WHITEPAPER

Understanding Core Email Protection API and Adaptive Email DLP

proofpoint®

Thank you for taking the time to evaluate Proofpoint Core Email Protection API and Adaptive Email DLP. In this paper, you'll discover comprehensive architecture details—including data synchronization flows and data storage and privacy mechanisms—that are used in our products. You'll learn about deploying the products via API, how the API works and the onboarding process to get started quickly. You'll also see the email flows for different deployment methods and how the end-user experience differs between them.

Introduction to Core Email Protection API and Adaptive Email DLP

PRODUCT OVERVIEWS

Core Email Protection API

Core Email Protection API **uses a layer of AI to stop email threats and prevent** lateral phishing. It stops phishing attacks by using behavioral AI that's trained on the industry's largest and most advanced dataset of known email threats. Core Email Protection API **provides email security, investigation and response, an abuse mailbox, internal mail detection and account takeover protection** in a single package. Users get **real-time coaching** with intuitive summaries of risks in their emails, helping them to avoid socially-engineered attacks and mistakes. To prevent account takeovers via lateral phishing, **our AI detects spikes in email volumes and unusual internal communications.**

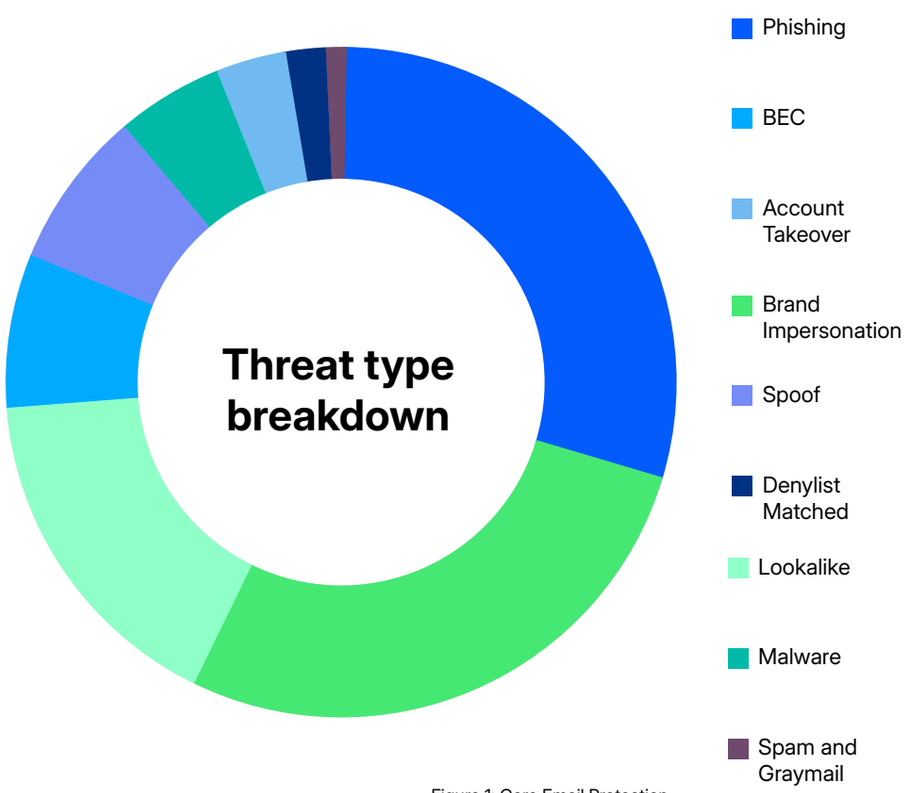


Figure 1: Core Email Protection API breaks down email threats by type to accelerate investigations.

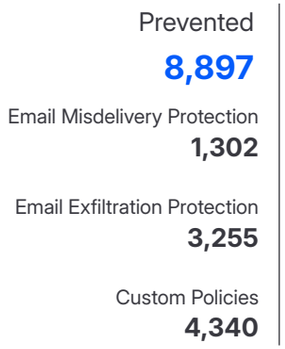


Figure 2: Adaptive Email DLP classifies email DLP incidents by type, enabling faster triage.

Adaptive Email DLP

Adaptive Email DLP **uses behavioral AI to prevent accidental and intentional data loss by email**. To recognize anomalous email behavior, it analyzes 12-plus months of email data to **learn employees' normal email behaviors, trusted relationships and how they handle sensitive data.** When it detects problems such as misdirected emails, misattached files or data exfiltration, Adaptive Email DLP **shows users warning messages in real time.** Users can fix their actions to avoid sensitive data loss without input from an administrator.

Overview of Proofpoint Nexus®

Proofpoint Nexus® is a comprehensive threat intelligence platform powered by artificial intelligence (AI), machine learning (ML) and real-time threat intelligence. Nexus mitigates the risks that people introduce to their organizations, especially in the face of rising phishing attacks, malware infiltration and cloud account takeovers. Nexus continuously analyzes billions of email, web and cloud interactions to detect and neutralize these threats before they compromise your data and systems.

Proofpoint Core Email Protection API and Adaptive Email DLP use each of the Nexus models described below:

Nexus Threat Intelligence (TI)	Nexus Language Model (LM)	Nexus Relationship Graph (RG)	Nexus Machine Learning (ML)	Nexus Computer Vision (CV)
Nexus TI integrates vast amounts of threat data to enhance detection capabilities across Proofpoint products. It provides real-time updates on emerging threats, attacker tactics and system vulnerabilities. With its focus on advanced threat intelligence, Nexus TI ensures Proofpoint solutions stay ahead of evolving cyberthreats, offering proactive detection and defense. This system is key to maintaining a resilient security posture against modern cyber adversaries.	**Nexus LM** harnesses the power of advanced AI language models to combat business email compromise (BEC). It carefully examines email content to detect common elements found in BEC attempts, such as transactional language and urgency. By recognizing subtle linguistic patterns and behavioral cues, Nexus LM identifies suspicious emails before they can cause harm. This cutting-edge solution adds a critical layer of defense, offering superior protection against sophisticated email-based attacks.	**Nexus RG** uses AI to monitor and assess user behavior, reinforcing cybersecurity defenses. By using behavioral analytics, machine learning and anomaly detection, Nexus RG spots deviations from normal user actions that may indicate a potential threat. Integrating seamlessly with our overall threat detection systems, Nexus RG enhances real-time defenses, providing you with comprehensive protection against behavior-driven cyber risks.	**Nexus ML** uses advanced machine learning to fortify our threat detection capabilities. By employing techniques such as supervised learning, unsupervised learning and ensemble methods, Nexus ML provides scalable and robust security solutions. This core AI technology ensures Proofpoint can detect and mitigate a wide range of evolving threats, providing you with comprehensive protection across multiple cybersecurity areas.	**CV** is an AI-powered module designed to identify and neutralize vision-based threats. Through advanced computer vision technology, Nexus CV detects threats hidden in visual elements, such as phishing sites, QR codes, malicious attachments and spoofed emails. By focusing on visual threat vectors, this module enhances security by providing you with a powerful response to attacks that involve embedded images and other graphical content.

MORE INFORMATION ABOUT PROOFPOINT NEXUS →

Nexus FAQs

What AI methods does Nexus use?

Nexus uses methods such as random forest, neural networks and natural language processing (NLP) to understand an employee's trusted relationships, the topics and projects they communicate about and what data they handle. Proofpoint uses these methods to analyze tens of thousands of email events. This powerful training enables Nexus to accurately distinguish unusual communications from normal ones.

Does Nexus use supervised or unsupervised machine learning?

Nexus models use unsupervised machine learning to analyze historical and real-time email data in order to understand users' behavior over email and identify when unusual behavior is occurring.

What data does Nexus use to build a behavioral profile for each user?

- **Email metadata –** To identify unusual content in emails, Nexus extracts and analyzes headers, names, attachments, links and more. To learn more, see the next section.
- **Email body –** To know when it should classify unusual content as malicious, Nexus uses NLP models to analyze email subjects and body text.
- **Historical email patterns –** Nexus uses deep learning methods to understand an employee's trusted relationships, the topics and projects they communicate about and what data they handle.

What languages does Nexus support?

Nexus is language-agnostic in its ability to detect potentially malicious, anomalous behavior in email.

Where do Nexus behavioral models store data?

Customer data is stored in Amazon Web Services (AWS) data centers in either Dublin, Ireland or Oregon, USA. During the onboarding process, customers can specify where they want their data to be hosted.

What data is retained and for how long?

- **Email metadata –** Retained for the period of service plus 30 days.
- **Full body emails –** Retained for up to 6 months from the point of collection. Customers can opt in to having full emails and attachments retained so that they can be used in advanced threat hunting and abuse mailbox workflows.

Does Proofpoint share my data with other tenants?

Proofpoint builds and retains behavioral statistics per tenant. We use these statistics to identify communication patterns between individuals. Such patterns include typical terms and topics, application types and project and attachment names. Proofpoint uses a specific tenant to store your portal data, behavioral statistics, and other user, account and configuration information. All of your data is logically segregated from other tenants.

The data that Proofpoint uses to train and improve ML models to detect malicious emails serves all tenants. This data includes attachment hashes and URLs that have been confirmed as malicious. Unlike generative AI such as ChatGPT, where users can extract text responses or "leak data" by careful prompt engineering that uses public APIs, our models are closed. We look for the likelihood of an email being malicious based on indicators in the email and return a disposition with a confidence number.

How does Nexus build its models and keep them current?

Nexus uses data from email environments to train its models to prevent cybersecurity incidents and mistakes. Proofpoint synchronizes historical and live email data from the email environment to our back end for processing and anomaly detection. Each of the data types below are required for the solutions to effectively perform their email cybersecurity functions.

Core Email Protection API permissions

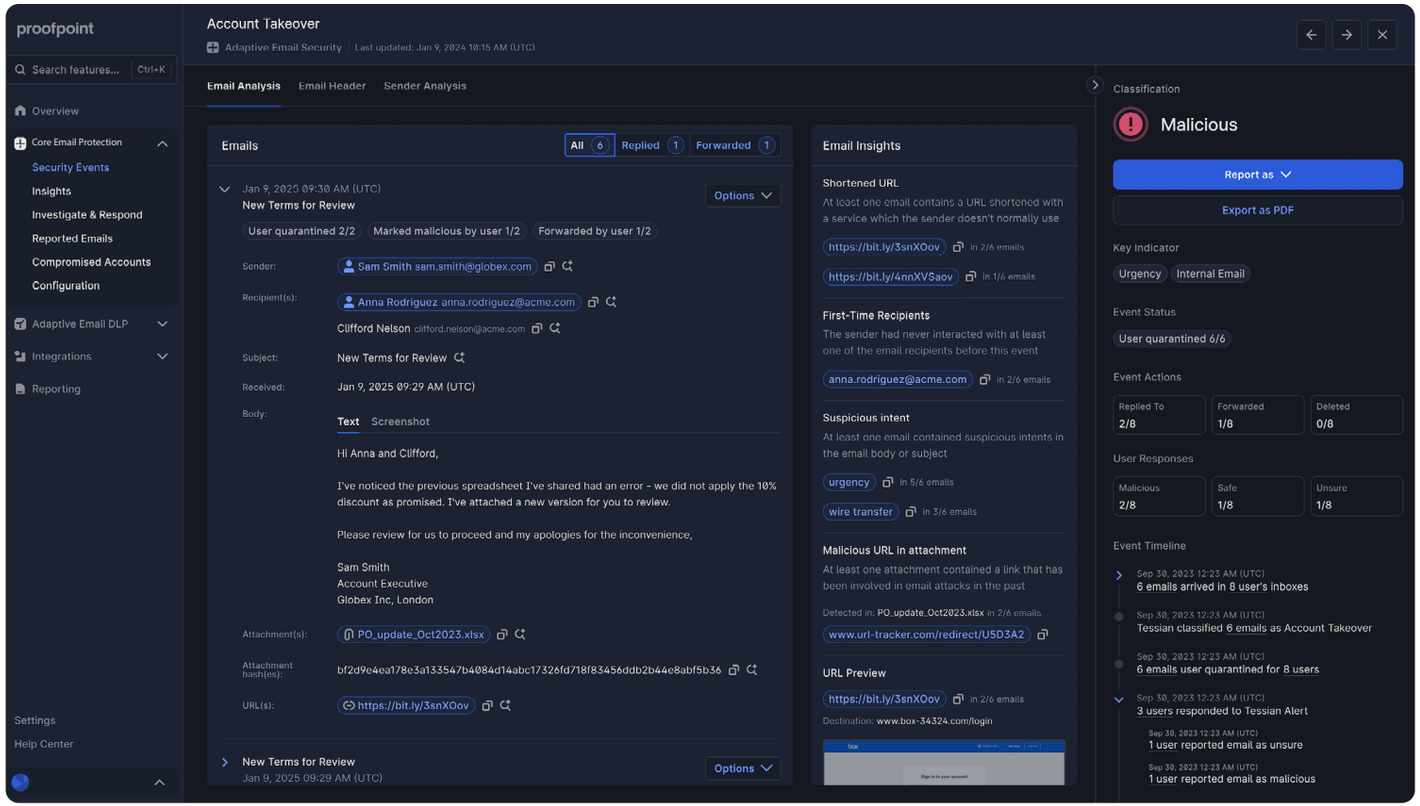
Can I limit access to certain types of data and actions in the platform?

Yes, organizations can create custom roles using the permissions matrix shown to the right. This includes restricting access to full email bodies to certain administrative users.

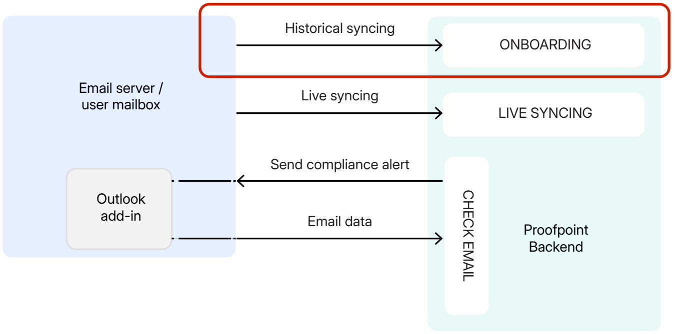
	Administrator	All Actions (except...	Read-only Adminis...
Action Quarantined Emails Release or delete quarantined emails	✓	✓	✓
Audit Trail View a record of actions taken by portal users within the Tessia...	✓	✓	✓
Constructor Filters View and edit Constructor filters	✓	✓	✓
Custom Policies View and edit Custom Policies filters and access other pages w...	✓	✓	✓
Email Exfiltration Filters & Custom Sensitivity View and edit Email Exfiltration filters. Customize Email Exfiltrat...	✓	✓	✓
Email Misdelivery Protection Filters View and edit Email Misdelivery Protection filters	✓	✓	✓
Email Search / Investigation & Response Search across all emails and report threats to Tessian	✓	✓	✗
Email Threat Defense Configuration View and edit Email Threat Defense configuration	✓	✓	✓
G Suite and O365 API Configure API deployment on Office 365 and Google Workspace	✓	✓	✗
Groups View and edit groups	✓	✓	✓
Integrations Access the Tessian API and other integrations	✓	✓	✓
Portal User Administration Manage who can log into the Tessian dashboard	✓	✗	✗
Remove From Inbox (All Emails) Remove any email from mailboxes anywhere in the Tessian plat...	✓	✓	✗
Security Events View security events in the portal and download reports in xlsx ...	✓	✓	✓
Security Settings Edit security settings, internal domains and download new Outl...	✓	✓	✓
User Monitoring Monitor which users are connecting to the Tessian server	✓	✓	✓
View Full Email Body (All Emails) View the email body and download attachments of any email in...	✓	✓	✗
View Full Email Body (Security Events Only) View the email body, download attachments, and remove email...	✓	✓	✓

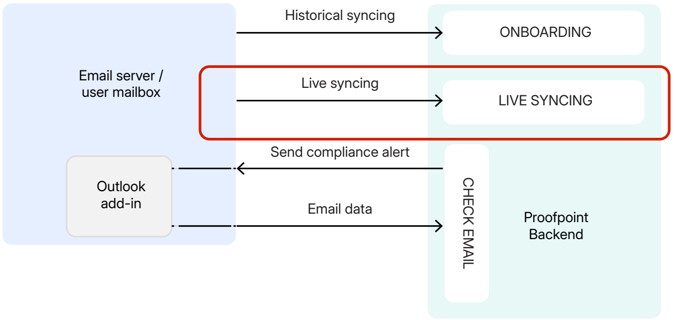
Core Email Protection API metadata

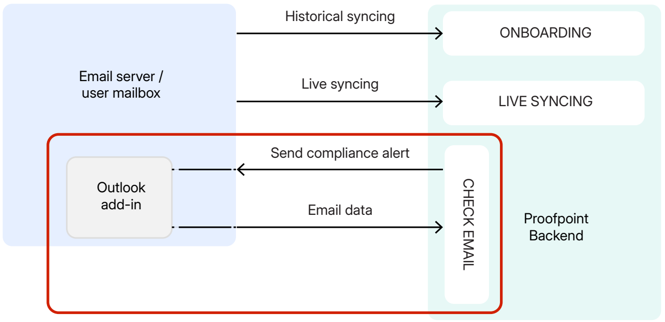
The following figure shows an indicative but non-exhaustive list of the metadata extracted by Core Email Protection API.



Data synchronization and email checks







Historical syncing

This syncing process is required to train the machine learning models that Core Email Protection API and Adaptive Email DLP use. The process looks at up to 12 months of historical email data. For Microsoft 365 and Gmail, the process uses backend API connections between Proofpoint and the email servers for those services. Proofpoint reads all of the email data, which is temporarily transferred (as part of the API response) to the Proofpoint backend environment. Proofpoint extracts metadata to store and then deletes the email. Because API connections are not available for Microsoft Exchange on-premise customers, the Outlook COM add-in is required for syncing this data from Outlook. In this case, only the email metadata is transferred to Proofpoint.

Live syncing

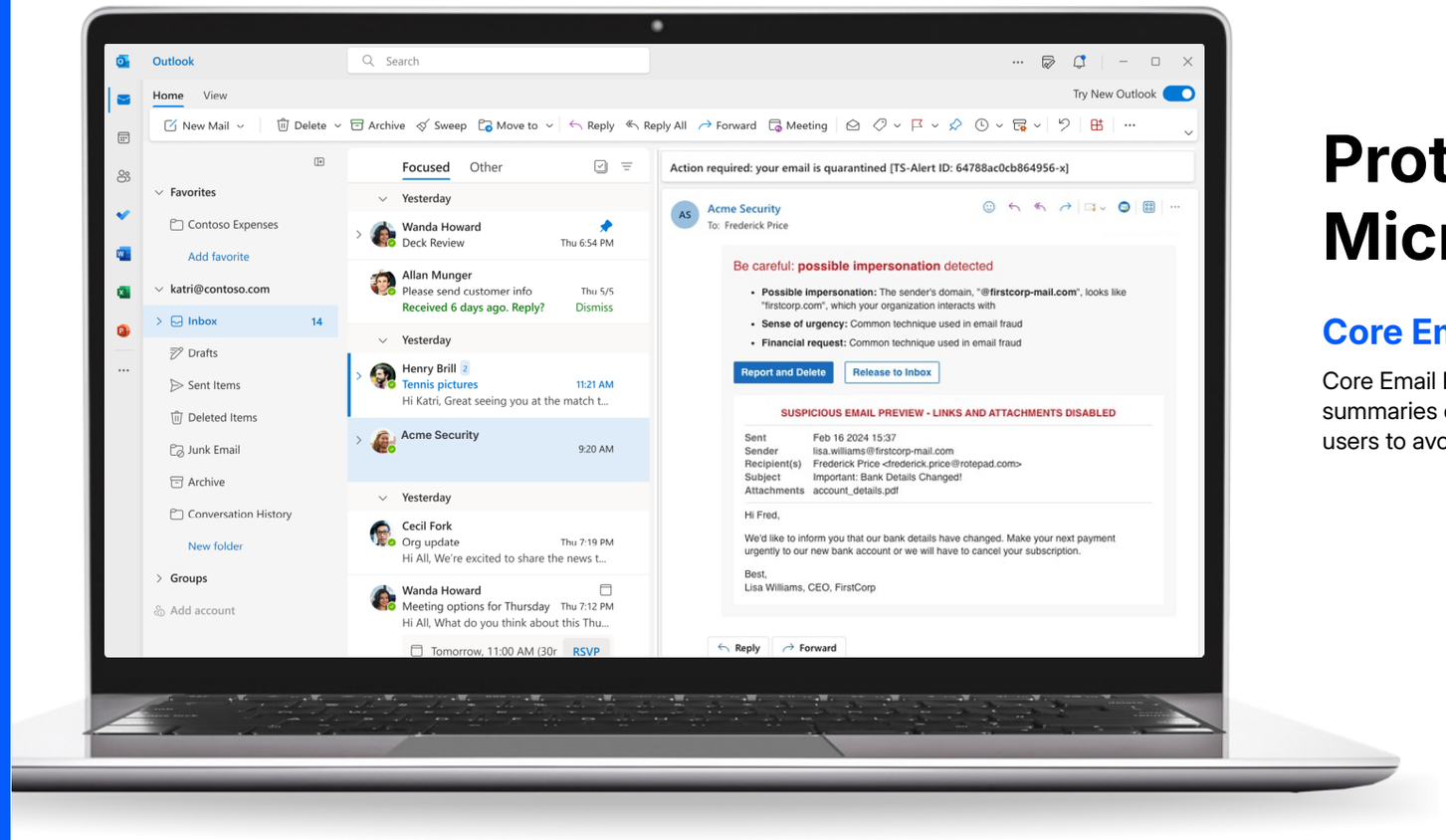
Similar to historical syncing, this process is required to keep the machine learning models up to date as users send and receive emails. For Microsoft 365, the process uses Graph APIs to read and process all user emails as they are sent and received. Proofpoint gets a notification of any new email. Using the ID in the notification, Proofpoint reads all of the email data, which is temporarily transferred (as part of the API response) to the Proofpoint backend environment. For MS Exchange on premise customers live syncing is enabled by a COM add-in. For Gmail customers live syncing is enabled via gateway.

Outbound email check

The email check process can occur in two places: via an Outlook add-in in the user's email client or while the email is passing through the email server. During a check, all the email and attachment data is temporarily sent to Proofpoint for processing*. When a user clicks Send, the Outlook add-in checks the email in real time. If the check returns a result in the allowed timeout period, the email is either cleared for sending or the user gets a warning. The warning dialog gives the user a choice of continuing to send the email or returning to the draft. If an email is sent without a check, the server-side, connector-based integration** acts as a backup and scans the email. If the check result requires an end-user alert, the alert is sent by an interactive email bounceback. Gmail customers must use the Gateway integration because there is no add-in support.

* The Outlook COM add-in sends only extracted metadata to Proofpoint, whereas both the Microsoft 365 Outlook add-in and gateway send the full email and attachment data.
** The server-side connector-based integration is the gateway.

proofpoint.



Protection for Microsoft 365

Core Email Protection API

Core Email Protection API coaches users in the moment with intuitive summaries of risks in their emails. These real-time interventions help users to avoid socially engineered attacks and mistakes.

Figure 8: Core Email Protection API automatically quarantines malicious emails. It also gives users real-time warnings about suspicious ones, while neutralizing links and attachments.

Deploying Core Email Protection API for Microsoft 365

For all devices, you deploy Proofpoint Core Email Protection API by using our Microsoft 365 Graph API. During onboarding, all new users must undergo an historical learning phase that trains Proofpoint machine learning models on past email sending patterns, behaviors and relationships. This enables our models to make better decisions and provide more accurate real-time alerts. When a user completes the onboarding phase, they become an active user in the portal. They can then receive Core Email Protection API alerts (subject to configuration).

The Microsoft 365 API during onboarding

The historical learning phase is a one-time, 12-month historical sync for all new users. The sync is initiated when you set up Microsoft 365 API integration in the Core Email Protection API portal. When the historical sync is complete for each user, Microsoft 365 API live syncing takes over.

How does the API work?

The API enables Core Email Protection API to extract email data directly from your Microsoft 365 mail servers. It downloads a copy of each full email being sent or received (or from the last 12 months in the case of the historical sync), including attachments. It then temporarily stores the email. Proofpoint servers extract and store the metadata required for analysis. When the processing and email check has finished, the full email is immediately deleted. Emails are never stored. The extracted metadata is used to train the Proofpoint machine learning models during your onboarding phase and throughout your Core Email Protection API contract.

Enabling user reporting

Enabling the Outlook add-in allows your end-users to report suspicious emails for further review in the Core Email Protection API abuse mailbox. This solution works with most “Report Phishing” buttons. Administrators need only to add an alert mailbox address that can send and receive emails.

Setting up Microsoft 365 API integration

Prerequisites:

- The person setting up the integration has the Global admin role for your Microsoft 365 domain.
- All the domains that you want to sync mailboxes for (both historical and live) are listed in your portal under Settings > Internal Email Domains.
- You know the names of any Azure groups that you want to scope the Proofpoint connection to. For example, an all-staff group or specific departmental groups. These groups cannot be dynamic.

The steps to complete the wizard are as follows:

1 In your Core Email Protection API portal, click **Integrations > Microsoft 365.**

2 In the first step of the wizard, select the feature(s) that you want to configure. For onboarding, select **Mailbox Protection.** This automatically selects the Azure Directory Sync, which is required.

3 Click **Next** to connect to your tenancy. Log into Azure to locate your **M365 Tenant ID**. Paste your tenant ID into the wizard. Proofpoint verifies this ID when it submits the whole integration.

4 Click **Next** to grant the relevant permissions for all the selected features. For Core Email Protection API, all of the permissions listed below are required. Each permission opens a new tab for you to log in and accept.

- Directory Sync
- Mailbox Onboarding & Actions
- Mailbox Live Syncing

5 Click **Next** to advance to the **Connect to Directory**. Add the groups that you want to import into the portal. These can be via display name or email. Proofpoint recommends importing an all-staff group or specific departmental groups to set up Microsoft Defender protection, email syncing and enhanced reporting.

6 Click **Next** to finish the setup and save the details in the portal.

(For new customers) On the **Mailbox tab,** specify which user mailboxes should be included in the historical email sync. Click **Save Settings.**

When you have granted permissions for the Microsoft 365 API, the Core Email Protection API onboarding team initiates the historical sync.

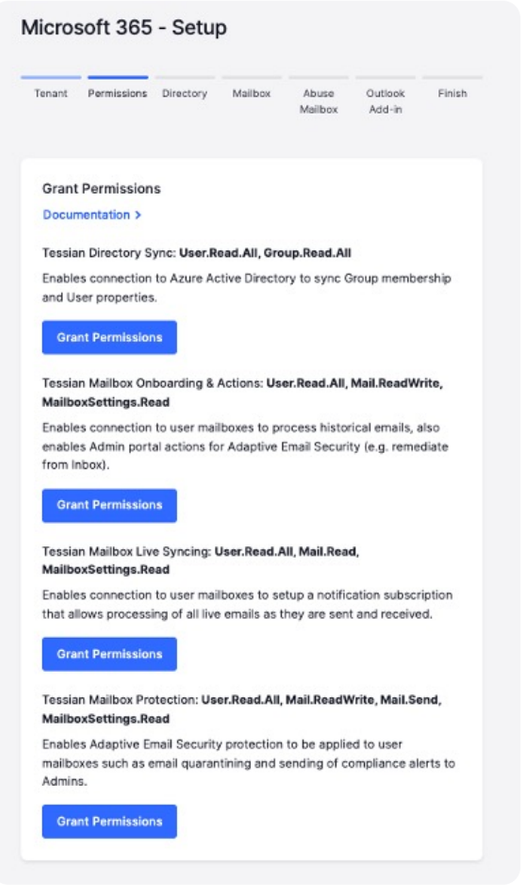


Figure 9: Overview of the Azure applications that Core Email Protection API needs to connect to the Microsoft Graph API

Mail flow architecture: Core Email Protection API deployment for Microsoft 365

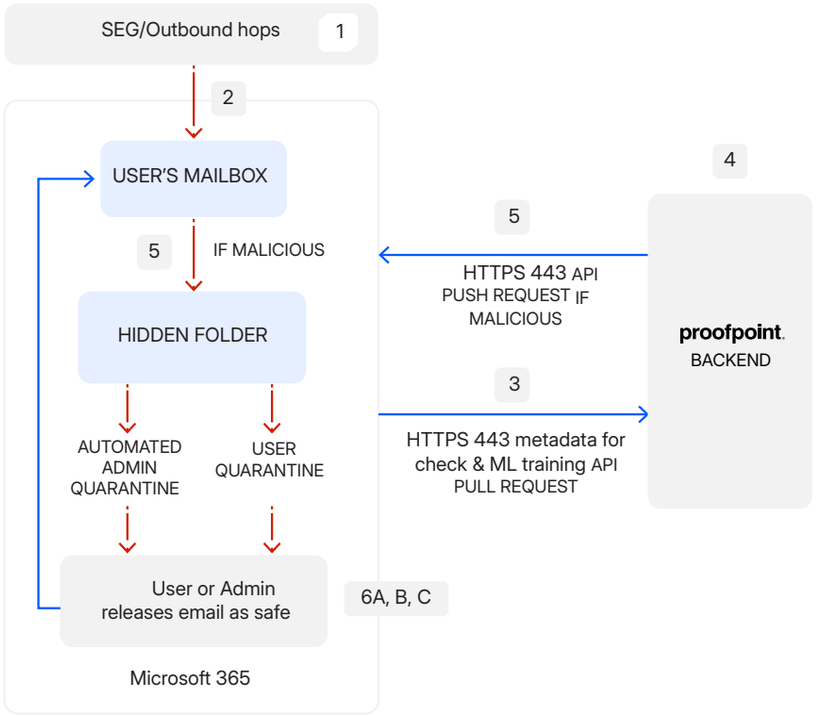


Figure 10: Mail Flow Architecture: Core Email Protection - API deployment for Microsoft 365.

1 If you're using a secure email gateway (SEG), the SEG scans for spam, signature-based malware, and emails from your domain blocklist or whitelist. It also performs scans based on threat intelligence and rule-based impersonation protection. For organizations that have consolidated their email security stack and are not using an SEG, Microsoft 365 performs the threat-intelligence-based scan.

2 The email is delivered to the end-user inbox.

3 Proofpoint gets a push notification from the API to read email data and attachments. Proofpoint also extracts the required metadata.

4 Proofpoint analyzes the extracted metadata to determine if the email is malicious. The Proofpoint backend stores the metadata and uses it to continuously train our algorithm.

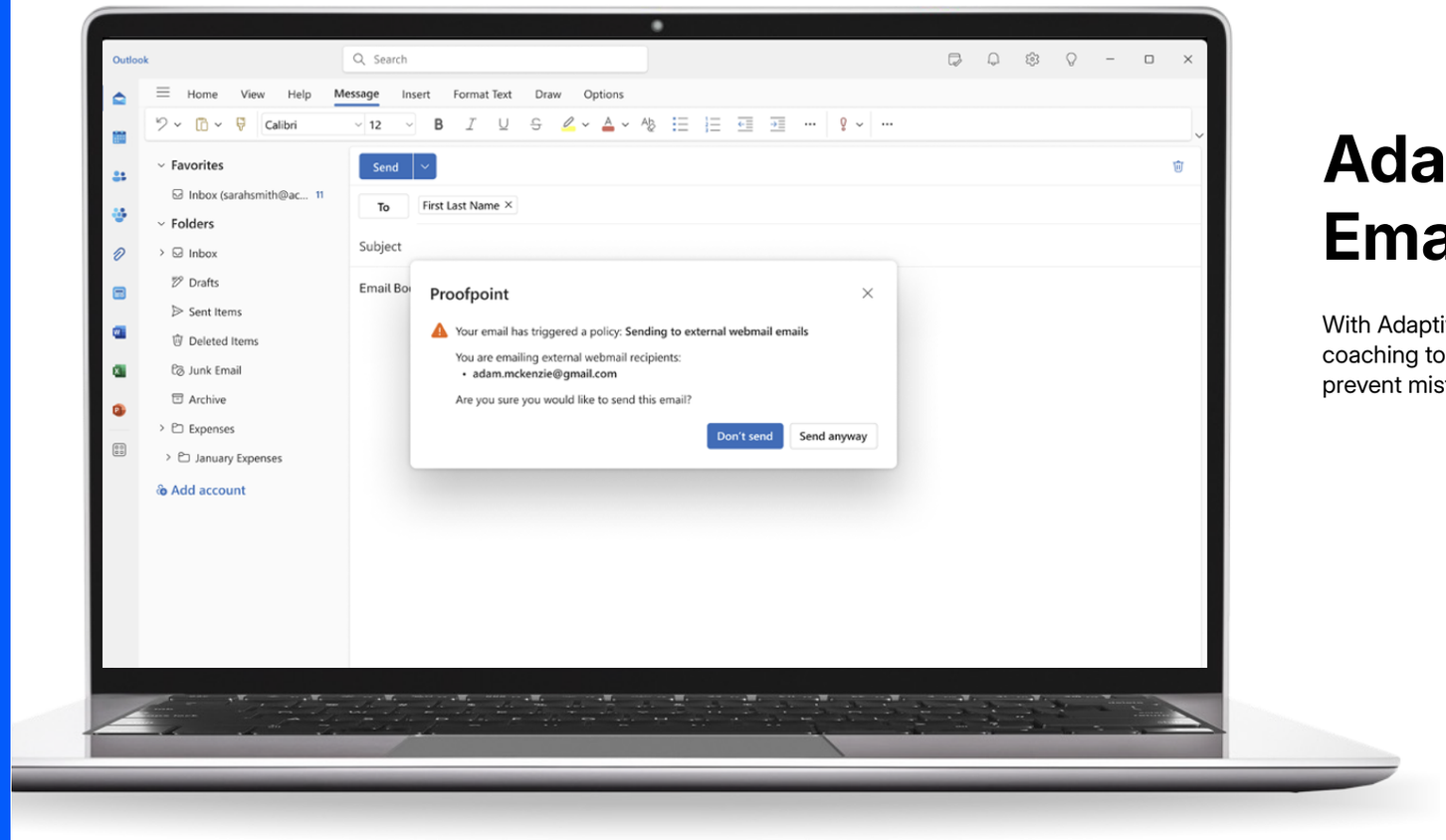
5 If Proofpoint determines that the email might be malicious, the API moves the email to the hidden folder.

6 Proofpoint's Admin Quarantine feature quarantines emails that have a high probability of being malicious.

Proofpoint's User Quarantine feature takes in emails with a lower probability of being malicious. Coached by a Proofpoint training banner along with a safe copy of the email, the user can review the email themselves. The email copy has the attachment removed and URL deactivated, preventing the user from accidentally opening these before ensuring that the email is safe.

The next steps are as follows:

- If the user marks the email as safe, the API moves the email back to the user mailbox.
- If the user marks the email as malicious, the email remains in the hidden folder.
- If the user takes no action, the email remains in the hidden folder.



Adaptive Email DLP

With Adaptive Email DLP, end users get real-time coaching to reinforce organizational policies and prevent mistakes.

Figure 11: Adaptive Email DLP provides in the moment pop-ups to users when the system detects an accidental or intentional data loss event.

Deploying Adaptive Email DLP for Microsoft 365

For all devices, you deploy Proofpoint Adaptive Email DLP by using our Microsoft 365 Graph API. During onboarding, all new users must undergo an historical learning phase that trains Proofpoint machine learning models on past email sending patterns, behaviors and relationships. This enables our models to make better decisions and provide more accurate real-time alerts. When a user completes the onboarding phase, they become an active user in the portal. They can then receive Adaptive Email DLP alerts (subject to configuration).

The Microsoft 365 API during onboarding

The historical learning phase is a one-time, 12-month historical sync for all new users. The sync is initiated when you set up Microsoft 365 API integration in the Adaptive Email DLP portal. When the historical sync is complete for each user, Microsoft 365 API live syncing takes over.

How does the API work?

The API enables Adaptive Email DLP to extract email data directly from your Microsoft 365 mail servers. It downloads a copy of each full email being sent or received (or from the last 12 months in the case of the historical sync), including attachments. It then temporarily stores the email. Proofpoint servers extract and store the metadata required for analysis. When the processing and email check has finished, the full email is immediately deleted. Emails are never stored. The extracted metadata is used to train the Proofpoint machine learning models during your onboarding phase and throughout your Adaptive Email DLP contract.

Enabling user reporting

Enabling the Outlook add-in allows end-users to report suspicious emails for further review in the Adaptive Email DLP abuse mailbox. The solution works with most “Report Phishing” buttons. Administrators need only to add an alert mailbox address that can send and receive emails.

Enabling mobile and backup protection

You can protect non-Outlook email clients and Outlook Mobile by deploying the Adaptive Email DLP Outbound Gateway.

Setting up Microsoft 365 API integration

Prerequisites:

- The person setting up the integration has the Global admin role for your Microsoft 365 domain.
- All the domains that you want to sync mailboxes for (both historical and live) are listed in your portal under Settings > Internal Email Domains.
- You know the names of any Azure groups that you want to scope the Proofpoint connection to. For example, all staff or specific departmental groups. These groups cannot be dynamic.

The steps to complete the wizard are as follows:

1. In your Adaptive Email DLP portal, click **Integrations > Microsoft 365.**

2. In the first step of the wizard, select the feature(s) that you want to configure. For onboarding, select **Mailbox Protection.** This automatically selects the Azure Directory Sync, which is required.

3. Click **Next** to connect to your tenancy. Log into Azure to locate your **M365 Tenant ID**. Paste your tenant ID into the wizard. Proofpoint verifies this ID when it submits the whole integration.

4. Click **Next** to grant the relevant permissions for all the selected features. For Adaptive Email DLP, all of the permissions listed below are required. Each permission opens a new tab for you to log in and accept.
   - Directory Sync
   - Mailbox Onboarding & Actions
   - Mailbox Live Syncing
   - Mailbox Protection

5. Click **Next** to advance to the **Connect to Directory**. Add the groups that you want to import into the portal. These can be via display name or email. Proofpoint recommends importing an all-staff group or specific departmental groups to set up Microsoft Defender protection, email syncing and enhanced reporting.

6. Click **Next** to advance to the **Connect to Mailbox.** Choose the user mailboxes that you want enable live syncing for. You can choose any of the mailboxes that you imported, or all mailboxes. Live syncing is required to train the Proofpoint machine learning models. To enable Microsoft Defender warnings, specify an internal Microsoft 365 mailbox to send and receive the warning and user responses **(NOTE:** This cannot be a distribution group and must have the ability to send and receive emails).

7. Click **Next** to finish the setup and save the details in the portal.

8. (For new customers) On the **Mailbox tab,** specify which user mailboxes should be included in the historical email sync. Click **Save Settings.**

   When you have granted permissions for the Microsoft 365 API, the Adaptive Email DLP API onboarding team initiates the historical sync.

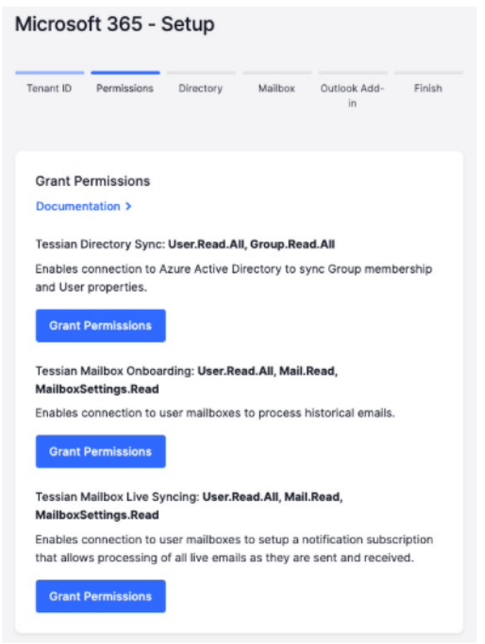


Figure 12: Overview of the Azure applications that Adaptive Email DLP needs to connect to the Microsoft Graph API

Mail flow architecture: Adaptive Email DLP API deployment for Microsoft 365

AEDLP M365 Add-in Data Flows

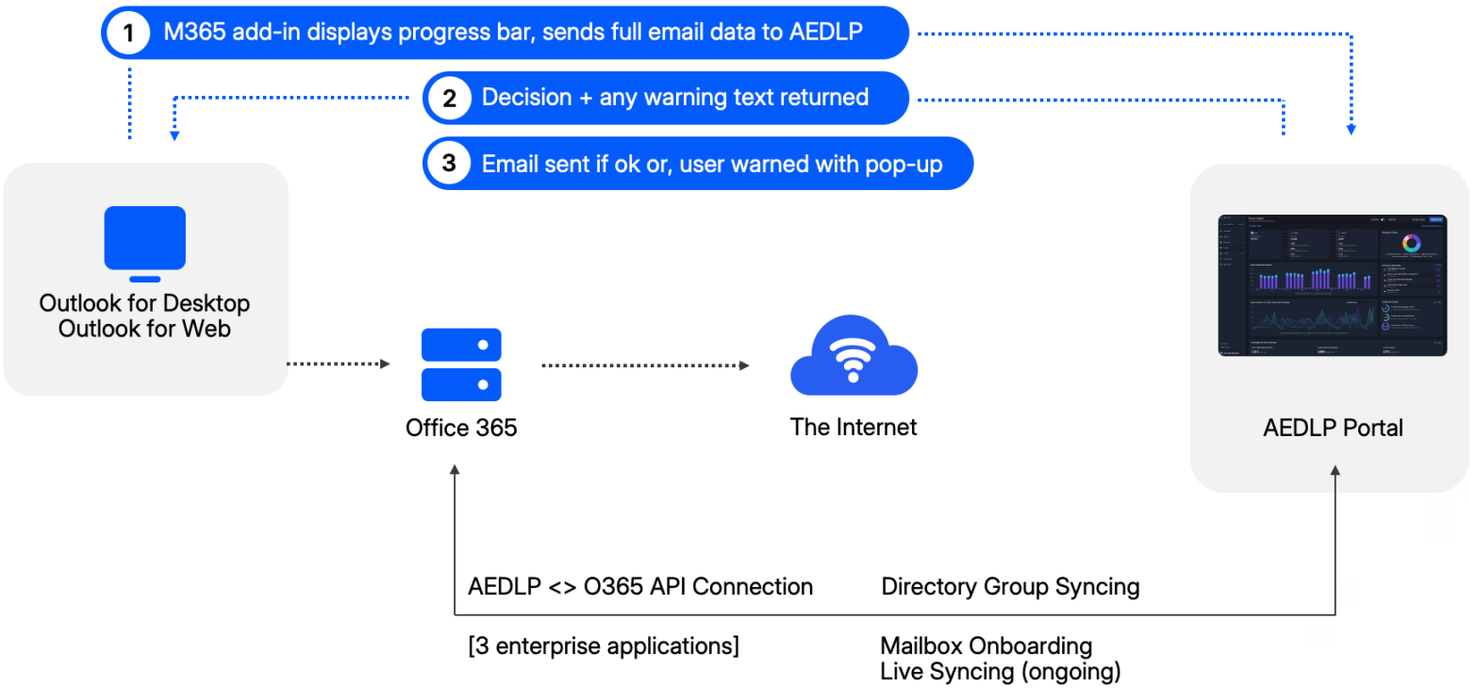


Figure 13: Overview of the Adaptive Email DLP Microsoft 365 add-in data flows.

Protection for Microsoft Exchange — quick links

Proofpoint provides protection for Microsoft Exchange email environments in both Core Email Protection API and Adaptive Email DLP. For instructions on setting up these protections and to learn about the deployment architectures, see the following links:

Core Email Protection API

- **Microsoft Exchange 2013, 2016, and 2019 inbound gateway instructions**
- **Microsoft Outlook add-in deployment instructions**
- **Gateway and add-in architectures**

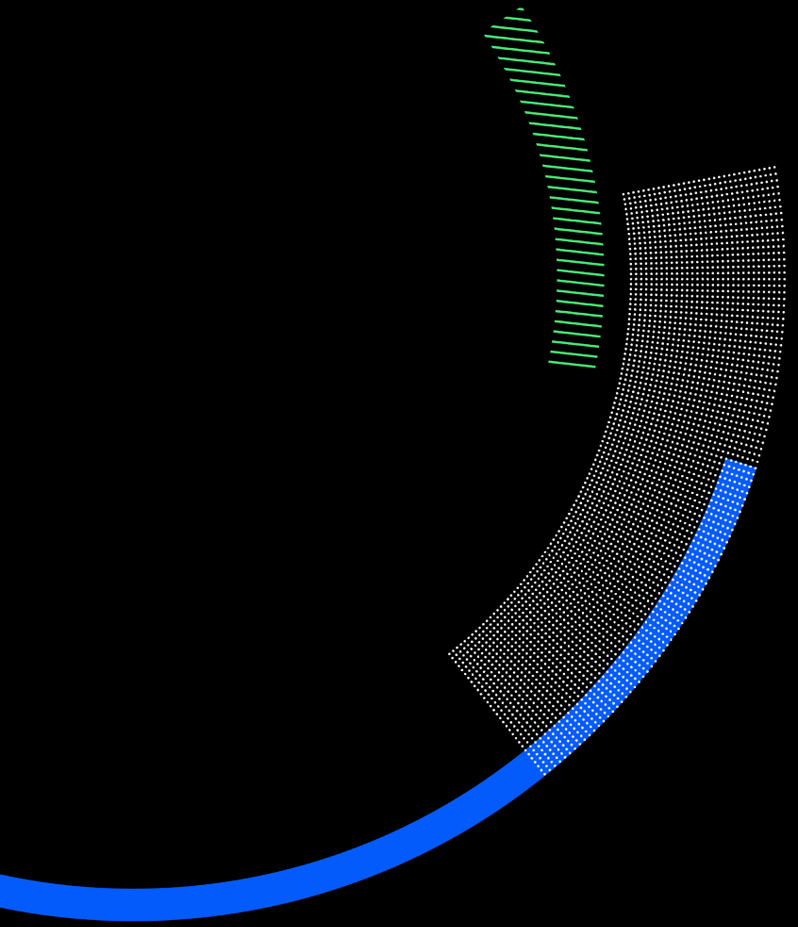
Adaptive Email DLP

- **Microsoft Exchange 2013, 2016, and 2019 inbound gateway instructions**
- **Microsoft Outlook add-in deployment instructions**
- **Gateway overview and user experience**

Protection for Google Workspace — quick links

Proofpoint provides protection for Google Workspace email environments in both Core Email Protection API and Adaptive Email DLP. For instructions on setting up these protections and to learn about the deployment architectures, see the following links:

- **Overview of Google Workspace integration**
- **Quick Start – Configuring Google Workspace integration**
- **Core Email Protection API gateway instructions**
- **Adaptive Email DLP gateway instructions**



proofpoint.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 85% of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

Connect with Proofpoint: LinkedIn

DISCOVER THE PROOFPOINT PLATFORM →

[Part number and date of collateral]