Proofpoint Email Data Loss Prevention and Encryption

KEY BENEFITS

- Manage and enforce email DLP and encryption centrally on our industry-leading email gateway
- Integrate with Proofpoint Enterprise DLP and comprehensively address the entire spectrum of people-centric data loss scenarios
- Analyze and classify confidential information within both structured and unstructured data
- Seamless user and mobile experience

COMPLIANCE

- 80+ built-in policies
- PCI, SOX, GLBA, SEC insider trading terms, and other global country specific templates
- GDPR, UK-DPA, EU-DPD, PIPEDA (Canada), UK National Insurance Number, Japanese credit card numbers
- PII, HIPAA, ICD-9, ICD-10, National Drug Code, other healthcare code sets

Proofpoint Email DLP and Encryption provides unique visibility and enforcement without the complexity and costs of disparate solutions. It provides automatic data classification and transparent encryption that are centrally managed at the gateway. It enhances better admin experience in defining and implementing policies across your email environment.

Email is the number one threat vector for inbound threats. It is also a critical threat vector for outbound data loss. With Email DLP and Email Encryption, you can increase control of your sensitive data. This allows you to satisfy compliance. And it provides a key layer of protection from attacks that dupe your users into sending sensitive information via email.

Prevent Potential Data Breach

Email DLP detects and keeps sensitive data and confidential information from leaking outside an organization through email. It accurately classifies sensitive information and detects data exfiltration transmissions via email. And it stops critical data from leaving your organization.

Exact data matching

The exact data matching feature in Email DLP allows you to easily upload or create custom dictionaries or custom identifiers. And they are unique to your organization. For example, it uses financial services account numbers, local forms of ID and medical record numbers to analyze email data that matters to you. You can expand existing dictionaries to include organization-specific terms and codes. Exact data matching detects sensitive information unique to your organization that needs to stay protected. And you can use route-based definitions to create policies for the inbound and outbound message streams.

Protect from email fraud

Email DLP has more than 80 fine-tuned policies that automatically find, classify and block messages. Typically, these messages are used as part of business email compromise (BEC) attacks. These policies greatly reduce the risk of sending employee records, W2s and executing wire transfers to impostors.

Deep analysis and fingerprinting

Email DLP accurately detects sensitive data within unstructured content. With Email DLP you can:

- Scan over 300 file types out of the box
- Ensure sensitive data located beyond standard Office and PDF attachments are properly handled
- Extend support to new, custom or proprietary file types such as patents and memos with the file type profiler
- Fingerprint sensitive documents with both full and partial matching capabilities—even if the data resides in different file formats

Automate Regulatory Compliance

Email DLP quickly discovers exposed sensitive data with pre-built dictionaries. It goes beyond simple regular expression matches. It provides:

- A high confidence of detection of non-compliant communications
- Detailed algorithmic checks built into smart identifiers
- Minimizes false positives for credit card numbers, identification numbers and a wide variety of sensitive information
- Advanced proximity and correlation analysis improve detection of multiple elements

Dictionary terms can be weighted to increase or decrease the matching strength of any term or to allow exceptions.

Improve Operational Effectiveness

Integration with Enterprise DLP

Email DLP is integrated with Proofpoint Enterprise DLP. It brings together our market leading DLP solutions for email, cloud and endpoint. Enterprise DLP combines content, behavior and threat telemetry from these channels. This allows you to address the full spectrum of people-centric data-loss scenarios comprehensively through a unified incident management interface. You can easily apply common classification across channels. So, it saves you time and removes administrative headache.

Smart Send

The Smart Send feature enables email senders to remediate their own outbound policy violations. This powerful, easy-to-administer tool helps educate users while freeing up IT resources for more strategic tasks. You can also define routing per policy—to reroute sensitive assets back to the user, HR, IT or anyone else.

Real-time reporting

Email DLP provides the visibility and workflow to help you make quick decisions and take action. It allows you to see real-time statistics and trends, manage current incidents and take appropriate actions on non-compliant messages. You can do all this from a centralized dashboard. And you can drill down into any incident for review—getting a side-by-side highlighted view of regions of an email or attachment and see what matches next to the original training document or policy. Comment on, track and search violations in the incident manager and export matching messages.

Graphical reports show breaches—by policy, by user, top offenders per policy and more—over time. View trends to help identify areas of success and opportunities. Reports can be emailed on a scheduled basis or published to an intranet site to free up your time.

Assured Encryption, Visibility and Controls

Email Encryption is enabled by policy based DLP engine. Its robust controls:

- Let you define encryption policies to meet the demands of your business
- Dynamically applies policies at the global, group and user level with integration into LDAP or AD
- Allows you to define encryption based on destination—for example—you can include business partner or supplier, sender attributes and message attributes—such as attachment types

Email Encryption can also serve as a TLS fallback to ensure a fail-safe encryption mechanism.

With Email Encryption, you can:

- Keep your business communications flowing securely
- Help organizations secure communications between groups or users as it offers internal-to-internal encryption capability and eliminates the need to route mail externally or deploy another solution that can be difficult to adopt
- Get granular revocation of encrypted emails lets users to revoke, expire or restore access to encrypted email without affecting other users or other messages to the same recipient

No-touch key management

You can eliminate the administrative overhead of key management and focus on your encryption needs. As keys are generated, they are securely stored and managed. And they are made highly available through our cloud-based infrastructure. Keys are stored separately from email content to ensure privacy and security.

Enhanced recipient experience

Seamless user experience is a must with email DLP and encryption solutions to prevent employees from working around the policies set in place. Proofpoint delivers multiple options for the user to access an encrypted message. The default secure reader method allows a user to click on an encrypted html attachment from the message. It directs them to the web portal where they can easily access the encrypted message. The other method is decrypt assist, which is specifically designed for mobile access. Within a message, a link is provided for the user to click. It takes them to the mobile optimized web portal for access to the encrypted message.

Users can access and manage encrypted messages from the Secure Reader Inbox. This gives them a seamless experience when dealing with encrypted messages. Also it allows the organization to easily manage messages they have. The unified Outlook add-ins feature allows users to easily send and read encrypted messages with a click of a button. And organizations can enable internal-to-internal encryption for sensitive employee-to-employee communication.

LEARN MORE

For more information, visit **proofpoint.com**.