
# How it Works: Trend Micro Hosted Email Security

A Trend Micro White Paper I March 2010

# Table of Contents

## Introduction

According to experts at TrendLabs, spam now comprises as much as 95% of all email and continues to grow. In the first three months of 2008, spam rates almost doubled over rates observed at the end of 2007, and average daily spam volumes are expected to keep increasing by 30 to 50 billion messages per day every six months.[1]

As spam continues to grow at these dramatic rates, traditional on-premise email security products are failing to keep up. These products often suffer from inherent hardware capacity limits, rendering them unable to handle large spam volumes. Once the amount of spam exceeds the limit, these solutions rapidly become overloaded, significantly slowing email delivery.

This traditional model also fails to stop spam before it enters the network, exposing the company to a steady stream of email threats while adding significant infrastructure costs, such as bandwidth and storage, as spam consumes staff and network resources.

On-premise email security products also require ongoing tuning to maintain effectiveness, and that usually means at least a partially dedicated person to keep the product up to date. Too often, then, organizations face a trade-off between two undesirable alternatives: on the one hand, suffering from lower user productivity due to more spam showing up in email boxes, and on the other, having IT staff spend a greater percentage of each day maintaining, tuning, and troubleshooting email security products.

These limitations explain why the IDC predicts that demand for hosted security solutions—also known as SaaS (Software as a Service) solutions—will grow by more than 30% annually through 2012. For context, the growth rate for hosted email security is projected to be more than eight times that of the traditional software email security market, and more than 60% faster than appliance-based email security solutions.[2]

**Why consider a hosted antispam and email security solution?**

We spoke with a number of Trend Micro customers about why they migrated from traditional, on-premise email security products to a hosted antispam solution. Some of the common complaints about legacy email security products included:

1. IT staff spending too much time on email security maintenance, or not being able to spend the time and seeing spam-blocking rates go down and false-positive rates go up
2. Lack of hardware necessary to handle growing email (and spam) volume
3. Low user productivity due to excess spam, especially for users of devices such as laptops and smartphones
4. Email retention policies in place dictating that all spam on the network must be stored for a particular length of time

[1] Trend Micro Threat Roundup and Forecast – 2H 2008, June 2008.
[2] IDC, "Worldwide Messaging Security 2007-2011 Forecast and 2006 Vendor Shares: DLP, Encryption, and Hosted Services Heating Up," December 2007.

## Solution Overview

No organization can afford to leave its mission-critical communications in the wrong hands. That's why it's especially important to choose a robust, cost-effective solution from an established vendor.

Trend Micro has more than 20 years of security experience, and currently scans more than 20 billion websites, email sources and files every day across both traditional and hosted environments to continuously improve antispam and email security. Trend Micro Hosted Email Security protects more than 30,000 organizations against spam, viruses, spyware, phishing, and other email threats.

Hosted Email Security requires no hardware or software to install and maintain. All email-based threats are kept completely off the network, helping organizations reclaim IT staff time, end-user productivity, network bandwidth, mail server storage, and CPU capacity. In addition, Trend Micro's worldwide team of experts manages all hot fixes, patches, updates, and application tuning to continuously optimize security and performance.

This email security solution is easily deployed, requiring organizations to merely redirect their MX record. The threat protection is set to default settings to provide immediate protection upon deployment, and the solution includes Trend Micro's industry-leading Service Level Agreement. With flexible management options, organizations are able to optimize spam-blocking and false-positive rates, as well as create content filtering and outbound email policy rules. Administrators also have the ability to add flexible content filtering rules to implement email use policies across the company. They can even integrate Hosted Email Encryption as an add-on solution, setting encryption as a rule action when filtering content.

This white paper explains each of these features and provides sample use cases to assist in their application.

## Industry-Leading Quality of Service—or Money Back

Trend Micro provides an aggressive Service Level Agreement (SLA) for Hosted Email Security that contractually binds Trend Micro to provide monetary compensation to customers if certain service performance levels are not met.[3]

| Service Level Agreement Provisions | Trend Micro Money-Back Commitment[3] | Monetary penalty if service performance levels are not met? |
|---|---|---|
| Availability/Uptime | 100% availability/uptime | Yes |
| Spam-Blocking | 99%+ spam-blocking effectiveness | Yes |
| False Positives | No more than .0003% false-positive rate | Yes |
| Email Delivery Latency | No more than one minute average email delivery latency | Yes |
| Virus Infection | Zero email-based viruses | Yes |
| Support Responsiveness | Response time commitment based on severity of issue and varies by region | Yes |

## Customized Threat Filtering

A leading antispam solution should be capable of identifying both inbound and outbound spam without blocking legitimate mail—a capability only possible with a sophisticated, multilayered filtering mechanism.

Trend Micro Hosted Email Security applies multilayered, customizable email scanning technologies for just that purpose. First, integrated threat intelligence from the Trend Micro™ Smart Protection Network™ is applied through an Email Reputation database that intelligently tracks and monitors millions of malicious IP addresses. Email Reputation blocks email threats from known spammers, along with emerging threats from botnets and zombies. The service then scans emails using both antispam and antivirus engines—powered by integrated security technologies—to stop yet more spam, phishing, viruses, spyware, and other malware. It also takes advantage of Web Reputation technology to block malicious URLs embedded in emails.

When Hosted Email Security is first deployed, the threat protection rules are implemented with default settings, giving administrators the option to set the desired action for spam: Delete, Quarantine, or Tag and Deliver. Administrators can even create and modify rules to customize threat protection based on an organization's email traffic.

[3] Money-back remedies are defined in the Hosted Email Security Service Level Agreement for service availability, email delivery latency, spam blocking, false positive rate, antivirus effectiveness, and support response.

## Rules for Viruses and Other Malicious Code

With Hosted Email Security, organizations can set multiple virus rules, applying rules to specific individuals or groups for one or more of the following actions.

**Intercept**

- Do not intercept messages
- Delete entire message
- Deliver now
- Quarantine
- Change recipient

**Modify**

- Clean cleanable viruses; delete those that cannot be cleaned
- Delete attachment
- Insert stamp in body (select text)
- Tag subject

**Monitor**

- Send notification
- BCC

**BEST PRACTICE USE CASE: Managing Executable Attachments**

1) In most cases, organizations will want to delete viruses, but they can determine how conservative they want to be. For example, they can delete the entire message, clean cleanable viruses, delete those that cannot be cleaned, or delete the attachment.

2) If a group within the company receives a lot of executable files as part of its normal course of business (such as media files from the marketing department), administrators may wish to avoid deleting the entire message for that particular group and instead quarantine the emails and delete the attachments.

   If an entire email is deleted, the administrator may wish to send a notification to the intended recipient. If an attachment is deleted, the administrator may wish to insert a stamp in the body of the email indicating as much.

## Rules for Spam or Phishing

Hosted Email Security includes two types of rules designed to catch spam or phishing email messages. The first rule stops emails that are generally defined as spam (unsolicited bulk email). The second rule identifies “spam-like” email messages—for example, newsletters, which may be considered spam by some recipients and legitimate mail by others. Companies are able to apply different antispam aggressiveness settings to each type of spam; for instance, companies will most likely want to be more aggressive at stopping definite spam and less aggressive at stopping spam-like messages. These rules can also identify phish and other suspicious content.

The default action for spam email messages is to delete them, and the default action for spam-like messages is to tag and deliver the email, with the option to change default actions. Trend Micro recommends that administrators Delete, Quarantine, or Tag and Deliver spam. In addition, administrators can choose from six different levels of aggressiveness: Lowest, Low, Moderately Low, Moderately High, High, and Highest (see Figure 1 below).

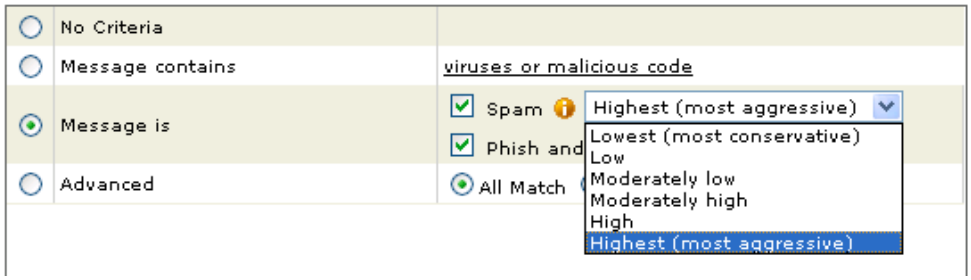


Figure 1: Setting Antispam Agressiveness

**BEST PRACTICE USE CASE: Maximizing Spam-Blocking Rates**

1) If organizations set a low antispam aggressiveness level, they can be more certain that the email identified is actually spam, and may want to set the action to Delete. However, this will catch a lower number of spam emails.

2) If organizations set a high antispam aggressiveness level, more spam will be caught, but they also risk a higher false-positive rate. In this case, the administrator may want to quarantine possible spam so that end users can check for false positives.

3) The Tag and Deliver action is helpful for organizations using Hosted Email Security as part of a layered email security approach. For example, when used in conjunction with Trend Micro™ ScanMail™ for Microsoft® Exchange, the administrator can use Tag and Deliver to send the emails identified through the service to the Microsoft Outlook® spam folder created by ScanMail. This allows end users to view all of their spam in one location, regardless of which product identified the email as spam.

## Other Threat Protection Rules

### Exceeding Message Size or Allowed Number of Recipients

Hosted Email Security provides other threat protection rules as well. One rule is designed to protect against bulk mail attacks such as Distributed Denial of Service (DDoS) attacks, limiting the size of the email that the organization is willing to accept as well as the number of recipients that can be listed in a single email. Customers have the flexibility to adjust these rules to fit their particular needs.

**High-Risk Attachments**
Another rule protects against high-risk attachments. Administrators define which file types they consider to be high risk. For example, file types may include executables (.exe) or files that hide their true file type. In this case, a malware writer may use a different file extension that does not identify the true file. For example, a media file (.mp3) may use a text file extension (.txt) to try to hide the true nature of the file and attempt to bypass antivirus protection.

Two types of file extensions are provided based on the level of danger they pose to companies:

A) File extensions that Trend Micro strongly recommends the administrator block
B) File extensions that the administrator should also consider blocking

Each list includes a check box next to each file type, and administrators can select the file extensions they wish to apply. Administrators can also select file types for MIME content-type files and true file types that they wish to block. All high-risk attachments are deleted before the email is delivered to the recipient.

**Password-Protected Zip File Attachments**
Hosted Email Security enables administrators to decide how they would like to handle password-protected zip files. By default, messages with a password-protected zip file attachment are passed through to the recipient, and a notification is placed in the body of the email stating that the attached file was not scanned. However, the administrator can modify this rule; for example, the attachment can be deleted instead of delivered to the recipient.

The threat protection rules in this section all use the “Advanced” message attribute options in Figure 2 below. Different attributes are selected depending on the type of rule. This same attribute list is used when applying content filtering rules described in the Content Filtering Capabilities section below.

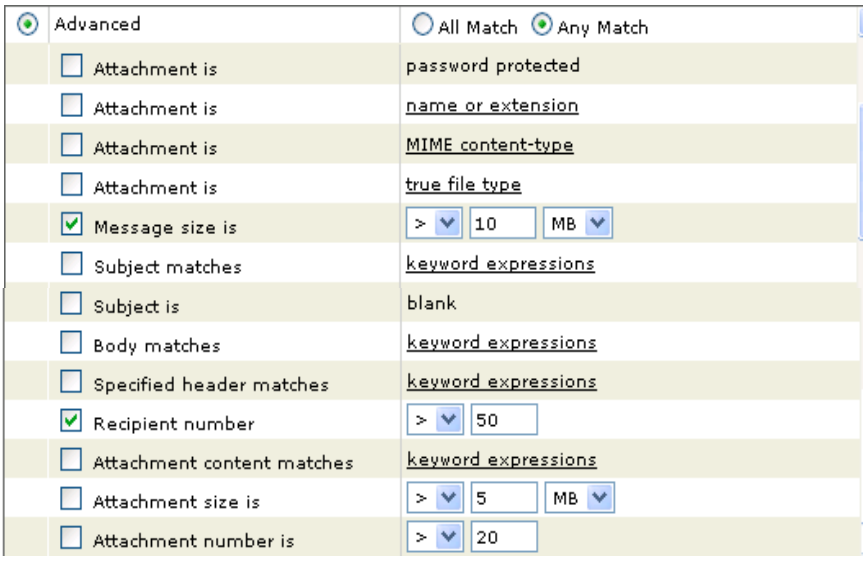


Figure 2: Advanced Message Attributes

## Outbound Email Filtering

Inbound email filtering is a critical component in any email security solution. But that's only half of the equation—a company's reputation suffers whenever an internal user inadvertently sends a contaminated file to an external recipient. Therefore, for the most robust security possible, companies should endeavor to scan and filter outbound email as well.

Unlike many other hosted email security vendors, Trend Micro provides outbound filtering at no additional cost to Hosted Email Security users. Outbound filtering will scan outgoing emails for email threats as well as apply any content filtering rules created by the administrator.

### Benefits of Outbound Filtering

- Outbound threat filtering prevents internal machines infected by malicious code from spreading spam or viruses externally. For example, companies with a large percentage of employees with laptops should consider this option.
- Outbound content filtering enforces compliance, prevents data leaks, and implements internal email use policies.

## Content Filtering Capabilities

Each industry applies different regulations and standards to corporate email, and each organization observes its own unique interpretation of those regulations. That's why it's especially important for administrators to be able to filter content so that they can comply more completely with both internal and regulatory standards.

Hosted Email Security provides flexible and easy content filtering options that enable administrators to flag virtually any type of content. These capabilities can be used to meet a wide range of standards that regulate the use of confidential information—including governmental, industry, or internal standards. Content filtering also helps prevent data leaks and can be used to implement email use policies, protecting the organization from legal fees and fines, preserving the company's reputation, and helping to maintain good business practices.

When creating a rule, administrators should follow these steps:

1. Specify if the rule applies to inbound email or outbound email
2. Determine the sender/recipients for the rule
3. Select the message attributes—i.e., what the filter is looking for
4. Indicate the rule action(s)—i.e., what happens when the rule is triggered
5. Name and save the rule

When indicating senders or recipients for a particular rule, administrators can use specific email addresses or select an entire domain. Administrators can also specify exceptions to a rule.

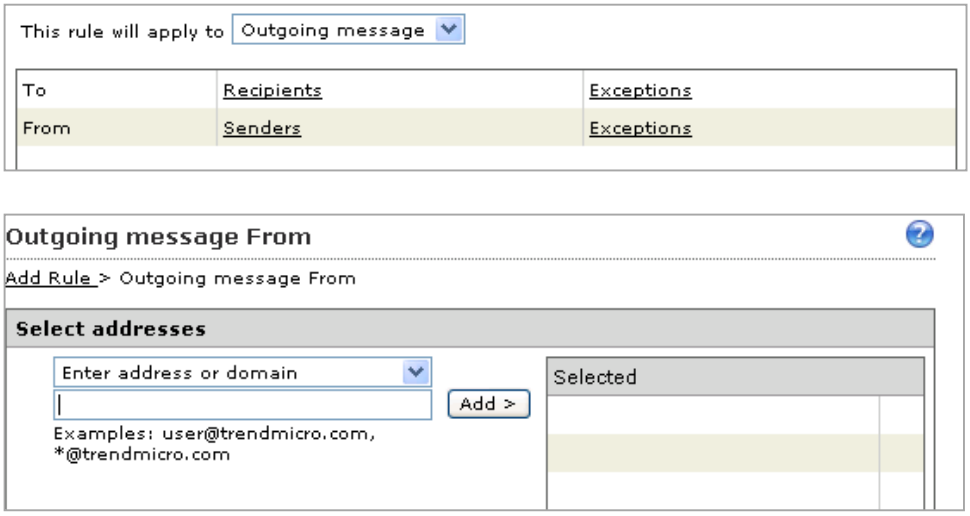


Figure 3: Specifying Senders and Recipients

For message attributes, Trend Micro filters identify content by attachment characteristics, keywords, lexicons, and customized data rules created through regular expressions and Boolean logic. Figure 2 on page 8 lists the initial content filtering options, such as where to search (header, subject, body, or attachment) and shows links that allow administrators to drill down to additional detail, enabling them to specify the search criteria.

The attachment characteristics include password protection, name or extension, attachment size, attachment number, and attachment content. Filtering can also be based on the content in the subject line, email body, or email header. When specifying content, administrators can apply the following:

- Word lists—either from a list created by the administrator or a list provided by the service, such as profanity, racial or sexual discrimination, chain mail, or fraudulent award notification identifiers
- Data format lexicons, such as the pre-defined content filters for social security or credit card numbers that come bundled with Hosted Email Security
- Or a combination of elements using regular expressions

To identify content, administrators create a “keyword expression.” Administrators may use any combination of keywords and regular expressions to define a keyword expression. Once created, administrators save and name the keyword expression. It can then be applied to multiple rules (for example, for different groups or for different message attributes, such as subject line, email body, attachment content, or email header).

After the message attribute has been defined, administrators must specify the action(s) that will be applied when the message attribute is flagged.

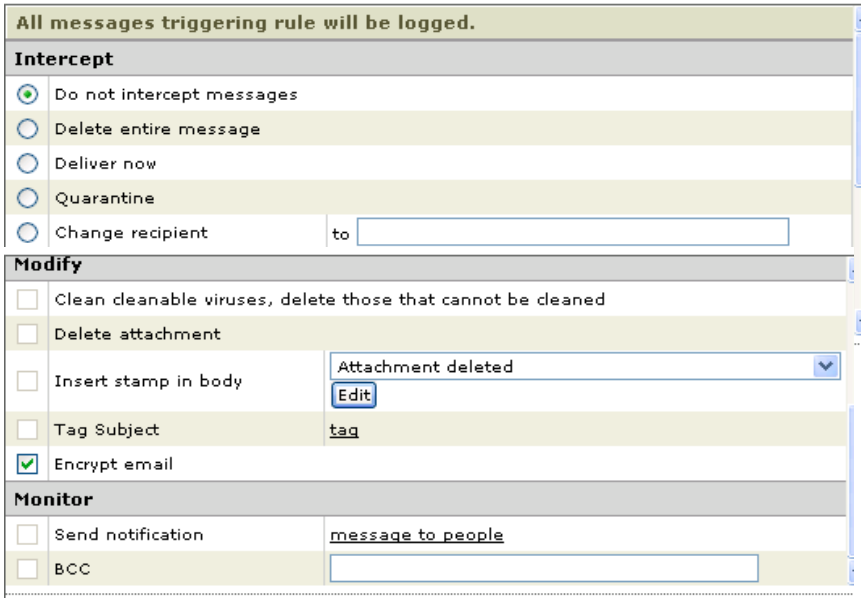


Figure 4: Action Options for Content Filtering Rules

**BEST PRACTICE USE CASE: Managing Sensitive Information**

1) Administrators can combine data format lexicons, such as credit card or social security number formats, with client name lists or account numbers to flag emails with personally identifiable information. This option helps organizations meet common regulatory requirements.

2) Key expressions for words like “encrypt” or “confidential” can make it easy to apply email use policies. Administrators can apply an action such as “encrypt” or limit permissible distribution if emails contain these flags.

3) Content filtering can also be used to help prevent data leaks. Key expressions can be defined that flag emails with intellectual property (for example, patent numbers, project names, etc.), helping ensure that this content is only distributed to particular recipients.

Once the action(s) has been designated, administrators merely name and save the rule. After creating a rule, administrators may edit or copy it as needed. Copying a rule makes it easy to create a similar rule—simply edit the copied rule with any desired changes.

## Hosted Email Encryption

Email frequently contains sensitive data that requires secure transmission to meet confidentiality and privacy requirements. Organizations also need to protect confidential emails for particular groups, such as executive management, human resources, or legal departments. In many cases, therefore, encryption is necessary to create a truly secure email environment.

Hosted Email Encryption is an add-on to Hosted Email Security and can be purchased as a separate service to help secure the transmission of confidential data. It provides policy-based email encryption that encrypts data using content filtering rules, applying encryption to emails with particular types of content or emails for particular groups.

Email Encryption is seamlessly integrated with the content filtering capabilities of Hosted Email Security; however, emails are not encrypted merely by turning on the service. Administrators will need to configure content filtering rules that apply encryption as a rule action. Figure 4 on the previous page shows Email Encryption as a rule action option under the Modify section. With policy-based encryption, organizations avoid relying on individual users to secure important content. Instead, encryption is automatically applied when content filtering rules are triggered, helping to ensure that organizations meet confidentiality and privacy requirements.

Recipients of the encrypted email receive an email notification in the form of an electronic sealed envelope. They can then download their own copy of the Hosted Email Encryption client or use their web browser to read and reply without the need to install any software.

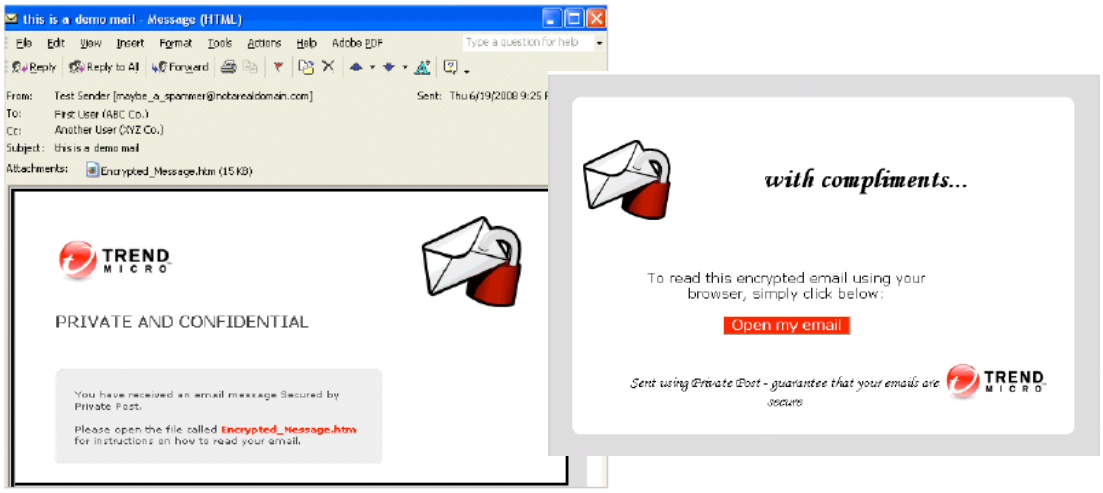


Figure 5: Email Encryption Recipient Experience: Encrypted Email Envelope and Browser Access

To use Hosted Email Encryption, organizations must have the full-featured version of Hosted Email Security. Organizations may request a trial of Hosted Email Encryption within the service console under Administration.

## Conclusion

Most companies already have a traditional email security product installed on-premise. Over time, these products can become overwhelmed by continuously increasing spam volume, requiring additional investments—in the form of additional hardware and sometimes licenses—to remain effective.

When working with on-premise email security products, IT staff can find themselves bogged down with the daily maintenance required to keep these products up to date. Frequently, these products run in "set and forget" mode, meaning that application maintenance, tuning, and troubleshooting can be neglected. As a result, spam-blocking effectiveness will decline over time.

Trend Micro currently scans more than 20 billion websites, email sources and files every day across both on-premise and hosted environments, and Hosted Email Security has more than adequate capacity to meet any increase in spam volume. Also, because Hosted Email Security is hosted in Trend Micro datacenters, Trend Micro's worldwide team of experts manages all hot fixes, patches, updates, and application tuning to continuously optimize security and performance.

Trend Micro backs Hosted Email Security with a contractually-binding SLA that provides 100% uptime along with industry-leading spam-blocking effectiveness and a .0003% false-positive rate.

All said, Hosted Email Security stops spam and other email threats before they reach the network, enabling organizations to reclaim IT infrastructure resources like network bandwidth, mail server storage, and CPU cycles. That means less spam, more time, and fewer headaches for organizations of all sizes.

**Trust the Experts in Threat Protection**
Since 1988, Trend Micro has held a singular focus on Internet content security. That's why thousands of companies continue to put their trust in Trend Micro—a company with 20 years of experience informed by a history of innovation.

## Related Resources

White Paper: How Trend Micro Hosted Email Security – Inbound Filtering Adds Value to Your Current Environment