

## HOSTED EMAIL SECURITY PREGUNTAS MÁS FRECUENTES

<b>INFORMACIÓN GENERAL Y VENTAJAS DE LA SOLUCIÓN .....</b>	<b>3</b>
1. ¿EN QUÉ CONSISTE HOSTED EMAIL SECURITY?.....	3
2. ¿CUÁLES SON LAS VENTAJAS EXCLUSIVAS DE IMPLEMENTAR HOSTED EMAIL SECURITY?.....	3
3. ¿POR QUÉ USAR UNA SOLUCIÓN ALOJADA PARA LA SEGURIDAD DEL CORREO ELECTRÓNICO EN VEZ DE UN PRODUCTO IN SITU? .....	3
4. ¿POR QUÉ COMPRAR UNA SOLUCIÓN ALOJADA DE TREND MICRO? .....	4
5. ¿ES HOSTED EMAIL SECURITY UNA SOLUCIÓN APROPIADA PARA GRANDES EMPRESAS? .....	4
6. SI YA TENEMOS SCANMAIL U OTRO PRODUCTO DE SEGURIDAD INSTALADO IN SITU, ¿REALMENTE NECESITAMOS HOSTED EMAIL SECURITY? .....	4
<b>ACUERDO DE NIVEL DE SERVICIO.....</b>	<b>5</b>
7. ¿EN QUÉ CONSISTE EL ACUERDO DE NIVEL DE SERVICIO (SLA) DE HOSTED EMAIL SECURITY? .....	5
8. ¿PUEDO CONSULTAR UNA COPIA DEL SLA? .....	5
9. ¿CÓMO RECIBEN LOS CLIENTES ESTE SLA? .....	5
10. ¿ES LEGALMENTE VINCULANTE ESTE SLA?.....	5
11. ¿SE APLICA EL SLA SI LOS CLIENTES USAN HOSTED EMAIL SECURITY COMO PARTE DE TREND MICRO™ WORRY-FREE™ BUSINESS SECURITY?.....	5
12. ¿PUEDEN LOS CLIENTES ACUMULAR MÁS DE UN CRÉDITO POR DIFERENTES NIVELES DE SERVICIO EN UN MES? .....	6
<b>CARACTERÍSTICAS DEL PRODUCTO Y SU FUNCIONAMIENTO.....</b>	<b>6</b>
13. ¿CUÁL ES LA DIFERENCIA ENTRE HOSTED EMAIL SECURITY Y LA OPCIÓN HOSTED EMAIL SECURITY – INBOUND FILTERING? .....	6
14. ¿CÓMO DETIENE EL SPAM Y OTRAS AMENAZAS DEL CORREO ELECTRÓNICO HOSTED EMAIL SECURITY? .....	6
15. ¿CÓMO FUNCIONA LA REPUTACIÓN DEL CORREO ELECTRÓNICO? .....	7
16. ¿QUÉ TIPOS DE EXPLORACIÓN DE AMENAZAS REALIZA HOSTED EMAIL SECURITY?.....	7
17. ¿QUÉ PROTECCIÓN ANTIMALWARE OFRECE HOSTED EMAIL SECURITY?.....	7
18. ¿QUÉ TECNOLOGÍAS USA EL MOTOR COMPUESTO ANTISPAM DE TREND MICRO? .....	7
19. ¿QUÉ CAPACIDADES DE FILTRADO DE CONTENIDOS OFRECE LA SOLUCIÓN? .....	8
20. ¿QUÉ OPCIONES DE CIFRADO PUEDEN USAR LOS CLIENTES DE HOSTED EMAIL SECURITY? .....	8
21. ¿QUÉ OFRECE TREND MICRO PARA AYUDAR A CUMPLIR LAS NORMATIVAS Y EVITAR LAS FILTRACIONES DE DATOS? .....	8
22. ¿EXISTE ALGÚN RIESGO DE QUE EL CORREO ELECTRÓNICO LEGÍTIMO SEA BLOQUEADO POR ERROR? .....	8
23. ¿PERMITE HOSTED EMAIL SECURITY A LOS USUARIOS FINALES GESTIONAR SUS PROPIAS CARPETAS DE CUARENTENA?.....	9
<b>INFORMACIÓN DE ACTIVACIÓN, ACTUALIZACIÓN Y COMPRA.....</b>	<b>9</b>
24. ¿CÓMO SE VENDE HOSTED EMAIL SECURITY? .....	9
25. ¿CÓMO SE CONSIGUE INFORMACIÓN ESPECÍFICA SOBRE PRECIOS? .....	9
27. ¿CON QUÉ FACILIDAD SE IMPLEMENTA HOSTED EMAIL SECURITY? .....	10
28. PARA EMPEZAR A USAR LA SOLUCIÓN, LOS CLIENTES DEBEN REDIRECCIONAR LOS REGISTROS MX A TREND MICRO. ¿QUÉ ES UN REGISTRO MX? .....	10
29. ¿SE PUEDE ACTUALIZAR DE LA OPCIÓN HOSTED EMAIL SECURITY – INBOUND FILTERING A HOSTED EMAIL SECURITY? .....	10
30. ¿CUÁLES SON LOS REQUISITOS PARA ACTUALIZAR A LAS NUEVAS VERSIONES DE HOSTED EMAIL SECURITY? .....	10

<b>CONFIDENCIALIDAD, ASISTENCIA Y CONTROL .....</b>	<b>10</b>
<b>31. ¿PROTEGE TREND MICRO EL CONTENIDO CONFIDENCIAL DEL CORREO ELECTRÓNICO? .....</b>	<b>10</b>
<b>32. ¿CUÁLES SON LAS OPCIONES DISPONIBLES DE RECUPERACIÓN TRAS DESASTRES? .....</b>	<b>10</b>
<b>33. ¿DISPONE TREND MICRO DE UN EQUIPO DEDICADO A LA SUPERVISIÓN Y GESTIÓN DE SOLUCIONES COMO HOSTED EMAIL SECURITY? .....</b>	<b>11</b>
<b>34. ¿PIERDEN LOS CLIENTES EL CONTROL DE LOS REGISTROS MX CUANDO LOS DIRIGEN A TREND MICRO? .....</b>	<b>11</b>
<b>35. ¿SE GUARDAN LOS MENSAJES DE LOS CLIENTES EN LOS SERVIDORES DE TREND MICRO? .....</b>	<b>11</b>
<b>36. ¿ES HOSTED EMAIL SECURITY UN "SERVICIO EXTERNALIZADO"? .....</b>	<b>11</b>

## **INFORMACIÓN GENERAL Y VENTAJAS DE LA SOLUCIÓN**

### **1. ¿En qué consiste Hosted Email Security?**

Trend Micro Hosted Email Security detiene más del 99% del spam y otras amenazas del correo electrónico antes de que lleguen a la red, lo que permite a las organizaciones recuperar tiempo del personal informático, productividad de los usuarios finales y recursos de la red. Además, Hosted Email Security puede incluir módulos de filtrado del contenido saliente y cifrado opcional como ayuda para garantizar el cumplimiento de normativas y evitar las filtraciones de datos. Como solución alojada, Hosted Email Security se puede implementar en menos de 48 horas sin requisitos de hardware ni software adicionales. Trend Micro se encarga de realizar todas las tareas de mantenimiento de la solución, incluida la implementación de parches, revisiones y ajustes de las aplicaciones, lo que garantiza un rendimiento continuamente optimizado de Hosted Email Security con escasa o ninguna intervención del cliente en cuestiones de mantenimiento.

[al principio](#)

### **2. ¿Cuáles son las ventajas exclusivas de implementar Hosted Email Security?**

Hosted Email Security ha conseguido el primer puesto en detección de spam de acuerdo con pruebas de rendimiento independientes<sup>1</sup>. Entre las capas de protección antispam se incluye el filtrado avanzado de reputación del correo electrónico, componente de la infraestructura Trend Micro™ Smart Protection Network™. Smart Protection Network correlaciona información sobre las amenazas recopilada mediante el correo electrónico, la Web y bases de datos de reputación de archivos con el objetivo de bloquear de inmediato las amenazas, antes incluso de que lleguen a la red. Por ejemplo, si nuestra tecnología de reputación Web detecta una URL maliciosa y en un mensaje de correo electrónico se descubre un enlace a esta dirección URL, la solución bloqueará ese mensaje.

Hosted Email Security incluye tecnología antivirus valorada como la n.º 1 en el bloqueo de malware según pruebas independientes<sup>2</sup>. Puesto que Trend Micro es la empresa creadora y propietaria de esta tecnología, nuestros clientes reciben una protección permanente y en tiempo real frente a las cambiantes tácticas del spam y a las nuevas y complejas amenazas Web del panorama actual.

Asimismo, Hosted Email Security es la única solución que puede ahorrar tiempo del personal informático gracias a sencillas herramientas de administración como el reprocesamiento de correo electrónico en cuarentena, las notificaciones automáticas a los usuarios finales si se infringen políticas de contenido del correo electrónico, la creación de reglas "y/o" para optimizar más fácilmente las tasas de bloqueo del spam y reducir los falsos positivos, así como el filtrado del contenido del correo electrónico, que puede analizar incluso archivos comprimidos, incrustados y protegidos mediante contraseña.

<sup>1</sup> West Coast Labs, pruebas comparativas de antispam (enero de 2009)

<sup>2</sup> NSS Labs, resultados de las pruebas comparativas de protección antimalware de ingeniería social para la seguridad de los puntos finales (septiembre de 2009)

[al principio](#)

### **3. ¿Por qué usar una solución alojada para la seguridad del correo electrónico en vez de un producto in situ?**

El uso de una solución alojada para la seguridad del correo electrónico puede ofrecer a las organizaciones las siguientes ventajas en comparación con un producto de seguridad in situ:

- Detiene el spam y otras amenazas del correo electrónico antes de que lleguen a la red.
- Permite a los clientes recuperar tiempo del personal informático, productividad de los usuarios finales, capacidad de almacenamiento del servidor de correo y de la CPU, ancho de banda de la red y otros valiosos recursos.
- No requiere hardware ni software adicionales y no precisa ningún mantenimiento, o muy poco.
- Se implementa en menos de 48 horas.
- Trend Micro lleva a cabo todas las tareas de mantenimiento, incluida la implementación de actualizaciones y el ajuste de las aplicaciones, con escasa o ninguna intervención del cliente en cuestiones de mantenimiento.

- Permite a las organizaciones distribuidas mantener una actitud unificada de seguridad. Puesto que la protección más reciente está disponible en todo momento para todos los usuarios, en cualquier lugar, no es necesario actualizar el software en varias ubicaciones.
- Tiene un menor coste total de propiedad que los productos de hardware y software tradicionales.
- Ofrece flexibilidad con planificación de la capacidad: una capacidad ilimitada del filtrado del spam y del correo electrónico a un precio fijo por usuario, sin los costes adicionales de hardware generalmente asociados a los productos de seguridad para el correo electrónico instalados in situ a medida que aumenta o disminuye el número de usuarios.

[al principio](#)

#### **4. ¿Por qué comprar una solución alojada de Trend Micro?**

Trend Micro protege actualmente a más de 30.000 clientes cada día en más de 120 países de todo el mundo gracias a Trend Micro Hosted Email Security. Además, Trend Micro es la compañía líder en contenido seguro y gestión de las amenazas y, a diferencia de muchos otros proveedores de soluciones alojadas, es una empresa consolidada de largo recorrido. Trend Micro brinda más de 20 años de experiencia en seguridad y, actualmente, analiza diariamente más de 20.000 millones de sitios Web, mensajes de correo y archivos de entornos tanto físicos como alojados. Smart Protection Network ofrece también protección correlacionada por Internet frente a múltiples amenazas gracias a los datos recopilados por todos los productos y servicios de Trend Micro para responder a las amenazas más rápida e inteligentemente.

[al principio](#)

#### **5. ¿Es Hosted Email Security una solución apropiada para grandes empresas?**

Sí. Hosted Email Security se puede adaptar a las necesidades de las empresas de todos los tamaños, desde aquellas con 5 usuarios hasta multinacionales y proveedores de servicios de Internet. El seguimiento del correo correlaciona los registros para que los administradores puedan detectar rápidamente el estado de cualquier mensaje de correo y determinar el impacto que han tenido las políticas en el correo electrónico y en la ubicación actual. Por otro lado, los informes detallados permiten a los administradores acceder a informes de auditoría y conocer rápidamente el valor del servicio. Además, las reglas de uso del correo electrónico y del filtrado de contenido conceden a los administradores un control minucioso sobre el correo electrónico de la organización.

Asimismo, el acuerdo de nivel de servicio líder del sector, las características de recuperación tras desastres y las medidas de protección de la privacidad satisfacen los requisitos del correo electrónico de una empresa. Hosted Email Security ofrece a las empresas las ventajas de una solución alojada, descongestionando considerablemente la red y ahorrando recursos informáticos, sin privar a los administradores del control sobre el correo electrónico corporativo que cabría esperar de una solución in situ.

Hosted Email Security es también idónea para grandes organizaciones con multitud de delegaciones que invierten demasiado tiempo y dinero en realizar actualizaciones del software en varias ubicaciones. Con Hosted Email Security, las empresas siempre contarán con la mejor y más reciente seguridad, lo que se traduce en una protección inmediata de su flujo de correo con las ventajas de una menor complejidad.

[al principio](#)

#### **6. Si ya tenemos ScanMail u otro producto de seguridad instalado in situ, ¿realmente necesitamos Hosted Email Security?**

Sí. Existen numerosas ventajas inherentes a la protección del correo electrónico en distintos puntos de la red. ScanMail se integra con el servidor de correo (Microsoft Exchange o IBM® Lotus® Domino™) para proteger la red desde el gateway, centrándose en el correo externo, la seguridad del almacén de correo, la exploración del correo electrónico de usuarios remotos y ofreciendo el primer punto de inspección para el correo saliente. Además, ScanMail for Microsoft Exchange también ofrece capacidades de cuarentena del usuario final en Outlook que se pueden integrar en Hosted Email Security. Esto permite a los usuarios finales visualizar el spam recibido en la carpeta de correo no deseado de Outlook. La protección del nivel del cliente se centra específicamente en el equipo de sobremesa del usuario, lo que supone otra capa adicional de protección. Esta cobertura desde el

gateway hasta el equipo de sobremesa en el punto vulnerable es necesaria para detener las amenazas en su origen.

[al principio](#)

## **ACUERDO DE NIVEL DE SERVICIO**

### **7. ¿En qué consiste el acuerdo de nivel de servicio (SLA) de Hosted Email Security?**

Hosted Email Security incluye un acuerdo de nivel de servicio legalmente vinculante que ofrece las siguientes garantías: 100% de disponibilidad del servicio, no más de un minuto de latencia del correo electrónico, eficacia del bloqueo del spam de más del 99%, tasa de falsos positivos no superior al 0,0003%, ninguna infección de virus y excelente capacidad de respuesta del equipo de asistencia. Si estas garantías no se cumplen en un mes dado, los clientes pueden reclamar la devolución del dinero.

<b>Disposiciones del acuerdo de nivel de servicio</b>	<b>Hosted Email Security</b>	<b>Hosted Email Security - Inbound Filtering</b>
Disponibilidad	100% de tiempo de actividad	100% de tiempo de actividad
Virus	Cero infecciones por virus provenientes del correo electrónico	Cero infecciones por virus provenientes del correo electrónico
Eficacia del bloqueo antispam	99% o superior	N/D
Falsos positivos	No más del 0,0003%	N/D
Respuesta del equipo de asistencia	Ajustada a la gravedad del incidente	Ajustada a la gravedad del incidente
Latencia para la entrega del correo electrónico	No más de un minuto de latencia	No más de un minuto de latencia

[al principio](#)

### **8. ¿Puedo consultar una copia del SLA?**

Sí. Puede acceder a una copia del SLA tras iniciar sesión en la consola de Hosted Email Security, en la sección de administración. Solo tiene que seleccionar la región o el idioma que le interese del menú desplegable.

[al principio](#)

### **9. ¿Cómo reciben los clientes este SLA?**

El SLA está incluido en Hosted Email Security cuando los clientes adquieren el servicio.

[al principio](#)

### **10. ¿Es legalmente vinculante este SLA?**

Sí. Al igual que el contrato de licencia de usuario final (EULA), el SLA fue diseñado como parte integrante de Hosted Email Security. Si hubiera algún conflicto entre las disposiciones de ambos documentos, tendrán preferencia las disposiciones del SLA. Tanto Trend Micro como los clientes son responsables de cumplir las disposiciones del SLA. Nota: el SLA y el EULA pueden ser actualizados o modificados ocasionalmente.

[al principio](#)

### **11. ¿Se aplica el SLA si los clientes usan Hosted Email Security como parte de Trend Micro™ Worry-Free™ Business Security?**

Sí. El SLA es aplicable a Hosted Email Security – Inbound Filtering como parte de Worry-Free Business Security.

[al principio](#)

**12. ¿Pueden los clientes acumular más de un crédito por diferentes niveles de servicio en un mes?**

Sí. Los clientes pueden enviar varias solicitudes de compensación en un mes natural. Algunos niveles de servicio individuales permiten únicamente una solicitud de compensación por mes. Por ejemplo:

- Disponibilidad
- Latencia
- Falsos positivos
- Antivirus

Otros niveles de servicio permiten varios envíos en un mes dado (por ejemplo, los niveles de servicio antispam y de asistencia técnica). Los clientes también pueden enviar solicitudes de compensación por diferentes tipos de niveles de servicio en un mes.

[Volver al principio](#)

**CARACTERÍSTICAS DEL PRODUCTO Y SU FUNCIONAMIENTO**

**13. ¿Cuál es la diferencia entre Hosted Email Security y la opción Hosted Email Security – Inbound Filtering?**

Tanto Hosted Email Security como Hosted Email Security – Inbound Filtering incluyen una tecnología muy eficaz para el bloqueo del spam, gestión basada en Web de la cuarentena del usuario final, así como funciones completas de registro, creación de informes y notificaciones. Además, ambas soluciones están respaldadas por un acuerdo de nivel de servicio.

**Hosted Email Security:** ofrece la opción de filtrar tanto el tráfico saliente del correo electrónico como el entrante. La versión avanzada permite al administrador modificar las políticas predeterminadas para las amenazas del correo electrónico con el fin de optimizar el bloqueo del spam, las tasas de falsos positivos y la eficacia de bloqueo de otras amenazas. El administrador también puede definir reglas para aplicar políticas de uso del correo electrónico, incluido el tamaño y el número de destinatarios, o bien crear reglas de filtrado de contenido para el encabezado, asunto, cuerpo y datos adjuntos (archivos PDF, documentos de Microsoft, etc.) de los mensajes de correo electrónico que contribuyan al cumplimiento de las políticas y a evitar filtraciones de datos. También se encuentran disponibles listados predefinidos de palabras y de formatos de datos, tales como números de tarjetas de crédito y de identificación personal (por ejemplo, el número de la seguridad social). Se puede adquirir un complemento de cifrado del correo electrónico basado en identidad para Hosted Email Security.

**Opción Hosted Email Security – Inbound Filtering:** disponible como una versión secundaria de Hosted Email Security con menos características, la opción Inbound Filtering analiza el tráfico entrante del correo electrónico para detener el spam y otras amenazas basadas en el correo electrónico con políticas de protección predeterminadas. Los administradores pueden definir las acciones que deseen para los mensajes spam (eliminar, poner en cuarentena o etiquetar y entregar) aunque no pueden modificar las políticas predeterminadas. Ambos servicios se gestionan mediante una única consola Web y todas las actualizaciones, correcciones, parches y ajustes de las aplicaciones son efectuadas por Trend Micro.

[al principio](#)

**14. ¿Cómo detiene el spam y otras amenazas del correo electrónico Hosted Email Security?**

Hosted Email Security analiza los mensajes de correo electrónico en tres fases:

- a. Reputación del correo electrónico
- b. Búsqueda de amenazas
- c. Filtrado del contenido (solo Hosted Email Security)

En la primera fase, el módulo Email Reputation detiene las amenazas del correo electrónico según la reputación del remitente. La exploración de las amenazas usa motores de amenazas para explorar el contenido del correo electrónico e identificar y bloquear así las amenazas que pueda contener. El

filtrado de contenido permite al cliente aplicar políticas de uso del correo electrónico, las cuales constituyen una excelente ayuda para cumplir los requisitos gubernamentales, internos y del sector.

[al principio](#)

#### **15. ¿Cómo funciona la reputación del correo electrónico?**

Email Reputation usa dos tipos de servicios de reputación para detener las amenazas del correo electrónico. El primero verifica las direcciones IP del correo electrónico entrante con la base de datos de reputación más extensa y fiable del mundo. El segundo de ellos ofrece un servicio de reputación dinámico, que identifica los nuevos orígenes de amenazas del correo electrónico e incluso detiene equipos zombi y redes robot en cuanto aparecen. Email Reputation supervisa y realiza el mantenimiento de las valoraciones de reputación de acuerdo con historiales de spam y envío de amenazas así como muestras de correo electrónico, garantizando que cada estado de reputación sea verificable y se mantenga actualizado.

Este servicio de reputación forma parte de la infraestructura Trend Micro Smart Protection Network incluida en los productos y servicios de Trend Micro. Smart Protection Network correlaciona información sobre las amenazas recopilada en mensajes de correo electrónico, la Web y bases de datos de reputación de archivos.

[al principio](#)

#### **16. ¿Qué tipos de exploración de amenazas realiza Hosted Email Security?**

Trend Micro usa las técnicas más recientes según las últimas tendencias para ofrecer una exploración realizada por dos motores que filtran el correo electrónico en busca de amenazas maliciosas. El primer motor busca virus, spyware y otros tipos de malware, mientras que el motor antispam de Trend Micro se encarga de buscar spam y phishing.

[al principio](#)

#### **17. ¿Qué protección antimalware ofrece Hosted Email Security?**

Trend Micro incluye un filtrado de reputación Web que filtra las URL maliciosas incrustadas en el correo electrónico. Además, Hosted Email Security incorpora tecnología antimalware que ha sido valorada como la mejor entre las de otros proveedores de seguridad por pruebas independientes realizadas por NSS Labs. La protección antivirus de Trend Micro, con incontables galardones y excelentes valoraciones, incluye el reconocimiento de archivos de patrones de virus conocidos así como protección de día cero. Y, para proporcionar esta protección de día cero, usamos tecnologías heurísticas que buscan indicadores de virus sin depender de un determinado archivo de patrones. Este enfoque heurístico aplica técnicas de predicción para detener los virus no conocidos. Hosted Email Security también ofrece antispymware y protección frente a otros tipos de malware.

[al principio](#)

#### **18. ¿Qué tecnologías usa el motor compuesto antispam de Trend Micro?**

El motor compuesto antispam integra las tecnologías siguientes:

- Análisis de estadísticas, que evalúa indicadores de spam y ofrece una valoración de "probabilidad de spam" (los umbrales definidos determinan si el correo electrónico es spam)
- Técnicas heurísticas avanzadas, que aplican reglas sofisticadas basadas en el comportamiento de las amenazas
- Técnicas heurísticas específicas para identificar el spam en los datos adjuntos
- Filtros basados en firmas, que evitan los mensajes de correo con spam conocido
- Listas de remitentes bloqueados y permitidos
- Detección de URL incrustadas para bloquear los mensajes de correo con enlaces a sitios Web maliciosos
- Detección del spam de imágenes
- Detección del spam multilingüe, que identifica el spam en numerosos idiomas
- Tecnología antiphishing, que aplica técnicas heurísticas, firmas y la detección de URL incrustadas adaptadas específicamente para bloquear los mensajes de correo electrónico de phishing

[al principio](#)

**19. ¿Qué capacidades de filtrado de contenidos ofrece la solución?**

Ofrecemos un filtrado de contenidos muy flexible para el que se pueden crear reglas personalizadas mediante una intuitiva interfaz de usuario. Por ejemplo, los administradores pueden crear reglas para el encabezado, el asunto, el cuerpo y los tipos de datos adjuntos (archivos PDF, documentos de Microsoft, etc.) de los mensajes de correo electrónico. Estas reglas permiten a los administradores analizar y etiquetar numerosos tipos de contenido. Para simplificar la creación de las reglas, se pueden usar los listados predefinidos de palabras y de formatos de datos, tales como números de tarjetas de crédito y de identificación personal (por ejemplo, el número de la seguridad social). El administrador también puede definir reglas que ayuden a cumplir las políticas de uso del correo electrónico como, por ejemplo, sobre el tamaño o el número de destinatarios de un mensaje.

Las reglas se pueden aplicar al tráfico de correo entrante o saliente y se pueden seleccionar remitentes o destinatarios específicos (así como crear excepciones), lo que permite a los administradores aplicar las reglas a toda la empresa o a departamentos, grupos o empleados concretos.

Las organizaciones también tienen la posibilidad de seleccionar la acción que se llevará a cabo si se activa una política. Hay numerosas acciones donde elegir, como insertar un texto de renuncia de responsabilidad en el cuerpo del mensaje o cifrar todo el mensaje (si se ha adquirido el servicio de cifrado opcional).

[al principio](#)

**20. ¿Qué opciones de cifrado pueden usar los clientes de Hosted Email Security?**

Trend Micro Hosted Email Encryption está disponible para Hosted Email Security como un servicio opcional. Trend Micro usa el cifrado basado en identidad, un método sencillo de usar tanto para los remitentes como para los destinatarios. El módulo de cifrado del correo electrónico se integra con las funciones de filtrado de contenido de Hosted Email Security con tan solo activarlo en las opciones de configuración del filtrado saliente. Los administradores pueden configurar fácilmente nuestro cifrado basado en políticas mediante la creación de reglas que activan el cifrado cuando se cumplen los criterios correspondientes.

Además, Hosted Email Security incluye el protocolo de seguridad de la capa de transporte (TLS), que cifra el "circuito" del correo electrónico (no el correo electrónico en sí), siempre que el remitente y el receptor del mensaje activen también TLS. No obstante, con TLS, no hay modo de garantizar que todos los destinatarios del correo electrónico activarán el protocolo TLS, y el correo electrónico suele realizar varios saltos por el proveedor de servicios de Internet antes de llegar a su destino final. Por ello, no es posible tener la total certeza de que el correo electrónico estará protegido durante todas las etapas de su recorrido.

TLS es un complemento de gran utilidad para Hosted Email Encryption pues protege el circuito del correo electrónico desde la ubicación del cliente hasta el servicio de Hosted Email Security, donde se puede aplicar el cifrado basado en identidad directamente a todos los mensajes de correo electrónico.

[al principio](#)

**21. ¿Qué ofrece Trend Micro para ayudar a cumplir las normativas y evitar las filtraciones de datos?**

Además de Email Encryption, Trend Micro brinda una completa propuesta para la privacidad y la protección de los datos. Por ejemplo, el antivirus de Trend Micro mantiene la integridad de los datos al evitar que los virus los puedan dañar o corromper. Algunas normativas exigen explícitamente a las organizaciones la aplicación de una completa protección antivirus. Además, el antispyware y el antiphishing evitan el robo de datos mientras que el filtrado de contenidos garantiza que la información confidencial únicamente es visualizada por los destinatarios autorizados.

[al principio](#)

**22. ¿Existe algún riesgo de que el correo electrónico legítimo sea bloqueado por error?**

Todas las soluciones de seguridad del correo electrónico pueden bloquear accidentalmente un mensaje válido en algún momento. Esto se conoce como generar un falso positivo, pero Hosted Email Security garantiza por contrato una tasa de falsos positivos no superior al 0,0003% y un bloqueo de más del 99% del spam.

Si en un mes dado la tasa de falsos positivos excede este valor máximo garantizado del 0,0003% (o las tasas de bloqueo de spam descienden repetidamente por debajo del 99%), el cliente puede reclamar un crédito de hasta el 100% del coste mensual de Hosted Email Security.

Además, puesto que consideramos que la entrega del correo electrónico es básica para el funcionamiento de cualquier empresa, ponemos a su disposición varias herramientas exclusivas de administración para detectar y entregar con rapidez cualquier mensaje de correo que se haya puesto en cuarentena incorrectamente como spam. Entre ellas, podrá disponer de herramientas para el reprocesamiento automático del correo electrónico puesto en cuarentena, la gestión centralizada de los registros y el seguimiento integral del correo, además de herramientas Web de fácil uso que permiten a los usuarios finales gestionar sus propias carpetas de cuarentena.

[al principio](#)

**23. ¿Permite Hosted Email Security a los usuarios finales gestionar sus propias carpetas de cuarentena?**

Sí. Hosted Email Security ofrece una herramienta de cuarentena del usuario final (EUQ) basada en Web con la que los usuarios finales gestionan sus propias carpetas de cuarentena para el spam, con el consiguiente ahorro del tiempo del personal informático. Los clientes también pueden usar la función de "etiquetar y entregar" para crear una regla en el cliente de correo electrónico por la que se creará una carpeta de cuarentena en el usuario final. Si los usuarios también son clientes de ScanMail™ for Microsoft® Exchange, pueden usar la carpeta de cuarentena creada en Outlook y visualizar así todos los mensajes spam en una sola carpeta, independientemente de la solución que haya identificado el spam.

[al principio](#)

**INFORMACIÓN DE ACTIVACIÓN, ACTUALIZACIÓN Y COMPRA**

**24. ¿Cómo se vende Hosted Email Security?**

Hosted Email Security se vende mediante una suscripción anual a precio fijo por usuarios finales, sin cuotas de mantenimiento ni de garantía. El precio de la suscripción cubre un volumen ilimitado de correo electrónico y spam. La compra mínima es de cinco usuarios. Los clientes pueden adquirir la opción Hosted Email Security – Inbound Filtering o Hosted Email Security. Los clientes de Hosted Email Security también tienen la posibilidad de adquirir el servicio complementario Hosted Email Encryption.

Asimismo, los clientes que compren Trend Micro™ Worry-Free™ Business Security Advanced recibirán la opción Hosted Email Security – Inbound Filtering como parte del paquete Worry-Free Business Security Advanced. Los clientes de la opción Hosted Email Security – Inbound Filtering y Worry-Free Business Security Advanced pueden comprar igualmente una actualización a Hosted Email Security.

[al principio](#)

**25. ¿Cómo se consigue información específica sobre precios?**

Póngase en contacto con un socio del canal o con un representante de ventas de su región para obtener información específica sobre precios.

[al principio](#)

**26. ¿Cómo pueden activar el producto y empezar a utilizarlo los clientes que hayan comprado Hosted Email Security?**

El proceso de registro y activación de Hosted Email Security depende de las regiones, algunas de las cuales usan un proceso de registro en línea. El cliente accede a una URL determinada e introduce una clave de registro que se envía a un servidor centralizado. A continuación, el servidor envía un mensaje de correo al cliente con los códigos de activación (AC) y las instrucciones pertinentes.

En otras regiones, el distribuidor proporciona un código de activación al cliente. El cliente introducirá los códigos de activación (AC) en la ubicación correspondiente de la consola de administración de Hosted Email Security.

Independientemente del método utilizado, los clientes reciben luego un mensaje de correo con las instrucciones sobre cómo añadir las direcciones IP y los nombres de dominio del servidor de correo, junto con información sobre cómo redireccionar su registro MX a Trend Micro para empezar a utilizar el servicio.

[al principio](#)

**27. ¿Con qué facilidad se implementa Hosted Email Security?**

La asignación de cuentas de Hosted Email Security se realiza en menos de 30 minutos. En colaboración con el cliente, Trend Micro validará la propiedad de los dominios de correo electrónico y realizará las comprobaciones pertinentes para garantizar la entrega del correo electrónico. Tras facilitar la información de la cuenta, además de los datos de las direcciones IP y los dominios del servidor de correo, el sistema solo pide al cliente que redirija sus registros de correo Exchange (MX) a Trend Micro.

[al principio](#)

**28. Para empezar a usar la solución, los clientes deben redireccionar los registros MX a Trend Micro. ¿Qué es un registro MX?**

Un registro de correo Exchange (MX) es una entrada en una base de datos de nombres de dominios, que identifica al responsable del servidor de correo de la gestión del correo electrónico para ese dominio (similar a una dirección principal de correo postal). Con Hosted Email Security, los clientes redireccionan los registros MX a Trend Micro para que todos los mensajes de correo se dirijan primero a Trend Micro a través del filtrado de Hosted Email Security, antes de entregarse en los servidores de correo de los clientes. Por último, llegan a los usuarios finales.

[al principio](#)

**29. ¿Se puede actualizar de la opción Hosted Email Security – Inbound Filtering a Hosted Email Security?**

Sí, los clientes pueden actualizar de la opción Hosted Email Security – Inbound Filtering a Hosted Email Security. Póngase en contacto con su representante de ventas para conocer más detalles.

[al principio](#)

**30. ¿Cuáles son los requisitos para actualizar a las nuevas versiones de Hosted Email Security?**

Hosted Email Security no se suministra en versiones. Al ser una solución alojada, Trend Micro implementa las características nuevas en los clientes tan pronto como están disponibles. Además, es Trend Micro quien lleva a cabo todas las actualizaciones, lo que reduce la carga de TI en los clientes.

[al principio](#)

**CONFIDENCIALIDAD, ASISTENCIA Y CONTROL**

**31. ¿Protege Trend Micro el contenido confidencial del correo electrónico?**

Sí. Todos los mensajes de correo electrónico válidos se procesan automáticamente sin intervención humana. El personal de Trend Micro no tiene acceso a estos mensajes, que solo se guardan si el sistema del cliente no está disponible, como medida de recuperación tras desastres. Sin embargo, ningún mensaje de correo se guarda en el disco duro, a no ser que el cliente lo indique expresamente.

[al principio](#)

**32. ¿Cuáles son las opciones disponibles de recuperación tras desastres?**

Hosted Email Security se aloja actualmente en tres centros de datos (dos en los Estados Unidos y uno en Alemania). Estos centros de datos ofrecen grandes sistemas de recuperación tras desastres en una arquitectura distribuida de equilibrio de la carga.

En caso de que se produzca un error en el servidor de correo del cliente, Trend Micro pondrá en cola los mensajes durante cinco días si el sistema del cliente deja de estar disponible. Cuando el sistema del cliente vuelve a funcionar, los mensajes de correo se envían mediante un control de flujo inteligente que evita la sobrecarga del sistema.

[al principio](#)

**33. ¿Dispone Trend Micro de un equipo dedicado a la supervisión y gestión de soluciones como Hosted Email Security?**

Sí. Además de nuestro equipo de TrendLabs formado por expertos en seguridad de todo el mundo, Trend Micro cuenta con un equipo dedicado a la supervisión y gestión ininterrumpidas de soluciones como Hosted Email Security. Asimismo, le ofrecemos un competitivo acuerdo de nivel de servicio (SLA) que obliga de forma contractual a Trend Micro a garantizar una disponibilidad del servicio del 100%, un máximo de un minuto de latencia de entrega del correo electrónico, un bloqueo del 99% del spam como mínimo, una tasa de falsos positivos no superior al 0,0003%, ninguna infección de virus y un inmejorable tiempo de respuesta del equipo de asistencia.

[al principio](#)

**34. ¿Pierden los clientes el control de los registros MX cuando los dirigen a Trend Micro?**

No. El registro MX estará siempre bajo el control del cliente. Los clientes pueden reconfigurar los registros MX para que vuelvan a apuntar directamente a sus servidores de correo en el momento que deseen.

[al principio](#)

**35. ¿Se guardan los mensajes de los clientes en los servidores de Trend Micro?**

A diferencia de muchas empresas que ofrecen seguridad alojada para el correo electrónico, Trend Micro no aplica ningún proceso de almacenamiento y reenvío para filtrar los mensajes, lo que supondría almacenarlos en los servidores para explorarlos y, finalmente, enviarlos. En lugar de ello, Hosted Email Security filtra el mensaje de correo en tiempo real y, si es válido, lo reenvía sin intervención humana. Los mensajes de correo solo se guardan si el sistema del cliente no está disponible (como medida de recuperación tras desastres). El personal de Trend Micro no tiene acceso a ellos. Sin embargo, ningún mensaje de correo se guarda en el disco duro, a no ser que el cliente lo indique expresamente.

[al principio](#)

**36. ¿Es Hosted Email Security un "servicio externalizado"?**

No. Con Hosted Email Security, su empresa nunca cede a una organización externa la gestión de los servidores de correo electrónico ni redirige la política del correo electrónico o la gestión de la misma. El correo siempre estará bajo su control.

[al principio](#)