

# Proofpoint Encryption



Proofpoint Encryption™ makes ad hoc, secure communication just as easy as traditional, non-encrypted messaging. Proofpoint's powerful, policy-driven encryption features mitigate the risks associated with regulatory violations, data loss and corporate policy violations, without adversely impacting business operations. Proofpoint Encryption is ideal for any organization that need to protect sensitive data, while still making it readily available to appropriate affiliates, business partners and end users.

## overview

As email has become the preferred medium for business communications, organizations have become increasingly concerned about ensuring the security of individual messages. Email is commonly used to transmit sensitive or confidential information—including operational data, trade secrets, legal documents, financial information, and personal healthcare and identity information—both inside and outside the enterprise.

The need to secure this confidential information—and comply with a growing body of regulations that govern the transmission of private data—have made policy-based email encryption a “must have” feature of a complete messaging security solution. Proofpoint Encryption meets these requirements with the industry's most powerful and flexible solution for policy-driven email encryption.

## features

### Policy-driven email encryption

Training end users in the proper use of encryption systems can be a significant barrier to successful deployment of traditional secure messaging solutions. But Proofpoint Encryption is much easier to use and manage. Proofpoint's secure messaging solution automatically and dynamically applies encryption or decryption based on your organization's policies, right at the gateway. As a result, end users don't need to take any special actions to take advantage of encryption features and your compliance and content security policies are consistently and accurately applied on an as-needed basis.

### Easy to administer

Unlike alternative approaches to encryption, Proofpoint's email encryption solution provides effective protection for sensitive information without the administrative burdens and infrastructure costs typically associated with secure messaging.

- **Easy policy management:** All encryption policies—whether they are driven by regulatory compliance, data security or internal corporate concerns—are centrally managed and enforced at the gateway. The Proofpoint Messaging Security Console™ provides a convenient graphical interface for defining encryption policies, which can be triggered based on message content identified by Proofpoint Regulatory Compliance™, Proofpoint Content Compliance™ or Proofpoint Digital Asset Security™.
- **Simplified key and certificate management:** Proofpoint Encryption eliminates the administrative overhead associated with traditional encryption systems. Using Proofpoint Encryption technology, keys are generated locally by each unique customer instance of Proofpoint, whether deployed on-premises or in the Proofpoint on Demand datacenters.
- **Minimal data storage and archive requirements:** Proofpoint Encryption simplifies the storage and backup overhead that is typically associated with message encryption. The Proofpoint Hosted Key Service™ handles all key management functions, using the Proofpoint on Demand SaaS infrastructure.



### Email Encryption Powered by Proofpoint's Next-generation SaaS Architecture

Proofpoint Encryption eliminates the administrative overhead of key management by including the Proofpoint Hosted Key Service.

As unique keys generated by Proofpoint Encryption, they are stored, backed up and made highly available via Proofpoint's cloud computing infrastructure. The Proofpoint Hosted Key Service eliminates the need for customers to manage their own encryption keys and certificates.

### How does the Proofpoint Hosted Key Service work?

For each email encrypted, the customer's unique instance of Proofpoint Encryption generates an encryption key that is used to encrypt the message. The encrypted message is then sent to the recipient. Simultaneously, the encryption key itself is sent to the Proofpoint Hosted Key Service.

When the recipient is ready to decrypt the message, a secure https request is made to the unique customer instance of Proofpoint Encryption for authentication. Once the recipient is authenticated, the customer instance requests the appropriate key from the Proofpoint Hosted Key Service, allowing the recipient to decrypt their message.

This architecture allows for comprehensive, ad-hoc secure messaging while eliminating the need for customers to manage their own encryption and decryption keys.

# Proofpoint Encryption

## features (continued)

### Easy to use

Proofpoint Encryption operates transparently to end users without requiring software downloads or the installation and maintenance of desktop 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.

### Low total cost-of-ownership

Proofpoint Encryption seamlessly interfaces with other Proofpoint DLP features including Proofpoint Regulatory Compliance and Proofpoint Digital Asset Security. Easy deployment and minimal ongoing management requirements greatly reduce the ongoing costs associated with managing your secure messaging solution. And Proofpoint's unparalleled ease-of-use for end users minimizes support, training and helpdesk costs.

## powerful, secure messaging policy enforcement

### Extremely granular control of encryption policies

As with Proofpoint's anti-spam, anti-virus and content security features, secure messaging policies are managed and enforced on an enterprise level from a single location, using the Proofpoint Messaging Security Console. Once defined, enterprise encryption policies are applied automatically at the gateway, eliminating the risk of user error.

The combination of Proofpoint Encryption and the Proofpoint Hosted Key Service enables extremely granular, per-message control over encrypted messages. For example, an individual message to a specific recipient can be revoked without affecting other users or other messages to the same recipient.

Message encryption policies can be extremely granular as well. Encryption can be triggered by any combination of:

- **Structured data matches:** Such as the presence of protected healthcare or financial information such as HIPAA codes, ABA routing numbers, domestic and international credit card numbers, US social security numbers, UK National Identity Card numbers and other "smart identifiers" as detected by Proofpoint Regulatory Compliance.
- **Unstructured data matches:** Such as the presence of confidential information as detected by Proofpoint Digital Asset Security.
- **Keywords and regular expressions** found in the subject line or content of messages as defined in Proofpoint's email firewall.
- **Message origin or destination:** Encrypt messages based on destination (e.g., a specific business partner or supplier) or sender. Messages can also be encrypted based on other message attributes such as attachment type.

### Apply inbound policies to encrypted messages

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

### Email Encryption: Simplified

Proofpoint Encryption ensures the security of sensitive email communications while minimizing the burden on end users.

Consider the case of a doctor who needs to send a message—containing confidential healthcare information—to a patient. The transaction works as follows:

- Doctor A writes and sends an email to Patient B using their regular email client. Proofpoint's data loss prevention features analyze the message and detect the presence of confidential healthcare information, triggering an encryption policy.
- Proofpoint Encryption encrypts the message using an AES-256 cipher and digitally signs the message with a DSA signature for authentication purposes before it is emailed to the recipient.
- Patient B receives the encrypted email and clicks the attachment to authenticate themselves and decrypt the message using the Proofpoint Secure Reader, a web-based application hosted within the customer's own instance of the Proofpoint on Demand service or on the customer's own Proofpoint appliance.
- Patient B is required to authenticate themselves to the Proofpoint Proofpoint Secure Reader. Upon authentication, Proofpoint Encryption requests the appropriate encryption/decryption key from the Proofpoint Hosted Key Service and decrypts the message.
- Using the Proofpoint Secure Reader, Patient B can securely reply to Doctor A.

### Additional Encryption Options

In addition to providing the Proofpoint Encryption module, Proofpoint easily integrates with a variety of popular third-party encryption solutions. Contact Proofpoint for up-to-date information about supported encryption solutions.

©2009 Proofpoint, Inc. Proofpoint Protection Server is a registered trademark of Proofpoint, Inc. in the United States and other countries. Proofpoint, Proofpoint Messaging Security Gateway, Proofpoint Content Compliance, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint Encryption and Proofpoint MLX are trademarks of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are the property of their respective owners. 09/09

