

FREQUENTLY ASKED QUESTIONS

Proofpoint Adaptive Email DLP



General questions

What is Proofpoint Adaptive Email DLP?

Proofpoint Adaptive Email DLP uses an adaptive, human-centric approach to prevent accidental and malicious email data loss. It stops misdirected emails (emails sent to wrong recipients by mistake), unauthorized emails (sensitive emails sent to personal accounts) and non-compliance with company email policies. Our software integrates directly with Microsoft Outlook and requires no change to how you send or receive emails.

How does Adaptive Email DLP work?

Adaptive Email DLP uses machine learning (ML) to learn your employees' email behaviors, their trusted relationships and how they share data. By analyzing more than 12 months of historical email data, our ML models learn to recognize unusual email activity when it happens.

Questions for desktop users

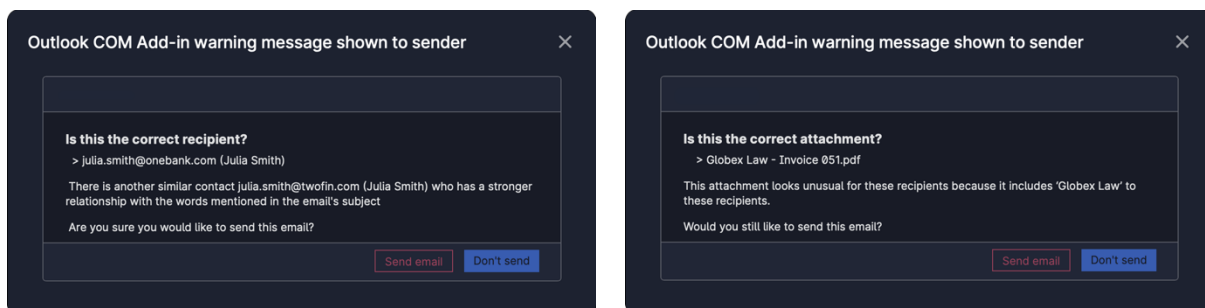
How does Adaptive Email DLP protect desktop users?

Adaptive Email DLP prevents data breaches caused by human error. Our ML models recognize when a user accidentally emails the wrong person or attaches the wrong file. When it detects a problem, Adaptive Email DLP shows the desktop user a warning message in real time. The user can fix their actions to avoid sensitive data loss without any input from an administrator.

What happens when a user sees a warning message?

When it detects unusual behavior and shows a warning message, Adaptive Email DLP temporarily stops the email from being sent. The warning message describes the anomaly detected in the email. For example, it describes when the user is about to send an email to an incorrect recipient, has attached the wrong file or is sending sensitive information to a non-business account.

As shown in the figure, the warning dialog also gives the user two options: to continue sending the email or to stop sending it.



If the user chooses to stop sending the email, Adaptive Email DLP returns them to the draft, where they can make changes. User responses to these warnings continue to train the Adaptive Email DLP ML models, making the models smarter over time.

Can users still send paystips, receipts, reservations etc. to a personal account?

Yes, they can. Adaptive Email DLP is not intended to stop users from sending *any* email to personal email addresses. Its powerful and accurate ML models recognize the difference between a user forwarding a dinner reservation to their personal account and sending an email that contains sensitive company information.

Questions for mobile users

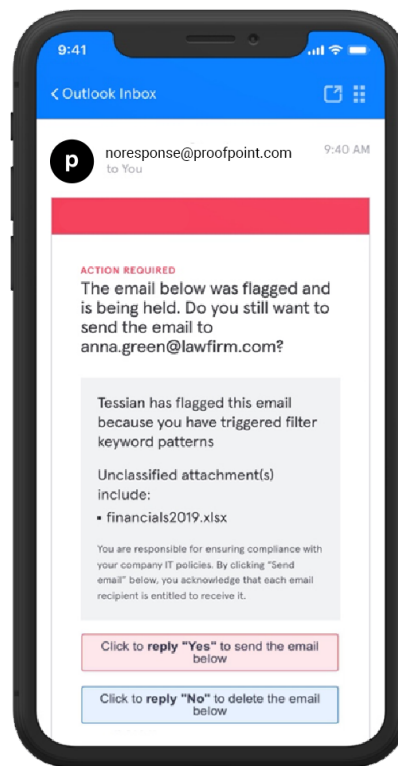
How does Adaptive Email DLP protect mobile users?

Adaptive Email DLP prevents data breaches caused by human error. Its ML models recognize when a user accidentally emails the wrong person or attaches the wrong file. When it detects a problem, Adaptive Email DLP sends the mobile user a bounceback warning email.

What happens when a user gets a bounceback warning email?

The bounceback warning email from Adaptive Email DLP temporarily stops the original email from being sent. The original email is held at the gateway during this time. The bounceback email describes the anomaly detected in the original email. For example, it describes when the user is about to send an email to an incorrect recipient, has attached the wrong file or is sending sensitive information to a non-business account.

As shown in the figure, the warning email also gives the user two options: to continue sending the original email or to stop sending it, which deletes it from the gateway.



User responses to these bounceback emails continue to train the Adaptive Email DLP ML models, making the models smarter over time.

What happens if a user misses or doesn't immediately reply to a bounceback warning email?

If a user misses the first bounceback email, Adaptive Email DLP sends another one after 10 minutes. It then resends the bounceback email every hour until the expiry time. The expiry time is shown at the bottom of the bounceback email. If the original email is still being held at the gateway when the expiry time is reached, Adaptive Email DLP deletes the email.

How does a user modify their original email?

When a user gets a bounceback email and needs to modify their original email to fix an anomaly, they should choose the No option in the bounceback warning email. This action deletes the email from the gateway. The user can find the original email in their Sent Items mailbox, where they can modify it.