
A background image showing a laptop on a desk with a speedometer overlay. The speedometer has markings from 0 to 70 and a needle pointing towards 40. The scene is dimly lit, suggesting an office environment.

Email Encryption for InterScan™ Messaging Hosted Security

Trend Micro, Incorporated 

-  An overview of the email encryption add-on service for Trend Micro's hosted email security

Email Encryption for InterScan Messaging Hosted Security

Why Encrypt?

Today's confidentiality and privacy requirements drive organizations of all sizes and industries to secure sensitive data in email. Often particular types of data need to be encrypted, such as credit card numbers, intellectual property, or client information. Organizations also need to protect confidential emails for particular groups, such as executive management, human resources or legal departments.

Many organizations are turning to policy-based encryption to meet their encryption needs because it automatically encrypts data using content filtering rules that identify types of content or email for particular groups. Encryption is applied when the rules are triggered. With policy-based encryption, organizations avoid relying on individual users to secure important content.

Introducing Email Encryption for InterScan Messaging Hosted Security

Trend Micro offers Email Encryption as an add-on service to InterScan Messaging Hosted Security. It integrates seamlessly with the content filtering capabilities of Trend Micro's hosted email security service that protects against spam, viruses and inappropriate content. Trend Micro Email Encryption leverages Identity-Based Encryption (IBE) to efficiently secure email addressed to anyone. This approach eliminates the burdensome pre-registration and certificate management of traditional Public Key Infrastructure (PKI) technology with dynamic key generation. Encrypted content is simply pushed from senders to recipients like any other email.

For information on other email encryption solutions available from Trend Micro visit

<http://us.trendmicro.com/us/products/enterprise/email-encryption/index.html>

The Role of TLS

Transport Layer Security (TLS) is a type of encryption used by many hosted security vendors. TLS encrypts the email pipeline, but not the email itself. It can play an important role when paired with a hosted email encryption service, but is unreliable as a standalone solution. Both the sending and receiving server must enable TLS for the pipeline to be secure; there is no guarantee that the servers for the email recipient will have this enabled, and emails often take several hops through ISP servers before reaching their final destination, also breaking the chain of protection. This TLS is insufficient in protecting email content. See Figure 1.



Figure 1: TLS only protects a portion of the path along which the data travels and may not be supported along the complete pathway.

Email Encryption for InterScan Messaging Hosted Security

Enabling Policy-Based Email Encryption

Email Encryption is integrated with the content filtering capabilities of InterScan Messaging Hosted Security, which provides flexible and easy filtering options for most every type of content. Administrators simply configure content rules that apply encryption as a rule action.

Customers use TLS to secure email from their site to the InterScan Messaging Hosted Security server. Trend Micro provides TLS capabilities to all customers as part of the service to help secure transmission from the customer site to the service. The appropriate emails are then encrypted by the Email Encryption service based on policy rules created by the customer and sent securely to the recipients. (See Figure 2 below).



Figure 2: Email Encryption for InterScan Messaging Hosted Security efficiently secures email delivered to anyone with an email address.

To apply encryption as action to a content filtering rule, administrators follow these five easy steps:

1. Specify that the rule applies to outbound email
2. Determine the sender / recipients for the rule
3. Select the message attributes (What is the filter looking for?)
4. Specify Encrypt email as the rule action
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.

To identify content, administrators create a “keyword expression.” Administrators may use any combination of keywords and regular expressions to define a keyword expression (some preset word lists and data format lexicons are available). 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 attributes have been defined, administrators must specify encryption as the rule action by selecting the “Do not intercept messages” option and clicking on the *Encrypt email* action, as shown in Figure 3 below.

Email Encryption for InterScan Messaging Hosted Security

All messages triggering rule will be logged.

Intercept

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

Modify

- Clean cleanable viruses, delete those that cannot be cleaned
- Delete attachment
- Insert stamp in body
- Tag Subject
- Encrypt email

Monitor

- Send notification
- BCC

Figure 3: Selecting Encrypt Email as an Action Option

Sample Use Cases:

- 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, often required by regulations.
- 2) Key expressions for words like “encrypt” or “confidential” can make it easy to apply encryption as an action.

Once *Encrypt email* has been selected as the rule action, administrators merely name and save the rule. Once a rule has been created, it may be edited or copied (copying a rule makes it easy to create a similar rule—administrators merely edit the copied rule with any desired changes).

Email Encryption Recipient Experience

Recipients of the encrypted email receive an email notification in the form of an electronic sealed envelope. Recipients can download their own copy of Trend Micro Email Encryption Client or use their web browser to read and reply without the need to install any software. Figure 3 below shows a sample of the email sent to the recipient and a sample of the attached html file that contains a link to the web browser where the encrypted email can be viewed.

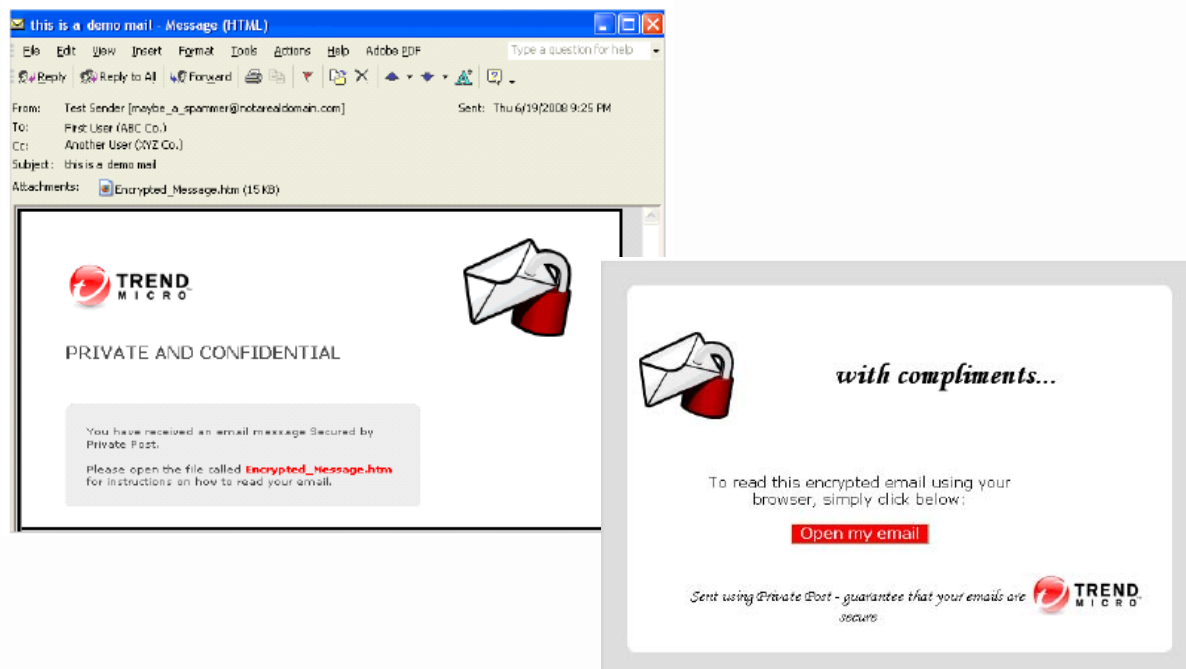


Figure 4: Email Encryption Recipient Experience: Encrypted Email Envelope and Browser Access

Activating Email Encryption

Trend Micro Email Encryption for InterScan Messaging Hosted Security is available only as an add-on service for the Advanced implementation with outbound filtering. Outbound filtering is available at no extra cost to Advanced customers and can be requested during the trial or registration process.

The activation options for Email Encryption depend on the InterScan Messaging Hosted Security license status, as shown in Table 1 below.

Email Encryption for InterScan Messaging Hosted Security

InterScan Messaging Hosted Security License Status	Email Encryption License Options
Purchased	Can try or purchase Email Encryption. <ul style="list-style-type: none">• See Starting a Free Trial of Email Encryption• See Purchasing Email Encryption
In Trial Period	Can only conduct a free trial of Email Encryption. <ul style="list-style-type: none">• See Starting a Free Trial of Email Encryption

Table 1: Email Encryption Activation Options


Starting a Free Trial of Email Encryption

Organizations can request a free trial of Email Encryption at the same time they request a trial of InterScan Messaging Hosted Security by selecting Email Encryption on the trial form posted to the service web page. If InterScan Messaging Hosted Security has already been purchased or is under trial, a free trial of Email Encryption can be initiated from within the service console under the Administration > Licenses section. (See Figure 4 below.)

Purchasing Email Encryption

To purchase this Email Encryption service, InterScan Messaging Hosted Security Advanced with outbound filtering must also be purchased. Organizations can conduct a free trial of Email Encryption while in the trial period for the Advanced service, but they cannot purchase Email Encryption until InterScan Messaging Hosted Security has also been purchased.

Both InterScan Messaging Hosted Security and Email Encryption can be purchased through a reseller. Resellers can be found through links provided on the service web page. In some regions, customers are given a Registration Key (RK) and must register online to receive an Activation Code. In other regions, an Activation Code is provided directly after purchase. In either circumstance, the customer must enter the Activation Code into the InterScan Messaging Hosted Security console in the Administration > Licenses section to initiate the service. (See Figure 4 below.)

Licenses (Activate an Account) 

If you have a **Registration Key**, [register online](#) to get an Activation Code.

Activation Type:

Trial Activation
Service Name
(An Activation Code is not required to activate a trial)

Purchase Activation
Service Name
Activation Code
(Insert Activation Code provided by email to activate purchase)

Figure 4: Email Encryption License Activation

Email Encryption for InterScan Messaging Hosted Security

It may take 24-48 hours for Trend Micro to verify your Email Encryption trial or purchase request and initiate Email Encryption for your account. Upon activation, Email Encryption appears as a rule action available when adding or editing a policy from the InterScan Messaging Hosted Security Policy screen.

Conclusion

With policy-based encryption, organizations avoid relying on individual users to secure important content. Conveniently, encryption is automatically applied when content filtering rules are triggered, helping to ensure that confidentiality and privacy requirements are met.

Trend Micro provides a policy-based email encryption solution that seamlessly integrates with the content filtering capabilities of InterScan Messaging Hosted Security. Administrators merely click a box to apply encryption as a rule action. Trend Micro's flexible Email Encryption solution leverages Identity-Based Encryption (IBE), eliminating the burdensome pre-registration and certificate management of Public Key Infrastructure (PKI) technology. Trend Micro Email Encryption makes it easy to securely encrypt content.

WP02_IMHSEncrypt_090219US. © 2008 by Trend Micro, Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, InterScan and Private Post are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners. Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice.