

A background image showing a laptop on a desk with a speedometer overlay, suggesting performance or security metrics.

Email Encryption for InterScan™ Messaging Hosted Security

Trend Micro, Incorporated ↩

- ➔ Descripción general del servicio complementario Email Encryption para la seguridad alojada para el correo electrónico de Trend Micro

Motivos para cifrar la información

Hoy en día los requisitos de confidencialidad y privacidad exigen la protección de la información confidencial en organizaciones de todos los tamaños y sectores. Con frecuencia, es necesario cifrar determinados tipos de datos, como los números de las tarjetas de crédito, la propiedad intelectual o información del cliente. Asimismo, las compañías deben proteger los mensajes de correo electrónico confidenciales dirigidos a grupos concretos, tales como los directivos, la sección de recursos humanos o el departamento jurídico.

En este sentido, un gran número de organizaciones están optando por el cifrado basado en políticas para cubrir sus necesidades de cifrado, ya que cifra automáticamente los datos mediante reglas de filtrado de contenido que identifican los tipos de contenido o correo electrónico para determinados grupos. El cifrado se aplica cuando se activan las reglas. Con el cifrado basado en políticas, las organizaciones dejarán de depender de los usuarios individuales para proteger el contenido importante.

Introducción a Email Encryption for InterScan Messaging Hosted Security

Email Encryption, que Trend Micro ofrece como servicio complementario de InterScan Messaging Hosted Security, se integra a la perfección con las funciones de filtrado de contenido del servicio de seguridad alojada para el correo electrónico de Trend Micro, destinadas a la protección frente al spam, virus y contenido inapropiado. Trend Micro Email Encryption utiliza el cifrado basado en la identidad (IBE) para proteger el correo electrónico dirigido a cualquier usuario con total eficacia. Se trata de un enfoque que elimina las molestas tareas de registro previo y gestión de los certificados de la tecnología de infraestructura de clave pública (PKI) con la generación de claves dinámicas. El contenido cifrado simplemente se transmite del remitente al destinatario como cualquier otro mensaje.

Para obtener información sobre otras soluciones de cifrado del correo electrónico disponibles en Trend Micro, visite <http://es.trendmicro.com/es/products/enterprise/email-encryption/index.html>

El papel de TLS

La seguridad de la capa de transporte (TLS) es un tipo de cifrado que emplean muchos proveedores de servicios de seguridad alojada. TLS cifra la canalización del correo electrónico, pero no el correo electrónico en sí, y puede desempeñar un papel fundamental si se usa junto con un servicio alojado de cifrado del correo electrónico, pero no es realmente fiable como solución independiente. Tanto el servidor de envío como el de recepción deben tener el cifrado TLS habilitado para que la canalización esté protegida, pero no hay garantía de que los servidores del destinatario del correo electrónico vayan a tener esta opción habilitada y, a menudo, los correos electrónicos efectúan varios saltos por diversos servidores ISP antes de llegar al destino final, con lo cual también se rompe la cadena de protección. En consecuencia, no basta con tener TLS para proteger el contenido del correo electrónico. Vea la ilustración 1.

Email Encryption for InterScan Messaging Hosted Security



Ilustración 1: TLS protege únicamente una parte de la ruta por la cual los datos se transmiten y es posible que no sea compatible en la ruta completa.

Activación del cifrado de correo electrónico basado en políticas

Email Encryption se integra con las funciones de filtrado de contenido de InterScan Messaging Hosted Security, que ofrece opciones de filtrado flexibles y sencillas para prácticamente cualquier tipo de contenido. Los administradores tan solo configuran las reglas de filtrado de contenido para aplicar el cifrado como una acción de regla.

Los clientes utilizan TLS para proteger el correo electrónico desde sus sitios hasta el servidor de InterScan Messaging Hosted Security. Trend Micro suministra funciones de TLS a todos los clientes como parte del servicio con el fin de ayudar a proteger la transmisión desde el sitio del cliente hasta el servicio. A continuación, el servicio Email Encryption cifra los correos electrónicos pertinentes en función de las reglas de políticas que el cliente ha creado y se envían a los destinatarios sin riesgo alguno. (Vea la ilustración 2 a continuación.)

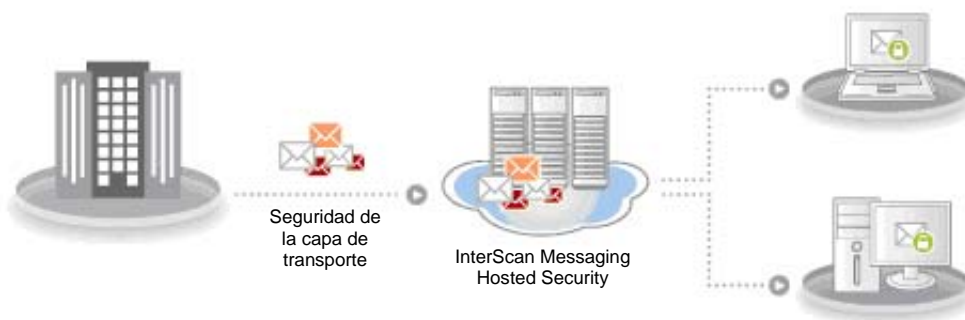


Ilustración 2: Email Encryption for InterScan Messaging Hosted Security protege eficazmente el correo electrónico enviado a cualquier usuario con una dirección de correo electrónico.

Para aplicar el cifrado como una acción a una regla de filtrado de contenido, los administradores realizan estos cinco sencillos pasos:

1. Especificar que la regla se aplica al correo electrónico saliente
2. Determinar los remitentes/destinatarios de la regla
3. Seleccionar los atributos del mensaje (¿Qué está buscando el filtro?)

Email Encryption for InterScan Messaging Hosted Security

4. Especificar "Cifrar correo electrónico" como acción de la regla
5. Nombrar la regla y guardarla

A la hora de indicar los remitentes o destinatarios para una regla determinada, los administradores pueden usar direcciones de correo electrónico específicas o seleccionar un dominio entero. Los administradores también pueden especificar las excepciones específicas de una regla.

Para identificar el contenido, los administradores crean una "expresión de palabra clave". Los administradores pueden usar una combinación de palabras clave y expresiones regulares para definir una expresión de palabra clave (hay disponibles algunas listas de palabras predefinidas y glosarios de formato de datos). Una vez creada, los administradores pueden guardar y dar un nombre a la expresión de palabra clave. Posteriormente, esto se puede aplicar a múltiples reglas (por ejemplo, para diferentes grupos o distintos atributos de mensaje, como la línea del asunto, el cuerpo del correo electrónico, el contenido del archivo adjunto o el encabezado del correo electrónico).

Cuando los atributos del mensaje estén definidos, los administradores deben especificar el cifrado como la acción de regla, para lo cual deben seleccionar la opción "No interceptar mensajes" y hacer clic en la acción *Cifrar correo electrónico*, tal y como se muestra en la ilustración 3 a continuación.

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

Ilustración 3: selección de Cifrar correo electrónico como una opción de acción

Ejemplos prácticos:

- 1) Los administradores pueden combinar glosarios con formato de datos, como formatos de números de tarjetas de crédito o seguridad social, con listas de nombres de clientes o números de cuentas para etiquetar los correos electrónicos con información de identificación personal, a menudo requerida por las normativas.
- 2) Las expresiones clave para palabras como "cifrar" o "confidencial" pueden facilitar la aplicación de las políticas como una acción.

Email Encryption for InterScan Messaging Hosted Security

Una vez que *Cifrar correo electrónico* se ha seleccionado como la acción de regla, los administradores simplemente nombran y guardan la regla. Cuando la regla se ha creado, se puede editar o copiar (si se copia, se facilita la creación de una regla similar; los administradores simplemente editan la regla copiada con los cambios que se desee).

Experiencia de Email Encryption de los destinatarios

Los destinatarios del correo electrónico cifrado reciben una notificación de correo electrónico en forma de sobre electrónico cerrado. Los destinatarios pueden descargar su propia copia de Trend Micro Email Encryption Client o utilizar el explorador Web para leer y contestar a mensajes sin necesidad de instalar el software. La ilustración 4 a continuación muestra un ejemplo de correo electrónico enviado a un destinatario y un ejemplo de archivo HTML adjunto que contiene un enlace al explorador Web donde el correo electrónico cifrado se puede ver.

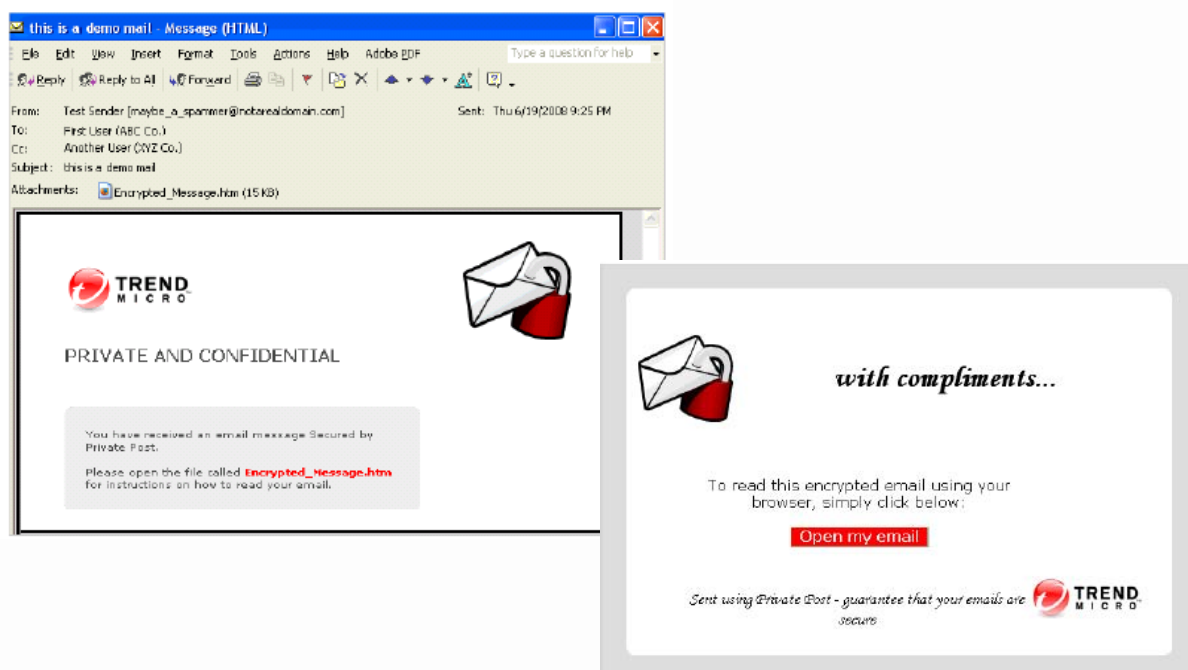


Ilustración 4: experiencia de Email Encryption de los destinatarios: sobre de correo electrónico cifrado y acceso del explorador

Activación de Email Encryption

Trend Micro Email Encryption for InterScan Messaging Hosted Security se encuentra disponible solo como servicio complementario en la implementación Advanced con filtrado saliente. Los clientes Advanced pueden obtener el filtrado saliente sin coste adicional solicitándolo durante el proceso de prueba o registro.

Tal y como se refleja en la Tabla 1 a continuación, las opciones de activación de Email Encryption varían en función del estado de la licencia de InterScan Messaging Hosted Security.

Email Encryption for InterScan Messaging Hosted Security

Estado de la licencia de InterScan Messaging Hosted Security	Opciones de licencia de Email Encryption
Adquirida	Email Encryption se puede probar o comprar. <ul style="list-style-type: none">• Consulte Inicio de una versión de prueba gratuita de Email Encryption• Consulte Compra de Email Encryption
En período de prueba	Solo se puede optar a una versión de prueba gratuita de Email Encryption. <ul style="list-style-type: none">• Consulte Inicio de una versión de prueba gratuita de Email Encryption

Tabla 1: opciones de activación de Email Encryption


Inicio de una versión de prueba gratuita de Email Encryption

Las organizaciones pueden solicitar una versión de prueba gratuita de Email Encryption al mismo tiempo que soliciten una versión de prueba de InterScan Messaging Hosted Security. Para ello, deben seleccionar Email Encryption en el formulario de prueba que aparece publicado en la página Web del servicio. En caso de que ya se haya adquirido InterScan Messaging Hosted Security o éste se encuentre en período de prueba, se podrá obtener una versión de prueba de Email Encryption desde la propia consola del servicio, en la sección Administración > Licencias. (Vea la ilustración 5 a continuación.)

Compra de Email Encryption

Para comprar el servicio Email Encryption, también se debe adquirir InterScan Messaging Hosted Security Advanced con filtrado saliente. Las organizaciones pueden disfrutar de una versión de prueba gratuita de Email Encryption durante el período de prueba del servicio Advanced, si bien no podrán comprarlo hasta que también se adquiriera InterScan Messaging Hosted Security.

Tanto InterScan Messaging Hosted Security como Email Encryption se pueden adquirir de un distribuidor. Encontrará diversos distribuidores a través de los enlaces recogidos en la página Web del servicio. En algunas regiones, se proporciona a los clientes una clave de registro con la que deben registrarse en línea para recibir un código de activación, mientras que en otras, este código de activación se suministra directamente una vez efectuada la compra. En cualquier caso, el cliente debe introducir dicho código de activación en la sección Administración > Licencias de la consola de InterScan Messaging Hosted Security para iniciar el servicio. (Vea la ilustración 4 a continuación.)

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)

Ilustración 5: activación de la licencia de Email Encryption

Trend Micro puede tardar entre 24 y 48 horas en comprobar la solicitud de prueba o compra de Email Encryption e iniciar Email Encryption para su cuenta. Tras la activación, Email Encryption aparece como una acción de regla disponible al añadir o editar una política desde la pantalla de políticas de InterScan Messaging Hosted Security.

Conclusión

Con el cifrado basado en políticas, las organizaciones dejarán de depender de los usuarios individuales para proteger el contenido importante. El cifrado se aplica de forma automática y oportuna cuando las reglas de filtrado de contenido se activan, lo que ayuda a garantizar que los requisitos de confidencialidad y privacidad se cumplan.

Trend Micro ofrece una solución de cifrado del correo electrónico basada en políticas que se integra a la perfección con las funciones de filtrado de contenido de InterScan Messaging Hosted Security. Los administradores tan solo tendrán que activar una casilla de verificación para aplicar el cifrado como una acción de regla. La solución Email Encryption de Trend Micro, de gran flexibilidad, utiliza el cifrado basado en la identidad (IBE), con lo cual elimina las molestas tareas de registro previo y gestión de certificados de la tecnología de infraestructura de clave pública (PKI). Trend Micro Email Encryption simplifica enormemente la tarea de cifrar el contenido de forma segura.

WP02_IMHSEncrypt_090219ES. © 2009 by Trend Micro Incorporated. Reservados todos los derechos. Trend Micro, el logotipo en forma de pelota de Trend Micro, InterScan y Private Post son marcas registradas o marcas comerciales de Trend Micro, Incorporated. El resto de los nombres de productos o empresas pueden ser marcas comerciales o registradas de sus respectivos propietarios. Trend Micro Incorporated se reserva el derecho de efectuar cambios en este documento y en los productos que en él se describen sin previo aviso.