

HOSTED EMAIL SECURITY FREQUENTLY ASKED QUESTIONS

| | |
|--|----------|
| OVERVIEW AND BENEFITS | 3 |
| 1. WHAT IS HOSTED EMAIL SECURITY? | 3 |
| 2. WHAT ARE THE UNIQUE BENEFITS OF DEPLOYING HOSTED EMAIL SECURITY?..... | 3 |
| 3. WHY USE A HOSTED SOLUTION FOR EMAIL SECURITY INSTEAD OF AN ON-PREMISE EMAIL SECURITY PRODUCT? | 3 |
| 4. WHY BUY A HOSTED SOLUTION FROM TREND MICRO? | 4 |
| 5. IS HOSTED EMAIL SECURITY SUITABLE FOR ENTERPRISES?..... | 4 |
| 6. IF WE ALREADY HAVE SCANMAIL OR OTHER ON-PREMISE SECURITY PRODUCT PROTECTION, DO WE NEED HOSTED EMAIL SECURITY? | 4 |
| SERVICE LEVEL AGREEMENT | 5 |
| 7. WHAT IS THE HOSTED EMAIL SECURITY SERVICE LEVEL AGREEMENT (SLA)? | 5 |
| 8. IS A COPY OF THE SLA EASILY ACCESSIBLE?..... | 5 |
| 9. HOW DO CUSTOMERS GET THE SLA? | 5 |
| 10. IS THE SLA BINDING? | 5 |
| 11. DOES THE SLA APPLY WHEN CUSTOMERS USE HOSTED EMAIL SECURITY AS PART OF TREND MICRO™ WORRY-FREE™ BUSINESS SECURITY? | 5 |
| 12. CAN CUSTOMERS ACCUMULATE MORE THAN ONE CREDIT ACROSS DIFFERENT SERVICE LEVELS IN ONE MONTH?..... | 5 |
| PRODUCT FEATURES AND HOW THEY WORK | 6 |
| 13. WHAT IS THE DIFFERENCE BETWEEN HOSTED EMAIL SECURITY AND HOSTED EMAIL SECURITY – INBOUND FILTERING OPTION?..... | 6 |
| 14. HOW DOES HOSTED EMAIL SECURITY STOP SPAM AND OTHER EMAIL-BASED THREATS? | 6 |
| 15. HOW DOES EMAIL REPUTATION WORK?..... | 6 |
| 16. WHAT TYPES OF THREAT SCANNING DOES HOSTED EMAIL SECURITY CONDUCT?..... | 6 |
| 17. WHAT MALWARE PROTECTION DOES HOSTED EMAIL SECURITY PROVIDE? | 7 |
| 18. WHAT TECHNOLOGIES DOES THE TREND MICRO ANTISPAM COMPOSITE ENGINE USE? | 7 |
| 19. WHAT CONTENT FILTERING CAPABILITIES ARE OFFERED? | 7 |
| 20. WHAT EMAIL ENCRYPTION OPTIONS ARE AVAILABLE TO HOSTED EMAIL SECURITY CUSTOMERS? | 7 |
| 21. WHAT DOES TREND MICRO OFFER TO HELP ENFORCE COMPLIANCE AND PREVENT DATA LEAKS? | 8 |
| 22. IS THERE A RISK THAT LEGITIMATE EMAIL WILL ACCIDENTALLY BE BLOCKED?..... | 8 |
| 23. DOES HOSTED EMAIL SECURITY ENABLE END-USERS TO MANAGE THEIR OWN SPAM QUARANTINE? | 8 |
| ACTIVATION, UPGRADE AND PURCHASE INFORMATION | 9 |
| 24. HOW IS HOSTED EMAIL SECURITY SOLD? | 9 |
| 25. HOW DO I GET SPECIFIC PRICING INFORMATION? | 9 |
| 27. HOW EASY IS HOSTED EMAIL SECURITY TO IMPLEMENT?..... | 9 |
| 28. TO GET STARTED, CUSTOMERS HAVE TO REDIRECT MX RECORDS TO TREND MICRO. WHAT IS AN MX RECORD?..... | 9 |
| 29. CAN WE UPGRADE FROM HOSTED EMAIL SECURITY – INBOUND FILTERING OPTION TO HOSTED EMAIL SECURITY? | 9 |
| 30. WHAT IS REQUIRED TO UPGRADE TO NEW VERSIONS OF HOSTED EMAIL SECURITY? | 9 |

| | |
|--|-----------|
| PRIVACY, SUPPORT AND CONTROL | 10 |
| 31. DOES TREND MICRO PROTECT THE PRIVACY OF OUR EMAIL CONTENT? | 10 |
| 32. WHAT DISASTER RECOVERY OPTIONS ARE AVAILABLE? | 10 |
| 33. DOES TREND MICRO HAVE A TEAM DEDICATED TO MONITORING AND MANAGING SOLUTIONS LIKE HOSTED EMAIL SECURITY? | 10 |
| 34. DO CUSTOMERS LOSE CONTROL OF MX RECORDS WHEN THEY POINT TO TREND MICRO? | 10 |
| 35. WILL CUSTOMER EMAIL BE STORED ON TREND MICRO SERVERS? | 10 |
| 36. IS HOSTED EMAIL SECURITY AN “OUTSOURCED SERVICE”? | 10 |

OVERVIEW AND BENEFITS

1. What is Hosted Email Security?

Trend Micro Hosted Email Security stops more than 99% of all spam and other email threats before they reach the network, enabling organisations to reclaim IT staff time, end-user productivity, and network resources. In addition, Hosted Email Security offers outbound content filtering and optional encryption to help enforce compliance and prevent data leaks. As a hosted solution, Hosted Email Security can be implemented in less than 48 hours with no hardware or software requirements. Trend Micro performs all solution maintenance including updates, patches, hot fixes, and application tuning to ensure that Hosted Email Security performance is continuously optimised with little to no time spent on maintenance by the customer.

[to top](#)

2. What are the unique benefits of deploying Hosted Email Security?

Hosted Email Security has the #1 spam catch rate, according to independent benchmarking tests.¹ The layers of spam protection include advanced email reputation filtering, which is part of the Trend Micro™ Smart Protection Network™. The Smart Protection Network correlates threat intelligence across email, web, and file reputation databases to immediately block threats before they reach the network. For example, if a malicious URL is noted by our web reputation technology and a link to this URL is found in an email, that email will be blocked.

Hosted Email Security includes antivirus technology that was rated #1 in blocking malware in independent tests.² Trend Micro created and owns all of this technology, allowing customers to receive continuous, real-time protection against rapidly evolving spam tactics and today's complex emerging web threats.

In addition, Hosted Email Security uniquely saves IT staff time with easy to use administration tools like reprocessing of quarantined email, automatic end-user notification when email content policies are violated, compound "and/or" rules to more easily optimise spam-blocking rates and lower false-positive rates, and email content filtering which can scan even zipped, embedded, and password-protected files.

¹ West Coast Labs Anti-Spam Comparative Test, January 2009

² NSS Labs Endpoint Security Socially-Engineered Malware Protection Comparative Test Results, September 2009

[to top](#)

3. Why use a hosted solution for email security instead of an on-premise email security product?

Organisations receive the following benefits when using a hosted email security solution instead of an on-premise email security product:

- Stops spam and other email threats before they reach the network
- Enables customer to reclaim IT staff time, end-user productivity, mail server storage and cpu capacity, network bandwidth, and other costly resources
- No hardware or software, with little to no maintenance required
- Deploys in less than 48 hours
- Trend Micro performs all maintenance, including updates and application tuning, with little to no maintenance work required from the customer
- Allows distributed organisations to maintain a consistent security posture—since the latest protection is available at all times to all users in all locations, there is no need for software upgrades at multiple locations
- Lower total cost of ownership than traditional hardware and software products
- Flexibility with capacity planning—unlimited email and spam-filtering capacity for one fixed price per user, with none of the additional hardware costs typically associated with on-premise email security products as user counts scale up or down

[to top](#)

4. Why buy a hosted solution from Trend Micro?

Trend Micro currently protects more than 30,000 customers every day in more than 120 countries around the world with Trend Micro Hosted Email Security. In addition, Trend Micro is a leader in secure content and threat management and (unlike many other vendors of hosted solutions) is a well-established, stable company. Trend Micro has more than 20 years of security experience and currently scans more than 20 billion websites, emails and files daily across both on-premise and hosted environments. In addition, the Smart Protection Network provides correlated in-the-cloud, multi-threat protection from data gathered across all Trend Micro products and services for faster, smarter threat response.

[to top](#)

5. Is Hosted Email Security suitable for enterprises?

Yes. Hosted Email Security will scale to meet the needs of businesses of all sizes, from five users to very large enterprises and ISPs. Mail tracking correlates logs to enable administrators to quickly find the status of any email and determine how policies have impacted the email and the current location, while detailed reports enable administrators to access reports for auditing purposes as well as quickly view the value of the service. In addition, email use and content filtering rules allow administrators to have granular control over the organisation's email.

Also, an industry-leading Service Level Agreement, disaster recovery features, and privacy protections support enterprise email requirements. Hosted Email Security provides enterprises with the benefits of a hosted solution, taking a load off the network and saving on IT resources, while still providing administrators the control over the enterprise's email that they might expect from an on-site solution.

In addition, Hosted Email Security is ideal for large distributed organisations that find regular software upgrades across multiple locations time-consuming and expensive. With Hosted Email Security, enterprises will always have the latest and greatest security, ensuring immediate protection of their mail stream with the benefit of less complexity.

[to top](#)

6. If we already have ScanMail or other on-premise security product protection, do we need Hosted Email Security?

Yes. There are inherent benefits for protecting email at different points in the network. ScanMail integrates with the mail server (Microsoft Exchange or IBM® Lotus® Domino™) to protect the network from within the gateway, focusing on interoffice email, protecting the mail store, scanning email from remote users, and providing the first inspection point for outgoing email. In addition, ScanMail for Microsoft Exchange also provides end-user quarantine capabilities in Outlook that can be integrated with Hosted Email Security, allowing end users to view their spam in a junk folder in Outlook. Client-level protection focuses specifically on the individual desktop, providing yet another layer of protection. Gateway-to-desktop coverage at the point of vulnerability is required to stop threats where they originate.

[to top](#)

SERVICE LEVEL AGREEMENT

7. What is the Hosted Email Security Service Level Agreement (SLA)?

Hosted Email Security includes a bundled, contractually-binding service level agreement which provides the following guarantees: 100% service availability, no more than one minute email delivery latency, 99%+ spam-blocking effectiveness, no greater than a .0003% false-positive rate, zero virus infections, and support responsiveness. If these guarantees are not met in any given month, customers are eligible for money back.

| Service Level Agreement Provisions | Hosted Email Security | Hosted Email Security - Inbound Filtering |
|------------------------------------|-----------------------------------|---|
| Availability | 100% uptime | 100% uptime |
| Viruses | Zero email-based viruses | Zero email-based viruses |
| Spam-blocking effectiveness | 99% or better | n/a |
| False positives | No more than .0003% | n/a |
| Support responsiveness | Matches incident severity | Matches incident severity |
| Email delivery latency | No more than a one minute latency | No more than a one minute latency |

[to top](#)

8. Is a copy of the SLA easily accessible?

Yes. A copy of the SLA may be accessed after logging into the Hosted Email Security console under the administration section. Simply select the applicable region/language from the drop down menu.

[to top](#)

9. How do customers get the SLA?

The SLA is included with Hosted Email Security when customers purchase the service.

[to top](#)

10. Is the SLA binding?

Yes. Just like the End User Licence Agreement (EULA), the SLA was created to be an integral part of Hosted Email Security. If there is a conflict between the provisions of the documents, the SLA will be followed. Both Trend Micro and the customer are responsible for complying with the provisions in the SLA. Please note: The SLA and the EULA may be updated or modified from time to time.

[to top](#)

11. Does the SLA apply when customers use Hosted Email Security as part of Trend Micro™ Worry-Free™ Business Security?

Yes, the SLA is applicable to the Hosted Email Security – Inbound Filtering portion of Worry-Free Business Security.

[to top](#)

12. Can customers accumulate more than one credit across different service levels in one month?

Yes. Customers can submit multiple remediation requests for a calendar month. Some individual service levels only allow for one remediation request per month. These include:

- Availability
- Latency
- False positives
- Antivirus

Other service levels allow for multiple submissions within one month (including the antispam and technical support service levels). Customers can also submit remediation requests for different types of service levels within one month.

[Back to top](#)

PRODUCT FEATURES AND HOW THEY WORK

13. What is the difference between Hosted Email Security and Hosted Email Security – Inbound Filtering Option?

Both Hosted Email Security and Hosted Email Security – Inbound Filtering Option include highly effective spam-blocking technology, web-based end-user quarantine management, extensive logging, reporting and notifications, and are backed by service level commitments.

Hosted Email Security: Provides the option to filter outbound as well as inbound email traffic. The advanced option enables the administrator to modify default email threat policies to optimise spam-blocking, false-positive rates, and other threat-blocking effectiveness. The administrator may also set rules to enforce email use policies, including email size and number of recipients, or create content filtering rules for the email header, subject, body, and attachments (PDF and Microsoft document files) to help enforce compliance and prevent data leaks. Predefined word lists and data format lexicons, such as credit card and personal identification numbers (for example, social security numbers), are also available. An identity-based email encryption add-on is available for Hosted Email Security.

Hosted Email Security – Inbound Filtering Option: Available as a secondary version of Hosted Email Security with fewer features, the Inbound Filtering Option checks inbound email traffic to stop spam and other email-based threats with default protection policies. Administrators may set desired actions for spam emails—delete, quarantine, or tag and deliver—but are not allowed to modify the default policies.

Both services are managed through one web-based console with all updates, hot fixes, patches, and application tuning conducted by Trend Micro.

[to top](#)

14. How does Hosted Email Security stop spam and other email-based threats?

Hosted Email Security scans emails in three phases:

- a. Email Reputation
- b. Threat scanning
- c. Content filtering (Hosted Email Security only)

Email Reputation stops email threats based on the reputation of the sender. Threat scanning uses threat engines to scan the content of the email to identify and block email threats. Content filtering allows the customer to apply email use policies to help enforce government, industry, and internal requirements.

[to top](#)

15. How does Email Reputation work?

Email Reputation uses two types of reputation services to stop email threats. The first verifies IP addresses of incoming email against the world's largest, most trusted reputation database. The second provides a dynamic reputation service, which identifies new email threat sources and even stops zombies and botnets when they first emerge. Email Reputation monitors and maintains reputation ratings based on spamming and threat-sending histories and email samples, ensuring each reputation status is auditable and stays current.

This reputation service is part of the Trend Micro Smart Protection Network, which powers Trend Micro's products and services. The Smart Protection Network correlates threat intelligence across email, web, and file reputation databases.

[to top](#)

16. What types of threat scanning does Hosted Email Security conduct?

Trend Micro uses the latest techniques based on the latest trends to provide threat scanning via two scanning engines that filter email for malicious threats. The first engine scans for viruses, spyware, and other malware, while Trend Micro's anti-spam engine scans for spam and phishing.

[to top](#)

17. What malware protection does Hosted Email Security provide?

Trend Micro includes web reputation filtering to filter out malicious urls embedded in email. In addition, Hosted Email Security includes anti-malware technology rate #1 over other security vendors by NSS Labs in independent tests. Trend Micro's top-rated award-winning antivirus protection includes the recognition of pattern files from known viruses as well as zero-day protection. And to provide zero-day protection, we use heuristics to look for virus indicators without having to rely on a specific pattern files. This heuristic approach applies predictive techniques to stop unknown viruses. Hosted Email Security also offers antispyware as well as protection against other types of malware.

[to top](#)

18. What technologies does the Trend Micro antispam composite engine use?

The antispam composite engine integrates the following technologies:

- Statistical analysis evaluates spam indicators and provides a "spam probability" rating (set thresholds determine if the email is spam)
- Advanced heuristics apply sophisticated rules based on threat behaviour
- Targeted heuristics identify attachment spam
- Signature filters prevent specific known spam emails
- Blocked and approved sender lists
- Embedded URL detection blocks emails with links to malicious websites
- Image spam detection
- Multilingual spam detection identifies spam in many languages
- Antiphishing technology applies heuristics, signatures, and embedded URL detection tailored specifically to block phishing emails

[to top](#)

19. What content filtering capabilities are offered?

We offer very flexible content filtering, with an intuitive user interface to create content filtering rules. Administrators can create rules for the email header, subject, body, and attachment types (for example, PDF and Microsoft document files). These rules enable administrators to scan and flag multiple types of content. Predefined word lists and data format lexicons, such as credit card and personal identification numbers (for example, social security numbers), are available to simplify rule creation. The administrator may also set rules to enforce email use policies, including email size or number of recipients.

Rules can be applied to inbound or outbound email traffic, and specific senders or recipients can be selected (or exceptions applied), allowing administrators to apply rules companywide, or by department, group, or individual.

Organisations also select the action that will be applied if the policy is triggered. Flexible action options are available, including inserting disclaimer text into the body of the email. The email can also be encrypted (if the separate email encryption service is purchased).

[to top](#)

20. What email encryption options are available to Hosted Email Security customers?

Trend Micro Hosted Email Encryption is available for Hosted Email Security as an optional service. Trend Micro leverages identity-based encryption, enabling easy to use encryption for both senders as well as recipients. Email encryption is integrated with the content filtering capabilities of Hosted Email Security by simply enabling encryption within the outbound filtering settings. Administrators can easily configure our policy-based encryption by creating rules that invoke encryption when the rule criteria is met.

In addition, Hosted Email Security includes Transport Layer Security (TLS), which encrypts the email pipeline (not the email itself) as long as the sender and receiver of the email also enable TLS. However, with TLS, there is no way to guarantee that all email recipients will enable TLS, and email often makes several hops through Internet Service Providers (ISPs) before reaching its final destination. This makes it difficult to ensure that the email is protected through all parts of its journey.

TLS is a useful complement to Hosted Email Encryption, securing the email pipeline from customer site to the Hosted Email Security service, where content-based encryption can be applied directly to emails.

[to top](#)

21. What does Trend Micro offer to help enforce compliance and prevent data leaks?

In addition to Email Encryption, Trend Micro offers a comprehensive approach to data privacy and protection. For example, Trend Micro antivirus keeps data intact by preventing viruses from damaging or corrupting it. Some regulations specifically require organisations to apply comprehensive antivirus protection. In addition, antispymware and antiphishing prevent data from being stolen, and content filtering ensures that sensitive data is only viewed by authorised recipients.

[to top](#)

22. Is there a risk that legitimate email will accidentally be blocked?

All email security solutions may accidentally block valid email at some point. This is known as generating a false positive, but Hosted Email Security contractually guarantees no more than a .0003% false-positive rate, as well as a 99%+ spam-blocking rate.

In the event that false positives exceed the .0003% maximum false-positive rate commitment (or spam-blocking rates fall consistently below 99%) in a given month, the customer may be eligible for a credit of up to 100% of the monthly cost of Hosted Email Security.

In addition, we regard email delivery as mission-critical to any business, and provide a variety of unique administrator tools to rapidly find and deliver any email that was inappropriately quarantined as spam. These tools include automatic reprocessing of quarantined email, centralised log management, and end-to-end mail tracking, as well as easy to use web-based tools that enable end-users to manage their own quarantines.

[to top](#)

23. Does Hosted Email Security enable end-users to manage their own spam quarantine?

Yes. Hosted Email Security offers a web-based End-User Quarantine (EUQ) tool to enable end users to manage their own spam quarantines and to save IT staff time. Customers can also opt to use “tag and deliver” capabilities to establish rules in the email client to create an end-user quarantine folder. If users are also ScanMail™ for Microsoft® Exchange customers, they can use the quarantine created in Outlook, enabling end-users to view all spam in one folder regardless of which solution identifies the spam.

[to top](#)

ACTIVATION, UPGRADE AND PURCHASE INFORMATION

24. How is Hosted Email Security sold?

Hosted Email Security is sold in a fixed-price per end-user annual subscription with no maintenance or warranty fees. This subscription price supports an unlimited email and spam volume. The minimum purchase is five users. Customers may purchase either Hosted Email Security – Inbound Filtering Option or Hosted Email Security. Hosted Email Security customers may also purchase the Hosted Email Encryption add-on service.

In addition, customers who purchase Trend Micro™ Worry-Free™ Business Security Advanced receive Hosted Email Security – Inbound Filtering Option as part of the Worry-Free Business Security Advanced bundle. Hosted Email Security –Inbound Filtering Option and Worry-Free Business Security Advanced customers may also purchase an upgrade to Hosted Email Security.

[to top](#)

25. How do I get specific pricing information?

Please contact a channel partner or sales representative in your region for specific pricing information.

[to top](#)

26. How do customers who have purchased Hosted Email Security activate and start using the product?

The Hosted Email Security registration and activation process varies by region. Some use an online registration process. The customer goes to a designated URL and enters a registration key, which is sent to a centralised server. The server then sends an email to the customer with the Activation Code(s) (AC) and activation instructions.

In other regions, the reseller provides the customer with an activation code. The customer will enter the AC(s) into the corresponding location in the Hosted Email Security administration console.

Regardless of which method is used, customers are subsequently sent an email with instructions on how to add in their mail server IP address(es) and domain name(s), followed by instructions on how to get started with the service by re-directing their MX record to Trend Micro.

[to top](#)

27. How easy is Hosted Email Security to implement?

Hosted Email Security account provisioning can be done in less than 30 minutes. Working with the customer, Trend Micro will validate email domain ownership and test to help ensure email delivery. After providing account information and mail server IP address and domain information the only action required on the part of customers is to redirect their mail exchange (MX) records to Trend Micro.

[to top](#)

28. To get started, customers have to redirect MX records to Trend Micro. What is an MX record?

A mail exchange (MX) record is an entry in a domain name database that identifies the email server responsible for handling email for that domain (similar to a primary postal address). With Hosted Email Security, customers redirect MX records to Trend Micro so all email travels first to Trend Micro and through Hosted Email Security filtering before being delivered to customer mail servers, and then on to end-users.

[to top](#)

29. Can we upgrade from Hosted Email Security – Inbound Filtering Option to Hosted Email Security?

Yes, customers can upgrade from Hosted Email Security – Inbound Filtering Option to Hosted Email Security. Contact your sales representative for details.

[to top](#)

30. What is required to upgrade to new versions of Hosted Email Security?

Hosted Email Security is not released in versions. Because it is a hosted solution, Trend Micro can roll out new features to customers as soon as the features are available. All updates are performed by Trend Micro, reducing the IT burden on customers.

[to top](#)

PRIVACY, SUPPORT AND CONTROL

31. Does Trend Micro protect the privacy of our email content?

Yes. All valid emails are passed through automatically without human intervention. Emails are not accessed by Trend Micro staff and are only stored if the customer system is unavailable as a disaster recovery measure. No emails are otherwise stored to disk except at explicit customer request.

[to top](#)

32. What disaster recovery options are available?

Hosted Email Security is currently housed in three data centres—two in the United States and one in Germany. These data centres provide extensive disaster recovery facilities across a distributed, load-balanced architecture.

In case of customer mail server failure, Trend Micro will queue mail for up to five days if a customer system is unavailable. When the customer system is back online, emails are delivered with intelligent flow control to avoid flooding the system.

[to top](#)

33. Does Trend Micro have a team dedicated to monitoring and managing solutions like Hosted Email Security?

Yes. In addition to our TrendLabs team of worldwide security experts, Trend Micro also has a team dedicated to monitoring and managing solutions like Hosted Email Security 24x7. We also provide an aggressive Service Level Agreement (SLA) that contractually commits Trend Micro to providing 100% service availability, no more than one minutes of average email delivery latency, 99%+ spam-blocking effectiveness, no more than .0003% false positives, zero virus infections, and support response time.

[to top](#)

34. Do customers lose control of MX records when they point to Trend Micro?

No. The MX record always remains in a customer's control. At any time, customers may re-configure MX records to point back directly to their mail servers.

[to top](#)

35. Will customer email be stored on Trend Micro servers?

Unlike a number of hosted email security companies, Trend Micro does not use a "store and forward" process for filtering messages which involves accepting your email, storing it on servers, scanning it, and then sending it on. Instead, Hosted Email Security filters email in real time, with valid email being forwarded without human intervention. Emails are only stored if the customer system is unavailable (as a disaster recovery measure) and are not accessed by Trend Micro staff. No emails are otherwise stored to disk except at explicit customer request.

[to top](#)

36. Is Hosted Email Security an "outsourced service"?

No. With Hosted Email Security, you never give up the management of your email servers, or redirect email policy or the management of email policy, from your company to an outside organisation. Your mail always remains under your control.

[to top](#)