



Your Cloud App Security Playbook

Securing Office 365 with Cytex



hello@cytex.io

cytex.io



Office 365 Protection with Cytex

Think of your Office 365 environment as a bustling city square, where information flows freely and collaboration thrives. However, without proper security measures, it can quickly become a target for cybercriminals. Cytex acts as your security architect, designing and implementing a robust security framework that protects your digital city square from all angles.

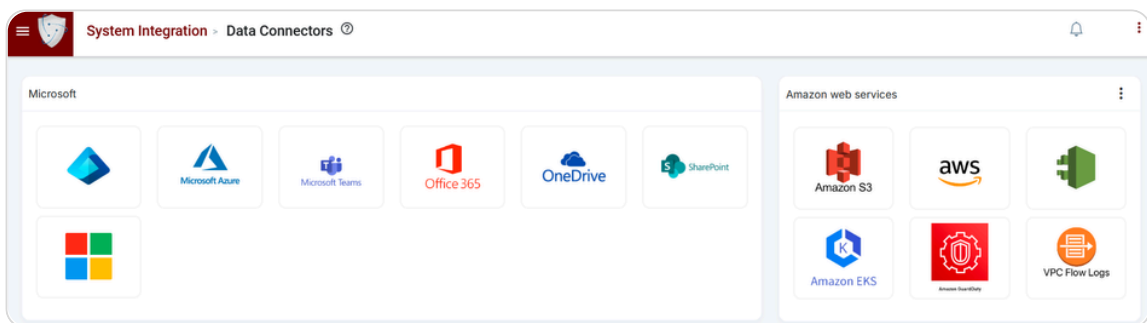


1

Seamless Office 365 Integration with Cytex

Cytex's connects seamlessly with Office 365 services, supporting both business and personal accounts. It ensures secure account management with options for evaluation thresholds.

- Log in to Cytex and open the main menu.
- Expand System Integration, then Integration Manager, and click on Data Connectors.
- Select Office 365 as the cloud asset on the Data Connectors page.



Account Integration Wizard

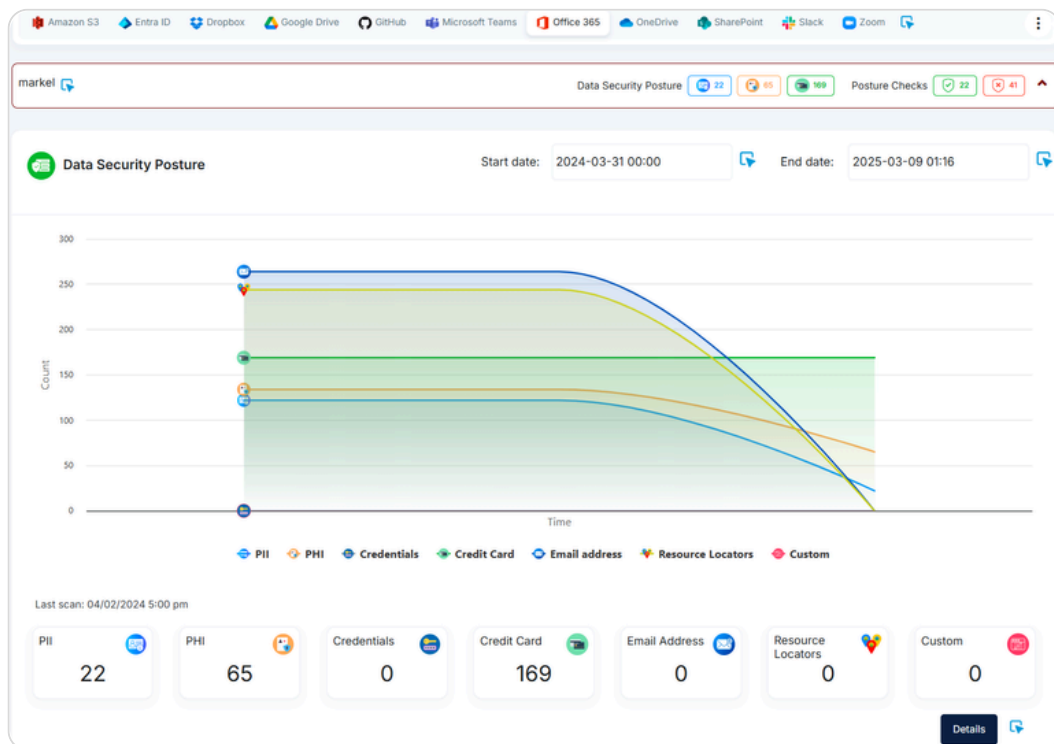
- Choose Account Type, create Account Name, and click Next.
 - Click the hyperlink *"Click to get the access code"* to get the access code from OneDrive by signing in with an admin account.
 - Enter the access code and click Next.
- Now select data collection frequency from the dropdown.
- Choose a DLP policy (Relaxed or Aggressive)
 - If you have previously added any custom DLP policies in Cytex's Cloud App Policy Management, they may also appear here.
- Optionally enable real-time events/logs for monitoring, event-based scans and log visibility ensure real-time monitoring and secure management of Office 365 accounts and data. When real-time events and log option is selected:
 - Select Log Frequency.
 - Toggle for immediate Data Security Posture scan; otherwise, it will run after 12 hours.
- Click Submit to complete integration and view the account in the account inventory data table below.

2

Office 365 security scan and insights : visualizing your cloud app security posture with Cytex

The Cytex Insights module offers both visual and numerical indicators to evaluate cloud application security and compliance. This ensures real-time monitoring and secure management of your Office 365 environment and resources. It also includes App Posture Checks to quickly view pass, fail, and alarm statuses.

- In the Cytex main menu expand Cloud Apps, then click Insights.
- On the insights page select Office 365. It will display the integrated accounts below.
- Click on the account name to view the extensive Data Security Posture and App Posture checks.



- Click on the Details button to dive deep into the Data Security Posture insights. Get detailed file information including filename, owner, access permissions, and more.

The Data Security Posture insights organize data into seven categories, classifying it by patterns while precisely identifying sensitive information according to the chosen policy.

The screenshot displays the 'Office 365' Data Security Posture insights page for account 'markel'. It shows the same category counts as the previous dashboard: PII (22), PHI (65), Credentials (0), Credit Card (169), Email Address (0), Resource Locators (0), and Custom (0). Below this, there are three tables of sensitive data:

Most pushed user		
Alice Johnson alice.johnson@gmail.com	12	
Bob Brown bob.brown@gmail.com	7	

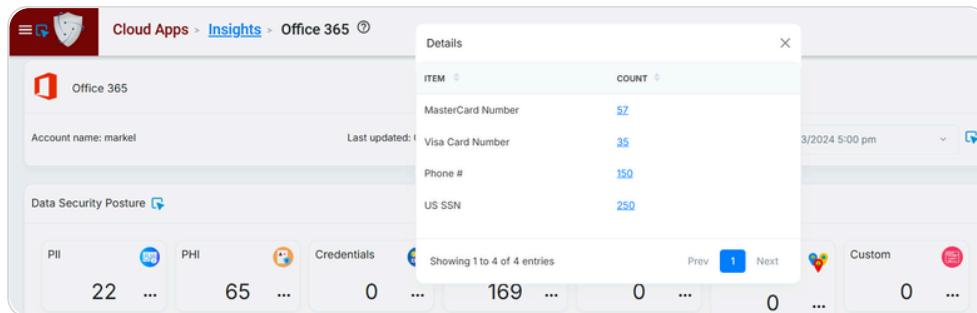
Sent emails with sensitive data		
John Doe john.doe@gmail.com	10	
Jane Smith jane.smith@gmail.com	5	

Received emails with sensitive data		
John Doe john.doe@gmail.com	10	
Jane Smith jane.smith@gmail.com	7	
Chris Johnson chris.johnson@gmail.com	5	

2

Office 365 security scan and insights : visualizing your cloud app security posture with Cytex

- For further insights you can click on any 'Category' and it will open a pop-up with a list of sensitive records.
 - Click on any sensitive record and it will populate the file list with sensitive records in the Detailed View section below.



3

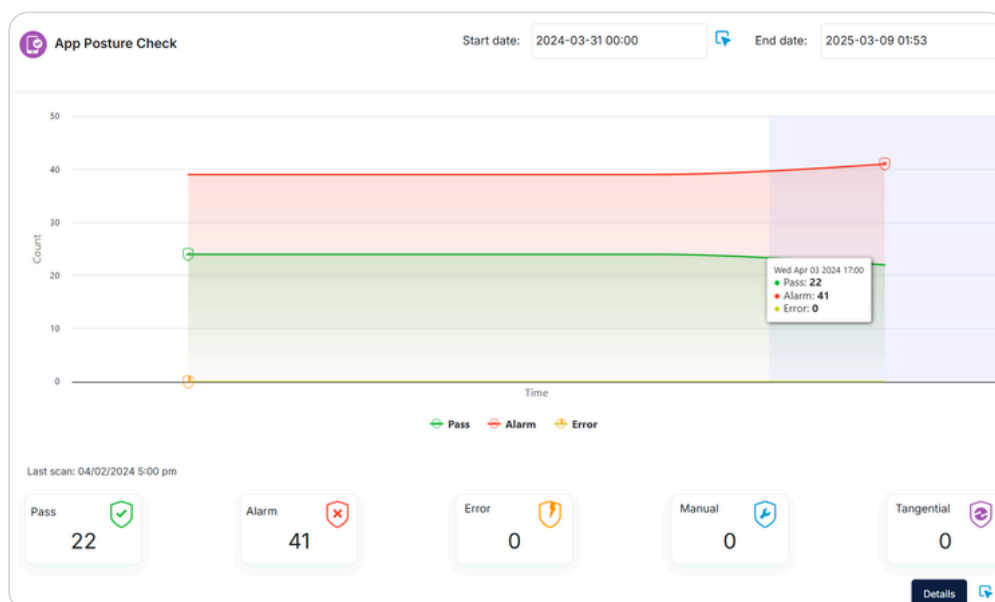
App posture check: Assessing your cloud app risk posture

The Cytex App Posture Check module provides a detailed view of the security and compliance status of your cloud applications, giving you insights into their overall risk posture.

- On the cloud apps insights page select Office 365 to display all the integrated accounts below.
- Click on the account name to expand and scroll down to the App Posture Check section.

App Posture Check evaluates user data against cloud security best practices and assign them different statuses pass, fail, and alarm statuses.

- **Pass:** Assets meeting the compliance requirements.
- **Alarm:** Issues that require immediate attention.
- **Error:** Detected misconfigurations.
- **Manual:** Tasks requiring manual intervention.
- **Tangential:** Compliance checks of lower priority.



3 App posture check: Assessing your cloud app risk posture

In the App Posture Check section, click the Details button to explore and assess the identified gaps in your Office 365 security, as evaluated against security best practices.

The screenshot shows the 'Best Practices' section of the Office 365 security dashboard. It displays the following data:

Category	Count	Status
Pass	22	Good (Green)
Alarm	41	Warning (Red)
Error	0	Good (Yellow)
Manual	0	Good (Blue)
Tangential	0	Good (Purple)

Below the Best Practices section, there are three rows representing different security domains:

- Apps:** 17 Good, 31 Warning, 0 Error, 0 Manual, 0 Tangential
- Data:** 0 Good, 4 Warning, 0 Error, 0 Manual, 0 Tangential
- Identity:** 5 Good, 6 Warning, 0 Error, 0 Manual, 0 Tangential

4 Strengthening OneDrive Security Posture with Cytex: Your Action Plan

Following Cytex's evaluation, you'll find a customized action plan with best practices specifically for your Office 365 environment, highlighting the gaps. The comprehensive guidance empowers you to elevate your OneDrive security.

The screenshot shows the 'User consent policy setting to install apps' section of the Office 365 security dashboard. It displays the following data:

Category	Count	Status
User consent policy setting to install apps	1	Good (Green)

Below the action plan, there is a guidance section:

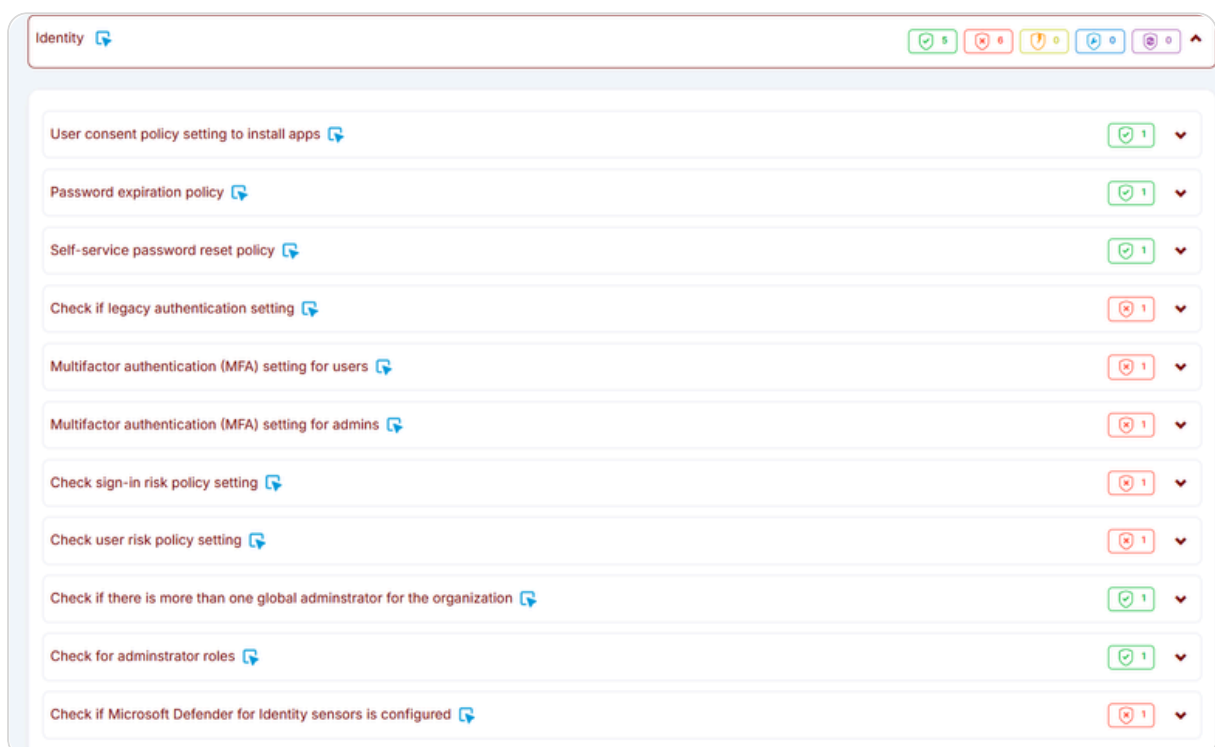
Guidance: To reduce the risk of malicious applications attempting to trick users into granting them access to your organization's data, we recommend that you allow user consent only for applications that have been published by a verified publisher.

Checkmark: You have a user consent policy in place.

5 Cytex's Action Plan

Identity:

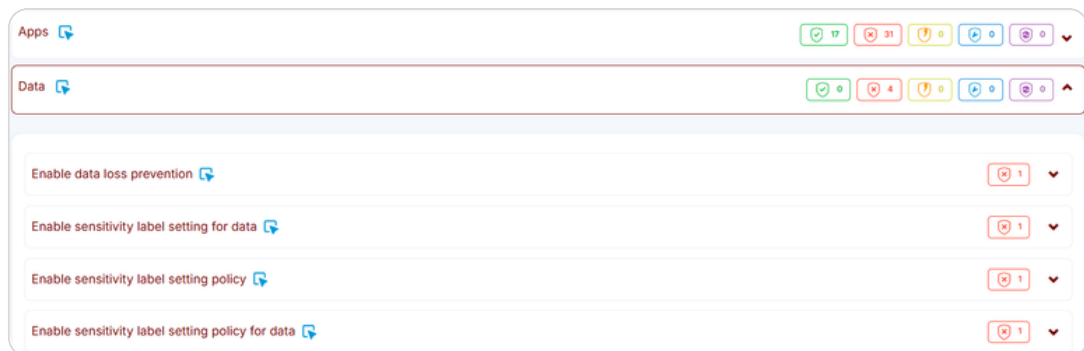
- ▶ Enable security default Multi-factor authentication (MFA) for everyone: admins and users.
- ▶ Make sure to have more than one global administrator for the organization. According to CIS O365 Benchmark 2.0.0, the suggestion is to have between two to four global admins.
- ▶ Enforce a password expiration policy.
- ▶ Enable self-service password reset policy in Microsoft Entra ID, so that users no longer need to engage help desk to reset passwords.
- ▶ Check for legacy authentication and block if found in any account as it does not support MFA.
- ▶ Turn on the sign-in risk policy so that suspicious sign-ins are challenged for MFA.
- ▶ Enable user risk policy in Microsoft Entra ID and configure a user risk Conditional Access policy to automatically respond to a specific user risk level.
- ▶ Assign roles like Password Administrator or Exchange Online Administrator instead of Global Administrator to ensure administrators have the least privilege necessary. Configure role-based access controls to maintain this principle.
- ▶ Install Microsoft Defender for Identity sensors to detect advanced threats in your entire identity infrastructure.
- ▶ Enable user consent policy for installing only verified publisher applications.



5 Cytex's Action Plan

Data Loss Prevention:

- ▶ Enable data loss prevention policy.
- ▶ Enable sensitivity labels for your data in order to track the data type without exposing sensitive data on other platforms.
- ▶ Setup and use data classification policies for data stored in your apps like Outlook, Word, SharePoint sites, and Office 365 groups.
- ▶ Enable sensitivity labels for data using Microsoft Purview Portal: enable auto built-in labeling for Office and PDF files in SharePoint and OneDrive, allowing users to apply sensitivity labels in Office for the web.



Applications:

- ▶ Microsoft Defender should be enabled for Office 365, OneDrive, SharePoint, and for Microsoft Teams to protect your organization from inadvertently sharing malicious files.
- ▶ Create a Calendar Sharing policy to restrict users from sharing their detailed calendars with external users.
- ▶ Enable Microsoft Defender safe documents policy, to scan documents and files for malicious content.
- ▶ Enable Microsoft Defender Connection Filter. These options include Exchange mail flow rules (also known as transport rules), Outlook Safe Senders, the IP Allow List (connection filtering), and allowed sender lists or allowed domain lists in anti-spam policies.
- ▶ Utilize the customer lockbox settings to set data access expiration time.
- ▶ Enable Microsoft Defender Zero-Hour Auto Purge (ZAP) spam filter.
- ▶ Enable Microsoft Defender Zero-Hour Auto Purge (ZAP) phishing filter.
- ▶ Enable Microsoft Defender Zero-Hour Auto Purge (ZAP) malware filter to quarantine the messages that contain malware attachment for both read, and unread, messages.

5 Cytex's Action Plan

Applications:

- ▶ Enable Microsoft Defender Zero-Hour Auto Purge (ZAP) safe attachments.
- ▶ Enable Microsoft Defender safe links for default base level safe links protection for everyone.
- ▶ Enable Microsoft Defender common attachments filter. You can use the default list of file types or customize it.
- ▶ Enable Microsoft Defender high confidence SPAM filter
- ▶ Set the Microsoft Defender spam action, the action that will be taken on phishing detection.
- ▶ Enable Microsoft Defender high confidence phish action, the action that will be taken on high confidence phishing detection.
- ▶ Enable Microsoft Defender bulk spam action
- ▶ Specify the Microsoft Defender quarantine retention period
- ▶ Enable Microsoft Defender allowed senders. Never add your own accepted domains or common domains (for example, microsoft.com or office.com) to the allowed domains list.
- ▶ Enable Microsoft Defender bulk threshold to specify the bulk complaint level (BCL) of a message.
- ▶ Enable Microsoft Defender spam action, the action that will be taken on spam detection.
- ▶ Enable Microsoft Defender auto forwarding mode.
- ▶ Configure the Microsoft Defender recipient external limit per hour limit, it is the maximum number of external recipients that a user can email per hour.
- ▶ Configure the Microsoft Defender recipient internal limit per hour limit, it is the maximum number of internal recipients that a user can email per hour.
- ▶ Configure the Microsoft Defender recipient limit per day, it is the maximum number of recipients that a user can send to within a day.
- ▶ Configure Microsoft Defender threshold reached reaction when any of the limits specified in the outbound anti-spam policy are reached.
- ▶ Enable Microsoft Defender mailbox intelligence that identifies users' email patterns with their frequent contacts to spot potential phishing attempts.
- ▶ Enable Microsoft Defender intelligence protection. This setting is available only if mailbox intelligence is enabled.

5 Cytex's Action Plan

Applications:

- ▶ Enable Microsoft Defender domains to prevent specified domains from being impersonated by the message sender's domain.
- ▶ Enable Microsoft Defender phish action threshold. The default value is 1, but 2 or 3 are the recommended values.
- ▶ Enable Microsoft Defender similar domains safety tips. This setting is available only if the enable impersonated domain protection setting is configured properly.
- ▶ Enable Microsoft Defender similar user safety tips. This setting is available only if the enable impersonated user protection setting is configured properly.
- ▶ Enable Microsoft Defender targeted domain protection. This setting is available only if enable impersonated domain protection setting is configured properly.
- ▶ Enable Microsoft Defender targeted user protection. This setting is available only if enable impersonated user protection setting is configured properly.
- ▶ Enable Microsoft Defender unusual characters safety tips. This setting is available only if the enable impersonated user protection setting is configured properly.
- ▶ Ensure that modern authentication is activated in Microsoft 365 to enable authentication features like MFA using smart cards, certificate-based authentication (CBA), and third-party SAML identity providers.
- ▶ Configure the Spam confidence level (SCL) with specific domains. In order to get a score for this security control, all the active transport rule that applies to specific domains must have a Spam Confidence Level (SCL) of 0 or higher.
- ▶ Check Microsoft 365 modern authentication configuration.
- ▶ Check if MailTips for ends users are enabled.
- ▶ Check Microsoft 365 audit log search setting. When audit log search in the Microsoft Purview compliance portal is enabled, user and admin activity from your organization is recorded in the audit log and retained for 90 days. However, your organization might be using a third-party security information and event management (SIEM) application to access your auditing data. In that case, a global admin can turn off audit log search in Microsoft 365.
- ▶ Check Mailbox auditing for users to track logins to a mailbox as well as what actions are taken while the user is logged in. Only certain mailbox types support default auditing setting 'On': User Mailboxes, Shared Mailboxes, and Microsoft 365 Group Mailboxes. The remaining mailbox types require auditing to be turned on at the mailbox level: Resource Mailboxes, Public Folder Mailboxes, and DiscoverySearch Mailbox.

5 Cytex's Action Plan

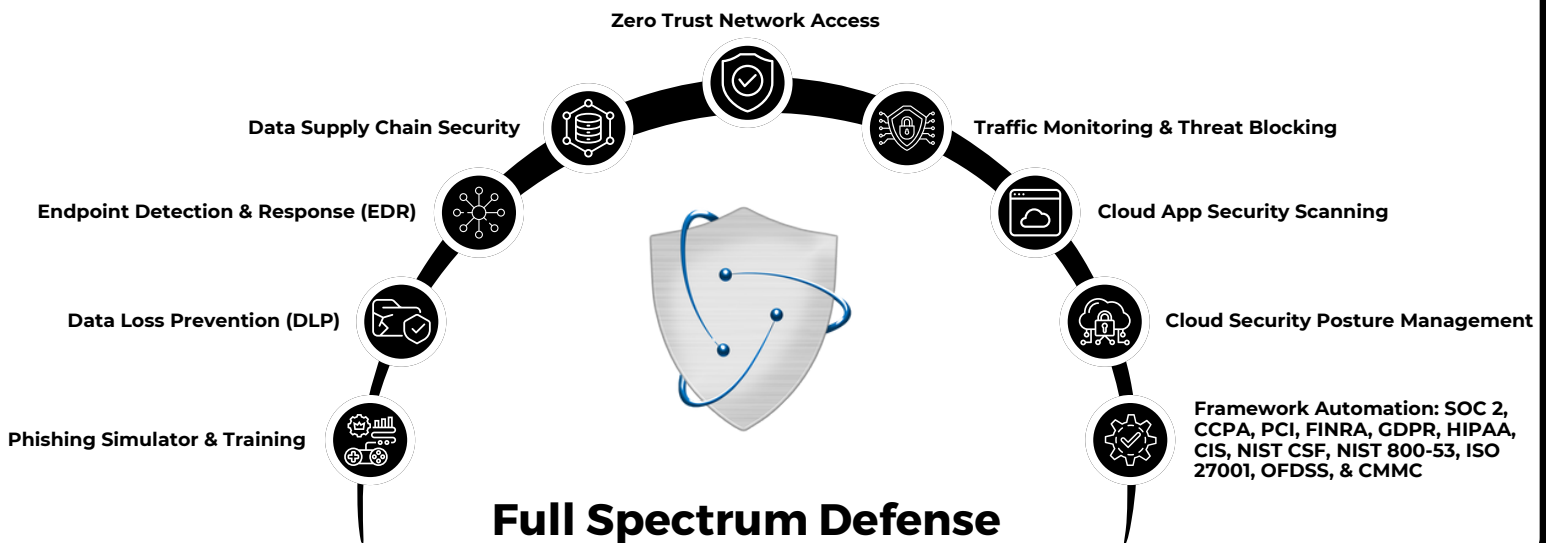
Applications:

- ▶ Check if users are allowed to open external files in Outlook. If allowed, keep in mind that Microsoft doesn't control the usage terms or privacy policies of those third-party services. By default additional storage providers are allowed in Office on the Web (such as Box, Dropbox, Facebook, Google Drive, OneDrive Personal, etc.). This could lead to information leakage and additional risk of infection from organizational non-trusted storage providers. Restricting this will inherently reduce risk as it will narrow opportunities for infection and data leakage.
- ▶ Check for Exchange Online Protection (EOP) policies. Configure Exchange Online Spam Policies to copy emails and notify someone when a sender in the organization has been blocked for sending spam emails.
- ▶ Check for Safe Attachments policy in emails to protect users from malware in email attachments by scanning attachments for viruses, malware, and other malicious content.
- ▶ Check if Safe Links policy for Office applications is set to allow URL's that exist inside of Office documents and email applications opened by Office, Office Online and Office mobile to be processed against Defender for Office time-of-click verification and rewritten if required.
- ▶ Check if Office 365 built-in default protections for phishing are enabled. The default policy applies to all users within the organization, and is a single view to fine-tune anti-phishing protection. Custom policies can be created and configured for specific users, groups or domains within the organization and will take precedence over the default policy for the scoped users.
- ▶ Check for Exchange Online flow of message policy. These are Remote domain, Transport Rules, and Anti-spam outbound policies.
- ▶ Specify the administrators and users who can install and manage add-ins for Outlook in Exchange Online. By default, users can install add-ins in their Microsoft Outlook Desktop client, allowing data access within the client application.



Explore **Cytex Unified Resilience Platform** today

[Schedule demo](#)



<https://cytex.io>



hello@cytex.io



[@cytexsmb](#)



[@cytexsecure](#)