Symantec® Encryption

Email Encryption

Overview

Email remains a fundamental communication channel for businesses, enabling efficient collaboration among employees. However, it is essential to acknowledge that the human element often poses the greatest security vulnerability. Inadvertently sending a file containing sensitive data can lead to detrimental consequences. The pressing question for organizations is whether users are diligently implementing measures to safeguard crucial information such as healthcare records, financial data, or strategic documents when transmitted through email.

A recent study by the Ponemon Institute revealed that within the past year, 60 percent of organizations encountered instances of data loss or unauthorized data transfer because of employee errors in email communication. Consequently, the IT department faces the formidable task of upholding the security of sensitive data, whether it is in transit, being utilized, or at rest.

This is where the Symantec® Encryption portfolio can provide a robust solution. Our encryption technology ensures the protection of sensitive data across its journey and storage, extending its coverage even to cloud-based email systems. With the Symantec Encryption portfolio, you can rest assured that your valuable information is shielded against potential breaches and mishandling.

Introducing Symantec Encryption

The Symantec Encryption portfolio offers versatile data protection through a variety of solutions, encompassing endpoint security, file and folder encryption, and email encryption. Furthermore, our portfolio boasts robust management capabilities, including individual and group key management, automated policy controls, and out-of-the-box compliance-based reporting. This document emphasizes the features of our email encryption products.

Benefits of Email Encryption

Preventing Accidental Data Leakage

Enabling Secure Business Collaboration

Ensuring Data Privacy Compliance

Delivering the Benefits of Email Encryption

Preventing Accidental Data Leakage

Symantec Desktop Email Encryption, which comes with the PGP® Encryption Suite, offers automated encryption, decryption, digital signing, and message verification in alignment with either individual or centrally managed policies. This encryption process takes place at the client level, ensuring that communications remain secure prior to traversing internal networks or being stored within cloud repositories.

For an alternative approach, Symantec Gateway Email Encryption, which is sold as a standalone product, enables the encryption of messages based on highly customizable encryption rules, eliminating the need for client-side software installation. Furthermore, the combination of Gateway Email Encryption with Symantec Messaging Gateway allows users to harness the synergy of PGP encryption alongside Symantec's premier anti-virus, malware, and spam filtering. This integration serves to bolster the security of email communications, safeguarding against external threats.

Enabling Secure Business Collaboration

Symantec Gateway Email Encryption facilitates the secure exchange of sensitive data outside an organization, eliminating the necessity for software installation or key exchange for encryption purposes. This secure exchange of data is achieved through a feature called Web Email Protection, which provides a secure web inbox hosted on the gateway server. Users can transmit secure content to recipients even if they lack PGP software. Copies of these messages are securely stored as PDFs on the gateway server. External recipients can enroll with the solution, granting them access to these emails through popular Internet browsers such as Chrome or Firefox.

Ensuring Data Privacy Compliance

As the implications of inadvertent and deliberate data leaks through email have become increasingly apparent, regulatory bodies and auditors are directing organizations to monitor and fortify email communications that involve sensitive data. Symantec Email Encryption not only safeguards email communications, but it also incorporates a FIPS 140-2 validated cryptographic module. This module aids customers in adhering to a spectrum of government and industry mandates, including CDM, PCI DSS, HIPAA, and GDPR.

Moreover, the fusion of Symantec Data Loss Prevention with Symantec email encryption solutions offers organizations an added layer of security in compliance with privacy regulations. Outbound email messages are cross-referenced against DLP policies. Should a message contain sensitive data, it can be rerouted to Symantec Gateway Email Encryption before transmission. This strategic integration also provides a comprehensive audit trail, invaluable for compliance auditing purposes.

Why Symantec Encryption?

- **Flexible delivery options** – Centralized management organizes keys and policies per user or group from a single web-based console, synchronizing them with Active Directory.
- **Interoperability** – Seamlessly integrates with existing standards-based email encryption solutions such as OpenPGP and S/MIME; supporting POP, IMAP, MAPI, and SMTP protocols; and ensuring compatibility with macOS and Microsoft Windows platforms.
- **Broader portfolio** – Capitalize on the most extensive encryption portfolio available in the market. Extend protection to other communication channels with solutions that include endpoint security, and file and folder encryption.

EMA-ENC-OT101 January 9, 2024