



# Proofpoint Enterprise Privacy

## A SaaS Email Compliance, Data Loss Prevention and Encryption Solution

The Proofpoint Enterprise Privacy™ suite provides a full lifecycle approach to protecting information of all types. It protects sensitive and private information, defends against leaks of confidential information and ensures compliance with common International, industry and U.S. (Federal and State) data protection regulations, including HIPAA and GLBA, as well as PCI standards. Proofpoint Encryption™, a part of the Proofpoint Enterprise Privacy Suite, can automatically encrypt email based on an organization's unique policies, mitigating the risks associated with regulatory violations, data loss and corporate policy violations.

**proofpoint**™

## Proofpoint Enterprise Privacy Benefits

- Guards against leaks of private and confidential information in email and web protocols with highly-accurate detection using smart identifiers, managed dictionaries, and advanced machine learning techniques.
- Smart identifiers and managed dictionaries provide automatically updateable policies for lowest administrative cost and highest accuracy.
- Customize policies with point-and-click ease.
- Communicate securely with customers, patients and cardholders using built-in policy-based email encryption.
- Easily remediate, track and report on compliance incidents and trends.
- Enterprise-class security ensures continuous service and complete security of an organization's data.

## Proofpoint Enterprise Privacy Features

- Advanced detection of private or confidential information in unstructured and structured data
- Pre-configured data protection policies
- Integrated policy-based email encryption
- Robust incident management and workflow for security and compliance officers
- Over 60 reports can be published and emailed, including dashboards for compliance officers

## Additional Capabilities

Add complete protection from targeted email threats with the Proofpoint Enterprise Protection Suite:

- Connection management
- Content analysis and scanning powered by Proofpoint MLX
- Signature- and zero-hour virus protection
- Deep content inspection
- Real-time message tracing
- Transport Layer Security (TLS) encryption and more

## Comprehensive privacy protection and data loss prevention

Across the globe, the trend toward more stringent data protection regulations promises stricter breach notification requirements, bigger fines and more headaches for organizations that fail to properly protect private data. Corporate email remains the number one source of privacy breaches. Easy to implement, use and maintain, Proofpoint Enterprise Privacy delivers exceptional data protection with the lowest total cost of ownership.

Proofpoint Enterprise Privacy gives an organization powerful data loss prevention capabilities with a full lifecycle approach, the most cost-effective way for organizations to prevent leaks of sensitive data via email, while enabling necessary business communications. The regulatory compliance service secures private data and protects an organization from liabilities associated with privacy and data security regulations including HIPAA, GLBA, PCI, SEC rules, and many more.

Customizable rules, managed dictionaries and "smart identifiers" automatically scan for non-public information, such as protected health information and personal financial information, and block or encrypt messages as appropriate.

Proofpoint Enterprise Privacy also keeps valuable corporate assets and data confidential by analyzing and classifying confidential documents. It monitors for that information in the outbound message stream, thereby stopping data leaks before they happen.

Proofpoint Enterprise Privacy is available as SaaS or on-premises using Proofpoint's cloud-enabled or virtual appliances.

## Full Lifecycle Approach

The requirements of the modern business world are not just about detecting information and blocking it, but utilizing secure methods of communication as a business enabler. A full lifecycle approach to data protection is necessary to effectively tackle today's data protection needs. Proofpoint addresses these requirements with a four-part defense strategy – Detect, Manage, Respond, and Govern.

### Detect

Proofpoint Enterprise Privacy uses multiple layers of defenses to protect all types of private information. It analyzes every aspect of an outgoing email message including content, attachments and message attributes; using a variety of techniques to deliver outstanding accuracy with minimal false positives.

While the common use case is to filter outgoing email, Proofpoint Enterprise Privacy can also be used to detect sensitive information for inbound traffic. For example, an organization can monitor any sensitive information coming from its business partners.

### Deep content analysis

Proofpoint Enterprise Privacy can create policies and detect violations based on a wide variety of message attributes, dictionary-based content, regular expressions and weighted keyword matches. Policies can be triggered by keywords and regular expressions found in the subject line, content of a message, and by attributes such as the message origin, destination or attachment type.

Proofpoint Enterprise Privacy analyzes structured data to detect all types of private information—including protected health information and personal financial information—using managed dictionaries and "smart identifiers" through an automated process.

Dictionaries include common protected health information (PHI) code sets—such as standard disease, drug, treatment, and diagnosis codes used by the healthcare industry to ensure HIPAA compliance. Financial privacy dictionaries—such as SEC, insider trading and trade confirmation terms used in the financial services industry—aid in compliance with GLBA, PCI and SEC regulations. Custom dictionaries can also be defined.

To address intellectual property, Proofpoint Enterprise Privacy employs patent-pending Proofpoint MLX™ machine learning technology to analyze the documents an organization wants to keep confidential by analyzing the information and storing the document's digital fingerprints in a secure repository. Negative cases can also be loaded to train the system to ignore common, non-confidential content, such as company boilerplate information. Access controls let an organization grant certain business users access to the training system and define which users can add documents to the system for training.

Proofpoint Enterprise Privacy	
Feature	Benefit
Multi-Layered Defense in Depth	Smart identifiers for SSNs, PANs, ABA routing numbers, etc.
	Proximity and correlation analysis
	Block or encrypt emails containing sensitive and/or private information
Integrated Encryption	Native, integrated, strong encryption technology
	Encrypt messages automatically, based on presence of sensitive data
Easy to Implement and Use	Deploy in days, not months
	Proofpoint Key Service eliminates key management overhead
	No end user training required
Advanced Workflow Capabilities	Self-remediation of messages due to inadvertent violations of DLP, saving IT and compliance resources from reviewing each individual incident
	DLP-specific interfaces and reports make it easy for IT and compliance resources to review, comment, track and escalate policy violations

### HTTP Protection

The power of Proofpoint Enterprise Privacy's data loss prevention features also cover web-based email and other HTTP streams by integrating with web proxy appliances that support the ICAP protocol. The same content security, regulatory compliance and acceptable use policies defined for SMTP-based communications can be applied to HTTP and HTTPS communications.

Web posting activity—such as Web-based email posting (including Webmail services such as MSN Hotmail, Yahoo! Mail, AOL Mail, and Google Gmail)—can be automatically intercepted and scanned for information leaks and policy violations, even inside SSL-encrypted sessions.

### Manage

Once messages have been identified and classified, they can be handled with a wide variety of disposition options, including blocking, redirecting, quarantining, modifying or encrypting the message. Proofpoint Smart Send enables administrators to determine a subset of users that may be allowed to remediate their own messages that have triggered minor violations, while severe and egregious incidents are left for security and compliance officers. All policies are customizable at the global, group and end user level, while integration with LDAP or Active Directory simplifies ongoing administration.

### Respond

Providing effective response is critical in protecting sensitive data while also providing the mechanisms so that business is not hampered. Most privacy and data protection regulations—federal laws like HIPAA, SOX and GLBA, security standards such as PCI-DSS and state laws such as Massachusetts 201 CMR 17—require enterprises to protect private data at rest and in transit using encryption. Proofpoint Enterprise Privacy helps meet these requirements by incorporating the industry's most powerful and flexible solution for policy-driven email encryption: Proofpoint Encryption.

### Policy-based encryption

Proofpoint Encryption makes ad hoc, secure communication just as easy as traditional, non-encrypted messaging. Fully integrated with Proofpoint's Enterprise Privacy best-in-class private data detection capabilities, policies can automatically and dynamically apply encryption. Extremely granular, per-message control, is provided over all encrypted messages. Based on policies, encrypted messages can be sent with a specific expiration period. For example, one set of messages may be sent with a 30-day expiration, while others may be available for a full year. Furthermore, it is possible to revoke access of an individual message to a specific recipient without affecting other users or other messages to the same recipient.

### Simplified key management

Proofpoint Encryption solves the deployment and administrative complexities commonly associated with encryption solutions. Proofpoint Encryption eliminates key management, backup and administration burdens through the Proofpoint Key Service™, which uses Proofpoint's next-generation SaaS infrastructure to provide secure, cost-efficient, highly-available and fully redundant key storage facilities.

### Govern

Detailed reports provide compliance officers with trends, allowing a proactive approach to addressing user behavior. Backed by actionable information, training may be targeted at a specific group of users, or policies may need to be adjusted.

