Proofpoint Email DLP and Email Encryption

Protect your users from attacks that dupe them into sending sensitive information via email

Key Benefits

- Manage and enforce email DLP and encryption centrally on our industry-leading email gateway
- Integrate with the Proofpoint Information and Cloud Security platform and comprehensively address the entire spectrum of people-centric data loss scenarios
- Detect and analyze sensitive data in email messages and attachments
- Seamless user and mobile experience

Compliance

- More than 240 built-in data identifiers
- 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 Data Loss Prevention (DLP) and Proofpoint Email Encryption provide unique visibility and enforcement without the complexity and costs of disparate solutions. They feature automatic sensitive data detection and transparent encryption that are centrally managed at the gateway. They enhance the admin experience in defining and implementing policies across your email environment.

Proofpoint Email DLP and Proofpoint Email Encryption give you increased control over your sensitive data to let you better meet compliance requirements. They help you protect your users from attacks that dupe them into sending sensitive data via email. Email is the No. 1 threat vector for inbound threats. It is also a critical threat vector for outbound data loss.

Email DLP—Prevent Potential Data Breaches

Proofpoint Email DLP accurately identifies sensitive data and detects data exfiltration transmissions via email. It keeps sensitive data from being leaked out of your organization.

Exact data matching

Proofpoint Email DLP features exact data matching. This detects sensitive data that needs to stay protected. It lets you easily upload or create custom dictionaries and identifiers that are unique to your organization. With it, for example, you can use financial services account numbers, local forms of ID and medical record numbers to analyze email data that matters to you. You can also expand existing dictionaries with custom terms and codes. And you can use route-based definitions to create policies for the inbound and outbound message streams.

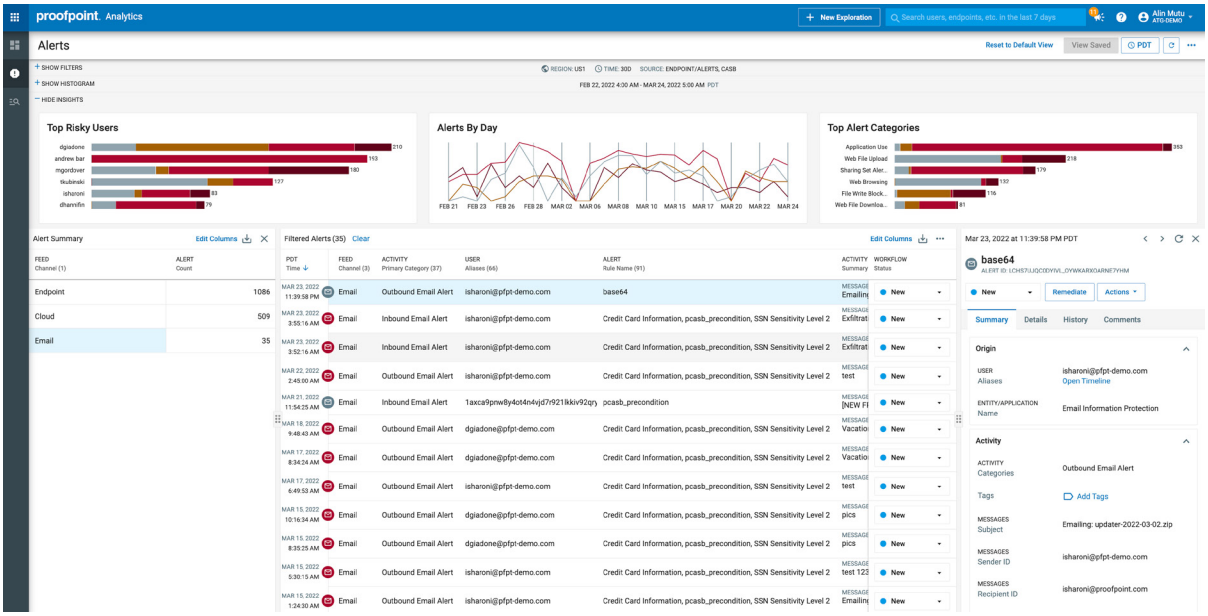

Figure 1: Get comprehensive visibility into your sensitive data in email messages and attachments.

Protect from email fraud

Proofpoint Email DLP has more than 240 fine-tuned identifiers. These identifiers can automatically detect and block messages that are typically used as part of business email compromise (BEC) attacks. They greatly reduce the risk of sending employee records, W2s and executing wire transfers to impostors.

Deep analysis, fingerprinting and OCR

Proofpoint Email DLP accurately detects sensitive data within unstructured content, including images. With Email DLP you can:

- Scan more than 300 file types out of the box.
- Ensure that sensitive data located beyond standard Microsoft Office and PDF attachments are properly handled.
- Use the file-type profiler to extend support to new, custom or proprietary file types. File types can include patents and memos.
- Fingerprint sensitive documents with both full and partial matching capabilities. You can fingerprint data even if it resides in different file formats.
- Add optical character recognition (OCR) to detections. This lets you protect sensitive data in images.

Automate regulatory compliance

Proofpoint Email DLP goes beyond simple regular expression matches. It can use prebuilt dictionaries to quickly discover exposed sensitive data. Email DLP provides:

- A high confidence of detection of non-compliant communications.
- Detailed algorithmic checks built into smart identifiers.
- Minimized false positives for credit card numbers, ID numbers and a wide variety of sensitive data.
- Advanced proximity and correlation analysis. This improves detection of multiple elements.

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

Improve operational effectiveness

Integration with the Information and Cloud Security platform

Proofpoint Email DLP is integrated with the Proofpoint Information and Cloud Security platform. It brings together our market-leading DLP solutions for email, cloud, web, endpoint and on-premises file repositories. Our platform combines content, behavior and threat telemetry from these channels. This lets you address the full spectrum of people-centric data-loss scenarios through a unified alert management interface. Common detectors let you deploy consistent DLP policies across channels. So, they save you time and they reduce administrative burden.

Smart Send

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

Proofpoint real-time reporting

Proofpoint Email DLP provides the visibility and workflow to help you make quick decisions and take action. It lets you see real-time statistics and trends. It also lets you manage current incidents as well as take appropriate actions on non-compliant messages. You can do all of this from a centralized dashboard. Drill down into any incident for review. Get 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 over time. You can view these breaches by policy, user, top offenders per policy and more. View trends to see areas of success and opportunities. Reports can be emailed on a scheduled basis. They can also be published to an intranet site to free up your time.

Email Encryption—Assured Encryption, Visibility and Controls

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

- Let you define encryption policies.
- Dynamically apply policies at the global, group and user levels with integration into LDAP or AD.
- Let you to define encryption based on destination. You can, for example, include business partner, supplier, or sender and message attributes, such as attachment types

Proofpoint Email Encryption can also serve as a TLS fallback. This ensures fail-safe encryption.

With Email Encryption, you can:

- Keep your business communications flowing securely.
- Help secure communications between groups or users. It offers an internal-to-internal encryption. And it removes the need to route mail externally or deploy another solution that can be difficult to adopt.
- Get granular revocation of encrypted emails. This lets users 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 remove the administrative overhead of key management and focus on your encryption needs. As keys are generated, they are securely stored and managed. They are also made highly available through our cloud-based infrastructure. Keys are stored separately from email content. This ensures privacy and security.

Enhanced recipient experience

By providing a seamless user experience, Proofpoint Email Encryption helps prevent employees from working around the policies. We offer multiple options for users to access encrypted messages. The default is the secure-reader method. This lets users click on an encrypted HTML attachment from the message. It then directs them to the web portal, where they can easily access the encrypted message. The other method is called decrypt assist. This is designed for mobile access. A link is provided in a message. When users click the link, it takes them to the mobile-optimized web portal so they can access 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. It also lets the organization easily manage messages they have. The unified Outlook add-ins feature lets users easily send and read encrypted messages with a click of a button. And you can enable internal-to-internal encryption for sensitive employee-to-employee communication.

LEARN MORE

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