

Para las empresas, el riesgo de la pérdida de datos confidenciales por medio del correo electrónico, ya sea por descuido o con malicia, es muy alto. Las empresas consideran un desafío intercambiar de forma segura y sencilla el correo electrónico que contiene datos confidencial.

Si bien es posible cifrar y firmar el correo electrónico confidencial mediante los clientes de correo electrónico, los empleados deben saber de qué manera utilizar correctamente la solución de seguridad. Por lo tanto, la implementación constante de la política de seguridad de una empresa depende directamente del conocimiento y de la disciplina de cada empleado, lo que no es un enfoque práctico.

SafeGuard MailGateway de Sophos simplifica la seguridad del correo electrónico al integrar los procesos criptográficos asociados con el cifrado y descifrado, y también con las firmas electrónicas y la verificación, desde un punto central en una red corporativa. La solución de seguridad es completamente transparente para el remitente e implementa automáticamente las pautas de seguridad internas de la empresa para la comunicación por correo electrónico. Los remitentes y destinatarios pueden comunicarse por correo electrónico de forma usual sin tener que preocuparse por la confidencialidad del contenido.

SafeGuard MailGateway garantiza que:

- Los procesos existentes de flujo de trabajo basados en correo electrónico se complementan con la confidencialidad, la autenticidad y la integridad de una forma simple y segura.
- El cifrado de correo electrónico y las firmas digitales se implementan desde una ubicación central, lo que permite la aplicación constante de las pautas de seguridad para el cumplimiento de políticas y normas.
- El programa puede descifrar automáticamente los mensajes de correo electrónico entrantes y salientes de los destinatarios en la red de la empresa o cifrarlos para los destinatarios externos.

Para cifrar o descifrar mensajes de correo electrónico y generar firmas digitales, SafeGuard MailGateway utiliza los estándares establecidos de Internet S/MIME y OpenPGP.

Para los destinatarios que no cuentan con una infraestructura de seguridad de correo electrónico, la innovación SafeGuard PDFMail de Sophos encapsula automáticamente un mensaje de correo electrónico, junto con los archivos adjuntos, en un archivo PDF cifrado. Luego, el archivo PDF cifrado se envía en un mensaje de correo electrónico a su destinatario, de modo que se garantiza la transmisión segura de los datos confidenciales.

El destinatario sólo necesita un lector PDF convencional y la contraseña correspondiente para descifrar el documento PDF y leer el contenido confidencial del correo electrónico. Los archivos adjuntos incluidos en el documento PDF conservan su formato original (por ejemplo, .doc, .xls, .ppt) y se pueden extraer y modificar. Más adelante, el destinatario puede enviar una respuesta cifrada mediante la función de respuesta integrada, además de incluir archivos adjuntos en la respuesta.

Por otro lado, SafeGuard PrivateCrypto y SafeGuard WebMail también pueden usarse para asegurar que las conexiones entre los participantes externos de las comunicaciones sean seguras sin una infraestructura de seguridad.

SafeGuard MailGateway es escalable desde pequeñas instalaciones, pasando por instalaciones redundantes, hasta el uso empresarial en grupos.

Ventajas clave

Seguridad

- » Protección de datos valiosos, tanto personales como corporativos, que se envían por correo electrónico
- » Solución de seguridad central, completa y escalable para utilizar con infraestructuras de correo electrónico SMTP
- » Definición flexible y detallada del conjunto de reglas
- » Compatibilidad con S/MIME, OpenPGP, SafeGuard PrivateCrypto, SafeGuard WebMail y SafeGuard PDFMail (SafeGuard PDFMail, SafeGuard PrivateCrypto y SafeGuard WebMail son las soluciones para los participantes externos de la comunicación sin compatibilidad con S/MIME o OpenPGP)
- » Cifrado, descifrado y firma automáticos para correo electrónico
- » Generación automática de claves y certificados para S/MIME y OpenPGP
- » Servidor de claves integrado para S/MIME y OpenPGP
- » Seguridad del sistema integrada
- » Compatibilidad con servicios de directorio y servidores de claves

Beneficios

Seguridad mejorada

- Implementación centralizada de políticas de seguridad empresarial para el cifrado de correo electrónico y firmas digitales
- Definición flexible y granular de reglas de cifrado y firmas
- Compatibilidad con S/MIME, OpenPGP, SafeGuard PrivateCrypto, SafeGuard WebMail y SafeGuard PDFMail
- Entidad de certificación (CA) integrada para la generación automática de claves y certificados
- Permite el análisis de virus para los mensajes de correo electrónicos cifrados
- La extensión ideal para los sistemas ILP y CMF

Fácil de implementar

- Instalación rápida y puesta en funcionamiento a través del concepto de dispositivo de software
- Integración perfecta en infraestructuras PKI y de correo electrónico existentes
- Servidor de claves integrado para S/MIME y OpenPGP
- Integración de servicios de directorio empresariales, como Microsoft Active Directory
- Métodos alternativos para el cifrado de correo electrónico, sin la necesidad de una infraestructura de certificados
- Independencia respecto de los servidores de correo electrónico, como Lotus Notes, Microsoft Exchange, etc.
- Escalabilidad desde las instalaciones más pequeñas hasta el uso en clústeres para toda la empresa

Fácil de implementar

- Transparencia para el usuario final
- Interoperabilidad con los estándares de seguridad de correo electrónico, lo que contribuye a la gran aceptación por parte del usuario
- Conjunto de reglas y administración de claves centralizados para proteger el tráfico del correo electrónico
- Interfaz de administración conveniente, que se explica por sí misma
- Escalabilidad, migración y mantenimiento sencillos

Requisitos del sistema

Hardware

- » CPU Intel
- » Memoria RAM mínima de 512 MB
- » Discos duros IDE/SCSI/SATA
- » Unidad de CD-ROM IDE/SCSI/USB
- » Adaptador de red Ethernet

Funciones del sistema

Sistema operativo

- » CentOS
- » Compatibilidad con VMware

Instalación

- » Instalación completa desde CD-ROM

Administración

- » Administración web que incluye ayuda detallada en línea

Productos complementarios de SafeGuard®

- » SafeGuard PrivateCrypto
- » SafeGuard CryptoServer (módulo de seguridad de hardware)

Interfaces y formatos

- » SMTP(S), TLS, HTTP(S), SSH, SCP, FTP, NTP, SMNP
- » LDAP(S), OCSP, HKP
- » S/MIME, OpenPGP, SafeGuard PrivateCrypto, SafeGuard WebMail
- » X.509, PEM, DER, PKCS #7, PKCS #12, CRL
- » Claves OpenPGP, PGP/MIME, PGP/Inline

Estándares criptográficos

- » Cifrado asimétrico: RSA, DSA, El Gamal
- » Cifrado simétrico: RC2, RC4, DES, 3DES, Blowfish, Twofish, Cast5, AES, AES192, AES256
- » Hash: MD2, MD5, MDC2, SHA, SHA-1, RipeMD160

Idiomas disponibles

- » Español
- » Alemán

Para más información, visite www.sophos.com