



Your Cloud App Security Playbook

Securing MS Teams with Cytex



hello@cytex.io

cytex.io



Best Practices for securing MS Teams

Overlooking crucial MS Teams settings is no longer a concern with Cytex. This cheat sheet demonstrates how easily you can prevent data breaches and unauthorized access while implementing a strategic plan to bolster organizational security, all through the intuitive Cytex platform.

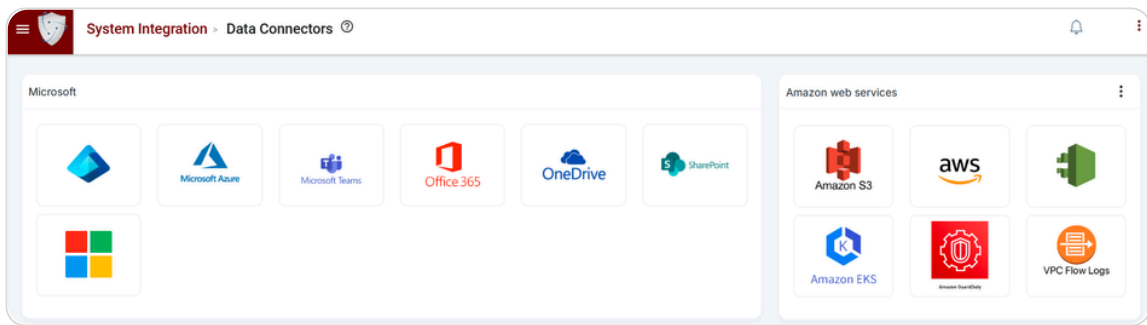


1

Seamless MS Teams Integration with Cytex

Cytex's connects seamlessly with Microsoft Teams' services, enabling secure communication and collaboration across both single and multi-tenant environments.

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



Account Integration Wizard

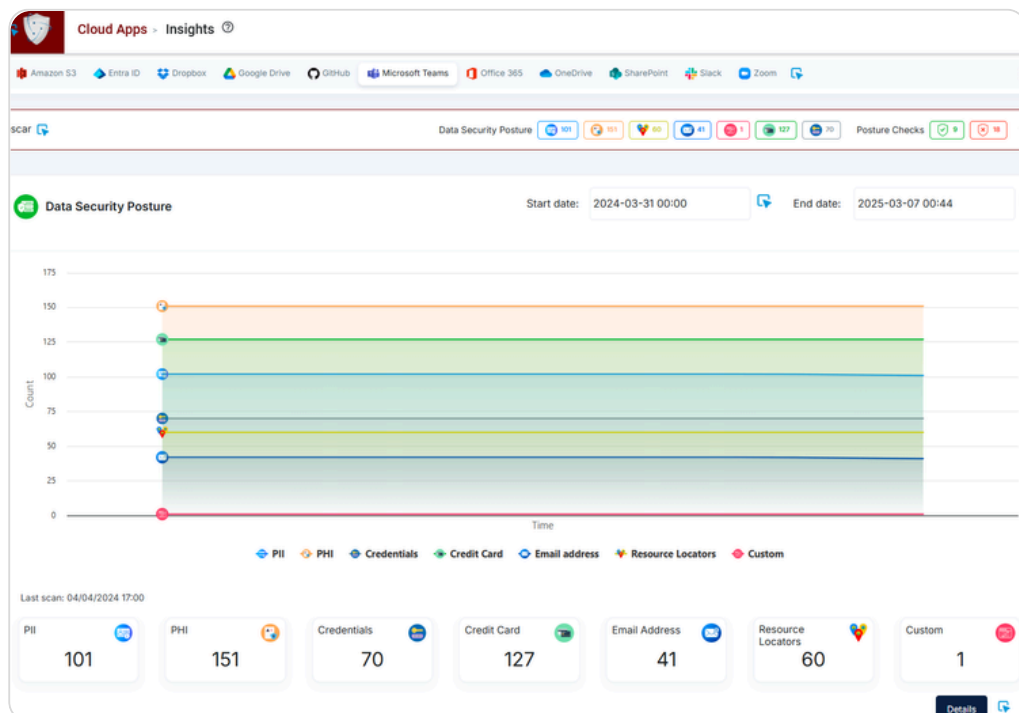
- Choose Account Type, create Account Name, and click Next.
 - Click the hyperlink *"Click to get the access code"* to get the access code from MS Teams by signing in with an admin account.
 - Enter the access code and click Next.
- Now select data collection frequency from the dropdown.
- Choose a DLP 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 MS Teams 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

MS Teams security scan and insights : visualizing your cloud app security posture with Cytex

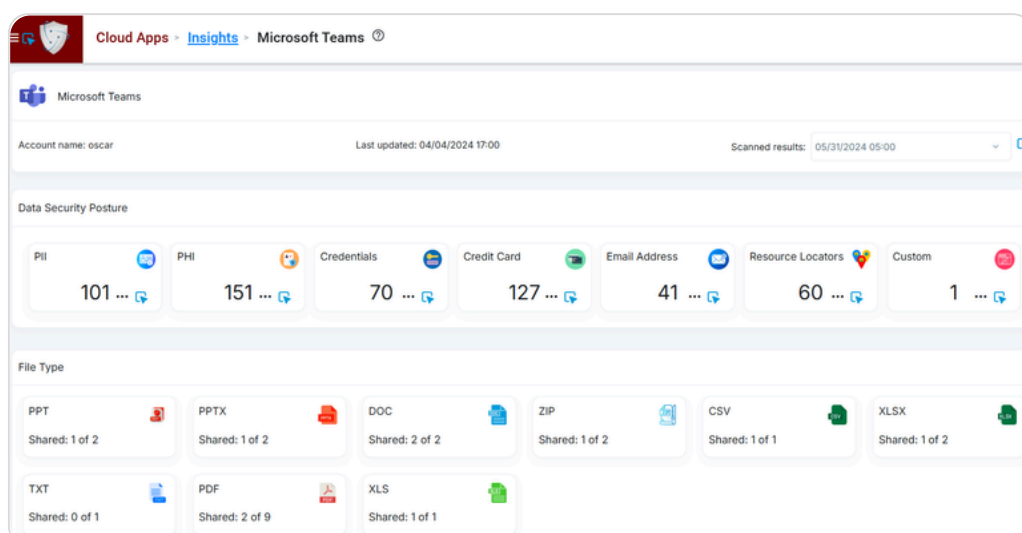
The Cytex Insights module offers both visual and numerical indicators to evaluate cloud application security and compliance. This ensures real-time monitoring and secure management of your MS Teams environment and resources. It also includes App Posture Checks to quickly view pass, fail, and alarm statuses.

- In the Cytex main menu expand Cloud Apps, then click Insights.
- On the insights page select MS Teams app. 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.



2

MS Teams 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.
- Chat Details: View and categorize chat data, including sensitive or flagged content.
- File Types: Tracks multiple file types shared within teams for compliance.
- Account Name: Displays the connected Microsoft Teams account name.
- Last Updated: Shows the most recent scan or update date.
- Scanned Results: Summary of categorized chats and files, highlighting key insights.



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.

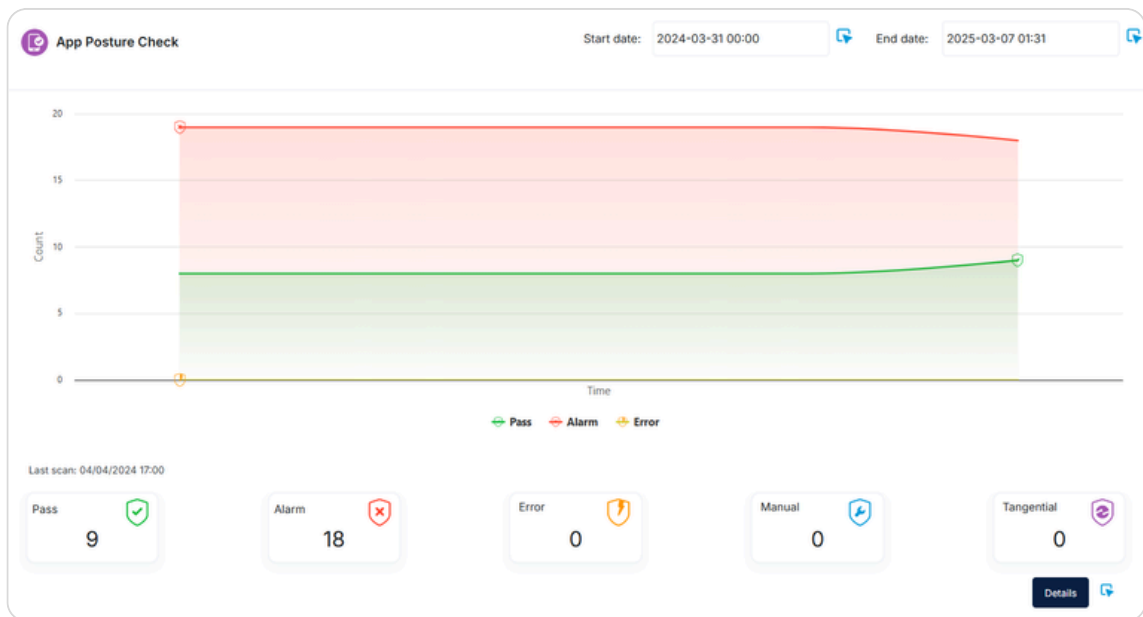
- On the cloud apps insights page select MS Teams to display all the integrated accounts below.
- Click on the account name to expand and scroll down to the App Posture Check section.



3 App posture check: Assessing your cloud app risk posture

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.



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

This view shows the 'Best Practices' section for Microsoft Teams. It includes the account name 'oscar', last updated '05/31/2024 05:00', and scanned results '05/31/2024 05:00'. The summary table at the top matches the dashboard above:

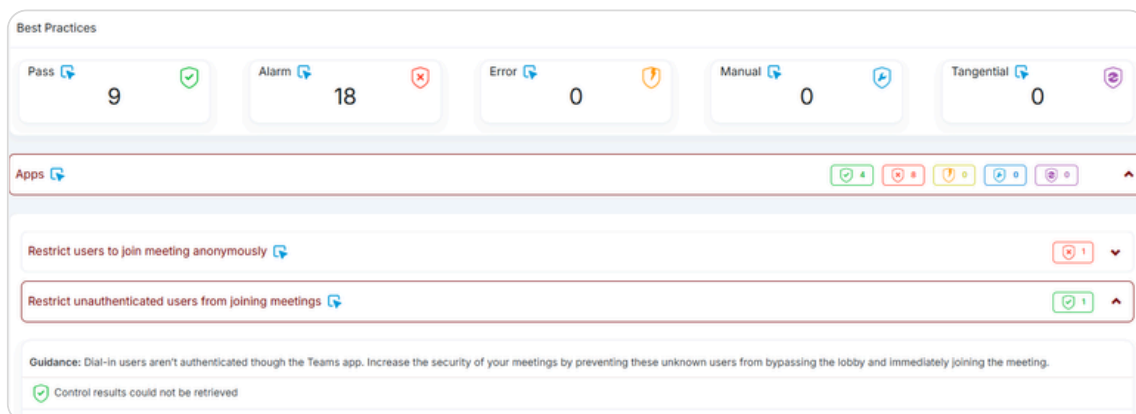
Status	Count
Pass	9
Alarm	18
Error	0
Manual	0
Tangential	0

Below the summary, there is a list of specific best practices with their status:

- Restrict users to join meeting anonymously: Alarm (1)
- Restrict unauthenticated users from joining meetings: Pass (1)
- Guidance: Dial-in users aren't authenticated through the Teams app. Increase the security of your meetings by preventing these unknown users from bypassing the lobby and immediately joining the meeting. Control results could not be retrieved.
- Limit external meeting participants permissions: Pass (1)
- Restrict anonymous users from starting meetings: Pass (1)
- Guest user meeting join policy: Alarm (1)
- Presenter rights sharing policy: Alarm (1)

4 Strengthening MS Teams Security Posture with Cytex: Your Action Plan

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



5 Cytex's Action Plan

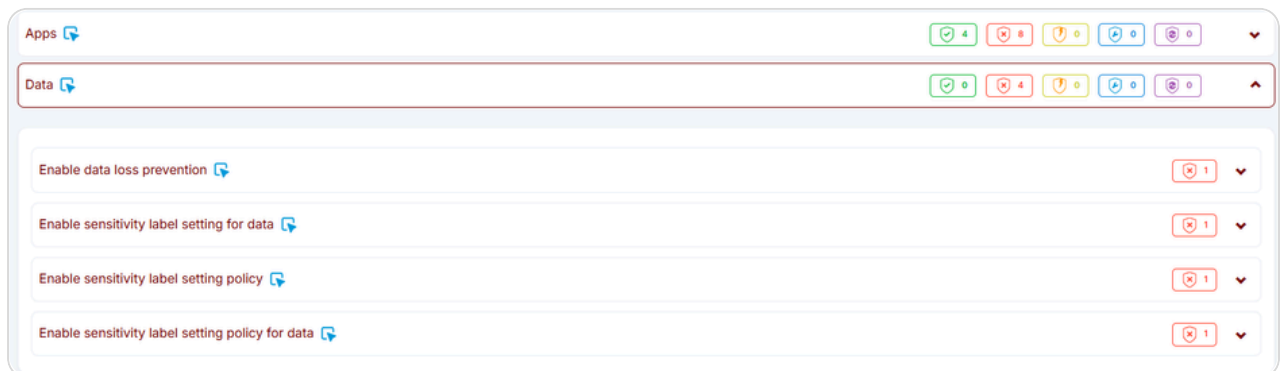
Identity:

- ▶ 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.



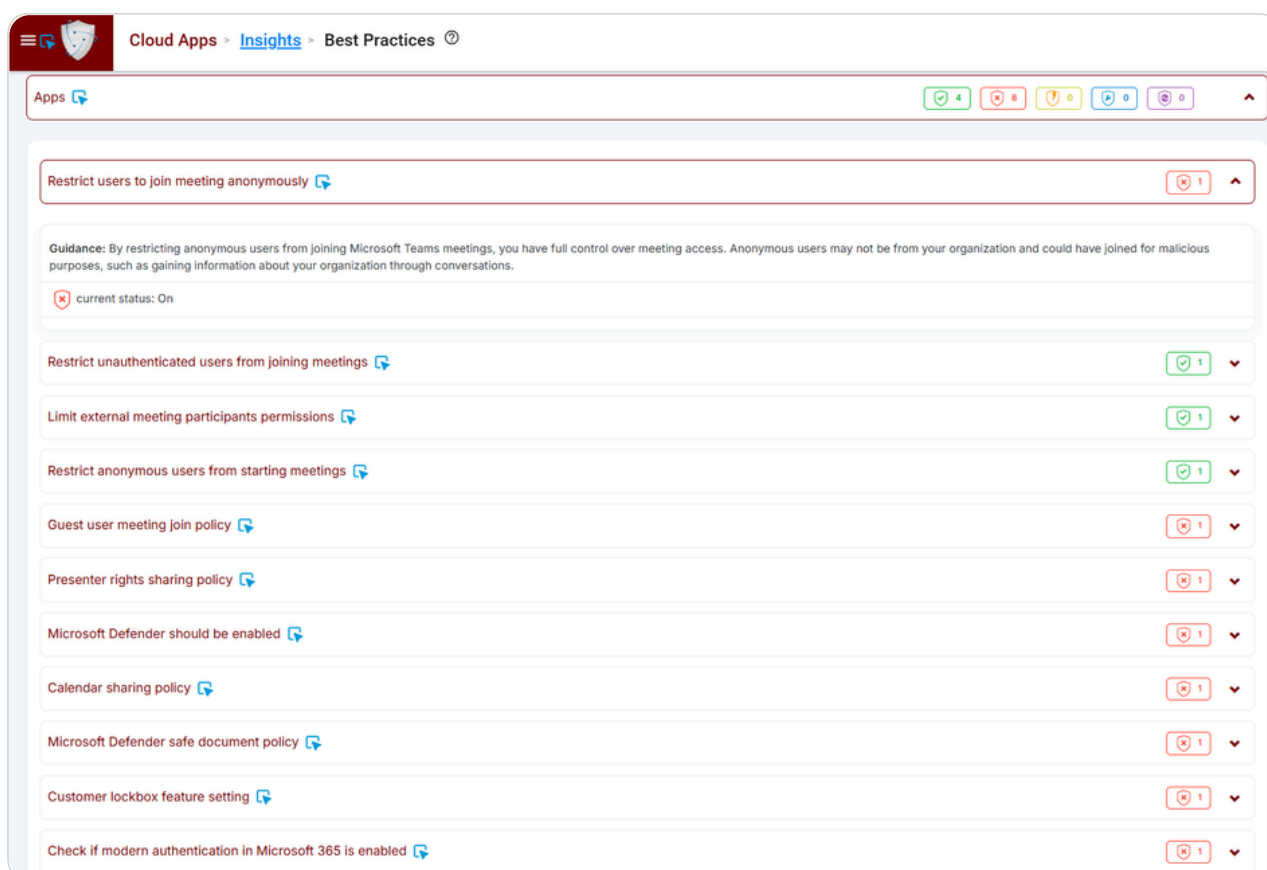
Applications:

- ▶ Restrict users to join meeting anonymously.
- ▶ Restrict unauthenticated users from joining meetings and also from bypassing the lobby and immediately joining the meeting.
- ▶ Configure external meeting participants' permissions. Restrict them from sharing content, or adding new users, and avoid inappropriate content being shared, or malicious actors joining the meeting.
- ▶ Restrict anonymous users from starting meetings and reduce the risk of data leakage.
- ▶ Set up and configure guest user meeting joining policy, so that uninvited/guest users are sent to the meeting lobby. The host can then decide whether or not to let them in.
- ▶ Configure the presenter rights sharing policy to ensure that only users with presenter rights are allowed to share content during meetings.
- ▶ Microsoft Defender should be enabled for MS Teams, OneDrive, Office 365 for and SharePoint, to protect your organization from inadvertently sharing malicious files.

5 Cytex's Action Plan

Applications:

- ▶ Enable Microsoft Defender safe documents policy, to scan documents and files for malicious content.
- ▶ Turn on the Audit Log in the Microsoft Purview portal or compliance portal. Audit logging is turned on by default for Microsoft 365 organizations. However, when setting up a new Microsoft 365 organization, you should verify the auditing status for your organization.
- ▶ Utilize the customer lockbox settings to set data access expiration time.
- ▶ 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.
- ▶ Create a Calendar Sharing policy to restrict users from sharing their detailed calendars with external users.



Cloud Apps > Insights > Best Practices

Apps

Restrict users to join meeting anonymously 1

Guidance: By restricting anonymous users from joining Microsoft Teams meetings, you have full control over meeting access. Anonymous users may not be from your organization and could have joined for malicious purposes, such as gaining information about your organization through conversations.

✗ current status: On

Restrict unauthenticated users from joining meetings 1

Limit external meeting participants permissions 1

Restrict anonymous users from starting meetings 1

Guest user meeting join policy 1

Presenter rights sharing policy 1

Microsoft Defender should be enabled 1

Calendar sharing policy 1

Microsoft Defender safe document policy 1

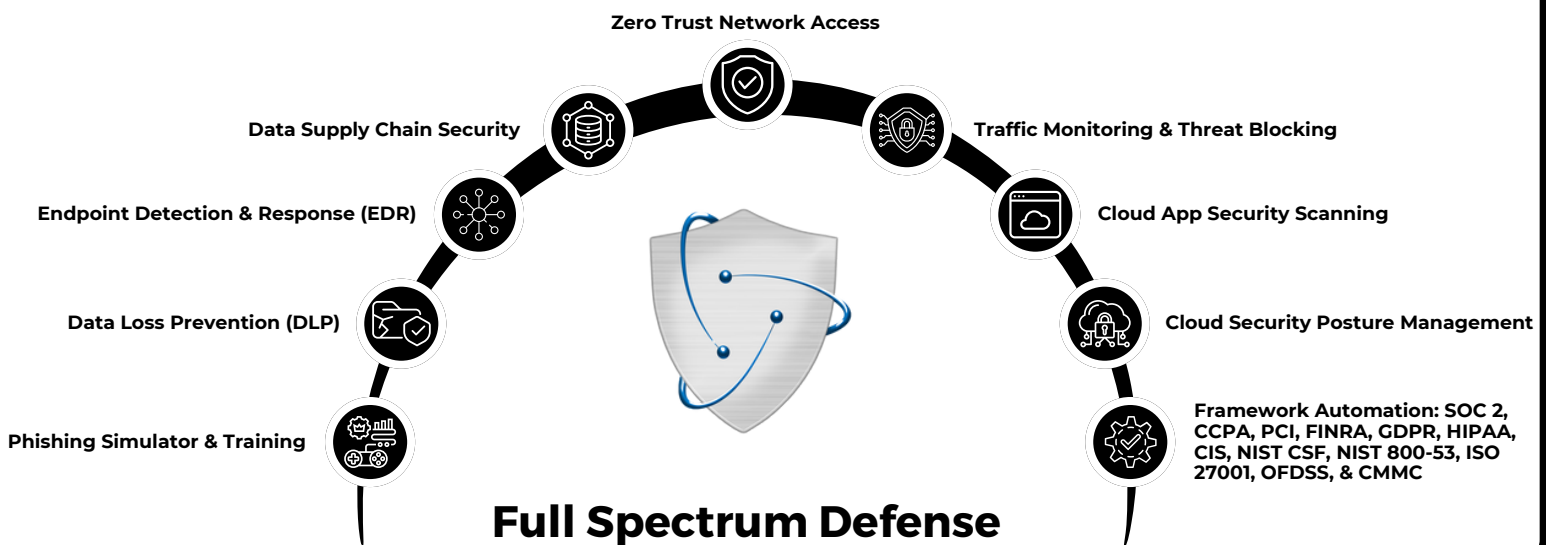
Customer lockbox feature setting 1

Check if modern authentication in Microsoft 365 is enabled 1



Explore **Cytex Unified Resilience Platform** today

[Schedule demo](#)



<https://cytex.io>



hello@cytex.io



[@cytexsmb](#)



[@cytexsecure](#)