



Your Cloud App Security Playbook

# Securing Dropbox with Cytex



[hello@cytex.io](mailto:hello@cytex.io)

[cytex.io](https://cytex.io)



# DropBox security best practices

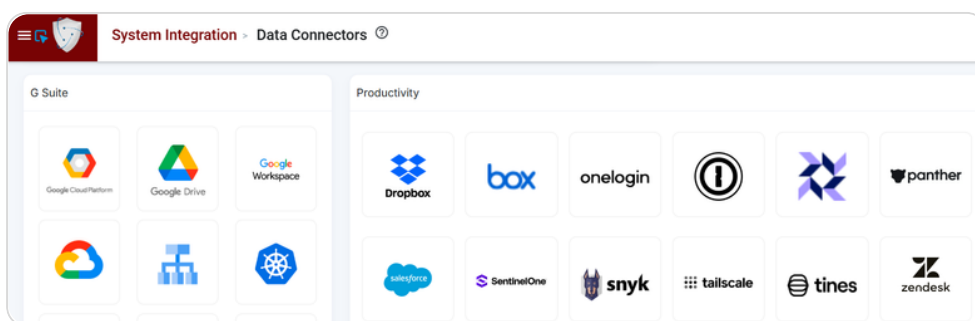
Managing cloud app security can be complex, and overlooking critical settings can leave your organization vulnerable. This playbook demonstrates how Cytex simplifies cloud app security posture management, providing automation, visibility, and control across your cloud environment. Let's get started.



## 1 Seamless Dropbox Integration with Cytex

Cytex's Dropbox integration provides seamless connection with Dropbox services, supporting both Personal and Business accounts. It ensures secure file storage and sharing with robust compliance features, including Data Loss Prevention (DLP).

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



### Account Integration Wizard

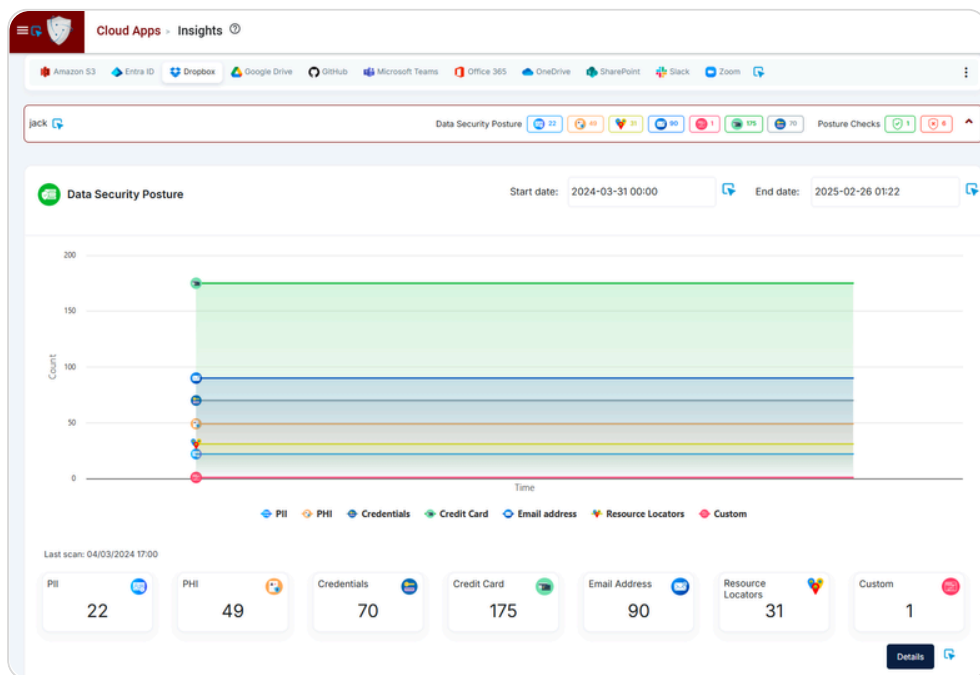
- Choose Account Type, create Account Name, and click Next.
  - Click the hyperlink *"Click to get the access code"* to get the access code from Dropbox by signing in with an admin account.
  - Enter the access code and click Next.
- Now select data collection frequency from the dropdown.
- Choose a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

## Dropbox security scan and insights : visualizing your cloud app security posture with Cytex

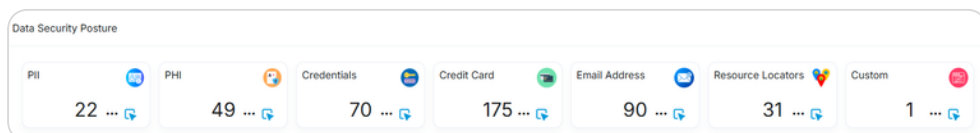
The Cytex Insights module offers both visual and numerical indicators to evaluate cloud application security and compliance. This ensures real-time monitoring and secure management of your Dropbox accounts and data. It also includes App Posture Checks to quickly view pass, fail, and alarm statuses.

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



- 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.

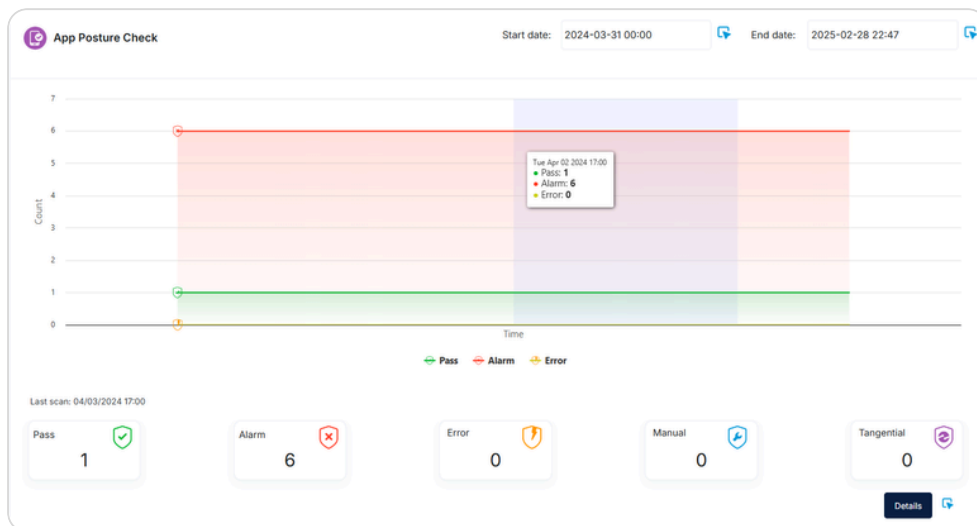
### 3 App posture check: Assessing your cloud app risk posture

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.

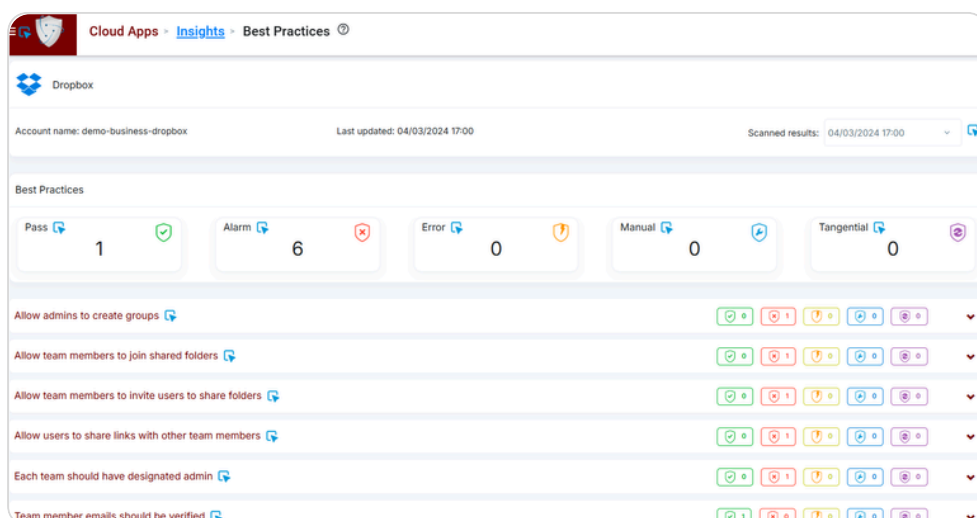
- On the cloud apps insights page select Dropbox app to display all the integrated accounts below.
- Click on the account name to expand and scroll down to the App Posture Check section.

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.

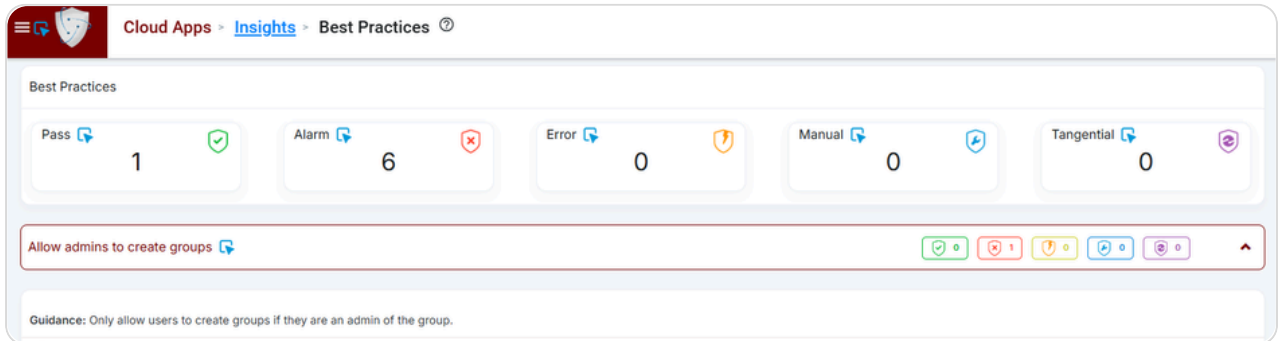


In the App Posture Check section, click the Details button to explore and assess the identified gaps in your Dropbox app's security, as evaluated against security best practices.



## 4 Strengthening Dropbox Security Posture with Cytex: Your Action Plan

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



Cloud Apps > Insights > Best Practices

Best Practices

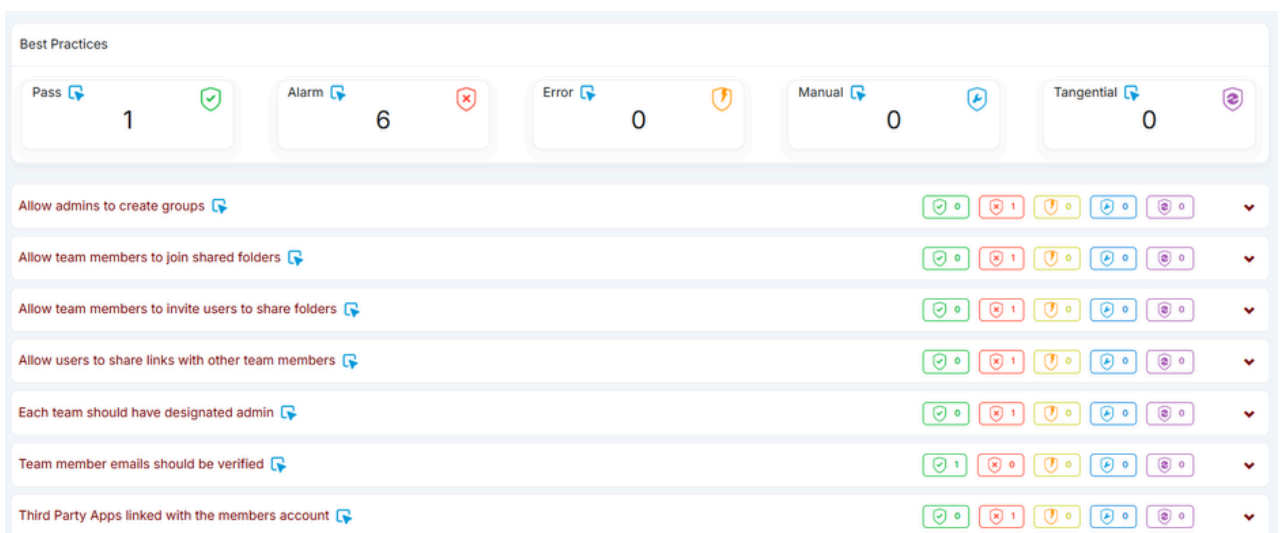
Category	Count	Status
Pass	1	Green
Alarm	6	Red
Error	0	Yellow
Manual	0	Blue
Tangential	0	Purple

Allow admins to create groups

Guidance: Only allow users to create groups if they are an admin of the group.

## 5 Cytex's Action Plan

- ▶ Allow users to create groups only if they are an admin of the group.
- ▶ Allow team members to join shared folders only if they are a member of that particular team.
- ▶ Authorize team members to invite users to share folders only if they are a member of the respective team.
- ▶ Allow users to share links with other team members only if they are a member of the team.
- ▶ Each team should have at least one designated admin.
- ▶ All team members must have a verified email address.
- ▶ Team members should not have linked any third party app linked with their account.



Best Practices

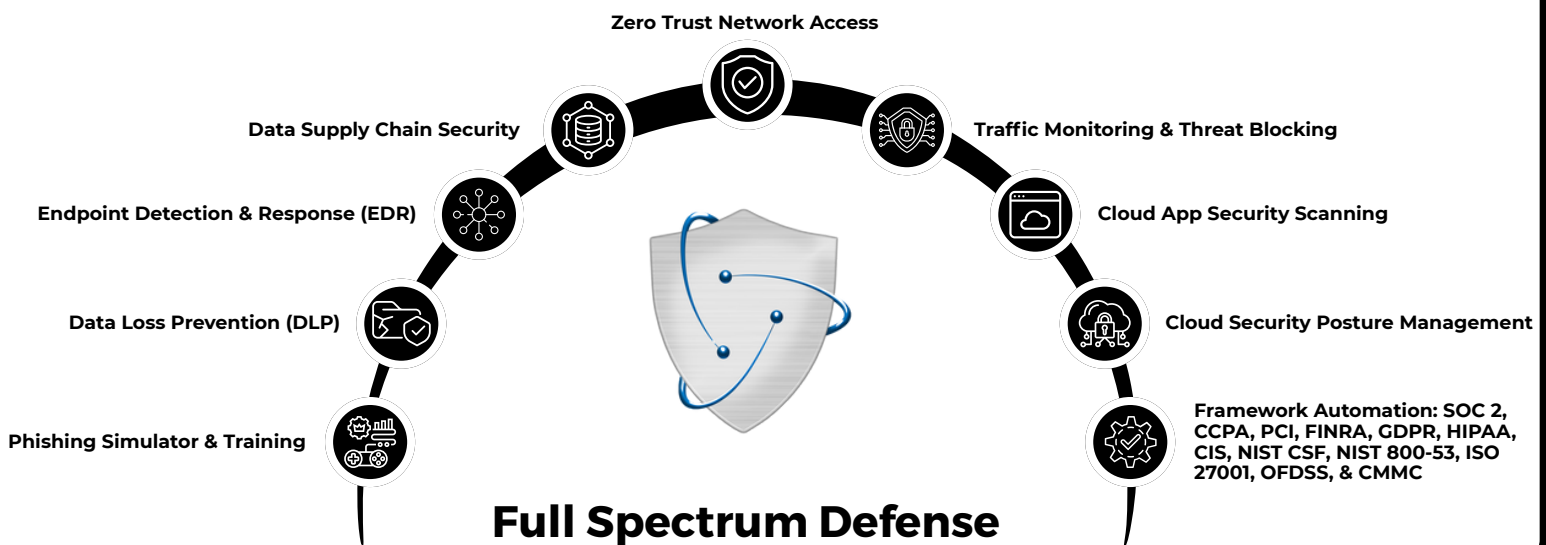
Category	Count	Status
Pass	1	Green
Alarm	6	Red
Error	0	Yellow
Manual	0	Blue
Tangential	0	Purple

- Allow admins to create groups
- Allow team members to join shared folders
- Allow team members to invite users to share folders
- Allow users to share links with other team members
- Each team should have designated admin
- Team member emails should be verified
- Third Party Apps linked with the members account



# Explore **Cytex Unified Resilience Platform** today

[Schedule demo](#)



<https://cytex.io>



[hello@cytex.io](mailto:hello@cytex.io)



[@cytexsmb](#)



[@cytexsecure](#)