Proofpoint Email DLP and Encryption

Identify sensitive data in emails to prevent loss and automate compliance

Key Benefits

- Manage and enforce email DLP and encryption centrally on Proofpoint's industry leading email gateway
- Detect and analyze sensitive data in email messages and attachments
- Integrate with Proofpoint Information Protection to comprehensively address the entire spectrum of human-centric data loss use cases

Compliance

- Hundreds of 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, ICD-11 National Drug Code other healthcare code sets

This solution set is part of Proofpoint's integrated human-centric security platform, mitigating the four key areas of people-based risks.

Email is a critical threat vector of outbound data loss. So a top priority for security teams must be to reduce the risk of sensitive data leaving an organization. To meet compliance requirements, they must be able to detect and control data in email messages. Proofpoint Email Data Loss Prevention and Encryption mitigates the risk of a data breach through email and attachments. It also lets you define and dynamically apply granular encryption policies to secure email between internal users and external business partners.

Data doesn't lose itself. People lose data. According to the 2023 Verizon DBIR,[1] 74 percent of all breaches that expose data to an unauthorized party involve the human element. Most analysts note that corporate users typically lose data. The underlying cause in these cases is usually simple carelessness, with negligent users the most significant sources of data loss through email.

Proofpoint Email DLP and Encryption accurately identifies sensitive information. It detects data exfiltration through email and it stops critical data loss. It also gives you increased control over your sensitive data to help meet compliance requirements.

Identify Data Unique to Your Organization

Email DLP and Encryption identifies data unique to your organization. It comes with hundreds of proven prebuilt data identifiers and dictionaries. These include financial services account numbers, local forms of ID and medical record numbers. You can also easily upload or create custom dictionaries or identifiers that are unique to your organization, as well as fine tune the matching strength of dictionary terms and exceptions. This allows you to analyze the email data that matters most to your organization.

1 Verizon. "2023 Data Breach Investigations Report." June 2023

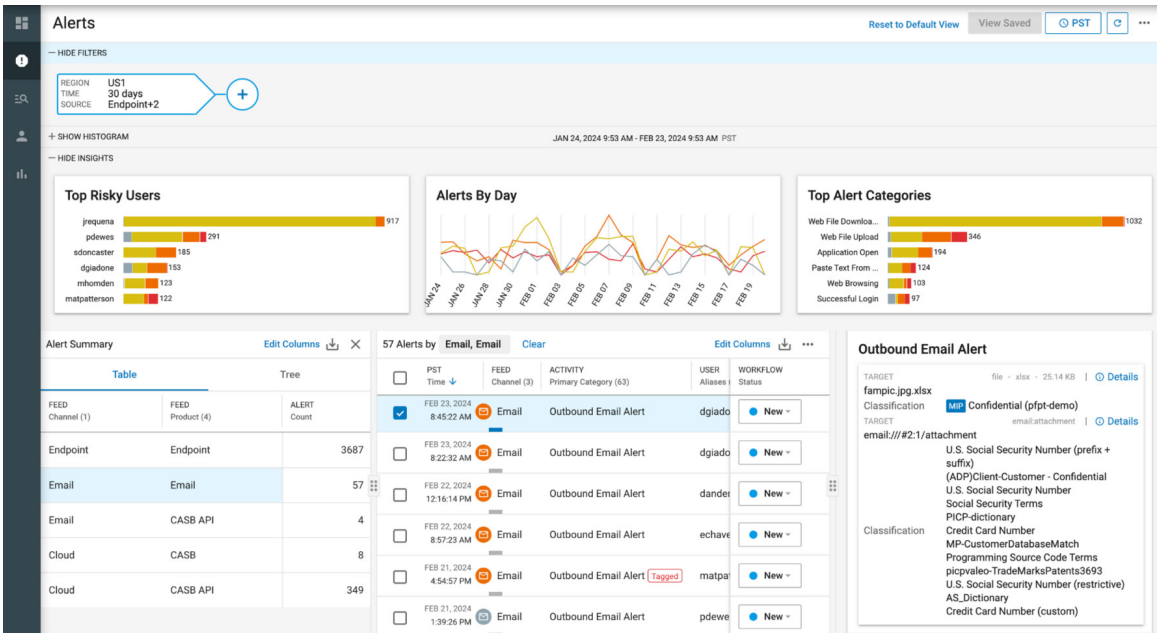

Figure 1: Proofpoint Email DLP and Encryption lets you address the full spectrum of human-centric data-loss scenarios through a unified alert management system.

Deep analysis and fingerprinting

Email DLP and Encryption accurately detects sensitive data within unstructured content. More than 300 file types can be scanned out of the box. The solution ensures that sensitive data located beyond standard Microsoft Office 365 and PDF attachments is properly handled. You can also use the file-type profiler to extend support to new, custom or proprietary file types, such as patents and memos.

Sensitive documents are fingerprinted—with both full and partial matching capabilities—even if the data resides in different file formats. You can also employ advanced methods for content-matching and text extraction from images. This includes index document matching, exact data matching and optical character recognition (OCR).

Automate Regulatory Compliance

Email DLP and Encryption automatically looks for all standard forms of restricted content. It quickly detects sensitive data with its prebuilt dictionaries. With detailed algorithmic checks built into smart identifiers, it minimizes false positives for credit card numbers and a wide variety of sensitive information. Advanced proximity and correlation analysis enhances detection analysis. The solution enables organizations to comply with PCI, SOX, GDPR, PII, HIPAA and more.

Real-time reporting

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

Improve operational effectiveness

Email DLP is part of our enterprise DLP approach. This allows you to find, track and safeguard data as users work in email, cloud applications and endpoints. It combines content, behavior and threat telemetry from these channels, which lets you address the full spectrum of human-centric data-loss scenarios through a unified alert management system. And you can easily apply common data detectors to deploy consistent DLP policies across channels. This helps save time and eliminates administrative headaches.

Routing policies like Smart Send make life easier for your DLP analysts. Emails can be sent back to the sender for self-remediation of outbound policy violations, or routed elsewhere—such as to HR, IT or business owner—as part of the workflow.

Assured Encryption, Visibility and Controls

Email DLP and Encryption keeps your business communications flowing securely. It secures external or internal-to-internal communication with a robust set of controls and no-touch key management. Enabled by a policy-based DLP engine, the solution lets you define and dynamically apply granular encryption policies at the global, group and user levels with integrations with LDAP and Active Directory.

You can automate encryption by destination (that is, business partner, supplier), sender or message attributes such as attachment types. Or you can enable users to selectively apply encryption. Email encryption also serves as a TLS fallback to ensure fail-safe encryption. Recipients have flexible options to access encrypted messages, including a web portal, mobile browser or Outlook client.

For seamless, secure communication with business partners who also use Proofpoint Email DLP and Encryption, our Trusted Partner Encryption provides a transparent user experience for your end users. Messages are encrypted by the sending gateway. And the business partner's Proofpoint gateway can automatically decrypt them before they are delivered to the internal email infrastructure.

Enhanced recipient experience

By providing a seamless user experience, Proofpoint Email DLP and Encryption prevents employees from working around the policies. The solution provides multiple options for users to access encrypted messages, including:

- **Secure Reader—**Lets users either click on an encrypted HTML attachment from the message or click a link in an email. It then directs them to a web portal, where they can easily access the encrypted message.
- **Secure Reader Inbox—**Provides users with a seamless experience when dealing with encrypted messages. It also lets the organization easily manage messages.
- **Microsoft Outlook Add-Ins—**Lets users easily send and read encrypted messages with a click of a button.
- **Internal-to-Internal Encryption—**Used for sensitive employee-to-employee communication.

Expertise Shortens Time to Value

Preventing data loss is not easy. It requires more than technical and product knowledge. It also requires a deep understanding of program objectives, data governance and data stewardship. We can be a trusted partner on your journey to ensure the success of your DLP program. Our managed service provides you with expertise that can help you optimize your technology investment, support your continuous operations and mature your data protection strategy.

LEARN MORE

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