

Protecting Enterprise Data with Proofpoint Encryption



Email Encryption Whitepaper:
Proofpoint Encryption 

More than ever before, enterprises are under pressure to protect private data.

Part of the pressure comes from the chilling examples of companies who failed to protect private data and then paid a high price in regulatory fines, disaffected customers, lost business, and damaged brands.

Part of the pressure comes from knowing just how frequently data breaches occur. In a recent survey of email decision makers at large U.S. companies, 34% reported that their business had been affected by the leak of sensitive or embarrassing information in the past year, 33% had been affected by the improper exposure or theft of customer information, and 28% had been affected by the improper exposure or theft of intellectual property. Thefts are common. Leaks are common. Enterprises, even cautious ones, are plainly at risk.

Proofpoint Encryption can help keep private data in email secure.

Contents

- Introduction.....1**
- Data Loss Prevention and Encryption.....1**
 - Data Loss Prevention1
 - Encryption2
- The Challenge of Implementing Encryption in the Enterprise2**
 - Applying Encryption2
 - Managing Encryption Keys3
- Proofpoint Encryption: SaaS-powered, Policy-based Email Encryption5**
 - Overview.....5
 - Flexible and Secure Policy-based Encryption.....5
 - Optimizing Secure Email Delivery on a Case by Case Basis6
 - A Closer Look at Proofpoint Encryption’s Push Delivery Service7
 - Making Key Management Easier than Ever Before.....9
- Conclusion11**
- For Further Reading11**
- About Proofpoint, Inc.12**

Introduction

More than ever before, enterprises are under pressure to protect private data.

Part of the pressure comes from the chilling examples of companies who failed to protect private data and then paid a high price in regulatory fines, disaffected customers, lost business, and damaged brands.

Part of the pressure comes from knowing just how frequently data breaches occur. In a recent survey of email decision makers at large U.S. companies, 34% reported that their business had been affected by the leak of sensitive or embarrassing information in the past year, 33% had been affected by the improper exposure or theft of customer information, and 28% had been affected by the improper exposure or theft of intellectual property.¹ Thefts are common. Leaks are common. Enterprises, even cautious ones, are plainly at risk.

Adding to the pressure are a growing number of government and industry regulations focused on data security. These regulations include federal laws such as SOX and GLBA, state laws such as Massachusetts 201 CMR 17, and security standards such as PCI which have been developed by industry consortia. The regulations also include the European Union's Data Protection Directive, as well as national data privacy acts enacted in the U.K., Canada, Japan, and elsewhere. Most of these regulations, whether at the regional or national level, require enterprises to protect private data through technologies such as encryption and access control. Many regulations also require enterprises to notify the public when data security breaches occur.

While data privacy laws are multiplying, older laws are being revised to become more comprehensive and strict. For example, provisions in the American Recovery and Reinvestment Act (ARRA) of 2009 increase the fines for data privacy violations under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Penalties can now reach an astounding \$1.5 million. The new ARRA provisions also give HIPAA investigators a powerful incentive for levying fines in the first place: fine proceeds go straight into the investigators' own budgets. The ARRA provisions also broaden the scope of HIPAA data privacy laws to cover not just health care organizations (HCOs), but also business partners of HCOs. If a law firm, accounting firm, or IT consultancy does work with an HCO, it's now covered by HIPAA privacy regulations and subject to HIPAA penalties for compliance failures.

Of course, protecting private data is also a best practice—an obvious choice to many CSOs and IT managers. Taking a proactive approach to data security is second nature to most IT professionals today.

But even if undertaken as second nature, the task of securing networks and enterprise data increasingly carries the strain of high risk, high costs, and a margin of error that is close to nil. In a world where a dangerous Trojan can infect a corporate network from a single data stick, where organized crime is more intent than ever to exploit all means—including theft and bribery—to gain access to private data, and where workers can accidentally divulge millions of private customer records simply by mistyping an email address, the task of keeping enterprise data and communications secure might feel to some IT managers like a never-ending, perilous performance on the high wire.

Data Loss Prevention and Encryption

To protect private data, security officers, compliance officers, and IT managers have several major technologies at their disposal. Two of the most important are Data Loss Prevention (DLP) solutions and encryption.

Data Loss Prevention

To prevent private data from leaving a corporate network through messaging applications such as email, DLP solutions scan traffic on enterprise networks, looking for private data in transit. Upon discovering private data (by matching keywords, phrases, hashes, or some other pattern), a DLP solution takes action. It can either block the data from leaving the network entirely

¹ *Outbound Email and Data Loss Prevention in Today's Enterprise, 2009*. Research conducted by Osterman Research and published by Proofpoint. Available at www.proofpoint.com/outbound.

or encrypt the data so that it leaves in secure format that only the intended recipients can access.

DLP products and services dramatically reduce the risk of customer records, business plans, financial reports, product blueprints, or other sensitive data ever ending up in the hands of competitors, hackers, or identity theft criminals. No wonder, then, that the enterprise adoption of DLP technology is expected to rocket from 33% to 80% in the next two years.² Businesses in every industry now recognize DLP as an essential security tool for data privacy.

Encryption

Encryption is an essential component of DLP. Without encryption, a DLP solution's only means of protecting private data in transit would be to block it entirely. But blocking all traffic—including email and FTP transfers—carrying private information is an unworkable solution in today's hyperconnected world. Email remains the dominant channel for business communications.³ It's inevitable that at least some business email will carry sensitive data. Sensitive business email must get through.

It can get through, if it's encrypted. Encryption is what makes DLP and secure messaging viable for businesses today. Encryption ensures that even if a sensitive message is intercepted by a malicious party, the message's contents will remain unreadable and hence untampered with. (The recipient will discover any tampering when he or she tries to decrypt the message.) Thanks to encryption, a recipient can be certain that the message received is the very same confidential message originally transmitted by the sender.

The Challenge of Implementing Encryption in the Enterprise

Encryption may be an essential technology for protecting data both inside and outside the network perimeter, but implementing encryption effectively in a large enterprise is no easy task. Security officers and IT organizations face significant challenges when it comes to enabling all business users in an organization to easily and reliably send encrypted email.

The first major challenge of implementing encryption involves the question of what gets encrypted and by whom.

Applying Encryption

Enterprise email carries both private data and non-private data. How should enterprises go about protecting the private data?

One approach would be to simply encrypt all outbound email to ensure that outbound email containing private data is protected.

But deploying a monolithic, one-size-fits-all solution that encrypts all data leaving the WAN is simply not practical. Encrypting absolutely every outbound communication degrades network performance, consumes computing resources, and makes business data harder to find and to use.

Once encrypted, data becomes inscrutable to network monitoring tools; the more network traffic that's encrypted, the less network traffic can be optimized for performance using protocol optimization and other optimization techniques. Network optimization is especially important for traffic to and from branch offices and passing through a server, such as an email server, located in a central data center.

Universal encryption also unnecessarily inflates IT costs. It requires more CPU power, for example, because messaging servers will likely end up encrypting extra terabytes or even petabytes of data every few weeks or months.

Universal encryption also makes it harder for users to find and manage non-private data, much of which ends up being stored indefinitely in email inboxes and other folders.

2 "Data leakage prevention going mainstream," Andreas M. Antonopoulos, Network World, September 1, 2009. DLP adoption statistics from Nemertes Research.

3 See *The Critical Need for Encrypted Email and Secure File Transfer Solutions*, Osterman Research, July 2009.

Finally, the numbers simply don't support such a monolithic approach. A recent survey of enterprise IT staff found that as much as 20% of outbound email messages may contain sensitive information, such as confidential customer data, health records, or patent information. Encrypting that sensitive 20% is essential; encrypting the remaining 80% is wasteful.⁴

An alternative approach is to count on users to consistently recognize sensitive data and to use special tools or procedures to encrypt it. This approach is risky.

In their busy workdays, users are unlikely to remember every security rule and data classification. If they're rushed or tired, they're also unlikely to consistently take the extra steps needed for encrypting or flagging sensitive content. In many cases, users will not even realize that the data they're transmitting requires encryption; they'll simply click "Send" and consider the matter settled.

Encrypting data automatically and selectively is the best choice.

The same scanning technology used for DLP solutions can be applied to email to ensure that messages carrying sensitive data are always encrypted and safe. To trigger encryption, IT managers and security officers define policies based on message content (such as keywords, phrases, identifiers such as Social Security numbers, and so on), as well as the identities of the sender and the recipient.

This policy-based approach to encryption avoids the ballooning IT costs associated with universal encryption, because it encrypts only that data that has been scanned and determined to be sensitive. With this approach, CSOs and others can rest assured that all data is detected and protected, without relying on end users infallibly recognizing and encrypting private data. Additionally, non-private data remains readily accessible to users, who can read it easily in their email inboxes and folders. The end result: better security, optimal network performance, and minimal impact on the daily work of employees.

Ultimately, the use of automated, policy-based encryption becomes a business enabler.

Policy-based encryption reliably protects private data as it flows among employees, partners, and customers, while minimizing operational overhead and the risk of regulatory fines, public censure, and customer turn-over.

Since policy-based encryption and DLP both involve scanning email and taking appropriate action on individual messages, it makes sense to coordinate, and possibly integrate, both applications.

Email encryption and DLP functions should work together to apply the same policies and protect private data, whether that data is traveling in an email message, a Webmail message, or content intended for a tweet or blog post.

Managing Encryption Keys

Even if an automated, DLP-style approach to encryption answers the question how and when encryption is performed, a second, equally daunting challenge remains: how to manage the keys used for encryption.

A key is a piece of information that determines the output of a cryptographic algorithm or cipher.⁵ Encryption software uses a key whenever it encrypts or decrypts information.

Encryption keys need to be issued, applied, and stored; occasionally, they may need to be revoked (for example, if an employee changes roles or leaves the company). Keys need to be backed-up and continuously available, since without its key a piece of encrypted content can never be decrypted and recovered.

An IT organization may decide to assign each user his or her own key for encryption, or the IT organization may decide to configure email software to encrypt each message with a unique

4 *Outbound Email and Data Loss Prevention in Today's Enterprise, 2009.* Research conducted by Osterman Research and published by Proofpoint. Available at <http://www.proofpoint.com/outbound>

5 Wikipedia entry for Key (cryptography).

key. (Typically, enterprises don't allow groups of users, such as departments, to share keys, because a shared key might give too many people access to a confidential message, and it makes the process of revoking keys especially cumbersome—suddenly the messages and files of many people become unreadable.)

Many IT organizations choose to encrypt each message with a unique key, so that they can manage email security on a message-by-message basis. Because users send so much email, this approach leads to IT organizations having to track and store tens, hundreds, or even thousands of keys for each user and perhaps as many as a million keys across the entire organization. In enterprises where thousands of users are sending tens or even hundreds of email messages every day, the number of keys required for email encryption grows at an astonishing rate.

How should enterprises go about managing all these keys?

One solution for managing keys is to distribute encrypted data through a secure, pull-based Webmail system.

This type of system offers users an authenticated, Webmail interface for uploading and downloading private messages. Senders log into the interface to upload and send private content. When a message is sent, the recipient receives an unencrypted notification that a new encrypted message has arrived. Clicking on a link in the notification redirects the recipient to a special Webmail page for authentication. The recipient logs in and retrieves the message. Each message (along with the key used to encrypt it) is stored on the secure Webmail server, rather than in a local folder. Because the key is stored centrally, IT organizations are spared the work of distributing keys to users or installing keys on desktops. Through centralization, therefore, Webmail systems simplify key management.

But the remote storage of high volumes of email content makes most secure Webmail services problematic. To minimize storage costs, most Webmail applications severely limit how long messages can be stored on their servers. Many of these applications automatically delete messages after a number of weeks or months. To preserve business-critical content, users may be forced to manually download content from the secure server to a local folder—a time-consuming and unproductive task. Ironically, downloading content this way may risk exposing the very data the Webmail application was meant to protect.

Another problem with secure Webmail applications is that they force users to continually move back and forth between their standard email clients and the Webmail interface. Email conversations may be fragmented across both applications, making it difficult for users to later find the information they're looking for. In addition, the burden of working with two different email interfaces may tempt some users to work around the encryption service altogether, sending data surreptitiously through their desktop client or through a third-party Webmail client such as Gmail, which can be more easily integrated with the desktop client.

To avoid the problems with secure Webmail servers, an enterprise may decide to give its users special desktop clients for sending and receiving secure email.

This approach offers users the benefit of being able to store encrypted content locally and hence indefinitely. A user will never spend time hunting for a message, only to discover that it expired on the secure Webmail server two days earlier.

But in most organizations, old habits die hard, and new mandates about special tools usually fizzle out. Forcing special client software on users rarely works in the long term. Users want to keep using the desktop tools they are most familiar with—for enterprise email, this means clients such as Outlook and Notes. After a while, users abandon the new special-purpose client and return to using their old, familiar client for all work.

And if an enterprise's own employees are reluctant to adopt a new tool, how much more reluctant will outsiders be. Business partners, customers, and especially prospects might wonder why they should have to install special software simply to communicate with one company. Their respective IT organizations will likely resent the imposition of a new software application on the desktop systems they closely control. Feeling hassled, many recipients may choose to simply ignore the encrypted messages directed at their inboxes.

Eventually, any enterprise trying to force new desktop software on other organizations will have to face facts and adopt an encryption solution that works the desktop tools its community members already have.

The optimal approach for email encryption would let users keep using the email clients they already know and like, while allowing enterprises to store business data indefinitely and to manage encryption keys in a convenient, reliable, and scalable way.

Building on its extensive experience with email security, email archiving, and DLP, Proofpoint is addressing the challenge of encrypted email and DLP with the Proofpoint Encryption™ solution and the Proofpoint Hosted Key Service™.

Proofpoint Encryption: SaaS-powered, Policy-based Email Encryption

Overview

Proofpoint Encryption is a complete enterprise-class solution for encrypting private email while simplifying encryption key management. Enterprises can use Proofpoint Encryption—available as part of the Proofpoint ENTERPRISE™ Privacy solution—to automatically:

- Discover and encrypt email messages carrying private information or other data that needs to be sent in encrypted form, based on customizable policies.
- Enforce detailed policies about how private data and encrypted messages should be handled.
- Alert security officers, compliance officers, and IT managers to potential data leaks and other email security threats.

Proofpoint Encryption provides complete security for email traffic, while avoiding the overhead of custom desktop clients or time-consuming procedures for managing keys. End users and IT staff all benefit from Proofpoint Encryption's intelligent analysis and secure messaging services.

Flexible and Secure Policy-based Encryption

Proofpoint Encryption is available as part of Proofpoint's SaaS, appliance, or software email security platforms. Regardless of how it is deployed, the solution can be up and running within minutes.

Proofpoint Encryption offers security officers, compliance officers, IT managers, and email administrators an easy-to-use dashboard for defining security policies that govern the encryption of email. Policies can trigger encryption based on:

- Message content (whether in the body of the email or in an attachment)
- User ID (sender or recipient)
- Group ID (sender or recipient)
- Domain (sender or recipient)

When used as part of Proofpoint's data loss prevention suite, Proofpoint Encryption can take action on messages by applying sophisticated data analysis techniques that ensure the comprehensive discovery of private data, while minimizing false-positive identifications that might trigger encryption when it's not strictly required. To identify private data, Proofpoint Encryption can use any combination of:

- Pre-defined dictionaries selected by the administrator. Proofpoint offers industry-specific dictionaries to simplify the configuration of Proofpoint Encryption for specific industries, such as healthcare and financial services.
- Custom dictionaries of terms and phrases defined by the customer.
- Smart Identifiers, which detect patterns of data warranting protection, while minimizing false positives. For example, Proofpoint's smart identifiers can distinguish Social Security

numbers from other nine-digit numbers, and credit card numbers from other 16-digit long strings.

Proofpoint supports a broad range of data loss prevention actions that can be triggered by policies. These actions include:

- Encrypting a message
- Redirecting a message
- Blocking a message
- Quarantining a message for review by security or IT staff
- Adding an X-header to a message
- Annotating a message

Proofpoint Encryption also allows administrators to define User Response Profiles, which grant specific message-response privileges to a group of users. For example, to prevent users from forwarding encrypted messages, an administrator can define a User Response Profile for that group, denying them the ability to forward messages, while granting them the ability to reply to messages.

The Proofpoint Encryption administration toolset also includes monitoring and reporting tools so administrators can discover any potential issues related to email encryption and user behavior. Using these tools, administrators can generate reports to demonstrate compliance with HIPAA and other regulations that mandate the use of encryption technology.

The branding of the Proofpoint Encryption user interface can be customized at any level—system-wide, at the group or department level, or even at the level of a specific user. Configuring an interface is as easy as customizing a template within the Proofpoint administrative interface. No HTML programming is required to change the look and graphical style of pages. Through these highly configurable templates, the Proofpoint solution can be easily integrated with business portals and IT management tools.

Proofpoint Encryption's policy-driven security spares employees the trouble of memorizing complex security rules or learning how to use special desktop clients. By automating policy enforcement and providing security officers and IT staff with fine-grained controls over email encryption, Proofpoint Encryption dramatically reduces the risk of security lapses and data leakage.

Optimizing Secure Email Delivery on a Case by Case Basis

Proofpoint customers have broad latitude in crafting the policies that Proofpoint solutions should take when managing email messages. For industries such as healthcare and financial services, Proofpoint offers pre-configured policies designed to help customers quickly configure their email security solution for specific industry regulations such as HIPAA, GLBA or PCI. But in all cases, email administrators can define whatever policies best make sense for their organization.

To get a sense of the flexibility of the Proofpoint solution, consider these typical email policies for protecting private data.

Upon detecting private content in an email message, the Proofpoint platform can take a wide variety of actions, depending upon an organization's unique policies, including the following:

If the message is being sent to an inappropriate recipient (e.g., a competitor or a suspicious domain in a foreign country), the Proofpoint service or appliance can block the message entirely. Optionally, it can also return an error message to the user, send an alert to an administrator, or take any combination of similar actions. Most importantly, sensitive information is intercepted and blocked at the email gateway before it leaves the network perimeter.

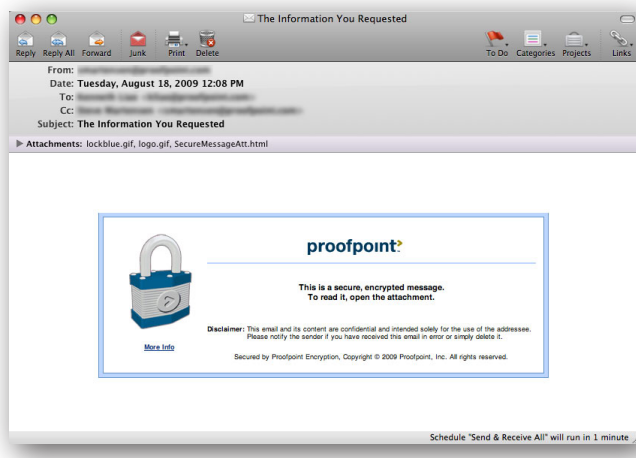
If the message is going to a branch office or partner site also configured with Proofpoint email solutions, the Proofpoint platform can be configured to use TLS to encrypt the messages for secure transmission between sites. The sender and the recipient both use their email clients normally, while Proofpoint Encryption works "behind the scenes" to encrypt, transmit, and decrypt the message, once it has passed safely through any public or insecure networks.

If the message is going to a recipient whose domain is not configured with Proofpoint Encryption, Proofpoint Encryption converts the message to a secure HTML document, which is pushed to the recipient's desktop. The recipient receives a message with an encrypted attachment. Upon opening the attachment, the recipient is presented with a Web form for authenticating to a Proofpoint Encryption server.

A Closer Look at Proofpoint Encryption's Push Delivery Service

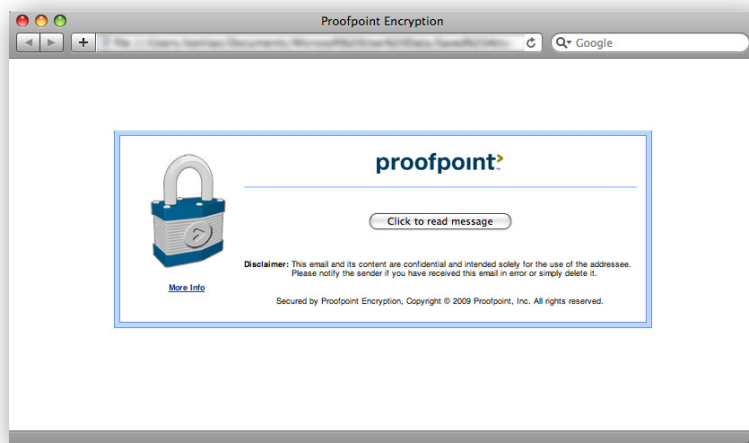
To deliver email securely to a user in another domain, Proofpoint Encryption encrypts the message as an HTML attachment, then sends a notification message along with the attachment to the user. To retrieve the message, the recipient follows a few easy steps to open the attachment and authenticate himself or herself, as shown below.

Using their standard email client, the recipient opens a message and sees a notice about encrypted content. The message instructs the recipient to open the message's attachment:

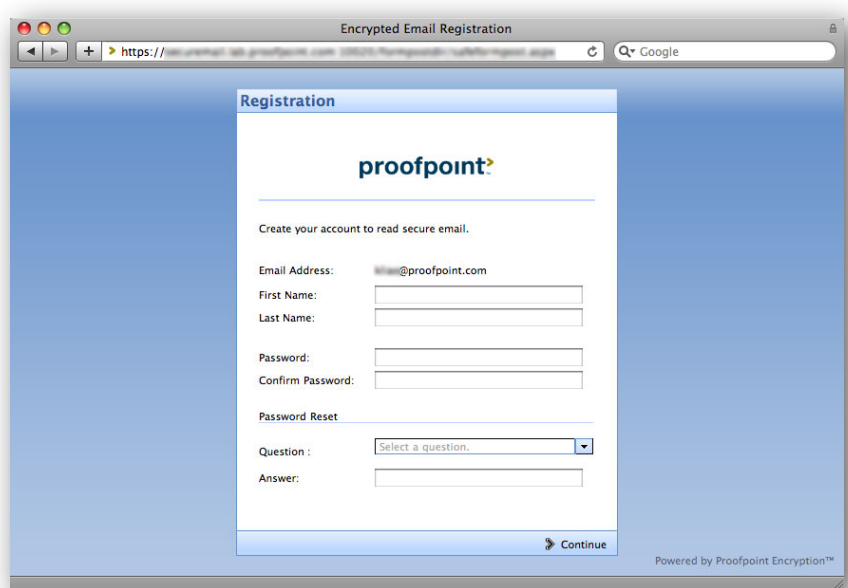


Note that the encrypted contents of the sent message, including its attachments, actually reside on the recipient's machine. That is, the encrypted content (ciphertext) is part of this email message. To decrypt the message contents, the recipient follows the instructions in the email.

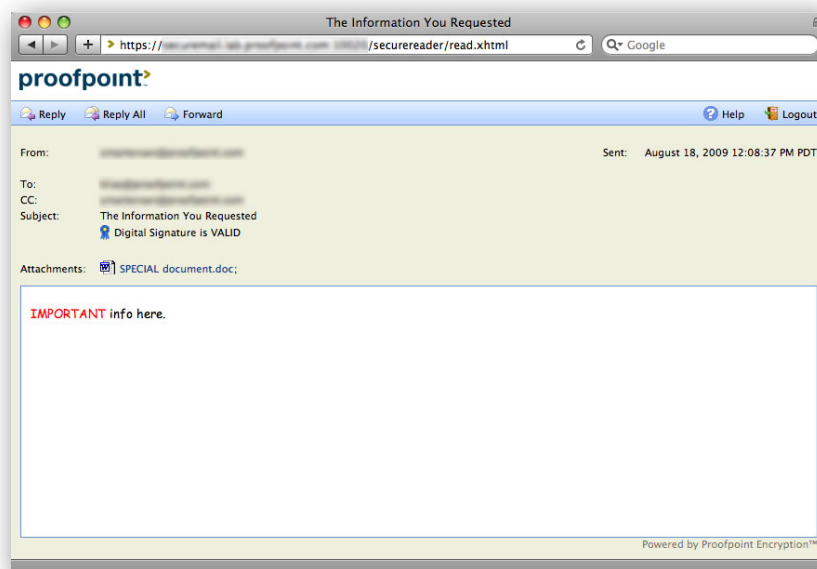
By clicking on a link in the attachment, the user is directed to an authentication page on the Proofpoint Encryption Registration Server, hosted in the sender's unique Proofpoint deployment (i.e., in their hosted Proofpoint on Demand instance or on-premises Proofpoint appliance).



If the recipient has already registered with the server—or if the server is linked to a pre-configured LDAP or custom directory—the user can simply log in. If the user is new to the Registration Server, he or she fills out a simple form to create an account, which allows them to view the decrypted message.



Once authenticated, the message contents are decrypted and displayed for the recipient in the Proofpoint Secure Reader interface. Like a conventional email message, the encrypted message may include multiple attachments, which are now displayed along with the decrypted message text.



Upon reading the message, the user has the option to reply to the message or to forward it, as appropriate. Replies and forwarded messages are also handled securely.

Note that the encryption key (automatically generated when the message was encrypted by Proofpoint Encryption when the encrypted message was sent) is stored securely by the Proofpoint Hosted Key Service, which is accessed only by the Proofpoint Secure Reader and Registration Server.

Proofpoint Encryption's push delivery service is accessible to authenticated users from any email client, Web browser or email kiosk. No special desktop client is needed. The process of opening an attachment and entering login credentials is so natural and straightforward that

even recipients who are new to the process can access their messages quickly and easily without requiring training.

At every point along the way, sending organizations have complete control of the encrypted messages they send. For example, security policies can be defined that control which users can perform which types of operations, such as forwarding or replying to secure messages.

Making Key Management Easier than Ever Before

Proofpoint Encryption works with the Proofpoint Hosted Key Service to make encryption key management as easy as ever, while giving IT managers and security officers complete control over the distribution, management, and revocation of keys.

The Proofpoint Hosted Key Services is a SaaS solution. Regardless of whether Proofpoint Encryption is running in on-premises appliances or “in the cloud” as a SaaS solution, it generates keys for secure email, then uses the Proofpoint Hosted Key Service to store, manage, and revoke keys, as needed.

Like other Proofpoint on Demand offerings, the Proofpoint Hosted Key Service is managed by Proofpoint in highly available, geographically distributed, secure data centers. All Proofpoint data centers are audited and certified for SAS-70 compliances. Proofpoint manages all routine data center operations, such as back-ups and upgrades, so Proofpoint customers never need to take extra steps to ensure that data is backed up and software up-to-date.

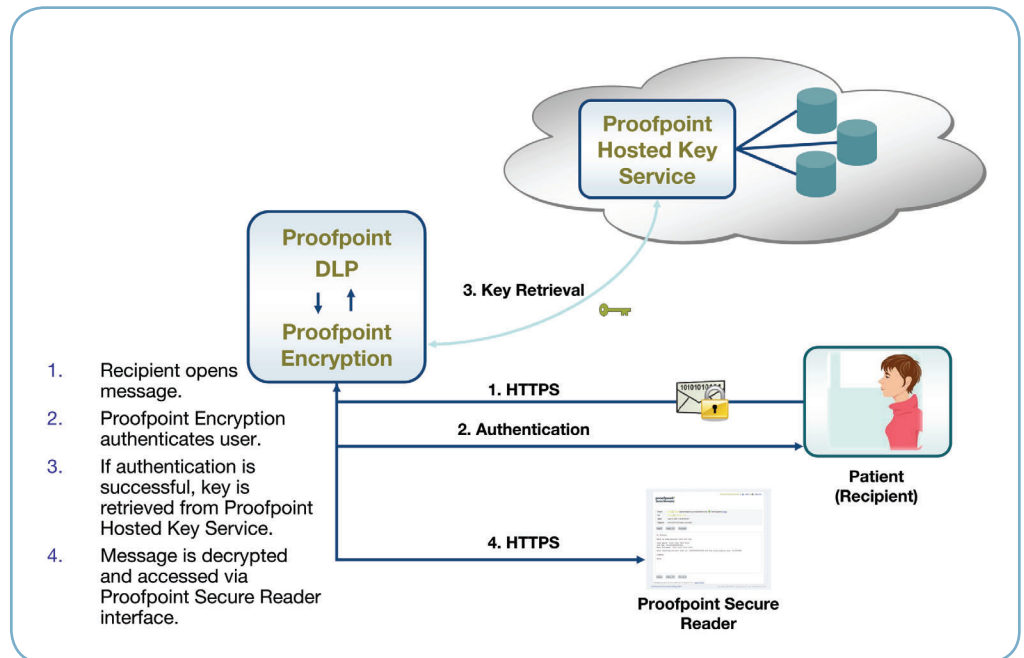
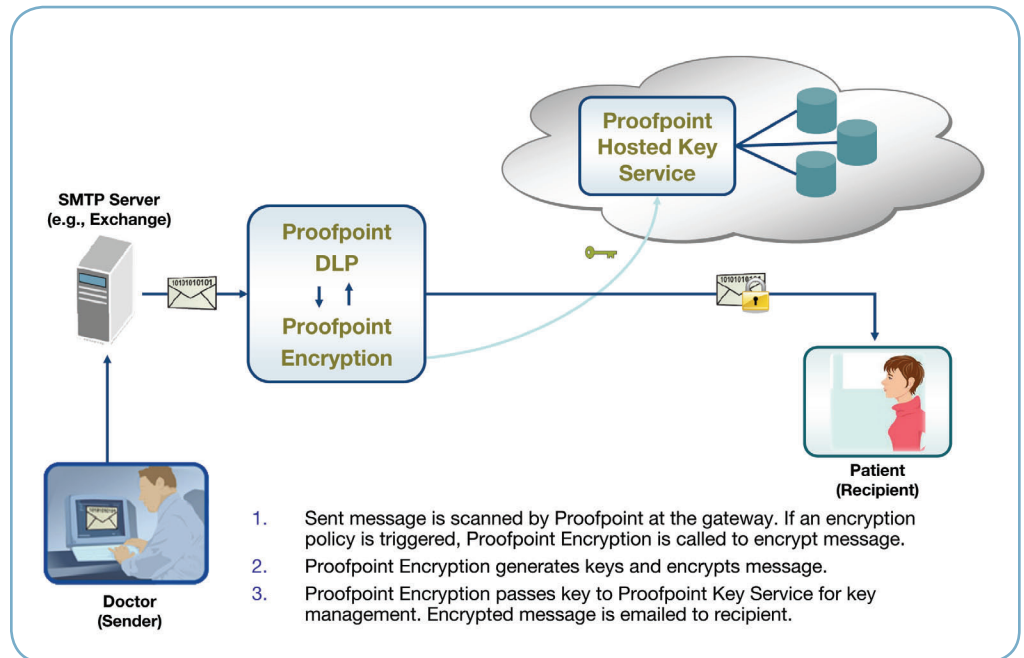
The Proofpoint Hosted Key Service is designed to provide Proofpoint customers with optimal, fine-grained control over encryption keys. Proofpoint Encryption generates a unique key for each encrypted message. This gives IT managers the ability to revoke a key for a particular message, without revoking keys for an overly broad selection of messages, such as all the encrypted messages sent to a particular user. Because the Proofpoint Hosted Key Service is storing and managing keys, customers never have to install their own key management software on business-critical email servers. Nor do Proofpoint customers have to take on other IT management tasks related to key management. The Proofpoint Hosted Key Service assigns each Proofpoint customer a unique database for key storage and ensures that only authorized users access keys and key management operations.

The Proofpoint Hosted Key Service offers customers both convenience and privacy. The service never accesses the contents of the messages it’s protecting. Instead, the service simply responds to requests from Proofpoint Encryption which have originated from authorized users.

The Proofpoint Hosted Key Service combines the best features of other models for encryption key management.

- **Security:** Keys are stored securely in SAS-70-compliant data centers
- **Availability:** Keys are continuously available, ensuring the users are never locked out of email. All keys are stored in two or more geographically distributed data centers to ensure that even a highly unlikely data center outage won’t keep users from their email.
- **Control:** Security officers, compliance officers, and IT managers have complete visibility into and control over the management of keys. Revoking all the keys associated with an employee who is leaving the company, for example, takes only a few keystrokes by an authorized IT administrator.
- **Ease of use:** End users continue to use the email clients and Web tools they are familiar with. Security staff and IT managers can manage the service through an easy-to-use Web interface.
- **Workload reduction:** IT staff can focus on productive work instead of the costly drudgery of distributing digital certificates or installing and configuring special desktop clients.

The diagrams below show how Proofpoint Encryption and the Proofpoint Hosted Key Service work together to securely deliver email to recipients.



Conclusion

Faced with increased regulatory scrutiny and relentless attacks by hackers, enterprises must be vigilant about data security. They need email security that complies with industry and government regulations, internal security guidelines, and IT best practices. The encryption must be rigorously implemented, while being easy to manage and easy to use. It should safeguard all email communications, even those sent and received in insecure environments.

Proofpoint ENTERPRISE Privacy delivers the best email privacy solution available for enterprises today. As an important component of the Proofpoint ENTERPRISE Privacy solution, Proofpoint Encryption unifies DLP and encryption technology to provide comprehensive protection for all kinds of private data in transit. Together with the Proofpoint Hosted Key Service, Proofpoint Encryption provides enterprises with a rapidly-deployable, easy-to-use security solution for email, without the costly overhead and IT management hassles commonly associated with email encryption and key management. Proofpoint Encryption and the Proofpoint Hosted Key Service make email security practical, flexible, and effective.

Proofpoint Encryption takes advantage of Proofpoint's extensive experience building enterprise-class secure messaging systems for Fortune 500 companies and government agencies. The solution can be deployed as part of any Proofpoint email security and data loss prevention deployment, whether on-demand or on-premises. For more information, please visit www.proofpoint.com.

For Further Reading

Proofpoint offers a variety of free educational whitepapers that further describe the legal, financial and regulatory risks associated with outbound email and the policies, processes and technologies that can be used to reduce those risks. Visit our online resource center at <http://www.proofpoint.com/resources> for the latest information.

The Critical Need for Encrypted Email and Secure File Transfer Solutions

This whitepaper from Proofpoint and Osterman Research discusses key issues around the encryption of both email and file transfer systems, some of the leading statutes that require sensitive content to be encrypted, and suggestions for moving forward with encryption:

<http://www.proofpoint.com/id/osterman-encryption-wp/index.php>

Outbound Email and Data Loss Prevention in Today's Enterprise

A summary of Proofpoint's annual research on outbound email and content security issues. Reports statistics on many on the prevalence of data breaches via email, the web and other channels; enterprise concerns about protecting confidential information; and the techniques and technologies enterprises have used to mitigate outbound email risks:

<http://www.proofpoint.com/outbound>

Global Best Practices in Email Security, Privacy and Compliance

This whitepaper discusses the impact of the latest global regulations that impact the email security policies and strategies of today's enterprises, universities and government organizations.

<http://www.proofpoint.com/id/email-security-best-practices-wp/index.php>

Email Archiving: A Proactive Approach to eDiscovery

This whitepaper addresses the key e-discovery challenges facing legal and IT departments today, including the impact of regulations such as the Federal Rules of Civil Procedure (FRCP) and how email archiving technology can help your organization be better prepared:

<http://www.proofpoint.com/id/email-archiving/index.php>

Leveraging SaaS Technology to Reduce Costs

These whitepapers from Proofpoint and Osterman Research discuss how Software-as-a-Service solutions for email security and email archiving can greatly reduce costs—without sacrificing the security of your organization’s most valuable data:

Using SaaS to Reduce the Costs of Email Security

<http://www.proofpoint.com/id/saas-email-security-costs-whitepaper/index.php>

Email Archiving: Realizing the Cost Savings and Other Benefits from SaaS

<http://www.proofpoint.com/id/saas-email-archiving-costs-whitepaper/index.php>

About Proofpoint, Inc.

Proofpoint secures and improves enterprise email infrastructure with solutions for email security, archiving, encryption and data loss prevention. Proofpoint solutions defend against spam and viruses, prevent leaks of confidential and private information, encrypt sensitive emails and archive messages for retention, e-discovery and easier mailbox management. Proofpoint solutions can be deployed on-demand (SaaS), on-premises (appliance), or in a hybrid architecture for maximum flexibility and scalability.

Proofpoint Solutions for Outbound Email Content Security, Data Loss Prevention and Regulatory Compliance

Proofpoint’s SaaS, appliance, virtual appliance and software solutions for email security and data loss prevention defend against all types of inbound and outbound message-borne threats.

Enforcing Email Acceptable Use Policies

Proofpoint makes it easy to define and enforce corporate acceptable use policies for message content and attachments. A convenient point-and-click interface simplifies the process of defining complex logical rules related to file types, message size, and message content. Proofpoint’s content compliance features can be used to identify and prevent a wide variety of inbound and outbound policy violations—including offensive language, harassment, file sharing, and violations of external regulations. Non-compliant messages can be acted on with a wide variety of options, including quarantine, reroute, reject, annotate, and other actions.

Preventing Leaks of Confidential and Proprietary Information

As email has become the most important communication channel in today’s enterprise, email systems have become the main repository for sensitive, confidential, and mission-critical information. The Proofpoint Digital Asset Security™ module keeps valuable corporate assets and confidential information from leaking outside your organization via email. Powerful Proofpoint MLX™ machine learning technology analyzes and classifies your confidential documents and then continuously monitors for that information in the outbound message stream—stopping content security breaches before they happen.

Ensuring Compliance with Data Protection and Privacy Regulations

The Proofpoint Regulatory Compliance™ module protects your organization from liabilities associated with data protection and privacy regulations such as HIPAA, GLBA and PCI. Pre-defined rules automatically scan for non-public information, including protected health information and personal financial information, and act on non-compliant communications, rejecting or encrypting messages as appropriate.

Enabling Policy-based Encryption

Proofpoint’s SaaS, appliance and software solutions for email security can all optionally be equipped with robust, policy-based encryption features that automatically encrypt individual messages based on an organization’s policies, without requiring end-users to take any special actions. Proofpoint’s flexible rules, managed dictionaries and “smart identifiers” are used to accurately detect non-public information—such as protected health information and personal financial information—and reject or encrypt messages as appropriate.

<http://www.proofpoint.com/encryption>

Protecting HTTP and FTP Streams: Multi-protocol Content Security

The Proofpoint Network Content Sentry™ extends Proofpoint's email protection to additional messaging streams, including HTTP and FTP. This module inspects all outbound network traffic in real-time, monitoring for confidential information, private customer or employee data (including private healthcare, financial or identity information) and other sensitive content that may leak outside the enterprise.

Archiving Email for eDiscovery Readiness, Compliance and Easier Mailbox Management

Proofpoint ARCHIVE™, a SaaS email and IM archiving solution, incorporates Proofpoint's patented DoubleBlind Encryption™ technology, which encrypts messages before transmission to Proofpoint's datacenters where they are stored in encrypted form. At the same time, Double-Blind Encryption ensures that data remains fully searchable via the secure Proofpoint ARCHIVE appliance. Proofpoint ARCHIVE helps organizations be prepared for eDiscovery events, improves end-user access to historical email and ensures compliance with your organization's email retention policies.

<http://www.proofpoint.com/emailarchiving>

Eliminating Risks Associated with FTP and Email Transmission of Large or Confidential Files: Secure File Transfer

Proofpoint Secure File Transfer™ lets end users send large files (or files that require enhanced security) easily and securely—while minimizing the impact of large attachments on your email infrastructure.

<http://www.proofpoint.com/sft>

©2009 Proofpoint, Inc. All rights reserved.
Proofpoint, Proofpoint Encryption, Proofpoint Secure Reader, Proofpoint ARCHIVE, Proofpoint ENTERPRISE, Proofpoint Secure File Transfer, Proofpoint Protection Server, Proofpoint Messaging Security Gateway, Proofpoint on Demand, Proofpoint MLX, Proofpoint Content Compliance, Proofpoint Regulatory Compliance, Proofpoint Network Content Sentry, Proofpoint Secure Messaging, DoubleBlind Encryption and Proofpoint Digital Asset Security are trademarks or registered trademarks of Proofpoint, Inc. in the US and other countries.
Version 10/09 - Rev A

For More Information

Proofpoint, Inc. US

Worldwide Headquarters

892 Ross Drive
Sunnyvale, CA 94089
USA
P 408 517 4710
F 408 517 4711
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. EMEA

Proofpoint, Ltd.
The Oxford Science Park
Magdalen Centre
Robert Robinson Avenue
Oxford, UK
OX4 4GA
Tel +44 (0) 870 803 0704
Fax +44 (0) 870 803 0705
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. Asia Pacific

5th Floor, Q.House Convent Bldg.
38 Convent Road, Silom, Bangrak
Bangkok 10500, Thailand
Tel +66 2 632 2997
E info@proofpoint.com
www.proofpoint.com

Proofpoint Japan K.K.

906 BUREX Kojimachi
Kojimachi 3-5-2, Chiyoda-ku
Tokyo, 102-0083
Japan
P +81 3 5210 3611
F +81 3 5210 3615
E sales-japan@proofpoint.com
www.proofpoint.co.jp

Proofpoint, Inc. Canada

60 Adelaide Street East, 9th Floor
Toronto, Ontario M5C 3E4
Tel +1 416 366 6666
Fax +1 416 366 6667
E info@proofpoint.com
www.proofpoint.com

Proofpoint, Inc. Mexico

Uxmal 165 int 7
Col. Narvarte
CP 03020
México D.F.
Tel: +52 55 5330 3382
E info@proofpoint.com
www.proofpoint.com