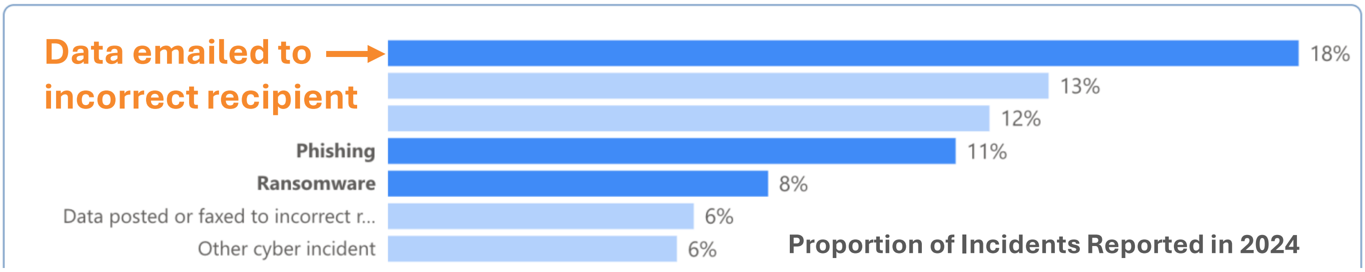
proofpoint. | Protect People. Defend Data.

Adaptive Email DLP:

Solving the #1 reported incident of email data loss

- The UK's ICO and Verizon's Data Breach Investigations Report show that the number one reported data loss incident was "Data emailed to incorrect recipient".
- Without visibility into these data loss events the risks of reputational loss, customer attrition or regulatory fines has dramatically increased.
- Misdirected emails and email exfiltration, poses a substantial risks to organisations.

Data Loss Reported to the ICO by Type



UK's ICO: https://ico.org.uk/action-weve-taken/data-security-incident-trends/

Rule-Based DLP is not enough...

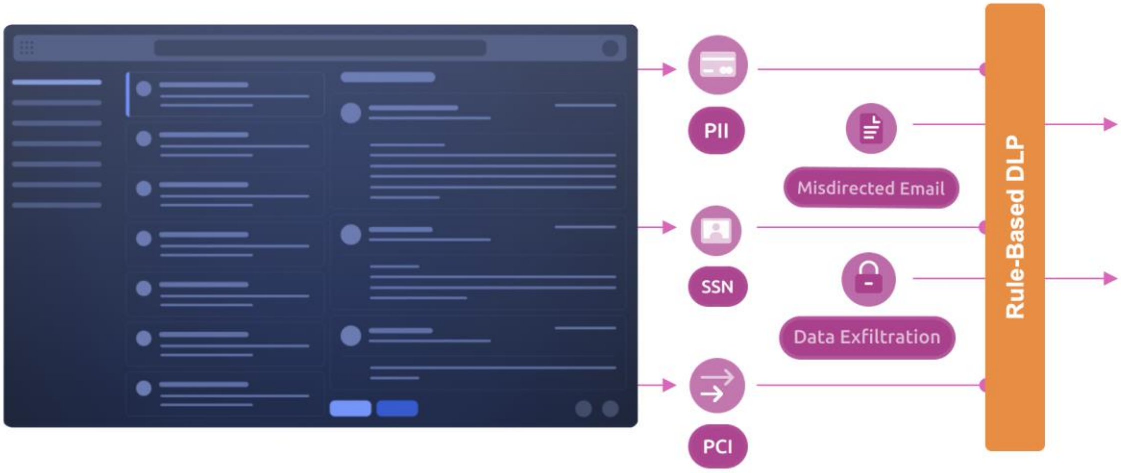
Adaptive Email DLP (AE-DLP) uses behavioural AI to learn about an employees' normal email sending behaviours, their trusted relationships and how they communicate sensitive data. It then analyses each email to detect anomalous behaviour, notifying admins of potential data loss incidents. And it warns the user in real time and prevents sensitive data loss through email missed by rule-based DLP technologies, like Symantec or Microsoft's Purview.

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 organization. It's also one that's challenging to stop with rules-based DLP approaches.

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 unauthorized accounts.



proofpoint. | Protect People.
Defend Data.

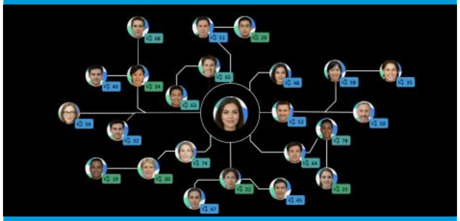
Adaptive Email DLP:

Leveraging Behavioural AI

Adaptive Email DLP uses behavioural AI to learn your employees' normal email sending behaviours, their unauthorised recipient addresses, and how they communicate sensitive data. It then analyses sending patterns to detect anomalous behaviour, creating an overview of potential data loss incidents.

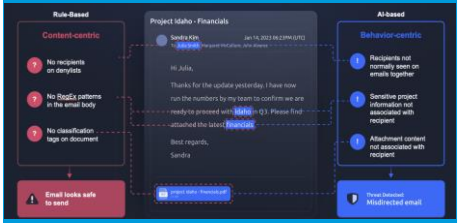
Real-time coaching for users can help them avoid mistakes and policy violations before they happen. As a complement to security awareness training, Adaptive Email DLP teaches your users about the risks in their emails in real time. This enables them to correct their mistakes and prevent sensitive data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

Behavioural Intelligence Modeling



- Learn normal vs. anomalous behaviour from up to twelve months of historical email data.
- Quantify human risk scores for security teams.

Automatic Prevention



Rule-Based

Content-centric

? No recipients on denylists

? No RegEx patterns in the email body

? No classification tags on document

Email looks safe to send

Project Idaho - Financials

Sandra Kim Jan 14, 2023 06:23PM (UTC)

To: Julia Smith Margaret McCallum, John Alvarez

Hi Julia,

Thanks for the update yesterday. I have now run the numbers by my team to confirm we are ready to proceed with Idaho in Q3. Please find attached the latest Financials.

Best regards,

Sandra

project idaho - financials.pdf

AI-based

Behavior-centric

! Recipients not normally seen on emails together

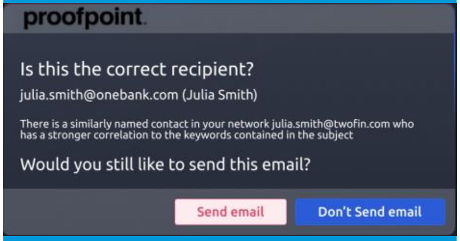
! Sensitive project information not associated with recipient

! Attachment content not associated with recipient

Threat Detected:
Misdirected email

- Automatically detects and prevents: Misdirected emails, Mis-attached files, data sent to unauthorized accounts
- No overhead for security teams and no disruption for employees.

In-The-Moment Security Coaching



proofpoint.

Is this the correct recipient?

julia.smith@onebank.com (Julia Smith)

There is a similarly named contact in your network julia.smith@twofin.com who has a stronger correlation to the keywords contained in the subject

Would you still like to send this email?

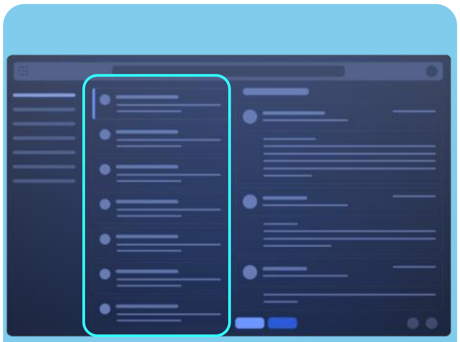
- Notify employees with contextual warning messages when incidents are detected.
- Employee feedback improves behavioral intelligence models.
- Customize warnings with logo and specific wording.

Deploy an Email Data Loss Assessment:

proofpoint.
Adaptive Email DLP
+
Microsoft Exchange
Google Workspace

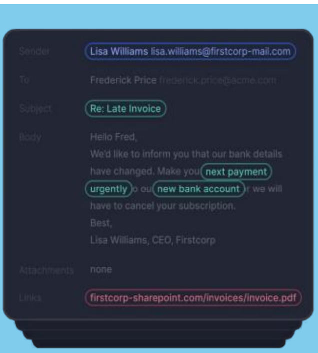
Deploys in Minutes

Adaptive Email DLP integrates with existing email infrastructure in <5 minutes via API



Learns in Hours

Adaptive Email DLP ingests up to 12 months of historical email data to automatically build user behavioural profiles



Sender Lisa Williams lisa.williams@firstcorp-mail.com

To Frederick Price frederick.price@acme.com

Subject Re: Late Invoice

Body Hello Fred,
We'd like to inform you that our bank details have changed. Make you next payment urgently to our new bank account or we will have to cancel your subscription.
Best,
Lisa Williams, CEO, Firstcorp

Attachments none

Links firstcorp-sharepoint.com/invoices/invoice.pdf

Protects in Days

24 hours after deployment, Adaptive Email DLP automatically detects and prevents data loss

Adaptive Email DLP:

Product and Competition Overview

Discovery Questions	• What visibility do you have over data loss on email? • If sensitive data was sent to the wrong person or exfiltrated via email, what would happen? • Who would get involved and what would they do? • Who would need to be notified? How much time would be spent? • How much time is spent on these types of activities? • How do you prevent misdirected emails or data exfiltration via email?

AE-DLP Market Overview:

	Email Exfiltration	Misdirected Emails
Market Trends	**4,300 Incidents a Year** Avg. No. reported for a 5,000 User Org **29% of orgs. lost a customer due to email data loss** Financial Times 2023	**#1 Reported Incident** UK ICO and Verizon Data Breach Inv. Report **40% of users email the wrong person** Financial Times 2023

AE-DLP Data	**95% Reduction** in number of Exfil. attempts after 1 month of deployment	**<1 hour per week** spent investigating alerts for a 10,000 user org.	**47%** F100 using Proofpoint DLP	**#2** DLP market share

Product Performance	**$50m** AE-DLP Revenue	**83%** POC to Close Conv	**63 Days** Average Sales Cycle

Add-on protection with AE-DLP: Adaptive Email DLP can either be sold as an upsell to existing Proofpoint customers as part of their platform or as a standalone technology for brand new customers, layering on top of Microsoft to stop sensitive data exfiltration and misdirected emails.

Competitive Differentiators:

Solution Efficacy:

Adaptive Email DLP uses machine learning to analyze 12-months of historical email data, providing day-one value. Low-cost solutions below **rely on finite rules, showing results months after deployment.**

Employee Disruption:

Adaptive Email DLP offers infrequent, clear warnings boosting productivity. Low-cost solutions listed below **send near daily alerts without context, causing alert fatigue.**

Solution Stability:

Adaptive Email DLP deploys via Microsoft Add-In, ensuring zero mail flow disruption. Low-cost solutions below **rely on Microsoft Moderator Mailbox, prone to outages.**

AE-DLP competes with:

egress SafeSend mimecast

proofpoint. | Protect People. Defend Data.

Adaptive Email DLP:

Engaging with customers

A great question to start the conversation:

Ask a customer if they have ever...

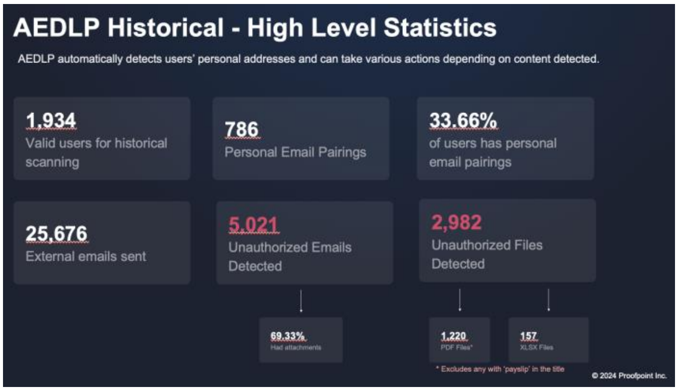
Sent an email to the wrong person?

Attached the wrong file to an email?

Sent documents to a personal email address?

Show the data... Run an Email Data Loss Assessment

- **Available via the** Partner Portal, AE-DLP can demonstrate critical business data being lost by reviewing data loss incidents to highlight sensitive data leaving an organisation.
- Lightweight, silent API deployment that only takes five minutes to set up.



AEDLP Historical - High Level Statistics

AEDLP automatically detects users' personal addresses and can take various actions depending on content detected.

1,934 Valid users for historical scanning

786 Personal Email Pairings

33.66% of users has personal email pairings

25,676 External emails sent

5,021 Unauthorized Emails Detected

2,982 Unauthorized Files Detected

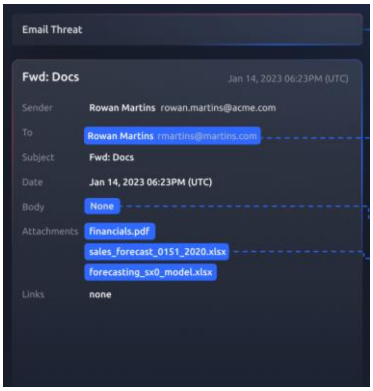
69.33% Had attachments

1,220 PDF Files*

157 XLSX Files

* Excludes any with 'payslip' in the title

© 2024 Proofpoint Inc.



Email Threat

Fwd: Docs Jan 14, 2023 06:23PM (UTC)

Sender Rowan Martins rowan.martins@acme.com

To Rowan Martins rmartins@martins.com

Subject Fwd: Docs

Date Jan 14, 2023 06:23PM (UTC)

Body None

Attachments financials.pdf
sales_forecast_0151_2020.xlsx
forecasting_sx0_model.xlsx

Links none

Subjects & Attachments of Emails that were Exfiltrated	
Passwords.txt	ZZ **Contract - Signed**-signed.pdf
Budget.xlsx	RE: OOOOOII Mechanical **Proposal**
FW: **Confidential** - Purchasing Map	2024-05 **Contacts.CSV**
FW: OOOII **Audit Package**	CM **Bonuses**
special board meeting 6.12.24.pdf	**Vendor Bid list.xlsx**
Collated**ProjectProfitability**0424.pdf	**Revenue_2023.xlsx**