

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 pour InterScan™ Messaging Hosted Security

Trend Micro, Incorporated ↩

- ➔ Aperçu du service complémentaire Email Encryption pour la sécurité de messagerie hébergée de Trend Micro

Pourquoi chiffrer les données ?

Les exigences actuelles en matière de confidentialité amènent les entreprises de toutes tailles et les différents secteurs de l'industrie à sécuriser les données sensibles dans les courriers électroniques. Le chiffrement de certains types de données (numéros de carte de crédit, propriété intellectuelle, informations client, etc.) s'avère souvent nécessaire. Les entreprises doivent aussi protéger le courrier électronique confidentiel de certains groupes, tels que les cadres supérieurs, le service des ressources humaines ou le service juridique.

De nombreuses entreprises adoptent le chiffrement basé sur des stratégies pour répondre à leurs besoins dans ce domaine car cette méthode chiffre automatiquement les données à l'aide de règles de filtrage du contenu qui identifient les types de contenu ou de courrier électronique pour des groupes spécifiques. Le chiffrement est appliqué lorsque les règles sont déclenchées. Grâce au chiffrement basé sur des stratégies, les entreprises n'ont plus à se fier aux utilisateurs individuels pour sécuriser les contenus importants.

Présentation d'Email Encryption pour InterScan Messaging Hosted Security

Trend Micro propose Email Encryption en tant que service additionnel d'InterScan Messaging Hosted Security. Email Encryption s'intègre parfaitement aux fonctions de filtrage de contenu du service hébergé de sécurité de messagerie de Trend Micro qui protège cette dernière contre les spams, les virus et les contenus inappropriés. Trend Micro Email Encryption exploite le chiffrement basé sur l'identité (Identity-Based Encryption ou IBE) pour sécuriser efficacement les courriers électroniques adressés à quelqu'un. Cette approche élimine les contraintes du préenregistrement et de la gestion des certificats de la technologie Public Key Infrastructure (PKI) grâce à une génération dynamique des clés. Le contenu chiffré est simplement transmis des expéditeurs aux destinataires comme tout autre courrier électronique.

Pour plus d'informations sur les autres solutions de chiffrement de messagerie disponibles chez Trend Micro, visitez le site : <http://fr.trendmicro.com/fr/products/enterprise/email-encryption/index.html>

Le rôle de TLS

La solution de sécurité de couche de transport (Transport Layer Security ou TLS) est un type de chiffrement employé par de nombreux fournisseurs de sécurité hébergée. TLS chiffre le pipeline de transport des courriers électroniques, mais pas les messages proprement dits. Ce protocole peut jouer un rôle important lorsqu'il est associé à un service de chiffrement de messagerie hébergé, mais il n'est pas fiable en tant que solution autonome. Les serveurs d'envoi et de réception doivent tous deux activer TLS pour que le pipeline soit sécurisé ; mais rien ne garantit qu'il sera activé sur les serveurs côté destinataire, et les courriers électroniques progressent souvent par sauts entre les serveurs des FAI avant d'atteindre leur destination finale, ce qui rompt également la chaîne de protection. Ce TLS est insuffisant pour protéger le contenu des courriers électroniques. Voir Figure 1.

Email Encryption pour InterScan Messaging Hosted Security



Figure 1 : TLS ne protège qu'une partie du chemin emprunté par les données et n'est pas forcément pris en charge sur tout le chemin d'accès.

Activation d'Email Encryption basé sur des stratégies

Email Encryption est intégré aux fonctions de filtrage du contenu d'InterScan Messaging Hosted Security, qui fournit des options de filtrage de contenu simples et flexibles pour pratiquement tous les types de contenu. Il suffit aux administrateurs de configurer des règles de contenu qui appliquent le chiffrement comme une action de règle.

Les clients utilisent TLS pour sécuriser le courrier électronique entre leur site et le serveur InterScan Messaging Hosted Security. Trend Micro fournit des fonctions TLS à tous ses clients dans le cadre du service pour contribuer à sécuriser la transmission du site du client jusqu'au service. Les courriers électroniques appropriés sont ensuite chiffrés par le service Email Encryption sur la base des règles de stratégie créées par le client, puis envoyés de manière sécurisée aux destinataires (voir Figure 2 ci-dessous).

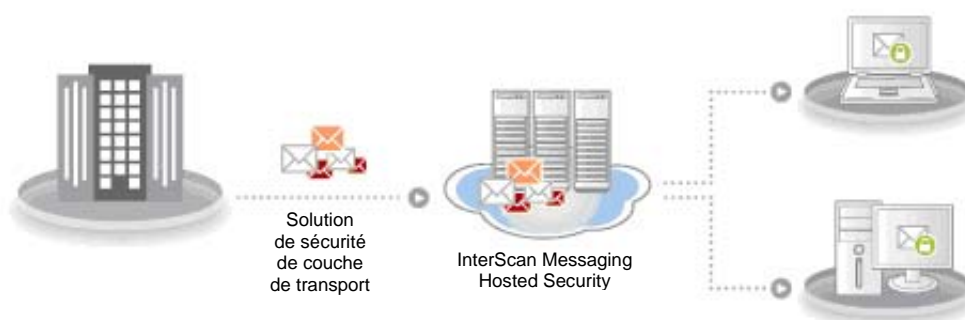


Figure 2 : Email Encryption pour InterScan Messaging Hosted Security sécurise efficacement les messages envoyés à toute personne ayant une adresse électronique.

Pour appliquer le chiffrement comme action à une règle de filtrage de contenu, les administrateurs suivent une procédure simple comportant cinq étapes :

1. Spécifier que la règle s'applique au courrier sortant
2. Déterminer l'expéditeur / les destinataires auxquels la règle s'appliquera
3. Sélectionner les attributs de message (Que recherche le filtre ?)

Email Encryption pour InterScan Messaging Hosted Security

4. Spécifier le chiffrement des messages comme action de règle
5. Nommer et enregistrer la règle

Pour indiquer les expéditeurs ou les destinataires d'une règle particulière, les administrateurs peuvent utiliser des adresses électroniques spécifiques ou sélectionner un domaine complet. Les administrateurs peuvent également spécifier des exceptions à une règle.

Pour identifier le contenu, les administrateurs créent une « expression de mots clés ». Ils peuvent utiliser une combinaison de mots clés et d'expressions régulières pour définir une expression de mots clés (des listes de mots et des lexiques de formats de données prédéfinis sont disponibles). Une fois qu'elle a été créée, les administrateurs peuvent enregistrer et donner un nom à l'expression de mots clés. Elle peut alors être appliquée à des règles multiples (par exemple pour différents groupes ou différents attributs de message tels que la ligne d'objet, le corps du message, le contenu de la pièce jointe ou l'en-tête du message).

Une fois que les attributs de message ont été définis, les administrateurs doivent spécifier le chiffrement comme action de règle en sélectionnant l'option « Ne pas intercepter les messages » et en cliquant sur l'action *Chiffrer les messages*, comme indiqué dans la Figure 3 ci-dessous.

All messages triggering rule will be logged.	
Intercept	
<input checked="" type="radio"/>	Do not intercept messages
<input type="radio"/>	Delete entire message
<input type="radio"/>	Deliver now
<input type="radio"/>	Quarantine
<input type="radio"/>	Change recipient to <input type="text"/>
Modify	
<input type="checkbox"/>	Clean cleanable viruses, delete those that cannot be cleaned
<input type="checkbox"/>	Delete attachment
<input type="checkbox"/>	Insert stamp in body <input type="text" value="Attachment deleted"/> <input type="button" value="Edit"/>
<input type="checkbox"/>	Tag Subject <input type="text" value="tag"/>
<input checked="" type="checkbox"/>	Encrypt email
Monitor	
<input type="checkbox"/>	Send notification <input type="text" value="message to people"/>
<input type="checkbox"/>	BCC <input type="text"/>

Figure 3 : Chiffrer les messages peut être sélectionné comme option d'action

Scénarios d'exemples d'utilisation :

- 1) Les administrateurs peuvent combiner des lexiques de formats de données, tels que des formats de numéro de carte de crédit ou de sécurité sociale, avec des listes de noms de clients ou des numéros de compte pour marquer les courriers électroniques contenant des informations personnelles identifiables, comme cela est souvent exigé par les réglementations.
- 2) Des expressions clés pour des mots tels que « chiffrer » ou « confidentiel » peuvent faciliter l'application du chiffrement comme action.

Email Encryption pour InterScan Messaging Hosted Security

Après avoir sélectionné *Chiffrer les messages* comme action de règle, les administrateurs n'ont plus qu'à nommer et enregistrer la règle. Une fois la règle créée, elle peut être modifiée ou copiée (la copie d'une règle facilite la création d'une règle similaire ; les administrateurs doivent simplement modifier la règle copiée pour lui apporter les changements souhaités).

Pour le destinataire d'Email Encryption

Les destinataires du message chiffré reçoivent une notification par courrier électronique sous la forme d'une enveloppe électronique scellée. Les destinataires peuvent télécharger leur propre copie de Trend Micro Email Encryption Client ou utiliser leur navigateur Web pour lire les messages et y répondre sans avoir à installer de logiciel. La Figure 3 ci-dessous illustre un exemple de message envoyé au destinataire et un exemple de pièce jointe au format HTML contenant un lien vers le navigateur Web où le message chiffré peut être consulté.

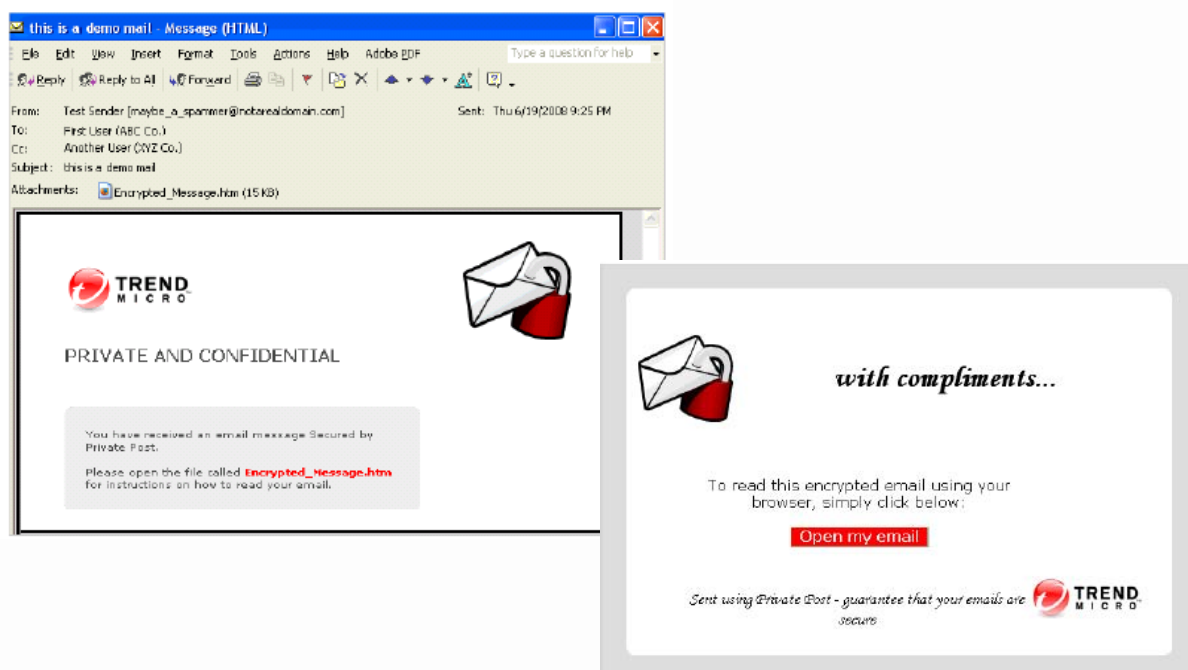


Figure 4 : Pour le destinataire d'Email Encryption : enveloppe de message chiffré et accès par navigateur

Activation d'Email Encryption

Trend Micro Email Encryption pour InterScan Messaging Hosted Security est disponible uniquement en tant que service additionnel pour la version Advanced avec filtrage du courrier sortant. Le filtrage du courrier sortant est disponible sans frais supplémentaires pour les clients de la version Advanced et peut être demandé pendant la période d'essai ou le processus d'enregistrement.

Les options d'activation pour Email Encryption dépendent de la licence InterScan Messaging Hosted Security, comme indiqué dans le Tableau 1 ci-dessous.

Email Encryption pour InterScan Messaging Hosted Security

Statut de la licence InterScan Messaging Hosted Security	Options de la licence Email Encryption
Licence acquise	Il est possible d'utiliser la version d'évaluation ou d'acheter Email Encryption. <ul style="list-style-type: none">• Voir Évaluation gratuite d'Email Encryption• Voir Acheter Email Encryption
Période d'évaluation	Il est seulement possible d'évaluer gratuitement Email Encryption. <ul style="list-style-type: none">• Voir Évaluation gratuite d'Email Encryption

Tableau 1 : Options d'activation d'Email Encryption

Évaluation gratuite d'Email Encryption

Les entreprises peuvent demander à évaluer gratuitement Email Encryption en même temps qu'InterScan Messaging Hosted Security en sélectionnant Email Encryption sur le formulaire d'évaluation publié sur la page Web du service. Si InterScan Messaging Hosted Security a déjà été acheté ou est en cours d'évaluation, une évaluation gratuite d'Email Encryption peut être initialisée depuis la console du service, section Administration > Licences (voir Figure 4 ci-dessous).

Achat d'Email Encryption

L'achat de ce service Email Encryption nécessite également l'acquisition d'InterScan Messaging Hosted Security Advanced avec filtrage du courrier sortant. Les entreprises peuvent évaluer gratuitement Email Encryption pendant la période d'évaluation du service Advanced, mais elles ne peuvent pas acheter Email Encryption sans InterScan Messaging Hosted Security.

InterScan Messaging Hosted Security et Email Encryption peuvent tous deux être achetés auprès d'un revendeur. Pour obtenir la liste des revendeurs, utilisez les liens présents sur la page d'accueil du service. Dans certaines régions, les clients reçoivent une clé d'enregistrement (RK ou Registration Key) et doivent s'enregistrer en ligne pour obtenir un code d'activation. Dans d'autres régions, un code d'activation est fourni directement après l'achat. Dans les deux cas, le client doit entrer le code d'activation dans la console InterScan Messaging Hosted Security (section **Administration > Licence**) pour initialiser le service (voir Figure 4 ci-dessous).

Licenses (Activate an Account) ?

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

Activation Type:

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

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

Figure 4 : Activation de la licence Email Encryption

Trend Micro peut mettre 24 à 48 heures pour vérifier votre demande d'évaluation ou d'achat d'Email Encryption et initialiser ce dernier pour votre compte. Après l'activation, Email Encryption apparaît

sous forme d'une action de règle disponible lorsque vous ajoutez ou modifiez une stratégie à partir de l'écran InterScan Messaging Hosted Security Policy.

Conclusion

Grâce au chiffrement basé sur des stratégies, les entreprises n'ont plus à se fier aux utilisateurs individuels pour sécuriser les contenus importants. Par commodité, le chiffrement est automatiquement appliqué lorsque les règles de filtrage de contenu sont déclenchées, ce qui garantit la conformité aux exigences de confidentialité.

Trend Micro fournit une solution de chiffrement des courriers électroniques basé sur des stratégies qui s'intègre parfaitement aux fonctions de filtrage de contenu d'InterScan Messaging Hosted Security. Il suffit aux administrateurs de cocher une case pour appliquer le chiffrement comme action de règle. D'une grande souplesse, la solution Email Encryption de Trend Micro exploite le chiffrement basé sur l'identité (Identity-Based Encryption ou IBE), éliminant les contraintes du préenregistrement et de la gestion des certificats de la technologie Public Key Infrastructure (PKI). Trend Micro Email Encryption permet de chiffrer facilement un contenu de manière sécurisée.

WP02_IMHSEncrypt_090219FR. © 2009 by Trend Micro, Incorporated. Tous droits réservés. Trend Micro, le logo t-ball de Trend Micro, InterScan et Private Post sont des marques commerciales ou des marques déposées de Trend Micro, Incorporated. Tous les autres noms de produit ou de société peuvent être des marques commerciales ou des marques déposées de leurs propriétaires respectifs. Trend Micro Incorporated se réserve le droit d'apporter des modifications à ce document et aux produits décrits dans celui-ci sans préavis.