Then
Write log message with 'Policy Breaches - Script and Code'
  And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

2.5.2 Objectionable Material (Inbound)

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

Rule: Block Vulgarity

User Matching Allowed

This rule blocks messages containing common obscenities and vulgarities.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Language - Mild Profanity'
Then
Write log message with 'Policy Breaches - Vulgarity'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Racist and Hate Language

User Matching Allowed

This rule blocks messages containing especially offensive language, such as racist or hate speech.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Language - Racist and Hate'
Then
Write log message with 'Policy Breaches - Racist and Hate Language'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Pornographic Language

User Matching Allowed

This rule blocks messages containing sexually explicit or pornographic language.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Language - Pornographic'
Then
Write log message with 'Policy Breaches - Pornographic Language'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Chain Letters

User Matching Allowed

This rule blocks messages which have the appearance of an Internet chain letter.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Generic Chain Letters'
Then

Write log message with 'Policy Breaches - Chain Letter'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Virus Hoaxes

User Matching Allowed

This rule blocks messages which have the appearance of a hoax virus warning chain letter.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Generic Virus Hoaxes'
Then
Write log message with 'Policy Breaches - Virus Hoax'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Block Script and Code

User Matching Allowed

This rule looks for indications that script and code in embedded in an email message, which could potentially be dangerous.

When a message arrives
And the message is incoming
Where message triggers system TextCensor script(s) 'Script and Code'
Then
Write log message with 'Policy Breaches - Script and Code'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.6 Package: Advanced Image Analysis

The rules in this package scan messages for attached images that are identified as containing specific types of content by a deep image analysis module.

2.6.1 Image Analyzer (Outbound)

Rule: Aircraft Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Aircraft'
Then
Write log message with 'Image Analysis – Aircraft'
And move the message to 'Quarantine (Outgoing)' with release action "continue processing"

Rule: Alcohol Images

User Matching Allowed

When a message arrives
And the message is outgoing

Where the attached image matches the category 'Alcohol'
Then
Write log message with 'Image Analysis – Alcohol'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Chat Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category ‘Chat’
Then
Write log message with 'Image Analysis – Chat’
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Credit Cards Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category ‘Credit Cards'
Then
Write log message with 'Image Analysis – Credit Cards'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Child Sexual Abuse Material Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Child Sexual Abuse Material’
Then
Write log message with 'Image Analysis – Child Sexual Abuse Material’
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Currency Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category ‘Currency’
Then
Write log message with 'Image Analysis – Currency’
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Documents Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Documents'
Then
Write log message with 'Image Analysis – Documents'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Drugs Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Drugs'
Then
Write log message with 'Image Analysis – Drugs'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Extremism Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Extremism'
Then
Write log message with 'Image Analysis – Extremism'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Gambling Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Gambling'
Then
Write log message with 'Image Analysis – Gambling'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Gore Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Gore'
Then
Write log message with 'Image Analysis – Gore'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: ID Documents Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'ID Documents'
Then
Write log message with 'Image Analysis – ID Documents'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Maps Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Maps'
Then
Write log message with 'Image Analysis – Maps'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Medical Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Medical Images'
Then
Write log message with 'Image Analysis – Medical’
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Memes Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Memes'
Then
Write log message with 'Image Analysis – Memes'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Motor Vehicles Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Motor Vehicles'
Then
Write log message with 'Image Analysis – Motor Vehicles'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Offensive Gestures Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Offensive Gestures'
Then
Write log message with 'Image Analysis – Offensive Gestures'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Pornography Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Pornography'
Then
Write log message with 'Image Analysis – Pornography'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: QR Codes Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'QR Codes'
Then
Write log message with 'Image Analysis – QR Codes'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Schematic Drawings Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Schematic Drawings'
Then
Write log message with 'Image Analysis – Schematic Drawings'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Swimwear and Underwear Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Swimwear and Underwear'
Then
Write log message with 'Image Analysis – Swimwear and Underwear'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Tattoos Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Tattoos'
Then
Write log message with 'Image Analysis – Tattoos'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

Rule: Weapons Images

User Matching Allowed

When a message arrives
And the message is outgoing
Where the attached image matches the category 'Weapons'
Then
Write log message with 'Image Analysis – Weapons'
And move the message to ‘Quarantine (Outgoing)’ with release action “continue processing”

2.6.2 Image Analyzer (Inbound)

Rule: Aircraft Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Aircraft'
Then
Write log message with 'Image Analysis – Aircraft’
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Alcohol Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Alcohol'
Then
Write log message with 'Image Analysis – Alcohol'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Chat Images

User Matching Allowed

When a message arrives
And the message is incoming

Where the attached image matches the category ‘Chat’
Then
Write log message with 'Image Analysis – Chat’
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Credit Cards Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category ‘Credit Cards'
Then
Write log message with 'Image Analysis – Credit Cards'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Child Sexual Abuse Material Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Child Sexual Abuse Material’
Then
Write log message with 'Image Analysis – Child Sexual Abuse Material’
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Currency Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category ‘Currency’
Then
Write log message with 'Image Analysis – Currency’
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Documents Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Drugs'
Then
Write log message with 'Image Analysis – Drugs'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Drugs Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Drugs'
Then
Write log message with 'Image Analysis – Drugs'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Extremism Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Extremism'
Then
Write log message with 'Image Analysis – Extremism'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Gambling Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Gambling'
Then
Write log message with 'Image Analysis – Gambling'
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Gore Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Gore'
Then
Write log message with 'Image Analysis – 'Gore’
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: ID Documents Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'ID Documents'
Then
Write log message with 'Image Analysis – ID Documents’
And move the message to ‘Quarantine (Incoming)’ with release action “continue processing”

Rule: Maps Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Maps'
Then
Write log message with 'Image Analysis – Maps'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Medical Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Medical Images'
Then
Write log message with 'Policy Breaches - Medical'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Memes Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Memes'
Then
Write log message with 'Image Analysis – Memes'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Motor Vehicles Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Motor Vehicles'
Then
Write log message with 'Image Analysis – 'Motor Vehicles'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Offensive Gestures Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Offensive Gestures'
Then
Write log message with 'Image Analysis – Offensive Gestures'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Pornography Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Pornography'
Then
Write log message with 'Image Analysis – Pornography'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: QR Codes Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'QR Codes'
Then
Write log message with 'Image Analysis – QR Codes'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Schematic Drawings Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Schematic Drawings'
Then
Write log message with 'Image Analysis – Schematic Drawings'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Swimwear and Underwear Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Swimwear and Underwear'
Then
Write log message with 'Image Analysis – Swimwear and Underwear'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Tattoos Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Tattoos'
Then
Write log message with 'Image Analysis – Tattoos'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

Rule: Weapons Images

User Matching Allowed

When a message arrives
And the message is incoming
Where the attached image matches the category 'Weapons'
Then
Write log message with 'Image Analysis – Weapons'
And move the message to 'Quarantine (Incoming)' with release action "continue processing"

2.7 Package: M365 Insider Threat Protection

2.7.1 Threat Protection

Rule: Block Phishing

User Matching Allowed

Applies Phishing detection to internal messages.

When a message arrives
And the message is internal
Where message is categorized as 'Phishing'
Then
Write log message with 'Spam - Phishing'
And move the message to 'Insider Threats (Internal)' with release action "continue processing"

Rule: Block BEC Fraud

User Matching Allowed

Applies Business Email Compromise Fraud detection to internal messages.

When a message arrives
And the message is internal
Where message is categorized as 'BEC Fraud v8'
Then
Write log message with 'BEC - Filter'
And move the message to 'Insider Threats (Internal)' with release action "continue processing"

About Trustwave

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave Fusion® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.