

SOLUTION BRIEF

Proofpoint Adaptive Email DLP data loss assessment

Detect insider exfiltration. Understand risk.
Stop email data loss with AI.

Key benefits

- Gain comprehensive visibility into insiders sending sensitive data to unauthorised accounts
- Detect personal email account pairings
- Quantify sensitive data exfiltration patterns over a six-month period
- Understand user behaviour and potential intent
- Receive an executive-ready readout report of findings

Email remains the number one channel for data exfiltration.

Sensitive data is regularly exfiltrated to personal email accounts or newly created external addresses—whether through malicious actions or simple mistakes—yet organisations often lack visibility into user intent or emerging risk patterns.

Proofpoint platform data shows that, on average, a 10,000-user organisation will experience 1,500-plus exfiltrations of highly sensitive data to unauthorised email accounts over a six-month period.

As AI accelerates content creation and sharing, **Proofpoint Adaptive Email DLP** detects behavioural and communication anomalies and prevents sensitive data from leaving via email.

Adaptive Email DLP combines behavioural AI, detection of sensitive content and comprehensive account relationship analysis. It identifies insider-to-external account pairings, detects unusual sending patterns and evaluates user intent. These capabilities provide deep visibility into highly sensitive data leaving the organisation by email to personal or unauthorised accounts.

The **Adaptive Email DLP data loss assessment** is designed to quantify this risk within your environment. It gives your organisation a clear, prioritised path to reducing insider-driven email data loss.

What's included

- ✓ **Detection of unauthorised email account pairings**
 - Identification of insider-to-external account pairings that indicate potential unauthorised or personal account usage
 - Detection of personal email account pairings (for example, webmail accounts)
 - Analysis of sensitive communication patterns between internal users and external accounts
- ✓ **Analysis of sensitive data exfiltration**
 - Identification of sensitive data sent to detected unauthorised or personal accounts (for example, personally identifiable information (PII), protected health information (PHI), financial data, intellectual property and confidential business information)
- ✓ **Six-month historical lookback to identify existing risk**
 - Identification of personal and unauthorised account pairings
 - Examination of sensitive data exfiltrated to personal and unauthorised accounts
 - Analysis of trends for repeat behaviour or escalating activity
 - Detection of persistent or developing insider risk patterns

✓ Executive readout, summary and tailored recommendations

At the end of the assessment, you'll receive:

- Executive summary readout of unauthorised and personal account pairings
- Detailed inventory of sensitive data exfiltrated and which users exfiltrated it
- Overview of risk trends identified during the six-month historical review
- Insights into user behaviour and potential intent indicators
- Executive-ready summary report of findings and prioritised recommendations to reduce insider-driven email data loss.

Getting started is easy and included at no charge

As a Proofpoint customer, you're entitled to an Adaptive Email DLP data loss assessment at no additional cost.

Getting started involves a brief call to initiate the assessment, which includes an overview of the following steps:

Directory sync—Synchronises group membership and user properties.

Mailbox onboarding—Enables historical processing and remediation.

Live sync—Enables processing of live emails as they're sent and received.

Mailbox protection—Required for compliance alerts. Permission not required for assessment.

After initiation, you'll see initial findings in approximately 48 hours (Microsoft 365 only). Proofpoint will deliver your comprehensive readout shortly afterwards.

There is no complex deployment, no disruption to users and no long implementation cycle—just rapid visibility into insider-driven email data exfiltration risk.

Schedule your data loss assessment

To schedule your 15-minute kickoff call or learn how this assessment applies to your environment, contact your Proofpoint account manager or visit <https://www.proofpoint.com/uk/learn-more/data-loss-assessment>.

proofpoint®

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises and millions of smaller organisations in stopping threats, preventing data loss and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organisations of all sizes protect and empower their people while embracing AI securely and confidently. ~~Learn more~~ at www.proofpoint.com/uk.

Connect with Proofpoint: [LinkedIn](#)

Proofpoint is a registered trademark or trade name of Proofpoint, Inc. in the United States and/or other countries. All other trademarks contained herein are the property of their respective owners.

DISCOVER THE PROOFPOINT PLATFORM →