proofpoint.

SOLUTION BRIEF

Modernize email data security with an adaptive approach

For multi-layered protection against email data loss, add Adaptive Email DLP

Key benefits

- Prevent accidental and intentional data loss through email
- Mitigate risks of damaged market reputation and customer attrition
- Reduce fines from breaches of the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA)
- Improve security awareness across your organization

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

Losing sensitive data can be disruptive and damaging to your business. In the Proofpoint *2024 Data Loss Landscape* report, 85% of surveyed companies said that they had a data loss incident in the previous year. For 50% of those companies, the incidents caused business disruption. Careless users were cited as the most common cause of data loss.

Email data loss prevention (DLP) is a critical component of your organization's overall data security strategy. It protects sensitive data from unwanted exposure through email. An effective email DLP program combines content scanning, real-time alerts, policy enforcement and user education. It prevents data loss and ensures your compliance with legal and regulatory requirements.

Traditional email DLP products can provide a solid foundation by enforcing rules and defined policies for known risks. However, you can significantly enhance your email data protection strategy by using both a traditional email DLP product and Proofpoint Adaptive Email DLP. This combined solution enables a more dynamic, human-centric approach to preventing data loss through email.

Here's how adding Adaptive Email DLP to your solution can benefit your organization:

More comprehensive protection

- **Traditional email DLP products** focus on content. They provide rule-based protection against known risks such as sensitive data being sent by email. They're effective at protecting known, well-defined, structured data. This includes personal identifiable information (PII), credit card numbers and more.
- **Adaptive Email DLP** looks at context. It extends the coverage given by traditional email DLP products to also protect you against unknown and evolving threats. Adaptive Email DLP uses behavioral AI to detect unusual user behavior. It can detect when a user sends sensitive data to an unintended recipient, shares files in an unusual pattern or sends an email to an unauthorized account.

1/3 of users

sent one or two emails to the wrong recipient.

Source: Proofpoint *2024 Data Loss Landscape* report

84%

of misdirected emails last year contained attachments.

Source: Proofpoint *2024 Data Loss Landscape* report

50%

In 2023, 50% of error-related breaches were caused by misdelivery.

Source: Verizon *2024 Data Breach Investigations* report

160,000

Adaptive Email DLP prevented more than 160,000 misdirected emails in 2024.

Source: Proofpoint

Adaptive detection

Adaptive Email DLP uses behavioral AI to detect email activity that differs from users' normal behaviors. Our AI doesn't just look for specific data patterns. Instead, it analyzes a broader context that includes:

- Who users typically send emails to
- What types of attachments users commonly share
- How users normally handle sensitive data

Adaptive Email DLP adapts to your employees' behaviors and evolving email patterns. It detects potential data loss incidents even when the data isn't well defined. For example, suppose an employee who doesn't normally send financial data suddenly tries to send an attachment that contains financial information to an unauthorized external contact. In this situation, Adaptive Email DLP detects the unauthorized email account and the sensitive attachment and flags it.

Stop misdirected emails

A misdirected email is when a user accidentally sends an email to the wrong person. Misdirected emails are a common source of data breaches. Proofpoint data shows that 33% of workers send one or two misdirected emails each year. They're also the most reported data loss behavior seen by the UK Information Commissioner's Office.[1] In addition, Verizon found that 50% of error-related breaches in 2023 resulted from misdelivery.[2]

Misdirected emails are challenging to stop with traditional email DLP products. By contrast, Adaptive Email DLP uses deep content inspection and behavioral analysis from Proofpoint Nexus® Relationship Graph (RG) to identify misdirected emails before they're sent. When a user tries to send an email to a wrong recipient, Adaptive Email DLP catches the error and intervenes with a warning. Proofpoint data shows that Adaptive Email DLP prevented more than 160,000 misdirected emails in 2024.

Prevent misattached files

A misattached file is when a user sends an email to the right person but attaches a wrong file. When our behavioral AI detects an attachment that seems unusual for a given recipient, it warns the user in real time. The user can fix the problem before a damaging data loss event occurs.

1. Information Commissioner's Office. "Common data protection mistakes (and how to fix them)." February 2025.
2. Verizon. *2024 Data Breach Investigations Report*. 2024.

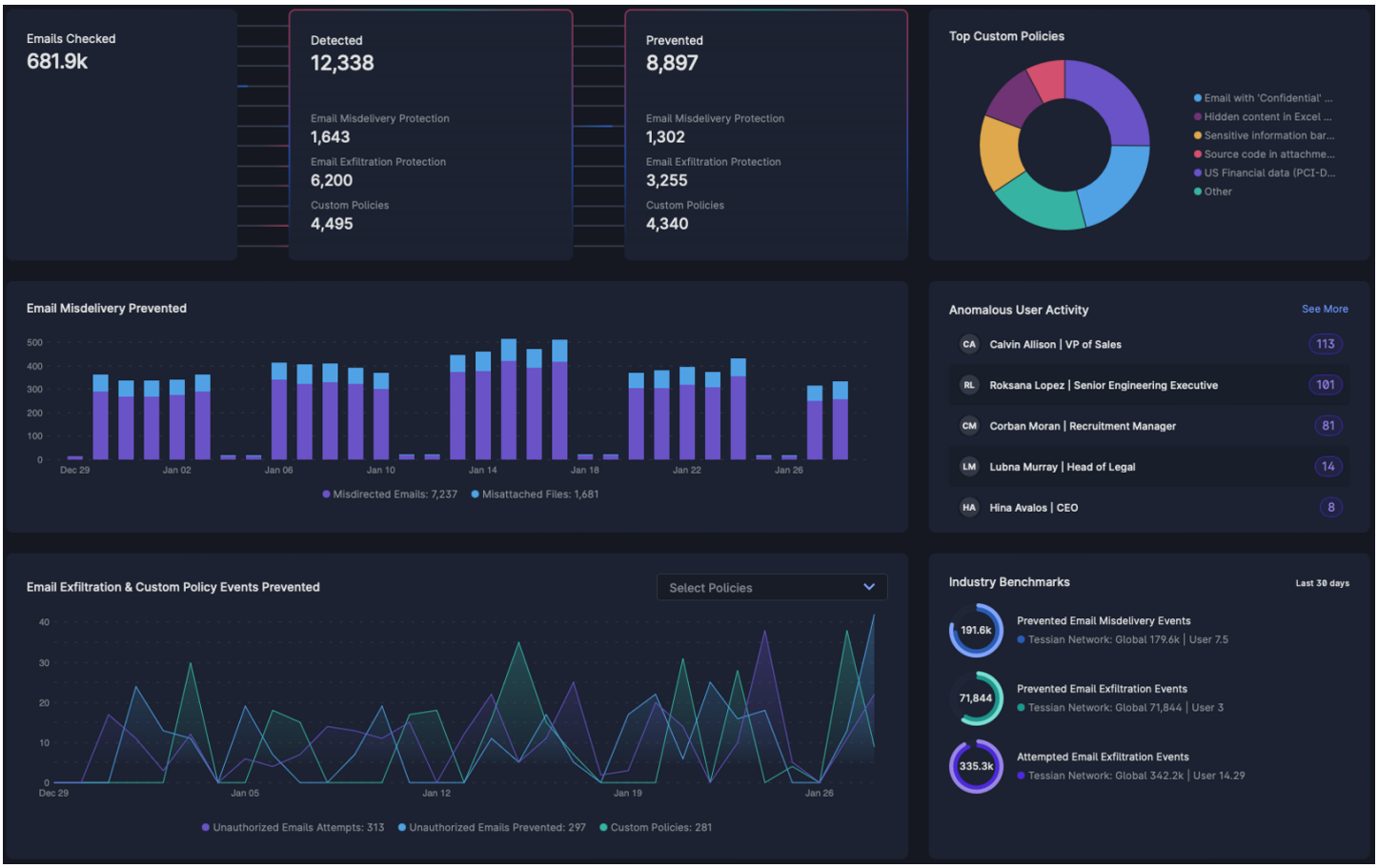

Figure 1: The Adaptive Email DLP dashboard gives information security teams full visibility and increased confidence about data loss prevention.

1,100,000

Adaptive Email DLP detected more than 1,100,000 data exfiltration emails in 2024.

Source: Proofpoint

Block costly email exfiltration

Exfiltration of sensitive data via email is costly for an organization to fix. The Ponemon Institute found that it takes a security team 48 to 72 hours to identify and remediate a successful data exfiltration event.[3] Adaptive Email DLP removes this ongoing burden on your team. It automatically analyzes and classifies your sensitive data. It also discovers the personal or unauthorized email accounts of your users. If a user tries to exfiltrate sensitive data to themselves or others, Adaptive Email DLP blocks or tracks their efforts, based on its configuration. Proofpoint data shows that Adaptive Email DLP detected more than 1,100,000 data exfiltration emails in 2024.

3. Ponemon Institute. "Email Data Loss Prevention: The Rising Need for Behavioral Intelligence." May 2022.

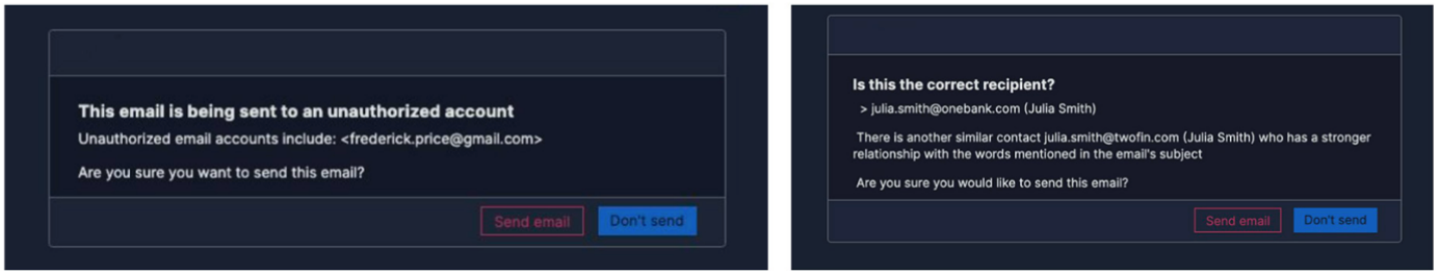

Figure 2: Adaptive Email DLP warns users in real time about emails to unauthorized accounts and misdirected emails.

Coach users in the moment

Real-time user coaching helps to stop mistakes and policy violations. As a complement to security awareness training, Adaptive Email DLP teaches users in real time about risks in their emails. Users can fix their own mistakes without the help of an administrator.

Better together

The consequences of losing sensitive data can be serious. These incidents can cost your company regulatory fines, reputation damage and lost business. They can also increase your labor costs because of investigations and regulatory and compliance reporting.

By integrating both a traditional email DLP product and Proofpoint Adaptive Email DLP, your organization can take a modern, multi-layered approach to email data security. This solution combines robust protection against known risks with dynamic, intelligent detection of unknown, human-centric data loss threats. You get enhanced data protection, improved user compliance, reduced operational overhead and a stronger overall email data security posture.

proofpoint.

DISCOVER THE PROOFPOINT PLATFORM →