



Your Cloud App Security Playbook

Securing OneDrive with Cytex



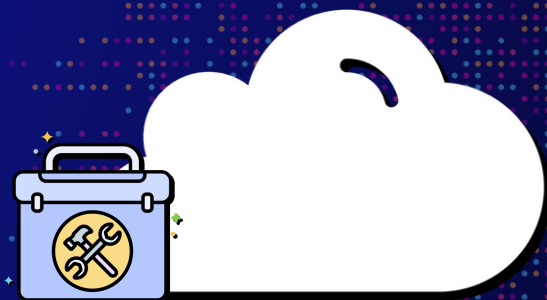
hello@cytex.io

cytex.io



Best Practices for securing OneDrive

Prevent breaches and secure your data in OneDrive with Cytex's comprehensive security configurations. Our platform automates the implementation of a strategic plan, addressing the risks posed by misconfigured environments and enhancing your organization's overall security posture.

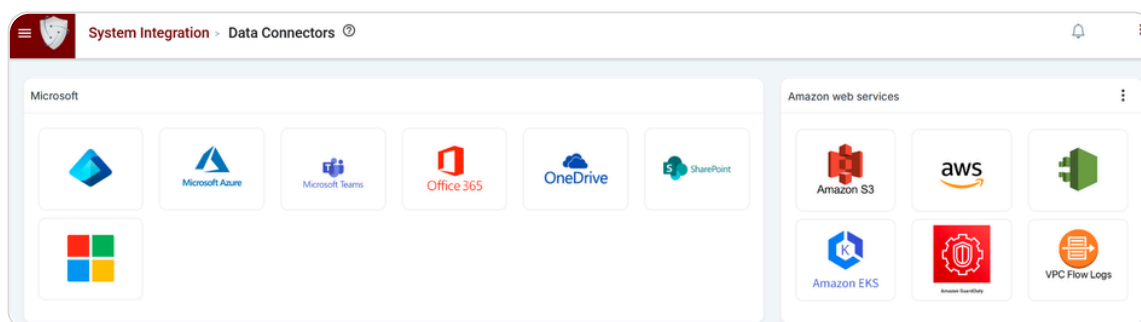


1

Seamless OneDrive Integration with Cytex

Cytex's OneDrive integration connects seamlessly with OneDrive services, supporting both business and personal accounts. It enables secure file storage and sharing while providing robust monitoring and compliance features.

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



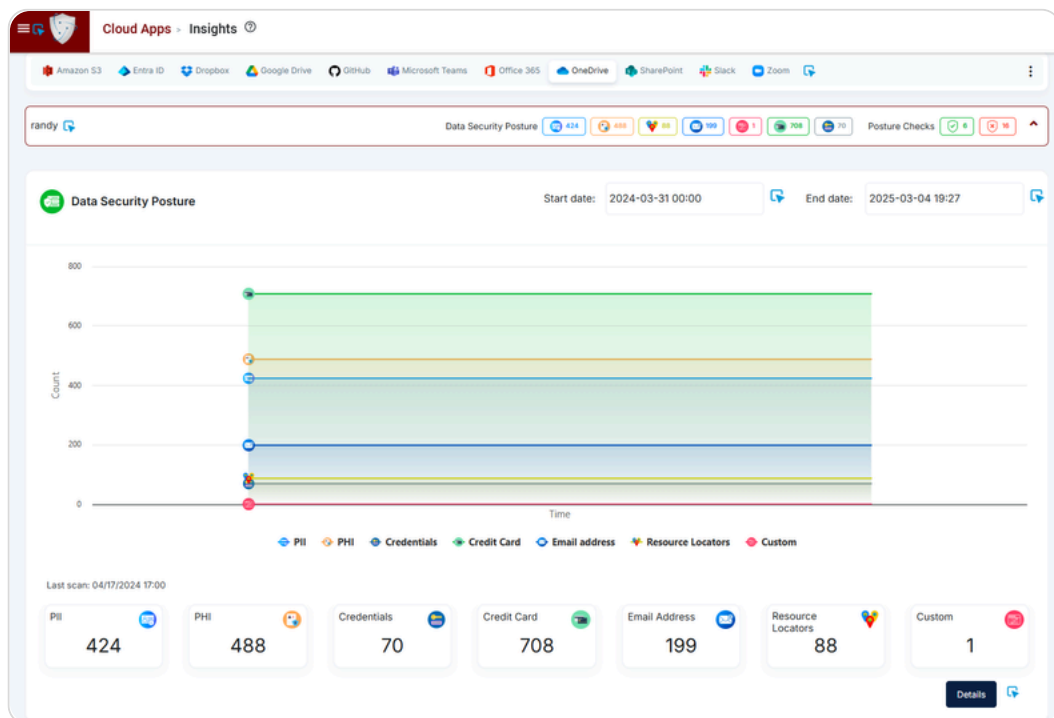
Account Integration Wizard

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

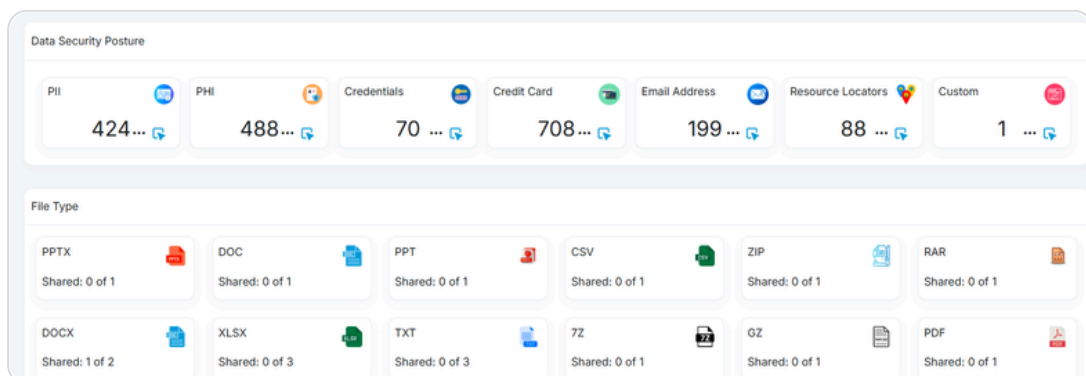
The Cytex Insights module offers both visual and numerical indicators to evaluate cloud application security and compliance. This ensures real-time monitoring and secure management of your OneDrive environment and resources. It also includes App Posture Checks to quickly view pass, fail, and alarm statuses.

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

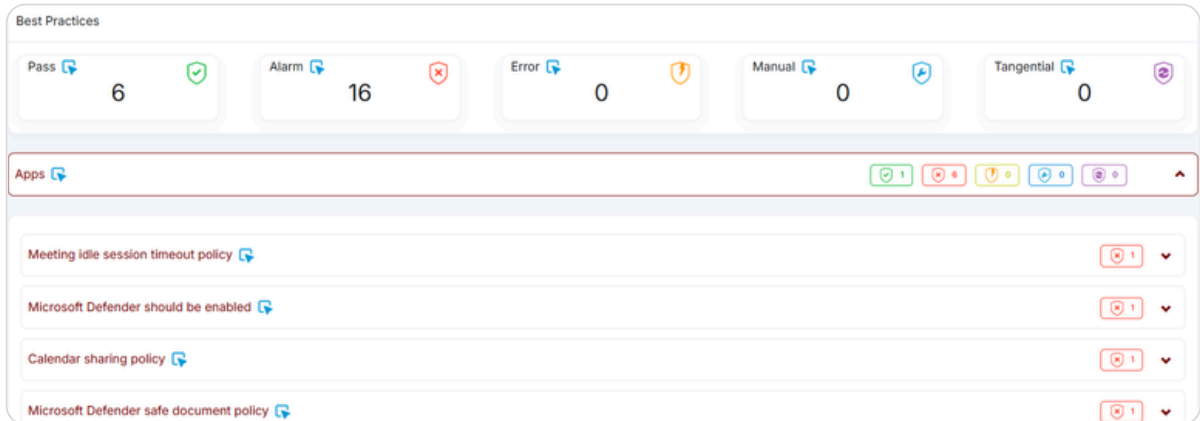


In the App Posture Check section, click the Details button to explore and assess the identified gaps in your OneDrive security, as evaluated against security best practices.

The detailed view shows the account name 'Harvey' and 'Last updated: 04/02/2024 17:00'. The scanned results are from '04/02/2024 17:00'. The 'Best Practices' section shows the same counts as the summary table: Pass (6), Alarm (16), Error (0), Manual (0), and Tangential (0). Below this, there are sections for 'Apps', 'Data', and 'Identity', each with a row of colored status icons representing different compliance levels.

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 OneDrive environment, highlighting the gaps. The comprehensive guidance empowers you to elevate your OneDrive security.



5 Cytex's Action Plan

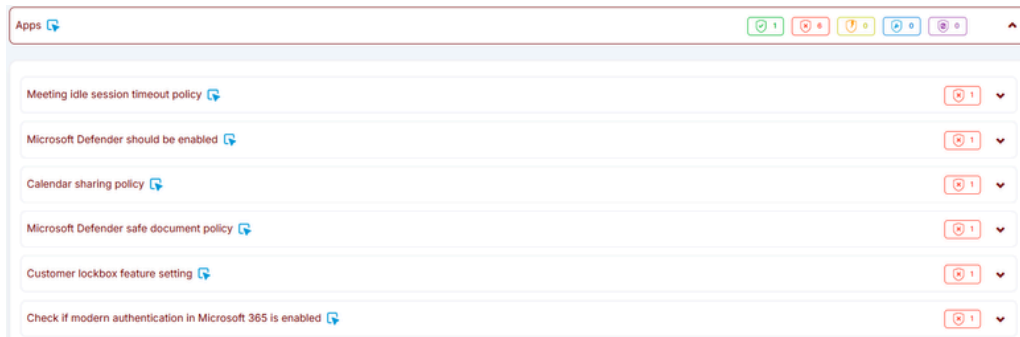
Identity:

- ▶ 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.



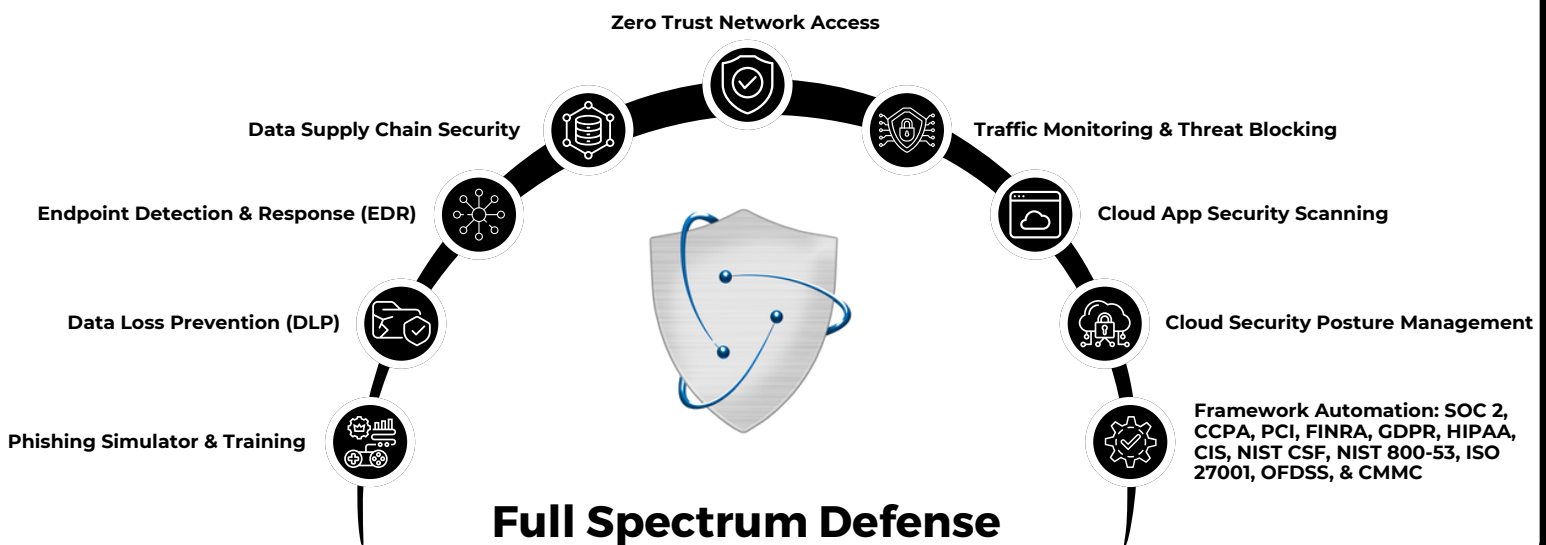
Applications:

- ▶ Microsoft Defender should be enabled for OneDrive, Office 365, SharePoint, and for Microsoft Teams to protect your organization from inadvertently sharing malicious files.
- ▶ 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 an idle session sign-out policy so that users are warned and are later signed out of Microsoft 365 after a period of browser inactivity in SharePoint and OneDrive.
- ▶ Create a Calendar Sharing policy to restrict users from sharing their detailed calendars with external users.



Explore **Cytex Unified Resilience Platform** today

[Schedule demo](#)



<https://cytex.io>



hello@cytex.io



[@cytexsmb](#)



[@cytexsecure](#)