proofpoint.

INFORMATION PROTECTION | SOLUTION BRIEF

Preventing Email Data Loss in Federal Agencies

Protect your users from attacks that trick them into sending sensitive information by email

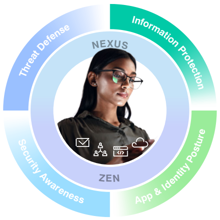
Key Benefits

- Manage and enforce email DLP policies and alerts centrally in our industry-leading on-premises or FedRAMP-hosted email gateway
- Detect and analyze sensitive data in email content and attachments
- Prevent Controlled Unclassified Information (CUI) and regulated data leaving your environment by reading and acting on Microsoft Information Protection (MIP) labels

Compliance

- 240-plus built-in data identifiers
- PCI, SOX, GLBA and SEC insider trading terms and other global, country-specific templates
- GDPR, UK-DPA, EU-DPD and PIPEDA (Canada)
- UK National Insurance and Japanese credit card numbers
- PII, HIPAA, ICD-9, ICD-10, National Drug Code and 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.



Proofpoint Email Data Loss Prevention (DLP) gives you unique visibility and enforcement of email security without the complexity and cost of disparate solutions. Our product automatically detects sensitive data, which you can manage centrally at the email gateway. Email DLP also makes it easier for you to define and administer policies across your email environment.

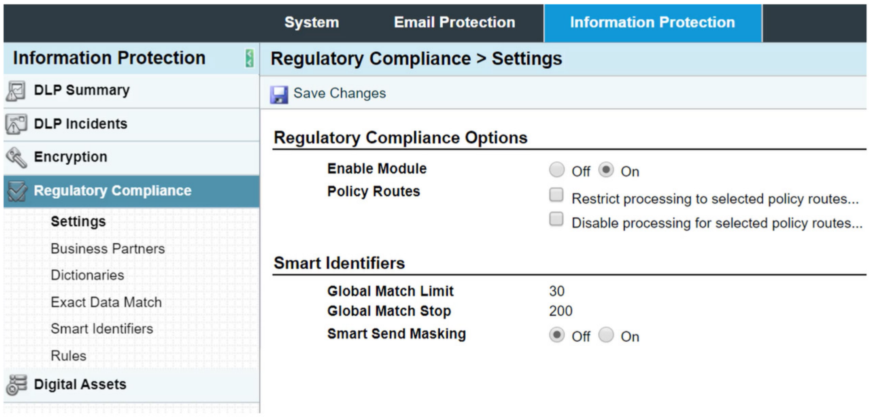
Email is the biggest vector for inbound threats. It is also a critical threat vector for outbound data loss. Proofpoint Email DLP gives you tighter control of your sensitive data. It helps you to protect your users from attacks that trick them into sending sensitive data by email. This increased security helps you to meet compliance standards such as CMMC 2.0, NIST 800-171, ISO 27001 and FedRAMP moderate.

Prevent data breaches

Email DLP identifies sensitive data and detects transmission of that data by email. This stops harmful data leaks from your company or agency.

Exact data matching

Email DLP has a feature called exact data matching. This feature detects sensitive data that must stay protected. You can upload or create custom dictionaries and identifiers that are unique to your company. For example, you might use financial account numbers, local forms of ID or medical record numbers to analyze email data that matters to you. You can expand the existing dictionaries with custom terms and codes. You can also use route-based definitions to create policies for inbound and outbound message streams.



Regulatory Compliance > Settings

Regulatory Compliance Options

Enable Module	○ Off ● On
Policy Routes	□ Restrict processing to selected policy routes... □ Disable processing for selected policy routes...

Smart Identifiers

Global Match Limit	30
Global Match Stop	200
Smart Send Masking	● Off ○ On

Figure 1: Centrally manage compliance and email DLP rules in the Proofpoint FedRAMP-hosted email gateway.

Protection from email fraud

Proofpoint Email DLP has more than 240 fine-tuned content identifiers. These identifiers detect and block messages that are typically used in business email compromise (BEC) attacks. They also greatly reduce the risk of sending employee records or W-2 forms, or of making wire transfers to impostors.

Deep analysis and fingerprinting

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

- Scan more than 300 file types out of the box.
- Use the file-type profiler to add support for new, custom or proprietary file types. File types can include patents and memos.
- Ensure that sensitive data outside standard Microsoft Office and PDF attachments is properly handled.
- Fingerprint sensitive documents with both full and partial matching. Fingerprint data even if it is in different file formats.

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:

- High confidence about the detection of non-compliant communications.
- Detailed algorithmic checks that are 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.

You can weight dictionary terms to increase or decrease their matching strengths. You can also weight terms to allow exceptions.

Smart Send

The Smart Send feature lets email senders fix their own outbound policy violations. Smart Send is powerful and easy to administer. It helps to educate users while freeing up your IT resources for other tasks. You can define routing for each policy. This lets you reroute sensitive assets back to the user, HR, IT or anyone else.

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.