

Axway Secure Messenger

Proteja su empresa con políticas basadas en correo electrónico encriptado



Ninguna empresa quiere acabar siendo noticia en los periódicos por una fuga de datos — especialmente una fuga accidental de información confidencial que provenga de un correo electrónico o archivo adjunto enviado de forma no segura por un empleado a la dirección equivocada. El coste de este tipo de fallos de seguridad puede ser devastador: pérdida de datos, interrupción del negocio, perjuicios a la marca y a su reputación y multas administrativas y pleitos.

Axway Secure Messenger™ puede proteger su empresa contra estas amenazas mejorando la seguridad del correo electrónico, la gobernanza y el cumplimiento de las normativas. Combinando un sistema de relay SMTP de vanguardia con políticas basadas en filtrado de contenidos, Secure Messenger inspecciona todos los correos electrónicos entrantes y salientes en el Gateway de Internet para identificar el contenido de los correos y archivos adjuntos que infringen las políticas de seguridad definidas por la empresa y redirecciona automáticamente los mensajes sospechosos a un canal seguro para entregarlo de forma encriptada, ponerlo en cuarentena, eliminarlo o realizar otra acción. Este sistema garantiza que todos los usuarios- internos y externos- cumplen las políticas de la empresa en todo momento sin tener que implementar o gestionar activamente, software encriptado en sus ordenadores ni cambiar su forma habitual de trabajar.

Funcionalidades clave y Beneficios

Funcionalidades completas de encriptado

Mensajes electrónicos entrantes y salientes seguros independientemente del canal, tanto si es de Gateway a Gateway, Gateway a desktop o a través de la web

- Encriptar y autenticar mensajes según políticas centralizadas y enrutamiento automatizado de los mensajes
- Utilice el correo electrónico para entregar información confidencial y corporativa y para documentar las transacciones de negocio confidenciales
- Despliegue funciones de correo electrónico seguro para cada empleado, cliente o partner, sin necesidad de que ellos instalen ni aprendan nuevo software. Encriptado automático de Gateway a Gateway que no precisa ninguna intervención del usuario final.



Funcionalidades clave y Beneficios	
<p>Potente gestión de las políticas de correo electrónico Defina y gestione políticas para analizar, gestionar, proteger y hacer el seguimiento y generar informes sobre el tráfico de correo electrónico entrante y saliente de su empresa</p>	<ul style="list-style-type: none"> ▪ Filtrado de contenido con una sencilla casilla de verificación, gestor de políticas intuitivo y encriptado automático de Gateway a Gateway facilita la prevención de fuga accidental de datos ▪ Aproveche las aplicaciones existentes y redes gracias a la gestión de servicios y contraseñas para inicio de sesión y sencilla integración con sistemas de gestión de identidades de terceros ▪ Defina y aplique las políticas de mensajería a nivel de dominio, grupo y a nivel individual
<p>Facilita el cumplimiento de normativas y simplifica la gobernanza Los léxicos especializados y las funciones mejoradas de escaneo y seguimiento hacen que sea más fácil cumplir con los estándares evolutivos de la industria y legislaciones gubernamentales</p>	<ul style="list-style-type: none"> ▪ Cree filtros de contenido para identificar la información personal que debe ser protegida según las leyes de protección de datos (Estándar de Seguridad de Datos PCI en EEUU, Directiva de Protección de Datos de la Unión Europea y Ley de Protección de Datos Personales Japonesa) ▪ Un léxico de servicios financieros escanea los mensajes, archivos adjuntos e información financiera personal para simplificar el cumplimiento de las normas SOX, GLBA y de otras normas del sector financiero ▪ Un léxico HIPAA escanea para proteger la información sobre salud (PHI) para asegurar el cumplimiento de las normas HITECH/HIPAA y de otras normas del sector sanitario ▪ El seguimiento de la entrega de mensajes hasta el desktop del destinatario crea un registro documentado con fines de auditoría y de conformidad con normativas

La solución más accesible de la industria para la encriptación de datos del correo electrónico

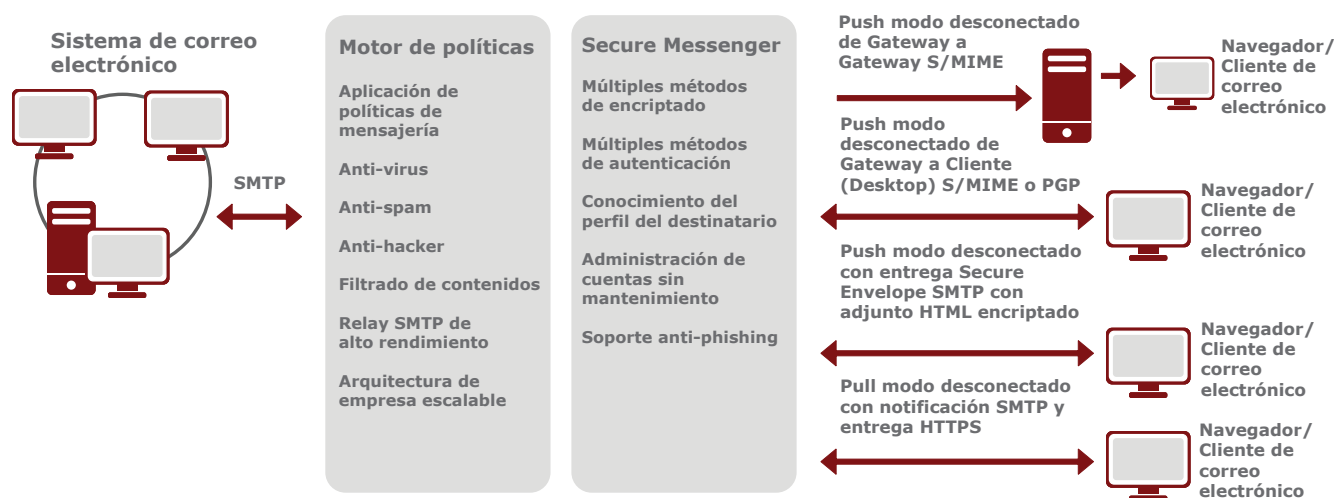
Como en general una empresa no puede imponer software especial en los ordenadores para enviar o recibir correo electrónico seguro fuera de su propia red, Secure Messenger proporciona una amplia gama de métodos de entrega de mensajes que funcionan con los clientes de correo electrónico y los navegadores web estándar por lo que no es necesario instalar o gestionar nuevo software.

Entrega on line mediante el mecanismo “pull” utilizando un navegador web (Secure Webmail)

Secure Webmail utiliza un enlace web incluido en un mensaje de correo electrónico para dirigir al destinatario a un servidor seguro donde podrá leer el mensaje via navegador web. Este método aprovecha las funcionalidades de encriptado SSL existentes del navegador para entregar los mensajes de forma segura a la vez que se utilizan los métodos de autenticación basados en navegador para garantizar que la única persona que puede ver el mensaje es el destinatario del mismo.

Los destinatarios pueden acceder a sus mensajes desde cualquier lugar por Internet y responder a los mismos a través del mismo canal seguro de entrega. Todos los usuarios tienen un buzón web seguro (Secure Inbox) que les permite enviar, recibir, clasificar, buscar, eliminar, guardar y organizar los mensajes desde cualquier lugar por Internet.





Entrega en modo desconectado (offline) mediante el mecanismo “push” utilizando un navegador web (Secure Envelope)

Secure Envelope entrega directamente en la bandeja de entrada del destinatario un mensaje encriptado utilizando correo electrónico SMTP estándar para el transporte pero incluyendo el contenido del mensaje encriptado en un archivo adjunto HTML. Los destinatarios abren el archivo adjunto con un navegador on line o en modo desconectado (offline) e introducen una contraseña para desencriptar y leer el mensaje.

Opciones de entrega

- Dispositivo Linux protegido
- Dispositivo Axway/Dell
- Dispositivo virtual VMware

Entrega en modo desconectado (offline) mediante el mecanismo “push” con S/MIME

Cuando hay un certificado digital disponible para encriptar y la infraestructura de correo electrónico del destinatario soporta el estándar S/MIME, Secure Messenger soporta la entrega en modo desconectado mediante el mecanismo “push” via Gateway a Gateway y Gateway a desktop S/MIME encriptado.

Seguridad completa del correo electrónico

- Despliegue de Axway Secure Messenger en una aplicación consolidada de Linux compatible con IPv6 junto con Axway MailGate, un gestor de seguridad de correo electrónico de entrada y salida corporativo, para resolver todos los problemas de seguridad de su correo electrónico con una solución integral en una única aplicación.
- Obtenga una licencia de Secure Messenger y una de MailGate juntas o por separado. Active ambas soluciones a la vez o progresivamente, según sus necesidades y conforme su empresa crezca.
- Un único asistente de instalación, una única interfaz de usuario de administración y una única interfaz de usuario final mejoran la instalación y facilidad de uso.



Alta disponibilidad/Recuperación tras desastre

- Utilice las funcionalidades de recuperación tras desastre para superar un fallo en el servidor o en los datos sin que el correo electrónico se vea afectado. Los datos con copia de seguridad pueden restaurarse.
- Utilice el almacenamiento de conexión a red (NAS) para habilitar la aplicación basada en la alta disponibilidad para conseguir una funcionalidad perfecta en caso de que se produzca un fallo en el sistema.

Más información

Para más información sobre cómo Axway Secure Messenger puede proteger su empresa contra las amenazas de fuga de datos mejorando la seguridad, la gobernanza y el cumplimiento de las normativas del correo electrónico, escríbanos a axwaysolutions@axway.com o visítenos www.axway.com/contact-us.