



Your Cloud App Security Playbook

Securing Slack with Cytex



hello@cytex.io

cytex.io



Slack security best practices

Cytex secures your Slack environment. This guide shows how our platform automates essential settings, preventing misconfigurations, data breaches, and unauthorized access for secure collaboration.

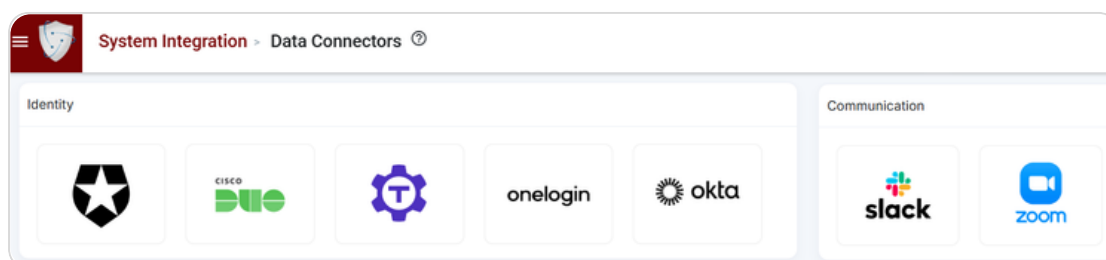


1

Seamless Slack Integration with Cytex

Cytex's integration provides seamless connection with Slack services, providing secure communication and collaboration features for your team or organization.

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



Account Integration Wizard

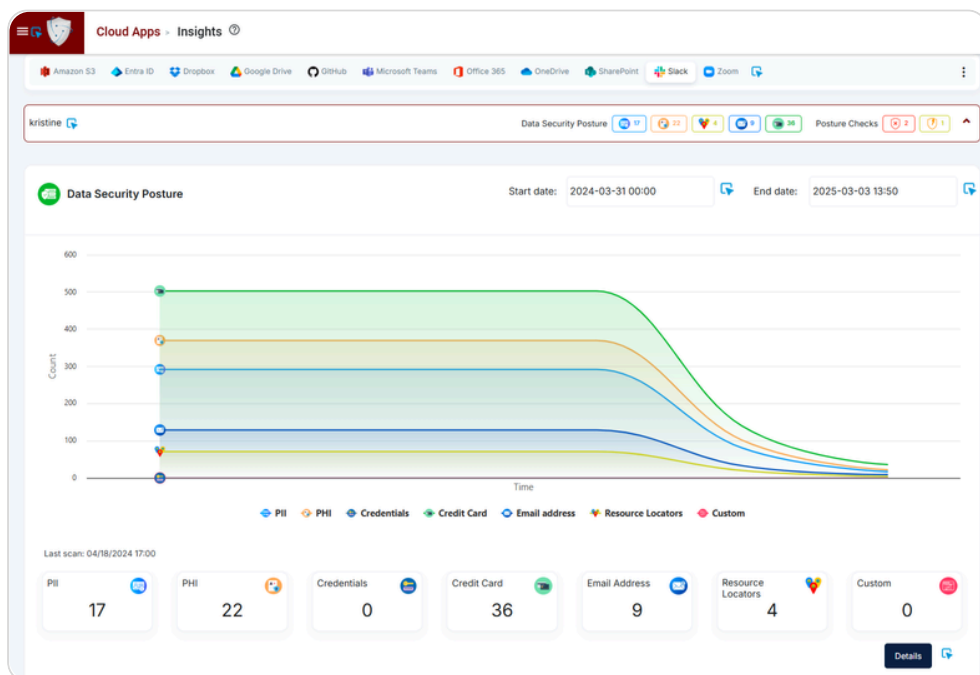
- Choose Account Type, create Account Name, and click Next.
 - Click the hyperlink *"Click to get the access code"* to get the access code from Slack by signing in with an admin account.
 - Enter the access code and click Next.
- Now select data collection frequency from the dropdown.
- Choose a DLP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

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

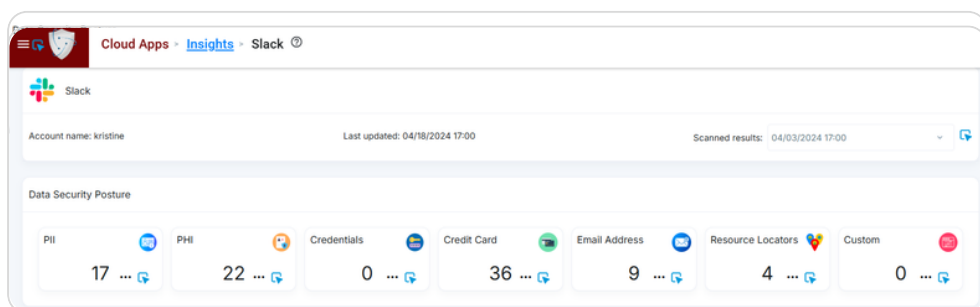
The Cytex Insights module offers both visual and numerical indicators to evaluate cloud application security and compliance. This ensures real-time monitoring and secure management of your Slack accounts and data. It also includes App Posture Checks to quickly view pass, fail, and alarm statuses.

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

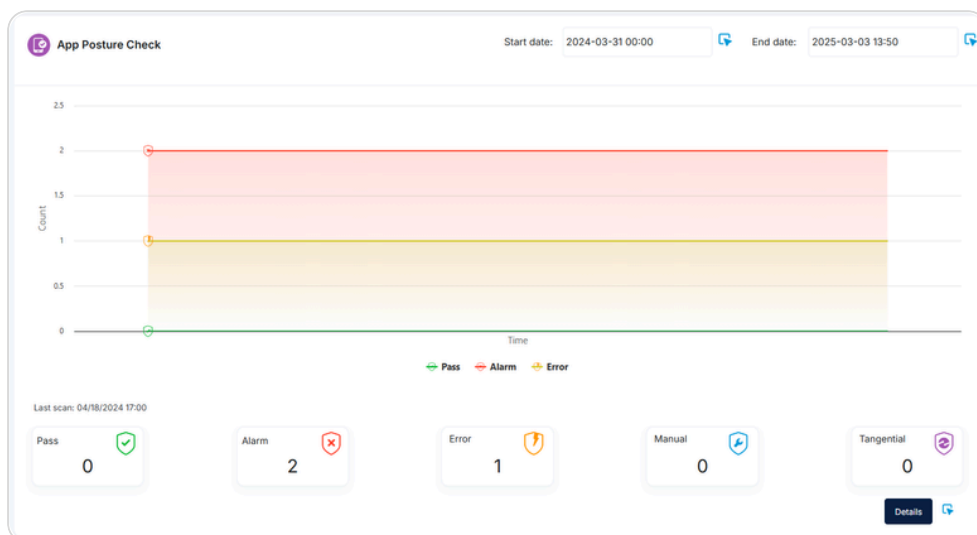
3 App posture check: Assessing your cloud app risk posture

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.

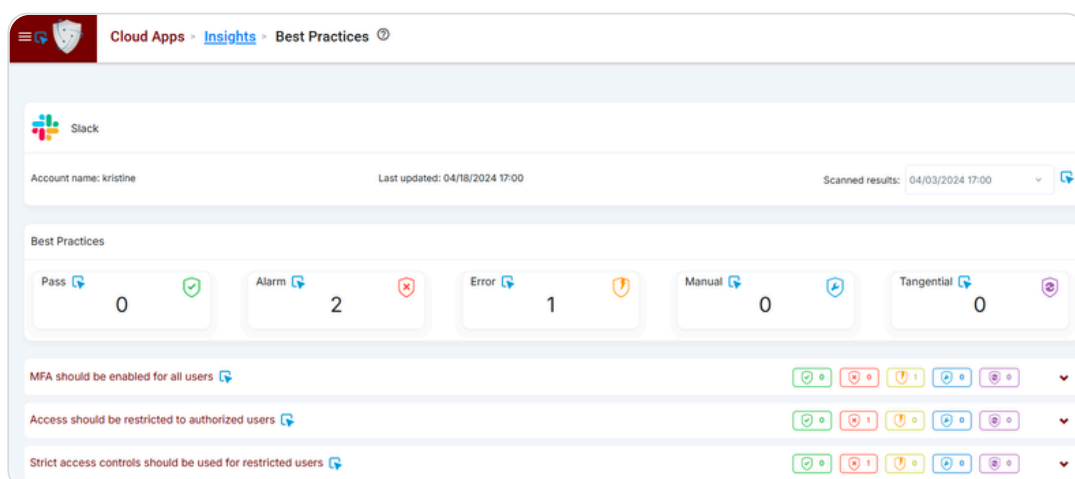
- On the cloud apps insights page select Slack app to display all the integrated accounts below.
- Click on the account name to expand and scroll down to the App Posture Check section.

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.

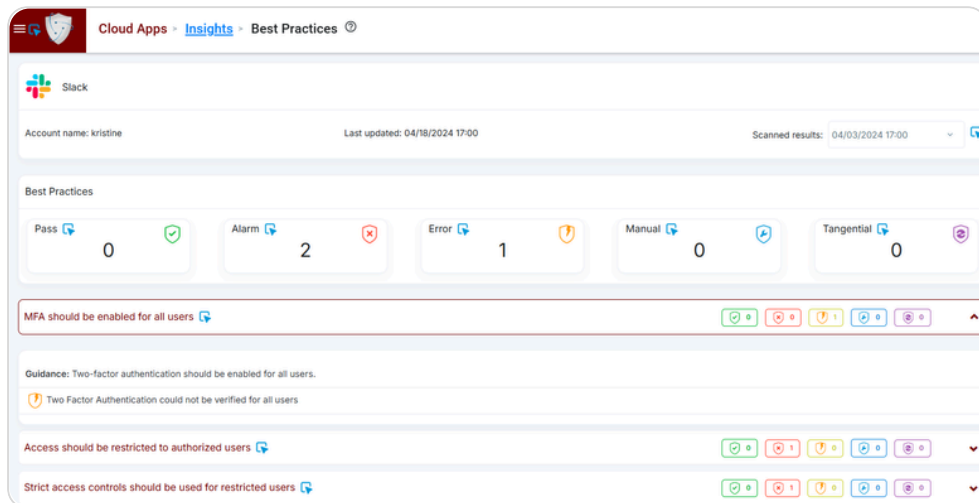


In the App Posture Check section, click the Details button to explore and assess the identified gaps in Slack’s security configurations, as evaluated against security best practices.



4 Strengthening Slack Security Posture with Cytex: Your Action Plan

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



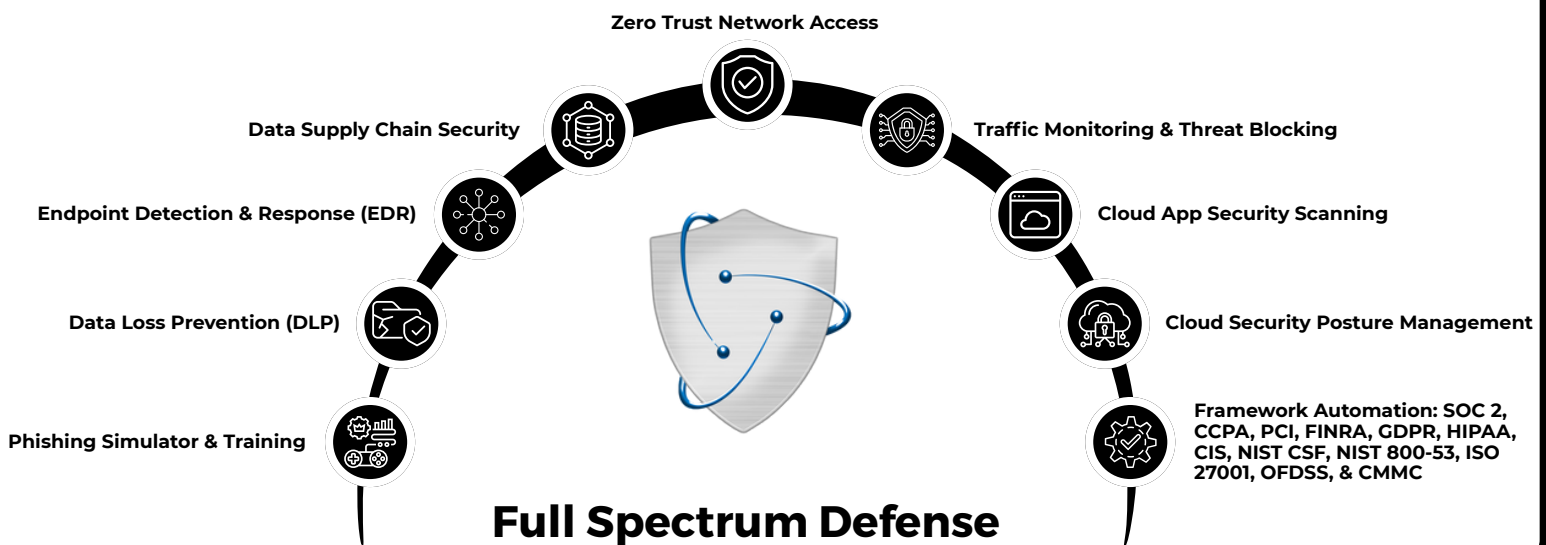
5 Cytex's Action Plan

- ▶ Access to Slack should be restricted to only authorized users.
- ▶ Enable mandatory workspace two-factor authentication (2FA).
- ▶ Workspace Owners and Org Owners can enable single sign-on (SSO) as an extra layer of security for their organization.
- ▶ Enable workspace-wide encryption, Enterprise Key Management (EKM) is available based on Enterprise Grid plan, you can manage encryption keys via AWS Key Management Service (KMS).
- ▶ Admins must enable Require Admin Approval to control workspace access and limiting guest access to specific channels.
- ▶ Admins should deactivate inactive accounts and former employees' accounts to prevent compliance lapses.
- ▶ Install and enable Enterprise Mobility Management (EMM) for your organization.
- ▶ Fine tune Slack Connect configurations for secure collaboration with external organizations.
- ▶ Adjust data retention settings to automatically delete data after a specified time and allow members to edit retention settings for specific channels and direct messages (DMs).
- ▶ Enable Legal Hold In Enterprise Grid subscriptions, compliance system admins can place holds on specific members to secure their messages and files in Slack.



Explore **Cytex Unified Resilience Platform** today

[Schedule demo](#)



<https://cytex.io>



hello@cytex.io



[@cytexsmb](#)



[@cytexsecure](#)