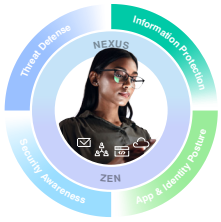
# Supporting MS Purview with Proofpoint Adaptive Email DLP

For stronger and smarter prevention of email data loss, pair Microsoft Purview with Proofpoint 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.




Microsoft Purview and Proofpoint Adaptive Email DLP both tackle email data loss prevention (DLP). But the products use separate approaches and mitigate different risks. To build the most comprehensive and robust protection against email data loss, support your Purview deployment with the intelligence of Adaptive Email DLP.

## How Purview and Adaptive Email DLP compare

Purview takes a policy-based approach that can deliver most of the features of secure email gateways. These include communication encryption and data governance and retention. But Purview relies on administrator-managed rules that are slow and error-prone to implement, hard to maintain, and not sufficient to stop all risks. Purview also lacks behavioral analysis to learn the intentions of your users. This understanding is crucial to distinguishing true risks from false positives.

Adaptive Email DLP uses behavioral artificial intelligence (AI) to prevent both accidental and intentional email data loss. By stopping misdirected emails, incorrect attachments and data exfiltration attempts, it reduces your risks and remediation costs. And because your security team spends less time investigating false positives, they can focus instead on fine-tuning your protection.

## Purview doesn't stop misdirected emails

Email rules in Purview can be effective at stopping specific, predefined types of content from leaving your company. But they can't stop a user from sending an email to the wrong person. Stopping misdirected emails requires a deeper understanding of employees' typical behaviors, based on historical email context and content.

Adaptive Email DLP analyzes more than 12 months of historical email data to learn typical communication patterns between senders and recipients. It uses this intelligence to identify and stop misdirected emails before they happen.

## Purview is ineffective against email data exfiltration

Most data exfiltration by email occurs when employees send sensitive data to themselves. Often, this can happen when an employee is leaving to work at a competitor.

In Purview, broadly blocking freemail services such as Gmail and Yahoo doesn't work because this also blocks valid business email. It also cannot stop a user from sending data to a personal email domain. Flagging every interaction with freemail services creates too many false positives for your security team to analyze.

Adaptive Email DLP uses advanced AI that is trained on the richest data in the industry. By analyzing your employees' email behaviors, it learns to distinguish normal communications from suspicious ones. This results in more accurate and meaningful alerts that speed up investigations and save you time and resources.

## Adaptive Email DLP coaches users in real time

In Purview, you can add policy tips that show warning messages when employees violate email policies. But these are time-consuming to configure and tune. And when warnings are too frequent, users can start to ignore them. This phenomenon is known as alert fatigue.

With no extra setup, Adaptive Email DLP gives users contextual, real-time warnings about their risky behaviors. Users can fix misdirected emails or wrong file attachments before they send them. If an employee tries to send confidential data to themselves or others, Adaptive Email DLP can block or track their efforts, based on its configuration.

# Better together

The consequences of email data loss 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.

To protect your most sensitive data and avoid these outcomes, you need a flexible and intelligent email DLP solution that goes beyond a static, rules-based approach.

By pairing Purview with the AI-driven power of Adaptive Email DLP, your company can build comprehensive and robust protection against email data loss.

## Learn more at proofpoint.com