Adaptive Email DLP

Stop sensitive data loss by augmenting rules-based DLP with AI

Key Benefits

- Prevent accidental and intentional data loss through email
- Mitigate risks of market reputation and customer attrition
- Reduce fines from breaches of GDPR and CCPA
- Improve security awareness across the organisation

Despite existing email data loss prevention (DLP) controls, the top reported GDPR data breach type is "data emailed to the wrong person." While rules-based DLP plays a critical role in protecting known sensitive data such as PII, Social Security numbers and payment card data, there are risks it fails to detect. These include sensitive data being sent to the wrong party, and employees exfiltrating data to themselves and other unauthorised recipients.

Adaptive Email DLP uses behavioural AI to learn about your employees' normal email sending behaviours, their trusted relationships and how they communicate sensitive data. It then analyses each email to detect anomalous behaviour, notifying admins of potential data loss incidents. And it warns the user in real time and prevents sensitive data loss through email.

Stop Misdirected Emails

A misdirected email occurs when a user accidentally sends an email to the wrong person. It's a common source of data breaches in every organisation. It's also one that's challenging to stop with rules-based approaches.

Adaptive Email DLP can stop these breaches. It uses relationship graphs, deep content inspection and behavioural analysis to understand typical employee behaviour and identify data loss incidents. That means your organisation's sensitive data is protected when emails are sent to the wrong recipient or employees share the wrong attachment.

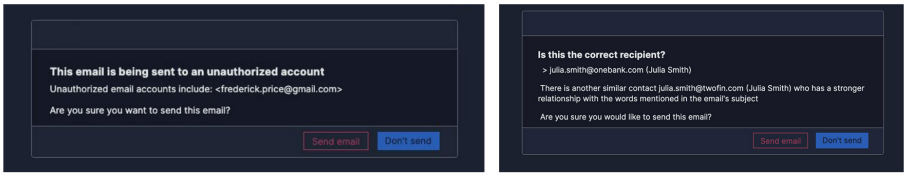

Figure 1: Adaptive Email DLP warns users in real time about potentially misdirected messages to prevent the loss of sensitive data through email.

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

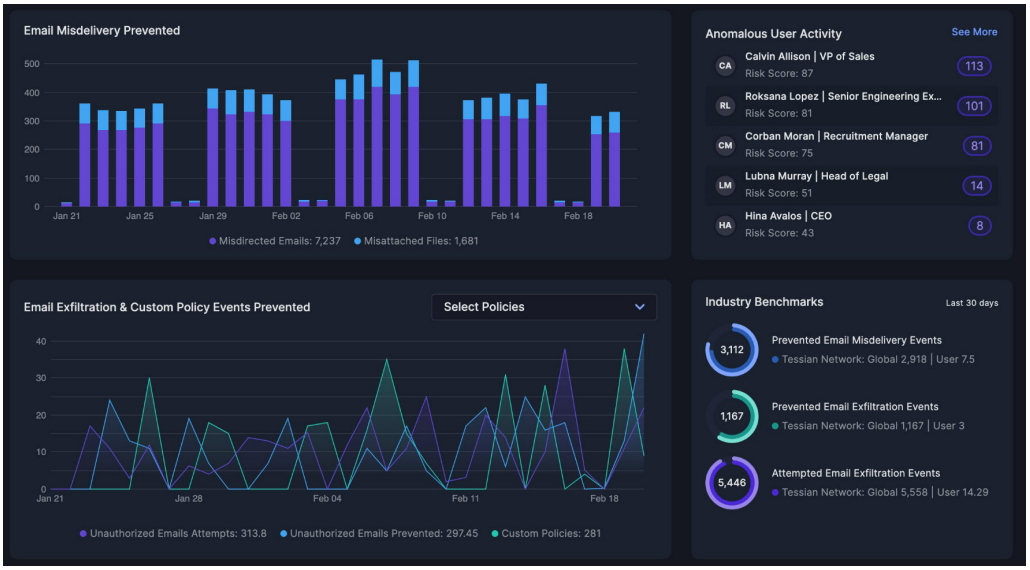

Figure 2: Security teams have increased confidence into email data loss visibility.

Prevent Misattached Files

A misattached file is when a user sends an email to the correct person, but accidentally attaches the wrong file.

When the behavioural AI detects an attachment that looks unusual for a recipient, Adaptive Email DLP resolves the issue. It automatically warns the user in real time before sensitive information is inadvertently sent to the wrong person.

Stop Email Exfiltration

Rules-based DLP is critical in preventing sensitive data loss, but only for predefined risks like PII, PCI and Social Security numbers. Breaches persist from insiders that share sensitive data that isn't pre-defined to personal emails and other unauthorised accounts.

Adaptive Email DLP stops sensitive data exfiltration by automatically classifying sensitive data. It also discovers the personal email accounts of users based on their email behaviour. So if an employee tries to exfiltrate data to themselves or others, these attempts are automatically blocked or tracked based on configuration.

Coach Users in the Moment

Real-time coaching for users can help them avoid mistakes and policy violations before they happen. As a complement to security awareness training, Adaptive Email DLP teaches your users about the risks in their emails in real time. This enables them to correct their mistakes and prevent sensitive data loss incidents.

LEARN MORE

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