



## Trend Micro Hosted Email Security Stop Spam. Save Time.



How Hosted Email Security –  
Inbound Filtering Adds Value to  
Your Existing Environment

A Trend Micro White Paper | March 2010



## Table of Contents

<b>Introduction</b> .....	<b>3</b>
<b>Solution Overview</b> .....	<b>3</b>
<b>Industry-Leading Quality of Service—or Money Back</b> .....	<b>4</b>
<b>How Inbound Filtering Works</b> .....	<b>4</b>
What is reputation-based filtering? .....	4
What is content-based filtering? .....	5
<b>Best Practice Defaults for Hosted Email Security – Inbound Filtering</b> .....	<b>5</b>
Rule Type 1: Antivirus .....	6
Rule Type 2: Exceeding Message Size or Allowed Number of Recipients .....	6
Rule Type 3: Spam or Phishing .....	6
Rule Type 4: Newsletter or Spam-Like .....	7
Rule Type 5: Password-Protected and Zipped Files .....	7
<b>Leveraging User Directories Against Backscatter and Directory Harvest Attacks</b> .....	<b>7</b>
<b>Approved Sender Lists Reduce False Positives</b> .....	<b>8</b>
<b>End-User Spam Management Reduces Your Administrative Burden</b> .....	<b>9</b>
Spam Quarantine .....	9
<b>Easy Management Tools Enable Flexible Administration</b> .....	<b>10</b>
<b>Conclusion</b> .....	<b>11</b>
<b>Related Resources</b> .....	<b>11</b>



## 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 2009, spam rates almost doubled over rates observed at the end of 2008, and average daily spam volumes are expected to keep increasing by 30 to 50 billion messages per day every six months.

As spam continues to grow at these dramatic rates, many traditional, on-premise email security products are being supplemented with hosted email security. That's because most security products require sustained maintenance over time to stay effective. Too often, however, maintenance can be delayed as other critical business projects take priority. Businesses and companies can then be vulnerable not only to spam - which can consume employee productivity and expensive infrastructure resources - but inbound email-based threats such as malicious urls and other malware embedded in email.

## Solution Overview

Hosted Email Security – Inbound Filtering 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. The Inbound Filtering solution also includes an industry-leading Service Level Agreement to ensure mission critical quality of service with 100% uptime, zero email-based viruses, no more than one minute of email delivery latency and support responsiveness – or money back.

Information on the additional features available with full-featured Trend Micro Hosted Email Security - which includes both inbound and outbound threat filtering and stronger SLA provisions - is contained in a separate white paper.

<sup>1</sup> Trend Micro Threat Roundup and Forecast – 2H 2008, June 2008.





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

Trend Micro provides an aggressive Service Level Agreement (SLA) for Hosted Email Security – Inbound Filtering that contractually binds Trend Micro to provide monetary compensation to customers if certain service performance levels are not met.<sup>2</sup>

Inbound Filtering Service Level Agreement (SLA) Provisions	Trend Micro Money-Back Commitment	Money back if service level commitments are not met?
Availability/Uptime	100% availability/uptime	Yes
Email Delivery Latency	No more than one minute email delivery latency	Yes
Virus Infection	Zero email-based virus infections	Yes
Support Responsiveness	Response time commitment based on severity of issue and varies by region	Yes

## How Inbound Filtering Works

Hosted Email Security – Inbound Filtering applies two primary layers of email filtering to ensure that spam, phishing attempts, and other email threats are blocked while valid email is delivered to the appropriate recipient. In addition, it assures email privacy with automated email pass-through rules that filter email with zero human intervention.

There are two primary layers of Trend Micro technology applied to all emails routed through the service:

- I) Email reputation filtering
- II) Content-based filtering

### What is reputation-based filtering?

When someone sends mail to a mail server protected by Hosted Email Security – Inbound Filtering, Trend Micro will check the sender’s reputation against our proprietary email reputation IP address databases which include more than a decade’s worth of data on known malicious IP addresses to determine whether the sender IP address is trustworthy. Web Reputation further protects by blocking malicious URLs embedded in emails. These reputation databases are continuously updated as Trend Micro scans, filters and correlates more than 20 billion websites, email and files daily across both hosted and traditional on-premise environments.

<sup>2</sup> 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.





Email Reputation not only blocks known spammers, it also stays current with new and emerging threats such as botnets—networks of compromised PCs. Experts estimate that close to 90% of all spam today originates from botnets. The challenge with stopping spam from botnets is that new PCs are being added to the botnet every day, so filtering based on known IP address reputations alone may not catch spam from this new botnet source. Fortunately, the Trend Micro™ Smart Protection Network™ infrastructure that powers Hosted Email Security is able to identify known threats more quickly than other antispam and email security solutions, and is more effective in stopping new and emerging threats in real time.

### **What is content-based filtering?**

After the message passes the first layer of protection, Inbound Filtering will scan email content for known spam patterns and malware, and apply dynamic heuristics to identify and stop new threats. Similar to reputation-based filtering, email content scanning is also continuously updated through Trend Micro's proprietary Smart Protection Network.

For example, the antispam content engine continuously updates signature filters to block specific known spam emails, continuously improving spam indicators against spam probability ratings to set thresholds that determine if an email is spam. In addition, Hosted Email Security – Inbound Filtering is also able to identify targeted spam attacks, attachment spam, image-based spam and embedded links to malicious websites.

Along with antispyware technology, Hosted Email Security – Inbound Filtering includes Trend Micro's award-winning antivirus technology, with full pattern-file and zero-day protection. In the case of zero-day protection, Trend Micro looks for virus indicators without having to rely on a specific pattern file—a heuristic approach that intelligently applies predictive techniques to stop new and emerging malware.

## **Best Practice Defaults for Hosted Email Security – Inbound Filtering**

Spam protection is only as good as the best practices behind it. Hosted Email Security – Inbound Filtering adds value to your current environments by implementing best practices to stop spam and other email-based threats before they reach your network.

The following five types of rules are set to default – with the exception of spam action – and provide administrators read-only policy access.

For the spam action default, administrators may set the spam action – that is, the action triggered when spam is detected - to one of three options:

- Delete
- Quarantine
- Tag and deliver

Administrators who have purchased full-featured Hosted Email Security may modify the default settings, the default actions, enable content filtering rules, scan and filter password-protected and zipped files, and add new rules.





Rules	Action	Order	Modified	Status
airfaire: Virus-mass-mailing	Delete	1	1/14/08	✓
airfaire: Exceeding msg size or # of recipients	Delete	2	1/14/08	✓
airfaire: Spam or Phish	Quarantine	3	2/11/08	✓
airfaire: Newsletter or spam-like	Quarantine	4	1/23/08	✓
airfaire: Virus-uncleanable	Del. Attach ...	5	1/14/08	✓
airfaire: High-risk attachment	Del. Attach ...	6	1/14/08	✗
airfaire: Virus-cleanable	VirusClean	7	1/14/08	✓
airfaire: Password protected	Stamp	8	1/14/08	✓

Figure 1: Default Policy Rules

### Rule Type 1: Antivirus

If any of the following are found, then the default rule is to delete the email.

- Mass mailing: A message is identified as containing an uncleanable virus associated with mass-mailing behavior
- Virus-uncleanable: A message is identified as containing a virus that cannot be cleaned
- Virus-cleanable: A message is identified as containing a virus that can be cleaned

### Rule Type 2: Exceeding Message Size or Allowed Number of Recipients

This rule is designed to protect the system from Distributed Denial of Service (DDoS) and Zip of Death attacks. Under this rule, Hosted Email Security – Inbound Filtering deletes an incoming message if its size exceeds the default limit of 50MB or if the message has been sent to more than 1,000 recipients.

### Rule Type 3: Spam or Phishing

This rule is designed to catch spam or phishing email messages. By default, all spam messages are deleted. Hosted Email Security – Inbound Filtering administrators cannot change the antispam aggressiveness, but they can select the spam action: Delete, Quarantine, or Tag and Deliver (which tags the subject line and delivers the email to the recipient). If Quarantine is selected, all quarantined messages are saved for seven days in the administrative web-accessible quarantine as well as an optional end-user web-accessible quarantine.





#### **Rule Type 4: Newsletter or Spam-Like**

This rule is designed to catch “grey mail” (such as newsletters) that may be considered good mail by some and spam by others. The default action for these spam-like email messages is to tag the subject line (with “**Spam>**”). We highly recommend that only the Tag Subject or Quarantine actions be used for this rule. All quarantined messages are saved for seven days in the administrative web-accessible quarantine as well as an optional end-user web-accessible quarantine.

#### **Rule Type 5: Password-Protected and Zipped Files**

This rule is designed to flag and notify end users that a password-protected or zipped file included in an email was detected but not scanned. The notification to the recipient will be placed in the body of the email. For example, the notification for a password-protected file will read: “The attachment named (attachment file name) could not be scanned for viruses because it is password-protected.”

## **Leveraging User Directories Against Backscatter and Directory Harvest Attacks**

Backscatter occurs when a Delivery Status Notification (DSN) is sent to an email address forged in a spam run or forged by a virus that propagates via email. In most cases, DSNs are welcome because the sender usually wants to know when a message has been delayed or cannot be delivered to the recipient. However, if an email address has been forged and used by a spammer or virus and used as the “from” address in a spam run, then the mail server supporting the email address domain may be overwhelmed with bounce-back emails.

In the case of a Directory Harvest Attack, a spammer will ping an organization’s mail server with email addressed to random recipients. Any emails that do not bounce back are considered valid and may then be used in spam runs or sold to other spammers.

Importing user directories enables Hosted Email Security – Inbound Filtering to stop backscatter and directory harvest attack by pre-identifying legitimate inbound email addresses and domains for the organization. The service provides tools to help with the directory import including an Active Directory client, and organizations can use either an automated tool that periodically sends directory files or a manual tool that sends directory files only as necessary.



## Approved Sender Lists Reduce False Positives

False positives (i.e., legitimate emails incorrectly identified as spam) can be as problematic as spam itself. With an approved senders function, mail administrators are able to pre-approve specific email addresses or domains to be automatically forwarded to the recipient. This process is known as white-listing and is a best practice used by mail administrators to reduce false positives.

The screenshot shows the 'Approved Senders' management interface. At the top, the 'Managed Domain' is set to 'supremeshoppingclub.com'. Below this is a table of approved senders with columns for 'Sender', 'Recipient Domain', and 'Date Approved'. A modal dialog is open over the entry 'nicoled7@earthlink.net', showing 'OK' and 'Cancel' buttons.

Sender	Recipient Domain	Date Approved
kevin_rudd@australia.gov.au	supremeshoppingclub.com	8/15/08 11:26:48 AM
angela_merkel@bundesregierung.de	supremeshoppingclub.com	8/15/08 11:16:08 AM
nicoled7@earthlink.net	supremeshoppingclub.com	08/16/08 01:41:56
nicolas_sarkozy@gouv.fr	supremeshoppingclub.com	8/15/08 11:14:55 AM
donald_tsang@gov.hk	supremeshoppingclub.com	8/15/08 11:39:39 AM
silvio_berlusconi@governo.it	supremeshoppingclub.com	8/15/08 11:25:58 AM
jose_zapatero@la-mondoa.es	supremeshoppingclub.com	8/15/08 11:24:49 AM
helen_clark@ministers.govt.nz	supremeshoppingclub.com	8/15/08 11:28:08 AM
stephen_harper@pm.gc.ca	supremeshoppingclub.com	8/15/08 11:36:16 AM
gordon_brown@pm.gov.uk	supremeshoppingclub.com	8/15/08 11:18:43 AM
rafael_delgado@presidencia.gob.ec	supremeshoppingclub.com	8/15/08 11:37:28 AM
felipe_calderon@presidencia.gob.mx	supremeshoppingclub.com	8/15/08 11:35:17 AM
lula_dasilva@presidencia.gov.br	supremeshoppingclub.com	8/15/08 11:34:17 AM
barack_obama@senate.us.gov	supremeshoppingclub.com	8/15/08 11:10:35 AM
john_mccain@senate.us.gov	supremeshoppingclub.com	8/15/08 11:10:25 AM

Figure 2: Adding Approved Senders

For senders that have been approved by the mail administrator, Hosted Email Security – Inbound Filtering will not block email messages based on email reputation or antispam scanning. However, all virus and attachment rules will still apply to the approved senders.



## End-User Spam Management Reduces Your Administrative Burden

### Spam Quarantine

One way to reduce IT burden is to empower end users to manage their own spam folders. The Hosted Email Security – Inbound Filtering End-User Quarantine (EUQ) is an easy-to-use interface that enables end users to manage spam email messages held in quarantine. End users can also set up their own unique lists of approved email senders—reducing false positives and eliminating the administrative burden for IT.

The EUQ allows end users to:

- Create a new account
- Configure quarantine spam actions and an approved senders list
- Change passwords

End users can access the web EUQ at the following URL: <https://us.emailsec-euq.trendmicro.com> and then subsequently manage their spam quarantine by sorting by date, sender, or subject line.

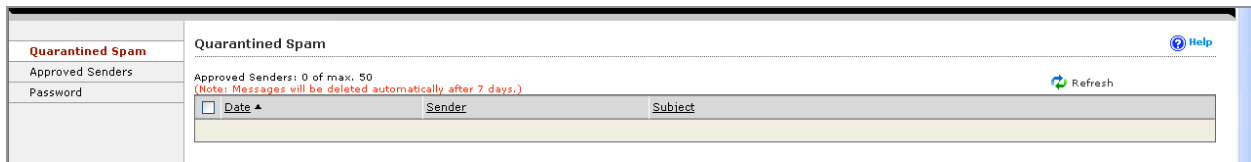


Figure 3: End-User Quarantine

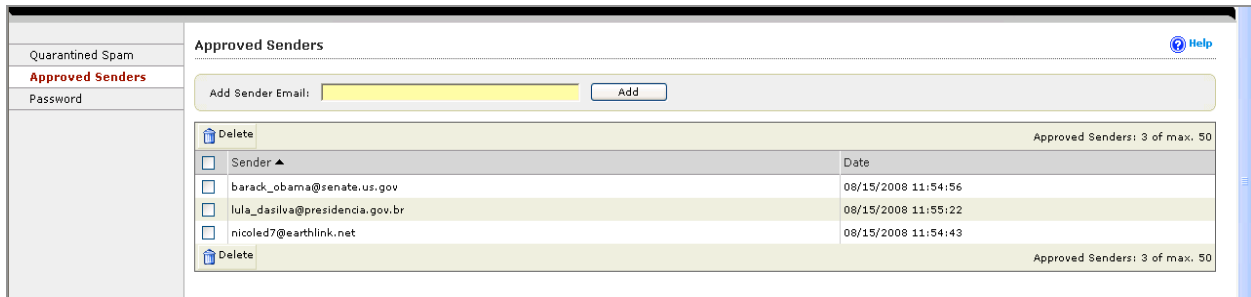


Figure 4: User-Managed Approved Senders

## Easy Management Tools Enable Flexible Administration

A leading antispam solution should not only enable users to manage their own quarantine folders—it should give administrators options for how they manage quarantines as well.

Hosted Email Security – Inbound Filtering offers flexible quarantine settings, enabling administrators to determine which emails will be quarantined. These quarantined emails then undergo further inspection (such as antivirus and content filtering). Administrators can also determine how frequently end users receive quarantine notification emails.

**Quarantine Settings**

Managed Domain: \*@supremeshoppingclub.com Disabled

**Digest Mail Schedule for supremeshoppingclub.com**

Daily  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday

Time: 12:00 AM UTC

**Digest Mail Template for supremeshoppingclub.com**

Sender's Email: %DIGEST\_RCPT%

Subject: Trend Micro IMHS quarantined spam %DIGEST\_DATE% for %DIGI  
(Maximum number of characters is 256.)

HTML content: Inline Action Disabled

```
<html><head><style>.data2b {BACKGROUND-COLOR: #eecedb;}</style></head><body><br/><b>Total number of quarantined spam message(s): %DIGEST_TOTAL_COUNT%</b><br/>Release quarantined spam messages: <a href = "https://us.imhs-euq.trendmicro.com" >https://us.imhs-euq.trendmicro.com</a> (username: %DIGEST_RCPT% )<br/>Number of days to keep quarantined spam messages: 7 <br/><br/>The following summary displays a maximum of 100 of the most recent quarantined spam messages:<br/><form id="01AE5E" method="post" action="%EUQ_HOST_SERVER%/emailRequest.imhs"><table border=1><tr>
```

Reset to Default HTML Content

Figure 5: Managing Quarantine Settings



## Conclusion

Hosted Email Security – Inbound Filtering adds value to your current environment by stopping spam and other email threats before they reach your 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.

By minimizing risk without incurring hardware or maintenance costs, Hosted Email Security – Inbound Filtering helps organizations achieve a fast return on investment (ROI) with an easy-to-deploy, easy-to-manage spam-blocking solution. In taking the fight against spam to the next level, organizations will have the tools they need to focus more energy on what they do best—running their businesses.

### **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 it Works: Trend Micro Hosted Email Security

