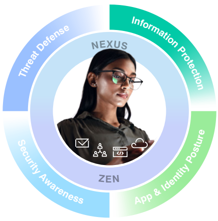
Preventing Email Data Loss in Merger and Acquisition Events

Use Proofpoint Adaptive Email DLP to stop the loss of sensitive data during mergers and acquisitions

Key Benefits

- Prevent accidental and intentional data loss by email
- Avoid damage to your company's reputation
- Improve security awareness across your company
- Get effective email security with easy administration and minimal user disruption
- See fast time to value, with protection in as little as 48 hours

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.



Mergers and acquisitions greatly increase the number of people sharing confidential information between companies by email. For information security teams, it is also difficult to track all the employees and third parties that are involved. These factors raise the risk of sensitive data being leaked.

Proofpoint Adaptive Email DLP (which stands for data loss prevention) solves these problems. Adaptive Email DLP uses behavioural artificial intelligence (AI) to learn your employees' email behaviours, their trusted relationships and how they share data. Our product analyses emails to detect unusual behaviour and notify administrators. And it warns users in real time, before critical leaks happen.

Why mergers and acquisitions increase risk

During mergers or acquisitions, companies must share a lot of highly confidential information. This might include personnel information, board documents, private equity data and other types of intelligence.

According to Gartner research, these transactions increase the risk of data loss in the following ways:

- There might be conflicts between the security practices of the two companies.
- Uncertainty or secrecy about the transaction can cause anxiety. This might lead employees to act in unusual or damaging ways.
- Often, there are new technical needs. For example, after the transaction closes, companies might have to secure three different operating modes: sunset, transition and future modes. The attack surface is much larger during this time.

How Adaptive Email DLP protects your sensitive data

Loss of sensitive data can damage your company's reputation and be costly to fix. Adaptive Email DLP prevents this damage. Our product uses behavioural AI to detect and stop accidental and intentional email data loss. The AI analyses more than 12 months of email data to learn your employees' email behaviours, trusted relationships and how they handle sensitive data.

Adaptive Email DLP uses this AI training to recognise anomalous email behaviour when it happens. Examples of this are an employee misdirecting an email, sending sensitive data to a less secure, unauthorised account or deliberately exfiltrating information. When it detects problems, Adaptive Email DLP shows users warning messages in real time. Users can fix their actions to avoid data loss, with no extra input from an administrator.

For mergers and acquisitions, these features mean that Adaptive Email DLP stops confidential data from ending up in the wrong hands while keeping critical communications flowing.

Stop misdirected emails

A misdirected email is when a user sends an email to the wrong person. These are a common cause of data leaks in companies. They're also hard to stop with rules and policies. By learning employee email habits, Adaptive Email DLP warns users about misdirected emails before they send them.

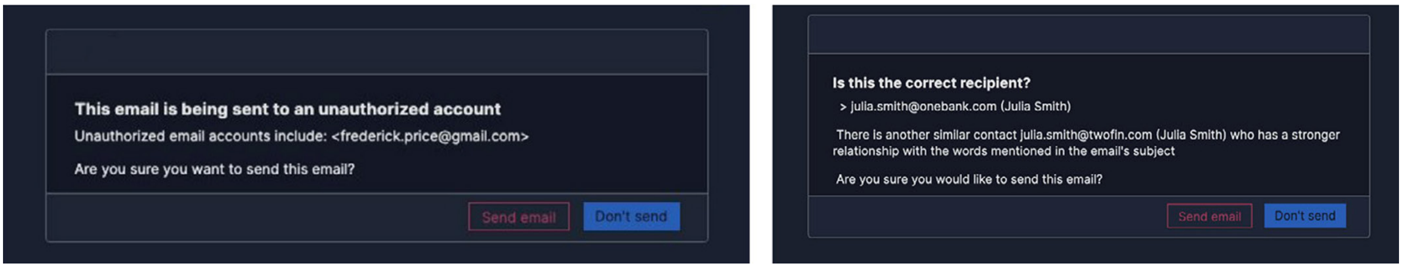
Prevent misattached files

A misattached file is when a user sends an email to the right person but attaches the wrong file. Like misdirected emails, Adaptive Email DLP uses AI to detect wrong attachments. It then warns users in real time.

Stop email exfiltration

Email rules can be effective in stopping data loss. However, these work only for known, predefined types of data, such as personal identifiable information (PII), payment card industry (PCI) information and social security numbers.

Adaptive Email DLP identifies and classifies your sensitive data. It also learns the personal email accounts of users, based on their email behaviour. If an employee tries to send sensitive data to themselves or others, our product can block or track their efforts based on its configuration.



This email is being sent to an unauthorized account

Unauthorized email accounts include: <frederick.price@gmail.com>

Are you sure you want to send this email?

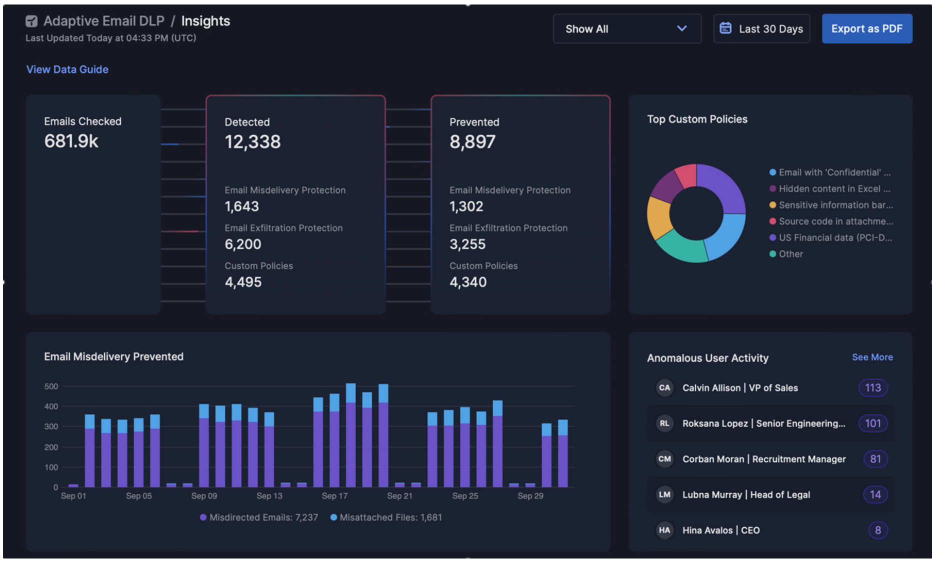
Is this the correct recipient?

> julia.smith@onebank.com (Julia Smith)

There is another similar contact julia.smith@twofin.com (Julia Smith) who has a stronger relationship with the words mentioned in the email's subject

Are you sure you would like to send this email?

Figure 1: Adaptive Email DLP warns users in real time about misdirected emails.



Adaptive Email DLP / Insights

Last Updated Today at 04:33 PM (UTC)

Emails Checked 681.9k

Detected 12,338
- Email Misdelivery Protection 1,643
- Email Exfiltration Protection 6,200
- Custom Policies 4,495

Prevented 8,897
- Email Misdelivery Protection 1,302
- Email Exfiltration Protection 3,255
- Custom Policies 4,340

Anomalous User Activity

CA	Calvin Allison | VP of Sales	113
RL	Roksana Lopez | Senior Engineering...	101
CM	Corban Moran | Recruitment Manager	81
LM	Lubna Murray | Head of Legal	14
HA	Hina Avalos | CEO	8

Show All
Last 30 Days
Export as PDF
View Data Guide
Top Custom Policies
● Email with 'Confidential' ...
● Hidden content in Excel ...
● Sensitive information bar...
● Source code in attachme...
● US Financial data (PCI-D...
● Other
Email Misdelivery Prevented
500
400
300
200
100
0
Sep 01
Sep 05
Sep 09
Sep 13
Sep 17
Sep 21
Sep 25
Sep 29
● Misdirected Emails: 7,237
● Misattached Files: 1,681
See More

Figure 2: The Adaptive Email DLP dashboard gives Information security teams full visibility of email threats.

Coach users in real time

Real-time coaching helps users avoid mistakes and policy breaches. As a companion to security awareness training, Adaptive Email DLP teaches users about risks in their emails. With this coaching, users can correct mistakes in real time and avoid data leaks.

Understand your threats

The Adaptive Email DLP dashboard gives an information security team a snapshot of all the emails the system is checking. The dashboard shows risky emails detected and blocked—including misdirected emails and misattached files—as well as email exfiltration attempts. It also shows security improvements over time for users and for the company.

Information such as top custom policies and riskiest users helps analysts to focus on what's most important. These insights speed up investigations and help security teams work with users to improve how they handle data.

Administer with ease

Adaptive Email DLP needs minimal setup or ongoing configuration. In just 48 hours, it starts preventing email data loss. It provides accurate and effective security interventions without disrupting the normal workflows of your users.

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' 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 organisations of all sizes, including 85 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**.