

EMAIL ENCRYPTION

Intercambio cifrado de correo electrónico para una comunicación fiable y segura por email.

Los correos electrónicos comerciales suelen contener contenidos internos de la empresa, personales u otro tipo de contenidos sensibles que pueden ser interceptados y espiados si no se protegen adecuadamente. Con Email Encryption, la información confidencial de la comunicación por correo electrónico se cifra de manera eficaz y segura.

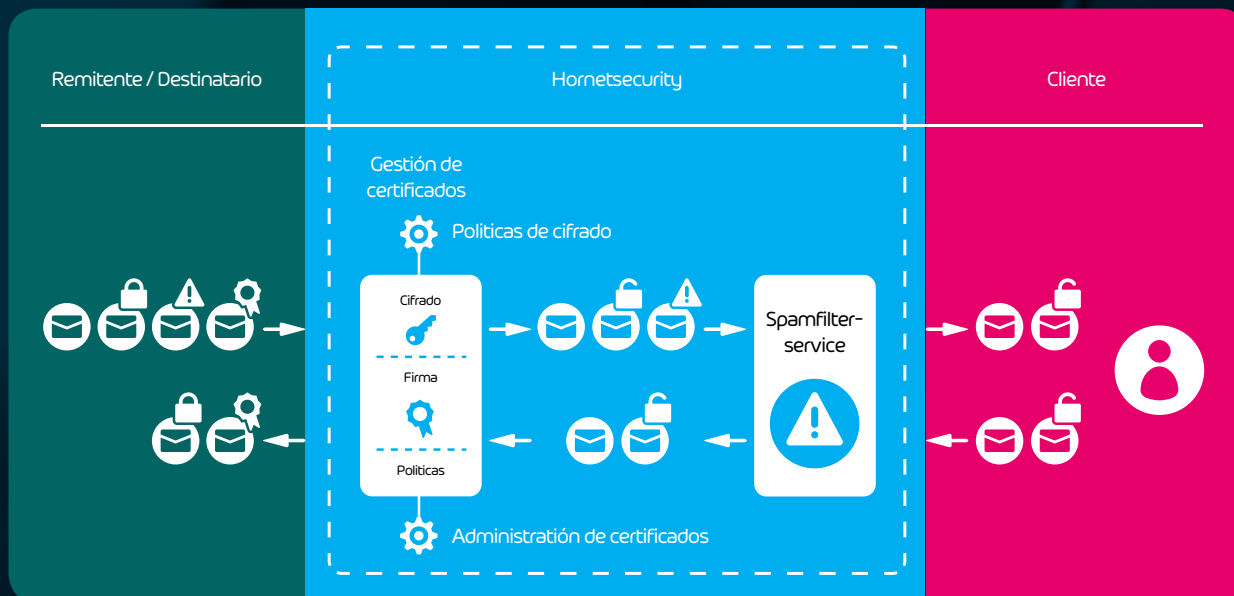
Protección contra:

Manipulación de mensajes de correo electrónico

Espionaje

Robo de información confidencial

INTEGRACIÓN DE EMAIL ENCRYPTION EN SISTEMA DE PROCESAMIENTO DE CORREOS



Email Encryption de Hornetsecurity se encarga de la gestión completa de los certificados.

Cifrado, descifrado y firmas automáticas y transparentes para correos electrónicos entrantes y salientes. Un requisito para garantizar la funcionalidad y eficiencia del cifrado de correo electrónico es la adquisición de Spam and Malware Protection.

AMPLIAS FUNCIONES PARA EL INTERCAMBIO SEGURO DE CORREOS ELECTRÓNICOS:

Firma digital automática y encriptación de correos electrónicos salientes mediante S/MIME y PGP: Protección de los correos electrónicos contra la modificación no autorizada o la lectura por parte de terceros durante su transmisión a través de redes públicas.

Gestión automática de certificados y almacenamiento de claves: Hornetsecurity se encarga de obtener e instalar los certificados necesarios. Estos se guardan en un almacén central de certificados.

Certificados de correo electrónico personal: Hornetsecurity utiliza certificados codificados de 2048 bits de una de las mayores y prestigiosas autoridades de certificación (CA). Cuando se encripta con S/MIME, cada usuario recibe su propio certificado. También se pueden importar y utilizar certificados suministrados por el cliente.

Descifrado automático de correos electrónicos entrantes: Si se dispone de la clave pública del remitente, los correos electrónicos se descifran automáticamente y se entregan al destinatario.

Configuración individual y definición de pautas de cifrado: En el panel de control puede definir los tipos de cifrado que desea utilizar para contactar con los socios de comunicación: TLS, S/MIME, PGP o Websafe. Puede aplicarse global o individualmente, para usuarios concretos, grupos o dominios. También puede definir cómo proceder si la clave de un destinatario no está disponible.

Opción de prueba de idoneidad de la encriptación: En el panel de control se puede comprobar qué opciones de cifrado tiene el interlocutor. Para ello, se introduce la dirección de correo electrónico del destinatario y luego se muestra qué tecnología de cifrado puede utilizarse en la comunicación con esa dirección.

Comunicación confidencial a través de Websafe: Aunque el interlocutor no pueda recibir correos electrónicos cifrados, se garantiza el cifrado y la confidencialidad de la comunicación por correo electrónico con determinadas personas.

ENCRIPCIÓN AUTOMÁTICA CON UNA MÍNIMA GESTIÓN:

Gestión de certificados de usuario: Pueden solicitarse, renovarse u obtenerse permanentemente nuevos certificados para los usuarios a través del panel de control (S/MIME Subscription).

Escalabilidad personalizada: Siempre es posible ajustar el número de usuarios de correo electrónico cifrado a las necesidades del cliente.

Actualización automática: Gracias al servicio de encriptación basado en la nube, las empresas siempre tienen a su disposición la última versión del servicio.