

Módulo Proofpoint Secure Messaging



Potenciado por Voltage IBE™

El módulo Proofpoint Secure Messaging™, un componente de Proofpoint Protection Server® y de Proofpoint Messaging Security Gateway™, hace que la comunicación segura ad hoc resulte tan simple como la mensajería tradicional sin encriptación. Las poderosas características de encriptación basadas en políticas de Proofpoint mitigan el riesgo asociado con violaciones de regulaciones, pérdida de datos y violaciones de políticas corporativas, sin impactar en forma adversa las operaciones comerciales. El módulo Proofpoint Secure Messaging es ideal para organizaciones pertenecientes a los sectores de la salud, los servicios financieros, gubernamentales y otros sectores que necesitan proteger datos confidenciales, los que a su vez deben estar inmediatamente disponibles para los afiliados, socios comerciales y otros usuarios finales pertinentes .

Generalidades

Como el correo electrónico se ha convertido en el medio preferido para las comunicaciones de negocios, las organizaciones han demostrado una creciente preocupación por asegurar la seguridad de los mensajes individuales. Normalmente, se utiliza el correo electrónico para transmitir información delicada o confidencial, incluyendo datos de operaciones, secretos comerciales, documentos legales, información financiera, e información personal sobre salud o identidad, tanto dentro como fuera de la empresa.

La necesidad de asegurar esta información confidencial, y dar cumplimiento a un creciente cuerpo normativo que regula la transmisión de datos privados, ha convertido a la encriptación de correo electrónico basada en políticas en un atributo indispensable para una solución de seguridad de mensajería completa. El módulo Proofpoint Secure Messaging cumple con estos requisitos por medio de la solución más poderosa y flexible en la industria para mensajería segura basada en políticas.

Características

Mensajería segura basada en políticas

La capacitación de los usuarios finales sobre el uso apropiado de los sistemas de encriptación puede constituir una barrera significativa para la implementación de las soluciones de mensajería segura tradicionales. Pero Proofpoint Secure Messaging es mucho más fácil de utilizar y gestionar. La solución de mensajería segura de Proofpoint aplica en forma automática y dinámica la encriptación o desencriptación directamente en el gateway en base a las políticas de su organización. Como resultado, los usuarios finales no deben tomar ninguna medida especial para aprovechar las características de encriptación, y sus políticas de conformidad y seguridad de contenidos se aplican en forma consistente y precisa según sea necesario.

Fácil de administrar

A diferencia de otras alternativas de encriptación, las características de encriptación basadas en identidad de Proofpoint proveen una protección efectiva para la información delicada sin las cargas administrativas y los costos de infraestructura típicamente asociados con la mensajería segura.

- **Gestión de políticas fácil:** Todas las políticas de encriptación, basadas en el cumplimiento de normativas, la protección de datos o inquietudes corporativas internas, se gestionan de manera centralizada y aplican en el gateway. Proofpoint Messaging Security Console™ proporciona una práctica interfaz gráfica para definir las políticas de encriptación, que puede accionarse sobre la base del contenido del mensaje identificado por los módulos Proofpoint Regulatory Compliance™, Content Compliance™ o Proofpoint Digital Asset Security™.
- **Gestión simplificada de claves y certificados:** Mediante el uso de la tecnología de IBE (Encriptación Basada en Identidad) de Voltage Security, se generan claves públicas a pedido, eliminando el desalentador ciclo de vida de los certificados y los requisitos para la gestión de claves de otras soluciones de encriptación. No se requiere un mantenimiento continuo de certificados y de Listas de Revocación de Certificados (CRL, por sus siglas en inglés).
- **Requisitos mínimos para el almacenamiento de datos y archivo:** Proofpoint Secure Messaging también simplifica el almacenamiento, respaldo y recuperación general usualmente asociado con la encriptación de mensajes. Al utilizar la tecnología IBE, no es necesario respaldar o almacenar mensajes y claves por períodos de tiempo prolongados.



¿Qué significa Encriptación Basada en Identidad?

El módulo Proofpoint Secure Messaging es potenciado mediante tecnología de Encriptación Basada en Identidad (IBE) de Voltage Security.

IBE de Voltage es un sistema de criptografía de claves públicas que utiliza identidades comunes (como una dirección de correo electrónico) como claves públicas, eliminando la necesidad de certificados, Listas de Revocación de Certificados y otras infraestructuras costosas. El resultado es una solución de encriptación poderosa que es fácil de implementar y de gestionar sin la sobrecarga y costo inherentes a las soluciones de seguridad tradicionales.

¿Cómo trabaja IBE?

Cualquier usuario puede comunicarse en forma segura con cualquier otro usuario utilizando la dirección de correo electrónico del destinatario como la clave de encriptación (o pública). Las claves de desencriptación (o privadas) son generadas por el módulo Proofpoint Secure Messaging según sea necesario. Estas claves pueden recrearse en cualquier momento, eliminando la necesidad de archivar o almacenar claves de desencriptación.

Estas propiedades básicas proporcionan un ambiente seguro de mensajería donde nunca se requieren certificados y los usuarios no necesitan saber nada aparte de sus direcciones de correo electrónico.



Módulo Proofpoint Secure Messaging

Potenciado por Voltage IBE™

Características (continúa)

Fácil de utilizar

Proofpoint Secure Messaging opera con transparencia para los usuarios finales sin requerir descargas de software o la instalación y mantenimiento de clientes de encriptación de escritorio. La solución de encriptación de Proofpoint encripta y desencripta automáticamente contenido delicado según sea necesario, sin que los usuarios finales deban utilizar y gestionar complicados certificados digitales o claves de encriptación.

Costo total de propiedad reducido

El módulo Proofpoint Secure Messaging interactúa de manera homogénea con otros módulos de Proofpoint incluyendo Proofpoint Regulatory Compliance y Proofpoint Digital Asset Security. Su fácil implementación y requisitos mínimos de gestión continua reducen en gran forma los costos actuales asociados con la gestión de su solución de mensajería segura. Y la facilidad de uso, sin precedente, para los usuarios finales de Proofpoint, minimiza los costos de soporte, capacitación y centro de asistencia técnica.

Potente aplicación de políticas de mensajería segura

Control extremadamente detallado de las políticas de encriptación

Al igual que en el antispam de Proofpoint, los módulos antivirus y de seguridad de contenidos, las políticas de mensajería segura se gestionan y aplican a nivel empresarial desde una ubicación única, utilizando la Proofpoint Messaging Security Console. Una vez definidas, las políticas de encriptación empresarial se aplican en forma automática en el gateway, eliminando el riesgo de errores por parte del usuario.

Las políticas de encriptación de mensajes pueden ser extremadamente detalladas; la encriptación puede activarse por medio de una combinación de:

- **Correspondencias estructuradas de datos:** Como la presencia de información de la salud o financiera protegida, como códigos de HIPAA, códigos bancarios de identificación ABA, números de tarjeta de crédito y números de seguridad social detectados por el módulo Proofpoint Regulatory Compliance.
- **Correspondencias no estructuradas de datos:** Como la presencia de información confidencial detectada por el módulo Proofpoint Digital Asset Security.
- **Palabras clave y expresiones comunes** que aparecen en la línea de asunto o en el contenido de los mensajes según se definen en el módulo Proofpoint Content Compliance.
- **Origen o destino del mensaje:** Encriptación de mensajes en base a su destino (p. ej., un socio comercial o proveedor específico) o remitente. Los mensajes pueden encriptarse también basándose en otros atributos del mensaje como el tipo de archivos adjuntos.

Aplice políticas entrantes a los mensajes encriptados

Los correos electrónicos pueden también desencriptarse en la gateway, permitiendo la aplicación de políticas antispam, antivirus y de conformidad de contenidos al correo electrónico encriptado antes de su entrega a los usuarios finales, asegurando un correcto manejo del spam encriptado, malware y mensajes no conformes.

La simplicidad de IBE

El uso de Proofpoint de la tecnología IBE asegura la seguridad de las comunicaciones por correo electrónico encriptado, minimizando la carga para los usuarios finales.

Considere el caso de un doctor que necesita enviar a un paciente un mensaje que contiene información confidencial relativa a su salud. La operación se realiza de la siguiente manera:

- El doctor A redacta y envía un correo electrónico al paciente B utilizando el correo electrónico habitual de su cliente. El software o dispositivo Proofpoint analiza el mensaje y detecta la presencia de información confidencial relativa a la salud y clasifica el mensaje activando una política de encriptación.
- El paciente B recibe el correo electrónico encriptado y selecciona el archivo adjunto para autenticarse en el módulo Proofpoint Secure Messaging a través de SSL.
- El módulo Proofpoint Secure Messaging desencripta el mensaje y lo hospeda en la memoria del servidor para que el paciente B lo pueda revisar. Luego de que el paciente B accede al mensaje, éste es eliminado de la memoria.
- Al utilizar la funcionalidad de webmail del módulo Proofpoint Secure Messaging, el paciente B puede responder de forma segura al doctor A.

Otras opciones de encriptación

Además de proporcionar el módulo Proofpoint Messaging Security, Proofpoint se integra fácilmente con una cantidad de soluciones generalizadas de encriptación de terceros. Comuníquese con Proofpoint para obtener información actualizada sobre las soluciones de encriptación soportadas.

Conozca más acerca de Proofpoint Secure Messaging

Por mayor información sobre las características de encriptación basada en identidad de Proofpoint, descargue nuestro folleto gratuito, *Encryption Made Easy*, visitando:

<http://www.proofpoint.com/encryptionwp>