

**INTERSCAN MESSAGING HOSTED SECURITY
FREQUENTLY ASKED QUESTIONS**

1. WHAT IS INTERSCAN MESSAGING HOSTED SECURITY?	2
2. WHAT ARE THE UNIQUE BENEFITS OF DEPLOYING INTERSCAN MESSAGING HOSTED SECURITY FOR EMAIL SECURITY?	2
3. WHAT IS THE INTERSCAN MESSAGING HOSTED SECURITY SERVICE LEVEL AGREEMENT (SLA)?	2
4. IS A COPY OF THE SLA EASILY ACCESSIBLE?	3
5. WHAT IS THE DIFFERENCE BETWEEN INTERSCAN MESSAGING HOSTED SECURITY STANDARD AND ADVANCED?	3
6. WHY USE A SAAS (SOFTWARE-AS-A-SERVICE) SOLUTION FOR EMAIL SECURITY INSTEAD OF AN ON-PREMISE EMAIL SECURITY PRODUCT?	3
7. WHY BUY A SAAS SOLUTION FROM TREND MICRO?	4
8. HOW DOES INTERSCAN MESSAGING HOSTED SECURITY STOP SPAM AND OTHER EMAIL-BASED THREATS?	4
9. HOW DOES EMAIL REPUTATION WORK?	4
10. WHAT THREAT SCANNING IS CONDUCTED IN INTERSCAN MESSAGING HOSTED SECURITY?	4
11. WHAT MALWARE PROTECTION IS PROVIDED IN INTERSCAN MESSAGING HOSTED SECURITY?	4
12. WHAT TECHNOLOGIES ARE USED IN THE TREND MICRO ANTISPAM COMPOSITE ENGINE?	5
13. WHAT CONTENT FILTERING CAPABILITIES ARE OFFERED?	5
14. WHAT EMAIL ENCRYPTION IS AVAILABLE TO TREND MICRO HOSTED MESSAGING SECURITY CUSTOMERS?	5
15. WHAT DOES TREND MICRO OFFER TO ENFORCE COMPLIANCE AND PREVENT DATA LEAKS?	6
16. DOES INTERSCAN MESSAGING HOSTED SECURITY ENABLE END-USERS TO MANAGE THEIR OWN SPAM QUARANTINE?	6
17. IS INTERSCAN MESSAGING HOSTED SECURITY SUITABLE FOR ENTERPRISES?	6
18. WHAT DISASTER RECOVERY OPTIONS ARE AVAILABLE?	6
19. HOW IS INTERSCAN MESSAGING HOSTED SECURITY SOLD?	7
20. HOW DO I GET SPECIFIC PRICING INFORMATION?	7
21. IF WE ALREADY HAVE SCANMAIL OR OTHER ON-PREMISE SECURITY PRODUCT PROTECTION, DO WE NEED INTERSCAN MESSAGING HOSTED SECURITY?	7
22. HOW DO WE ACTIVATE INTERSCAN MESSAGING HOSTED SECURITY?	7
23. CAN WE UPGRADE FROM INTERSCAN MESSAGING HOSTED SECURITY STANDARD TO ADVANCED?	7
24. WHAT IS REQUIRED TO UPGRADE TO NEW VERSIONS OF INTERSCAN MESSAGING HOSTED SECURITY?	8
25. DOES TREND MICRO HAVE A TEAM DEDICATED TO MONITORING AND MANAGING SAAS SOLUTIONS LIKE INTERSCAN HOSTED MESSAGING SECURITY?	8
26. IS INTERSCAN MESSAGING HOSTED SECURITY AN “OUTSOURCED SERVICE?”	8
27. HOW EASY IS INTERSCAN MESSAGING HOSTED SECURITY TO IMPLEMENT?	8
28. TO GET STARTED, I HAVE TO RE-DIRECT MY MX RECORD TO TREND MICRO. WHAT IS AN MX RECORD?	8
29. DOES TREND MICRO PROTECT THE PRIVACY OF OUR EMAIL CONTENT?	8
30. DO WE LOSE CONTROL OF OUR MX RECORD WHEN WE POINT IT TO TREND MICRO?	9
31. WILL OUR EMAIL BE STORED ON TREND MICRO SERVERS?	9
32. IS THERE A RISK THAT LEGITIMATE EMAIL WILL ACCIDENTALLY BE BLOCKED?	9



1. What is InterScan Messaging Hosted Security?

Trend Micro InterScan Hosted Messaging Security (IMHS) is a SaaS (software-as-a-service) email security solution that stops up to 99% of all spam and other email threats before they reach the network, enabling organizations to reclaim IT staff time, end-user productivity and network resources. In addition, InterScan Messaging Hosted Security offers optional content filtering and encryption to help enforce compliance and prevent data leaks. As a SaaS solution, InterScan Messaging Hosted 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 InterScan Messaging Hosted Security performance is continuously optimized with little to no time spent on maintenance by the customer.

2. What are the unique benefits of deploying InterScan Messaging Hosted Security for email security?

InterScan Messaging Hosted Security has the #1 highest spam catch rate according to independent benchmarking tests¹. 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 a email, that email will be blocked.

InterScan Messaging Hosted Security includes antivirus technology that enabled Trend Micro to be #1 in antivirus market share for the last seven years². All of this technology is 100% Trend Micro created and owned which enables our customers to be continuously protected in real-time against rapidly evolving spam tactics and today's complex emerging web threats.

In addition, InterScan Messaging Hosted 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 optimize 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) IDC, *Worldwide Antivirus 2006–2010 Forecast Update and 2005 Vendor Analysis*, Doc #204715, Dec 2006

3. What is the InterScan Messaging Hosted Security Service Level Agreement (SLA)?

InterScan Messaging Hosted Security includes a bundled, contractually binding service level agreement which provides the following guarantees: 100% service availability, less than two minutes of email delivery latency, 95% spam blocking effectiveness, .0004% false positive rate, zero virus infection and support responsiveness. If these guarantees are not met in any given month, Trend Micro will provide a refund back to the customer.

4. Is a copy of the SLA easily accessible?

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

5. What is the difference between InterScan Messaging Hosted Security Standard and Advanced?

Both Standard and Advanced options include highly effective spam blocking technology, web-based end-user quarantine management, extensive logging, reporting and notifications, and are backed by the service level agreement.

Standard option. Filters 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.

Advanced option. 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 optimize spam-blocking and false-positive rates and other threat-blocking effectiveness. The administrator may also set rules to enforce email use policies, such as email size, 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 InterScan Messaging Hosted Security Advanced.

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

6. Why use a SaaS (software-as-a-service) solution for email security instead of an on-premise email security product?

Organizations receive the following benefits when using a SaaS 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, and 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 organizations to maintain a consistent security posture, as the latest protection is available at all times to all users in all locations. 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 per user price with none of the additional hardware costs typically associated with on-premise email security products as user counts scale up or down.

7. Why buy a SaaS solution from Trend Micro?

Trend Micro is a leader in secure content and threat management and unlike many other SaaS vendors is a well-established, stable company. Trend Micro has more than 20 years of security experience and currently scans more than 1.2 billion emails daily across both on-premise and SaaS 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.

8. How does InterScan Messaging Hosted Security stop spam and other email-based threats?

InterScan Messaging Hosted Security scans emails in three phases:

- a. Email Reputation
- b. Threat Scanning
- c. Content Filtering (Advanced 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.

9. 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 and the second provides a dynamic reputation service, which identifies new email threat sources, stopping even 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

10. What threat scanning is conducted in InterScan Messaging Hosted Security?

The second layer of protection is threat scanning via two scanning engines that filter email for malicious threats. An antivirus engine scans for viruses, spyware, and other malware. Trend Micro's anti-spam engine scans for spam and phishing, using the latest techniques based on the latest trends.

11. What malware protection is provided in InterScan Messaging Hosted Security?

InterScan Messaging Hosted Security provides Trend Micro's award-winning antivirus, which includes pattern files of known viruses as well as zero-day protection. 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. InterScan Messaging Hosted Security also offers anti-spyware as well as protection against other types of malware.

12. What technologies are used in the Trend Micro antispam composite engine?

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 behavior
- 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
- Patent-pending image spam detection
- Multi-lingual spam detection identifies spam in many languages
- Anti-phishing technology applies heuristics, signatures, and embedded URL detection tailored specifically to block phishing emails

13. 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 attachments 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, such as 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 company-wide or by department, group, or individual

Organizations 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 or the email can be encryption (if the separate email encryption service is purchased).

14. What email encryption is available to Trend Micro hosted messaging security customers?

Email Encryption is available for InterScan Messaging Hosted Security Advanced 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 InterScan Messaging Hosted Security Advanced by simply enabling encryption within the outbound filtering settings. Our policy-based encryption is easy to configure by administrators who create rules which invoke encryption when the rule criteria is met.

In addition, InterScan Messaging Hosted 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, making it difficult to ensure that the email is protected through all parts of the email's journey.

TLS is a useful complement to Trend Micro's Email Encryption service, securing the email pipeline from customer site to the InterScan Messaging Hosted Security service, where encryption can be applied directly to emails, based upon their content.

15. What does Trend Micro offer to 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 the data intact by preventing viruses from damaging or corrupting the data. Some regulations specifically require organizations to apply comprehensive antivirus protection. In addition, anti-spyware and anti-phishing prevent data from being stolen, and content filtering ensures that sensitive data is only viewed by authorized recipients.

16. Does InterScan Messaging Hosted Security enable end-users to manage their own spam quarantine?

Yes. InterScan Messaging Hosted 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. Or if users are also ScanMail™ for 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.

17. Is InterScan Messaging Hosted Security suitable for enterprises?

Yes. InterScan Messaging Hosted Security will scale to meet the needs of any size customer from as small as five users to very large enterprises and ISPs. InterScan Messaging Hosted Security also provides the features required to support enterprise customers. 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. 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 organization's email.

Also, the aggressive SLA, disaster recovery features, and privacy protections support enterprise email requirements. InterScan Messaging Hosted Security provides enterprises with the benefits of a SaaS 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 may be used to with an on-site solution.

In addition, InterScan Messaging Hosted Security is ideal for large distributed organizations which find regular software upgrades across multiple locations time consuming and expensive. Enterprises will always be running the latest and greatest version, ensuring immediate protection of their mail stream with the benefit of less complexity, as their need to maintain software has been eliminated.

18. What disaster recovery options are available?

InterScan Messaging Hosted Security is currently housed in three data centers—two in the United States and one in Germany. These data centers 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 5 days if a customer system is unavailable, and when the customer system is back online, emails are delivered with intelligent flow control to avoid flooding the system.

19. How is InterScan Messaging Hosted Security sold?

InterScan Messaging Hosted 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 InterScan Messaging Hosted Security Standard or Advanced. InterScan Messaging Hosted Security Advanced customers may also purchase the Email Encryption add-on service.

In addition, customers who purchase Worry-Free Business Security Advanced receive InterScan Messaging Hosted Security Standard as part of the Worry-Free Business Security Advanced bundle. InterScan Messaging Hosted Security Standard and Worry-Free Business Security Advanced customers may purchase an upgrade to InterScan Messaging Hosted Security Advanced.

20. How do I get specific pricing information?

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

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

Yes. There are inherent benefits for protecting email at different points in the network. InterScan Messaging Hosted Security stops spam and other email-based threats before they reach the network while ScanMail integrates with the mail server (Microsoft Exchange or Lotus Domino/Notes), 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 InterScan Messaging Hosted 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.

22. How do we activate InterScan Messaging Hosted Security?

The InterScan Messaging Hosted Security activation process varies by region. Some regions use an on-line registration process. The customer goes to a designated URL and enters a registration key which is sent to a centralized server and the server 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 InterScan Messaging Hosted Security administration console.

Regardless of which method is used, customers are sent an email indicating that they must redirect their MX record to route mail through the hosted service.

23. Can we upgrade from InterScan Messaging Hosted Security Standard to Advanced?

Yes, customers can upgrade from InterScan Messaging Hosted Security Standard to the Advanced version. Contact your sales representative for details.



24. What is required to upgrade to new versions of InterScan Messaging Hosted Security?

InterScan Messaging Hosted Section is not released in versions. Because it is a SaaS 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.

25. Does Trend Micro have a team dedicated to monitoring and managing SaaS solutions like InterScan Hosted Messaging Security?

Yes. In addition to our TrendLabs team of worldwide security experts, Trend Micro also has a dedicated 24/7 team monitoring and managing SaaS solutions like InterScan Hosted Messaging Security. We also provide an aggressive Service Level Agreement (SLA) contractually committing us to providing 100% service availability, less than two minutes of email delivery latency, 95% spam-blocking effectiveness, .0004% false positives, zero virus infection and support response time.

26. Is InterScan Messaging Hosted Security an “outsourced service?”

No. With InterScan Messaging Hosted 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 organization. Your mail remains 100 percent under your control.

27. How easy is InterScan Messaging Hosted Security to implement?

InterScan Messaging Hosted Security provisioning generally occurs in less than 48 hours as Trend Micro validates email domain ownership and works with the customer to test and ensure email delivery. After providing account information, the only action required on the part of the customer is to redirect their mail exchange (MX) record to Trend Micro.

28. To get started, I have to re-direct my MX record 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 the InterScan Messaging Hosted Security, you re-direct your MX record to Trend Micro so all email travels first to Trend Micro and through InterScan Messaging Hosted Security filtering before being delivered to your mail server and then on to your end users.

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

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

30. Do we lose control of our MX record when we point it to Trend Micro?

No. The MX record always remains in your control. At any time, you may re-configure your MX record to point back directly to your mail server.

31. Will our 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, InterScan Messaging Hosted 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 feature and are not accessed by Trend Micro staff. No emails are otherwise stored to disk except at explicit customer request.

32. Is there a risk that legitimate email sent to our company will accidentally be blocked?

All email security solutions may at some point accidentally block valid email and this is known as generating a false positive. However, Trend Micro has contractually committed to less than .0004% false-positive rate with InterScan Messaging Hosted Security as well as a 95% spam-blocking rate.

In the event that false positives exceed the .0004% maximum false-positive rate commitment (or spam blocking rates fall consistently below 95%) in a given month, the customer may be eligible for a credit of up to 100% of the monthly cost of InterScan Messaging Hosted 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, centralized log management and end-to-end mail tracking as well as easy-to-use web-based tools to enable end users to manage their own quarantines.