proofpoint

PROOFPOINT ENCRYPTION

TECHNICAL DETAILS

Cryptographic Algorithms:

- Message Encryption: AES (256 bit)
- Digital Signature: ECDSA

Interfaces:

- Secure Reader Web Interface:
- Accessed via HTTPS

PROOFPOINT ENTERPRISE PRIVACY SUITE COMPONENTS

The following comprehensive data loss prevention components areoffered through the Proofpoint

Enterprise Privacy Suite:

- **Proofpoint Email Firewall™**

Detects sensitive information in message content and subject line

- **Proofpoint Regulatory Compliance™**

Detects protected information, including financial, healthcare, and other "smart identifiers"

- **Proofpoint Digital Asset Security™**

Detects presence of confidential information through advanced document fingerprinting

- **Proofpoint Encryption**

Automatically applies encryption based on an organisation's policies

SAAS-POWERED, POLICY-BASED EMAIL ENCRYPTION

Proofpoint Encryption™ offers powerful, policy-driven encryption features that mitigate the risks associated with regulatory violations, data loss and corporate policy violations, while positively enabling critical business communications. Proofpoint Encryption is ideal for any organisation that needs to protect sensitive data, while still making it readily available to appropriate affiliates, business partners and end users—on their desktops and mobile devices.

SOLVING EMAIL COMPLIANCE CHALLENGES

As email is the preferred medium for business communications, preventing confidential information from being leaked in outbound email messages must be a top priority in order to lower the risk of a data breach. Additionally, the number of government and industry regulations focused on data protection is on the rise, with federal laws such as HIPAA, SOX and GLBA; security standards such as PCI-DSS; and state laws such as Massachusetts 201 CMR 17. Most of these regulations mandate that enterprises protect private data through technologies such as encryption. Proofpoint Encryption meets these mandates with the industry's most powerful and flexible solution for policy-driven email encryption.

Proofpoint Encryption	
Feature	**Benefit**
Policy-based encryption	Encryption is automatically applied, based on an organisation's policies. Compliance, data loss prevention and content security policies are consistently and accurately applied. Internal-to-internal encryption is available with the desktop plug-in.
Streamlined storage	Key management, backup and administration burdens are eliminated through the Proofpoint Key Service, providing secure, cost-efficient, highly available and fully redundant key storage facilities.
Granular control	Provides granular message control by allowing expiration of encrypted messages and the ability to revoke any individual message to any one specific individual.
Secure messaging made simple	Makes ad hoc, secure communication just as easy as traditional, non-encrypted messaging. Recipients can easily view their encrypted email through the Secure Reader, an easy-to-use, customisable web-based interface.
Decrypt Assist	One-step encrypted email delivery for mobile, laptop, and desktop users.

PROOFPOINT ENCRYPTION: KEY TO SUCCESS

Training users in the proper use of encryption systems can be a significant barrier to successful deployment of traditional secure messaging solutions, but with Proofpoint Encryption, this process is much simpler. Proofpoint's email encryption solution automatically and dynamically applies encryption or decryption based on an organisation's policies. As a result, users don't need to take any special actions to take advantage of encryption features.

Simple to administer with no loss of control

Unlike alternative approaches to encryption, Proofpoint Encryption provides effective data protection without the administrative burdens and infrastructure costs typically associated with secure messaging.

- Easy policy management: All encryption policies are centrally managed and enforced at the gateway. A convenient graphical interface is provided for defining encryption policies, which can be triggered by messages containing regulated information or intellectual property.
- Simplified key management: Proofpoint Encryption eliminates the administrative overhead of key management by including the Proofpoint Key Service™. As keys are generated by Proofpoint Encryption, they are securely stored, managed and made highly available via Proofpoint's cloud computing infrastructure. Administrators can also choose to enable end user key management, providing end users with the ability to revoke, expire, or restore access to encrypted email messages.
- Message expiration and revocation: Administrators maintain complete control over encrypted messages. All messages can be set with specific expiration based on policy. In addition, an individual message to a specific recipient can be revoked without affecting other users or other messages to the same recipient.

Easy to Use

Proofpoint Encryption operates transparently to end users without requiring software downloads or installation and maintenance of desktop or mobile encryption clients. Proofpoint's encryption solution automatically encrypts and decrypts sensitive content as required, without end users having to use and manage complicated digital certificates or encryption keys. Furthermore, multiple authentication sources can be supported.

ENTERPRISE POLICY ENFORCEMENT

As with Proofpoint's threat protection and content security features, secure messaging policies are managed and enforced on an enterprise level from a single location. Once defined, enterprise encryption policies for compliance and content security are applied automatically, consistently and accurately, eliminating the risk of user error.

- Granular Control of Encryption Policies

Proofpoint Encryption enables extremely granular, per-message control over encrypted messages and policies. Encryption can be triggered by any combination of the following parameters:

- Deep content analysis: Regulated information—such as protected health information (PHI), non-public information (NPI), etc. – or confidential information through advanced document fingerprinting—with both full and partial matching capabilities.
- Message origin or destination: Messages can be encrypted based on destination, such as a specific business partner or supplier, on sender or on message attributes, such as attachment type.
- TLS fallback to Proofpoint Encryption: Messages are delivered with a TLS connection but will fallback to deliver messages securely with Proofpoint Encryption should the TLS connection fail.

Apply Inbound Policies to Encrypted Messages

Email can also be decrypted at the gateway, allowing Proofpoint's threat protection and content compliance policies to be applied to encrypted email before it is delivered to end users and ensuring that spam, malware and noncompliant messages are properly handled.