

The risk of confidential data leaking via emails, whether inadvertently or maliciously, is very high for enterprises. Enterprises find it challenging to securely and easily exchange email containing confidential content.

Although it is possible to encrypt and sign confidential emails using email clients, employees must know how to use the security solution correctly. Consequently, the consistent implementation of a company's security policy depends directly on the knowledge and discipline of each individual employee—not a practical approach.

Sophos's SafeGuard MailGateway simplifies email security by integrating the cryptographic processes involved in encryption/decryption, and also in electronic signatures and verification, at one central point in the corporate network. The security solution is fully transparent to the sender and automatically implements the company's internal security guidelines for email communication. The senders and recipients can communicate via email in the usual way without having to worry about the confidentiality of the content.

SafeGuard MailGateway guarantees that:

- Existing email-based workflow processes are supplemented by confidentiality, authenticity and integrity in a simple and secure way
- Email encryption and digital signatures are implemented from a central location, which enables consistent enforcement of security guidelines for policy and regulatory compliance purposes
- The program can automatically decrypt incoming and outgoing emails for recipients in the company's own network or encrypt them for external recipients

To encrypt or decrypt emails and generate digital signatures, SafeGuard MailGateway uses the established S/MIME and OpenPGP Internet standards.

For recipients who do not have the email security infrastructure, the Sophos innovation SafeGuard PDFMail automatically encapsulates an email, along with its attachments, into an encrypted PDF file. The encrypted PDF file is then sent in an email to its recipient, thus securing the safe transmission of confidential information.

The recipient merely requires a conventional PDF reader and the corresponding password to decrypt the PDF document and to read the confidential contents of the email. The attachments contained in the PDF document retain their original format (e.g., .doc, .xls, .ppt) and can be extracted and modified. Afterward, the recipient can return an encrypted reply using the integrated reply function, as well as include attachments in his or her reply.

Alternatively, SafeGuard PrivateCrypto and SafeGuard WebMail can also be used to ensure that connections between external communications partners are secured without a security infrastructure.

SafeGuard MailGateway is scalable from small installations through redundant installations to organization-wide use in clusters.

Key benefits

Security

- » Protects valuable enterprise data and personal data in emails
- » Comprehensive scalable, central security solution for use in SMTP-based email infrastructures
- » Flexible and detailed definition of set of rules
- » Supports S/MIME, OpenPGP, SafeGuard PrivateCrypto, SafeGuard WebMail and SafeGuard PDFMail (SafeGuard PDFMail, SafeGuard PrivateCrypto and SafeGuard WebMail are the solutions for communication partners without S/MIME or OpenPGP support)
- » Automatic email encryption, decryption and signatures
- » Automatic key and certificate generation for S/MIME and OpenPGP
- » Integrated key server for S/MIME and OpenPGP
- » Integrated system security
- » Supports directory services and key servers

Benefits

Enhanced security

- Central implementation of company-wide security policy for email encryption and signatures
- Flexible and granular definition of encryption and signature rules
- Supports S/MIME, OpenPGP, SafeGuard PrivateCrypto, SafeGuard WebMail and SafeGuard PDFMail
- Integrated certification authority (CA) for automatic key and certificate generation
- Enables virus scanning for encrypted emails
- Ideal extension to ILP and CMF systems

Easy to deploy

- Quickly installed and brought into operation via software appliance concept
- Seamless integration in existing PKI and email infrastructures
- Integrated key server for S/MIME and OpenPGP
- Integration of Company Director Services like Microsoft Active Directory
- Alternative methods for email encryption without the need for a certificate infrastructure
- Independent of mail servers such as Lotus Notes, Microsoft Exchange, etc.
- Scalable from small installations to company-wide usage in clusters

Easy to use

- Transparent to the end user
- Interoperable with the standards for email security, leading to high user acceptance
- Central set of rules and key management for securing email traffic
- Self-explanatory and convenient administration interface
- Easy scalability, migration and maintenance

System requirements

Hardware

- » Intel CPU
- » Minimum 512 MB RAM
- » IDE/SCSI/SATA hard disks
- » IDE/SCSI/USB CD-ROM drive
- » Ethernet network adapter

System features

Operating system

- » CentOS
- » Support of VMware

Installation

- » Complete installation from CD-ROM

Management

- » Web management including detailed online help

Complementary SafeGuard® products

- » Safeguard PrivateCrypto
- » SafeGuard CryptoServer (hardware security module)

Interfaces and formats

- » 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
- » OpenPGP keys, PGP/MIME, PGP/Inline

Cryptographic standards

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

Language versions

- » English
- » German

For full details, visit www.sophos.com