What Is Trend Micro Hosted Email Security?

Trend Micro™ Hosted Email Security provides always-up-to-the-minute email security with no maintenance required by IT staff to stop spam, viruses, and other malware before they reach your network.

How Hosted Email Security Works

❶ The originating mail server performs a DNS lookup to determine the location of the *example.com* domain. The Mail eXchange (MX) record for *example.com* holds the IP address of the service instead of the original IP address for *example.com*, since the service must first scan your company's mail before final delivery to your local email server.

❷ The originating mail server routes the mail to Hosted Email Security.

❸ Hosted Email security accepts the message and perform message filtering and policy matching on your behalf.

❹ If a message is slated for delivery according to its security policy or validity status, Hosted Email Security routes the message to the original *example.com* mail servers.

No new hardware or software is required when using Hosted Email Security

Internet
Hosted Email Security

Client
Your mail server
Client

Mail sent to the *example.com* domain...

...passes first through Hosted Email Security and...

...after scanning, arrives at the actual *example.com* domain
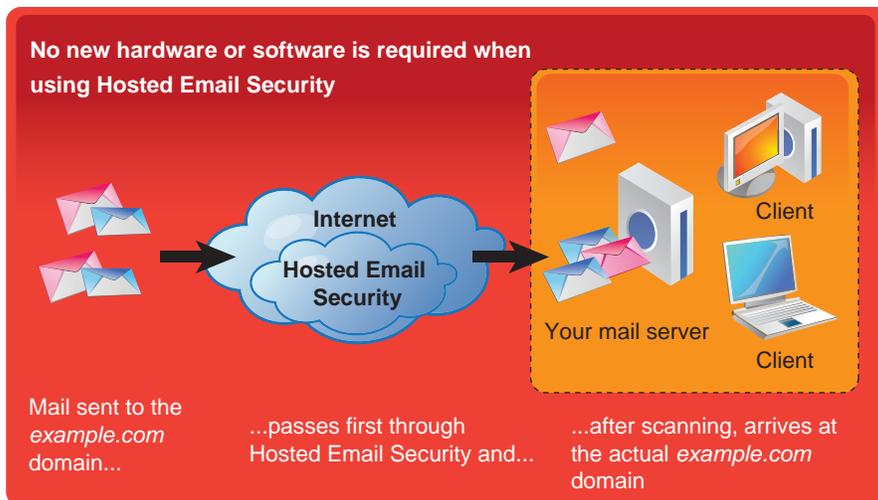
System Requirements

Hosted Email Security requires no hardware on your premises (other than your mail gateway). All scanning hardware is off-site at secure Trend Micro network operations centers. To access your web-based administration console, you need a personal computer with access to the Internet.

Software Requirements

Use of the web console requires JavaScript™ and Hosted Email Security supports the following browsers for the web console:

- Microsoft™ Internet Explorer™ 6.0 and 7.0
- Mozilla™ FireFox™ 2.0

To configure Hosted Email Security to work properly and effectively, follow these basic steps:

☐ 1. Submit account activation information
☐ 2. Log on to web-based admin console
☐ 3. Add one or more domains to manage
☐ 4. Confirm mail delivery through Hosted Email Security
☐ 5. Redirect MX record for your domain
☐ 6. Configure your MTA, if applicable

Onsite Network

Before activating Hosted Email Security, you need:

- An existing Internet gateway or workgroup SMTP connection
- Access to the DNS mail exchange record. (Contact your Internet service provider, if necessary, for more information or configuration help.)

Caution: Do not redirect your MX record until you receive confirmation that Trend Micro has established your account. If you make this change before your account is set up, your email may be lost. Trend Micro will provide redirection details.

Default Settings

To ensure high-quality, continuous service and to protect your network from common SMTP attacks such as mail floods and Zip of Death, Hosted Email Security system limitations by default include the following:

- Message size limits: 50MB per message
- Total embedded layers within a compressed file: 20 layers
- Total decompressed message size: 30MB
- Total files in a compressed archive: 353 files
- Total quarantine storage per seat: 50MB
- Total approved sender entries per seat: 50

Email on Hosted Email Security servers is retained for the following periods:

- Quarantined email in Europe, the Middle East, and Africa (EMEA) region: 21 days
- Quarantined email (all other regions): 15 days
- Mail tracking information: 7 days
- Mail queue when customer MTA is unavailable: up to 5 days
- Reporting logs: configurable

Registering and Activating Trend Micro Hosted Email Security

You need a Hosted Email Security Activation Code (AC) for activation. Depending on your region, you may also need a Registration Key (RK). If you have neither an AC nor an RK, contact your Trend Micro sales representative. Until you input a valid AC, you will be unable to use this service.

If you have your Registration Code or Activation code, you can register your Hosted Email Security account at the Trend Micro Online Registration website, at:
https://olr.trendmicro.com/registration/us/en-us/login.aspx

Email Encryption

The Email Encryption service is an add-on component to Hosted Email Security (full version) and so must be purchased and activated separately. Email encryption is not available to customers using the Hosted Email Security—Inbound Filtering version.You must have outbound filtering enabled before you can activate email encryption.

Submitting Account Activation Information

Before using the service, you must activate the account.

To activate the Hosted Email Security account:

❶ Locate your confirmation of purchase and a Registration Key in the email message received from Trend Micro.

❷ Visit the Trend Micro Online Registration site (URL provided in email message), choose a user name and password, and complete the registration process.Trend Micro sends you an email with the user name that you chose and the URL of the Hosted Email Security administrative console.

❸ Log on to the console with that user name. A dialog box prompts you to enter domain and IP information.

❹ Click **Submit**. Trend Micro will set up your account and send you a confirmation email. (Allow 24-48 hours.) This email will contain information about where to direct your MX record.

❺ Send a test email to your test email address to verify that email can pass through Hosted Email Security.

❻ Redirect your MX record as explained in the email mentioned above.

Registration Key and Activation Code

Registration Key (RK): If you are a customer in North America, Europe, the Middle East, or Africa, you need a product RK to register Hosted Email Security. This key uses 22 characters, including hyphens, in the following format:

XX-XXXX-XXXX-XXXX-XXXX

If you are in the above regions, register using a valid RK in order to receive an Activation Code, which enables you to begin using the service.

Activation Code (AC): Regardless of your region, you must have an AC. The administrative console displays the status of your license. An AC uses 37 characters, including hyphens, in the following format:

XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

After you have registered the service, Trend Micro will send your AC.

Redirecting Your MX Record

The Mail eXchange (MX) record determines the message routing for all email sent to your domain. To route messages destined for your domain through Hosted Email Security, you must redirect your MX record. The welcome email that you receive tells you where to redirect your MX record. You can make this change manually (typical for self-managed, smaller accounts) or through a support technician. If you need help configuring the MX records for your domain, contact your Internet Service Provider or your DNS technician.

> **Caution:** DNS propagation may take up to 48 hours. During this time, do not turn off any on-premise security. You may receive some email directly for a short time until the transition completes.

Configuring Your Mail Transfer Agent

By default, Hosted Email Security deletes all "spam or phish" messages, regardless of which version you are using. Full version customers can modify this rule. (See the *Trend Micro Hosted Email Security Administrator's Guide* for more information.)

> **Note:** Customers without the full version can modify the action portion of the spam-related rules. They can determine how the spam message will be handled: tag the subject as spam, delete, or quarantine the message.

You can configure your MTA to handle spam according to your company security policy. Hosted Email Security can forward tagged messages to a spam folder, can delete them, or can pass them on to the end user, and so on. If you choose to tag such messages, the subject line of spam messages will be tagged with **Spam/Phish>** followed by the original subject line.

Logging on for the First Time

The welcome packet that you received after signing up for Hosted Email Security contains a user name and password to log on initially. Use these credentials to log on to the console at the URL provided in the confirmation email.

Confirming Your Security Policy

You can verify that the service is working by sending one or more emails that violate one of the default policies. Send your test messages, and after two hours visit the Mail Tracking screen and query Hosted Email Security using the sender or recipient of the test message. The query results should display the blocked message(s).

Hosted Email Security features, by account type	Inbound Filtering	Full
Provides multitiered anti-spam, antivirus, and anti-phishing protection for inbound email traffic with streamlined management for complete security requiring minimal administration.	✔	✔
The simplified management console has preset protection settings and is updated and tuned by Trend Micro. ** Full version customers also begin with default rules but can modify them and create new rules.*	✔	✔
You can quickly create lists of approved senders designated by email address or domain.	✔	✔
Web-based End-User Quarantine is available.	✔	✔
Provides in-depth content filtering and policy management for more granular access and control. *Optional: Outbound message scanning.*		✔
Email messages and attachments can be filtered based on keywords, lexicons, and attachment characteristics, as well as more customized filtering rules.		✔
You can create rules by company, group, or individual and can set an enforcement action for each policy.		✔
Optional add-on feature: Email encryption. Provides policy-based encryption to secure email.		