



Your Cloud App Security Playbook

# Securing Zoom with Cytex



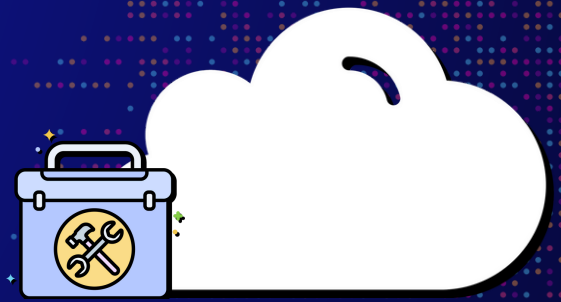
[hello@cytex.io](mailto:hello@cytex.io)

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



# Zoom security best practices

Proactively secure your Zoom environment with Cytex. This guide details how our platform automates best practices and configurations, safeguarding your organization from breaches, unauthorized access, and data leaks.

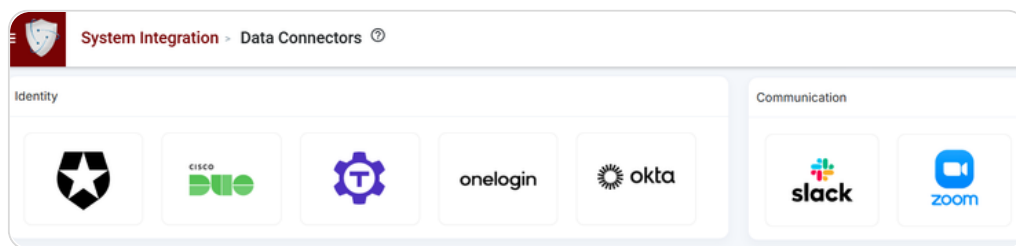


1

## Seamless Zoom Integration with Cytex

Cytex's Zoom integration offers a smooth connection to Zoom services, offering both Zoom Marketplace app and Zoom Server to Server app integrations for secure and efficient video conferencing management. It ensures a secure collaborative environment through strong compliance features, which include safeguarding sensitive data and meeting recordings from unauthorized access and potential data leaks.

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



### Account Integration Wizard

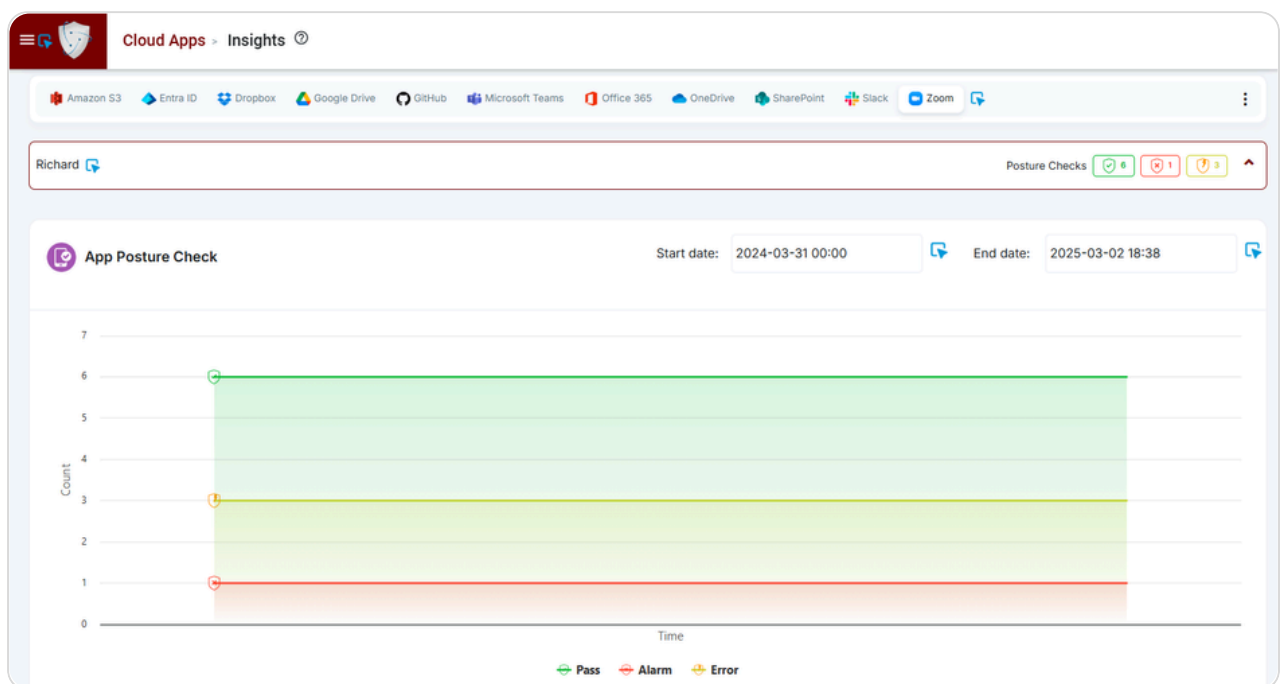
- Choose Account Type, create Account Name, and click Next.
  - Click the hyperlink *"Click to get the access code"* to get the access code from Dropbox by signing in with an admin account.
  - Enter the access code and click Next.
- Now select data collection frequency from the dropdown.
- Choose a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

## Zoom 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 Zoom environment. 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 Zoom app. It will display the integrated accounts below.
- Click on the account name to view the extensive App Posture checks.



## 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.

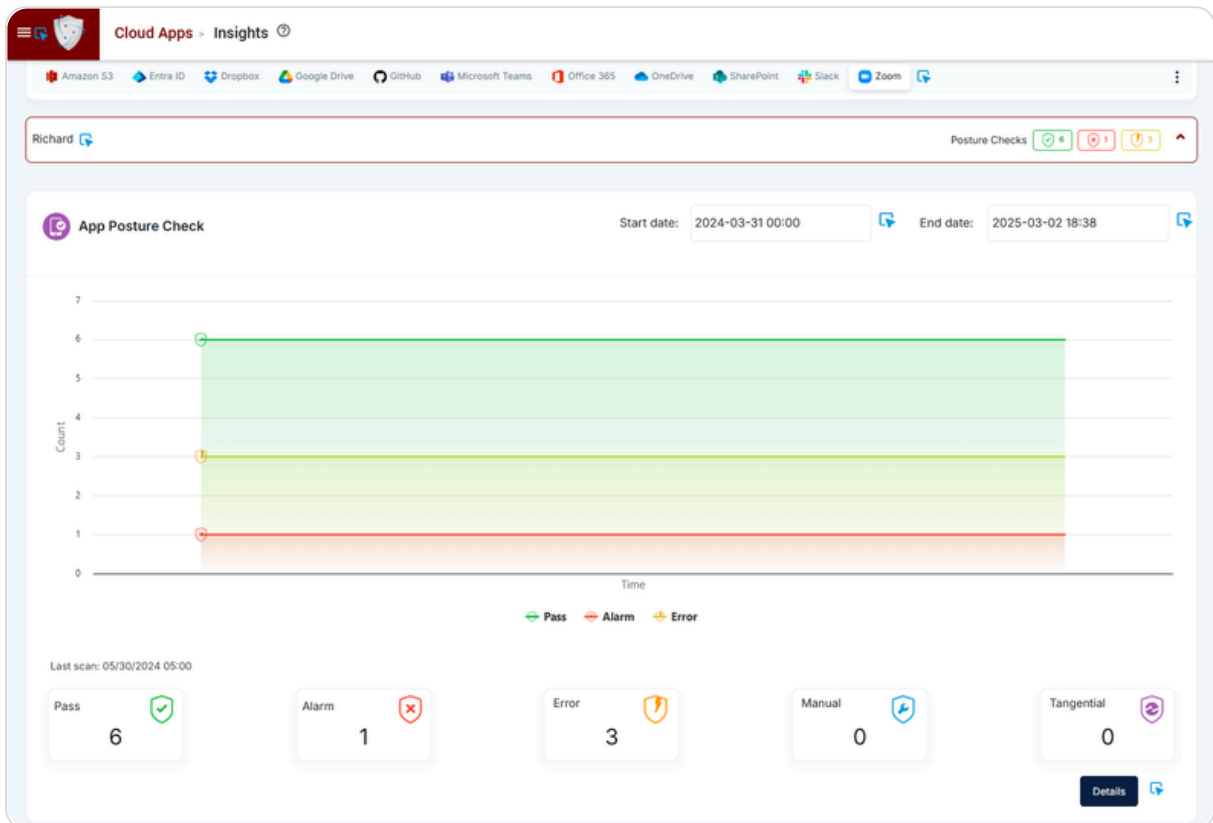
- Click on the Details button right below the App Posture check graph section to dive deep into the App Posture check.

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

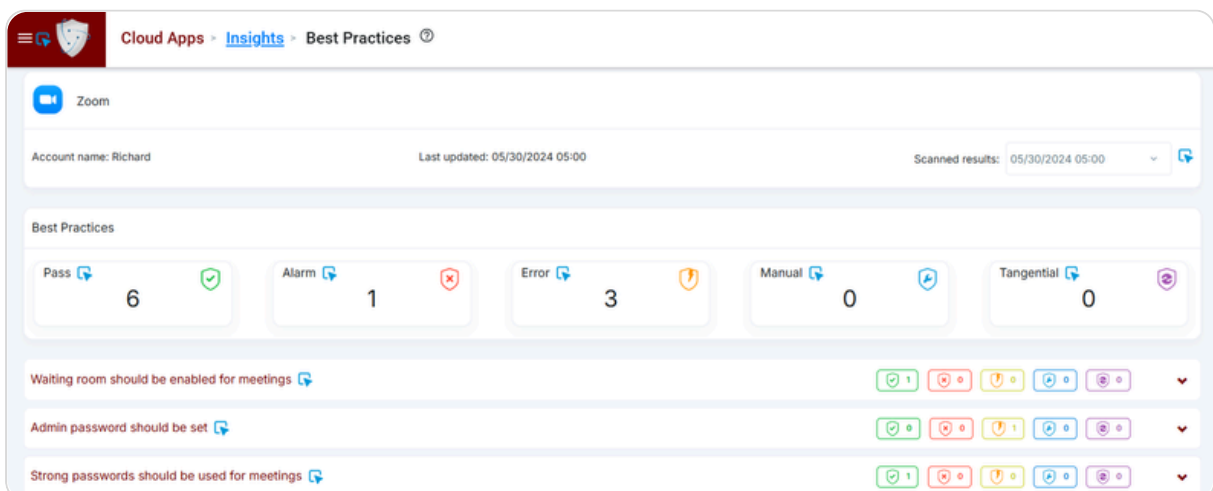
### 3 App posture check: Assessing your cloud app risk posture

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.

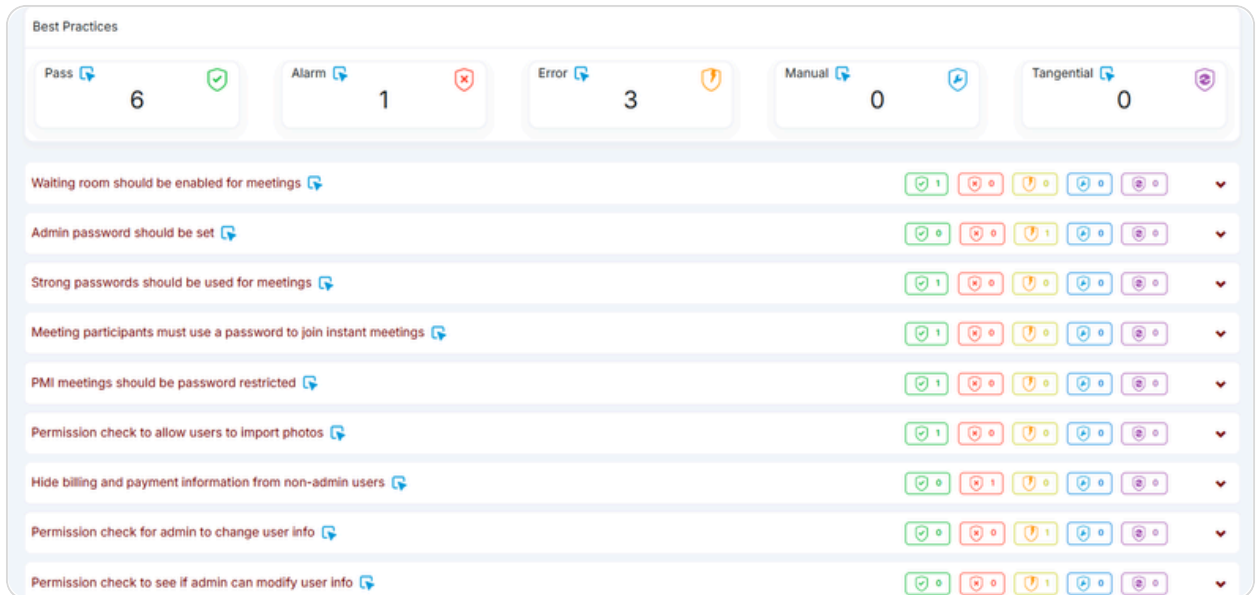


In the App Posture Check section, click the Details button to explore and assess the identified gaps in your Zoom app's security, as evaluated against security best practices.



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

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



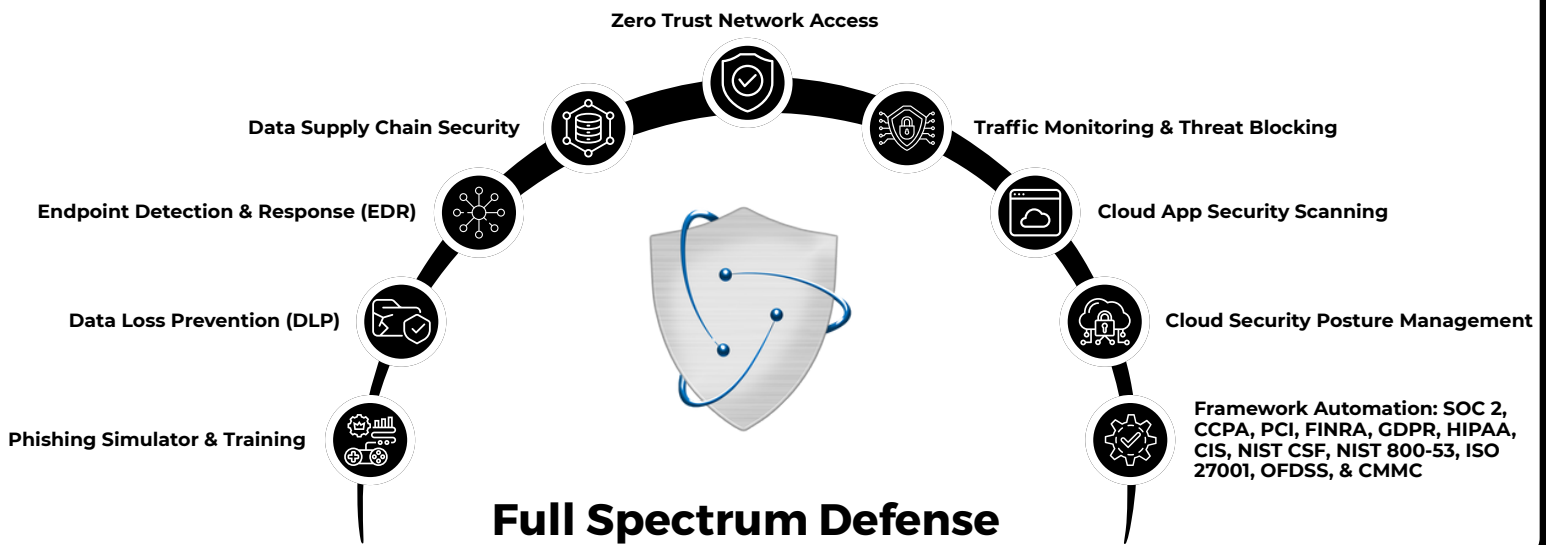
## 5 Cytex's Action Plan

- ▶ Ensure all participants are vetted before entering; enable the waiting room.
- ▶ Only authenticated users should be able to join meetings. Restrict access to users without a verified Zoom account.
- ▶ Enable end-to-end encryption (E2EE) for meetings.
- ▶ Disable join before host option to prevent participants from joining without the host.
- ▶ Set the admin password for the phone.
- ▶ Enable passcode protection for all meetings.
- ▶ Setup a strong password for all meetings.
- ▶ For recurring meetings, use a unique meeting ID instead of the personal meeting ID (PMI).
- ▶ Only an administrator role account should be able to change the account settings.
- ▶ Hide billing and payment information from non-admin users.
- ▶ Only admins should be allowed to change user information.
- ▶ Require passcode for recording access to ensure that only authorized users can view recordings.
- ▶ Disable downloading of shared recordings.
- ▶ Set an expiration date for stored recordings to limit long-term exposure.
- ▶ Regularly review and delete old recordings that are no longer needed.



# Explore **Cytex Unified Resilience Platform** today

[Schedule demo](#)



<https://cytex.io>



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



[@cytexsmb](#)



[@cytexsecure](#)