



Your Cloud App Security Playbook

Securing SharePoint with Cytex



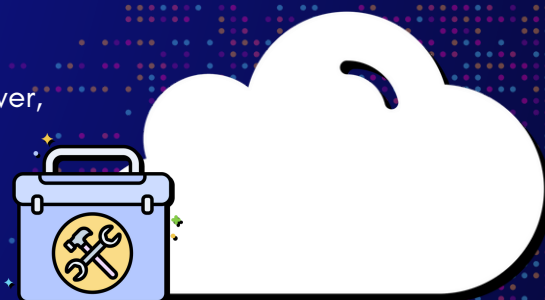
hello@cytex.io

cytex.io



Best Practices for securing SharePoint

SharePoint's potential to drive productivity is undeniable. However, without a robust security framework, that potential remains tethered to risk. This playbook explores how Cytex bridges the gap, offering an intelligent, automated approach to securing your SharePoint environment, allowing you to unlock its full collaborative power without compromising security.

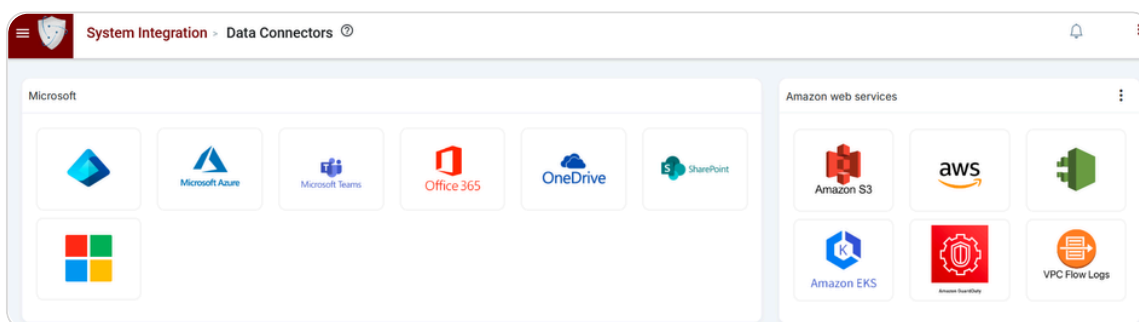


1

Seamless SharePoint Integration with Cytex

Cytex's connects seamlessly with SharePoint services, enabling secure communication and collaboration across both single and multi-tenant environments. It provides secure document management and collaboration with robust compliance features.

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



Account Integration Wizard

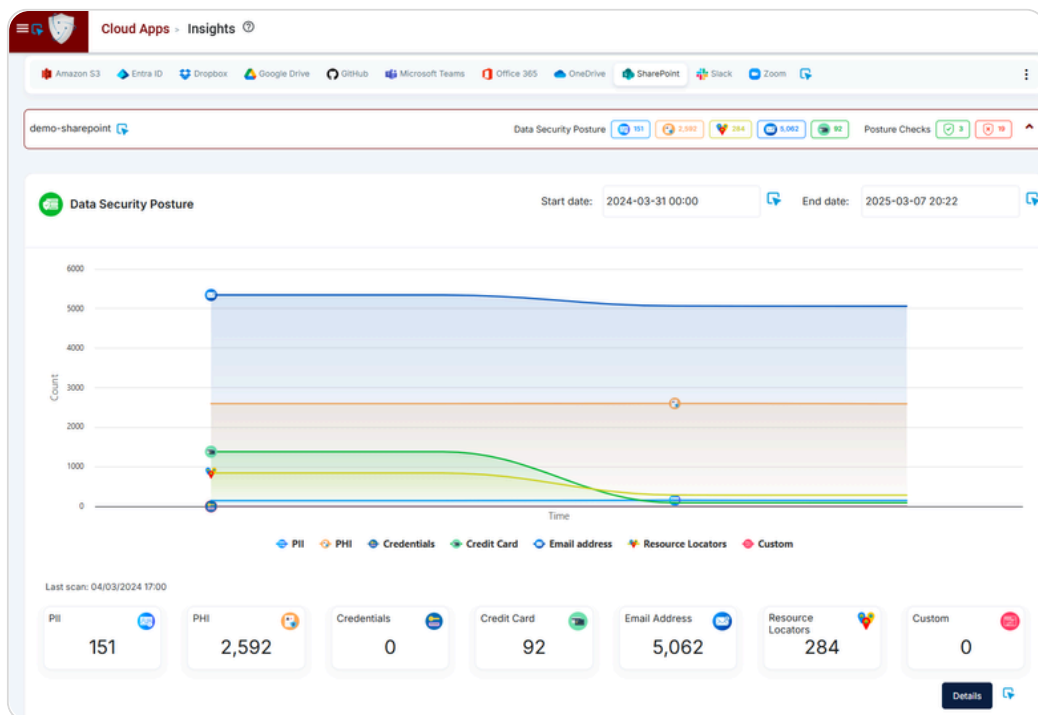
- Choose Account Type, create Account Name, and click Next.
 - Click the hyperlink *"Click to get the access code"* to get the access code from SharePoint by signing in with an admin account.
 - Enter the access code and click Next.
- Now select data collection frequency from the dropdown.
- Choose a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

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

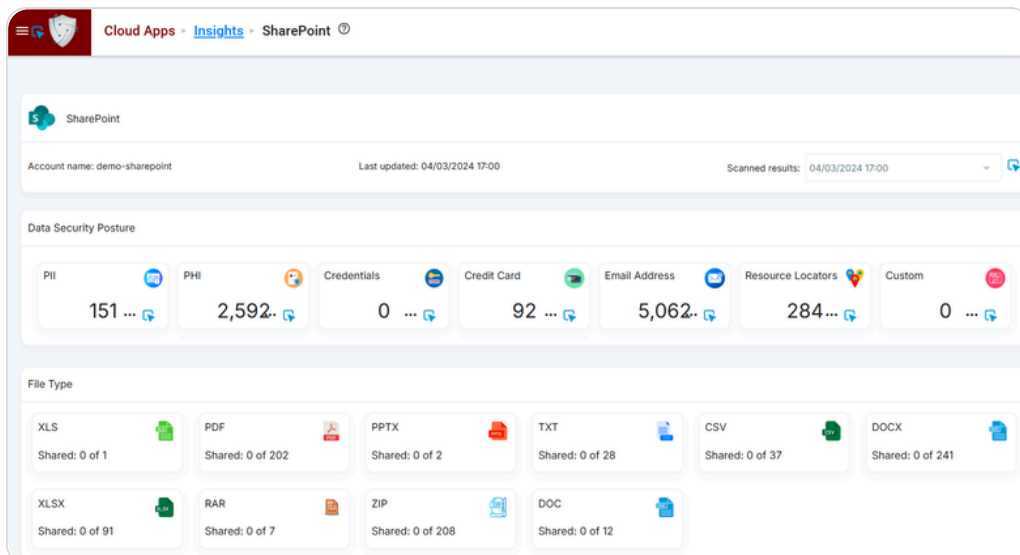
The Cytex Insights module offers both visual and numerical indicators to evaluate cloud application security and compliance. This ensures real-time monitoring and secure management of your SharePoint environment and resources. It also includes App Posture Checks to quickly view pass, fail, and alarm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

- In the Cytex main menu expand Cloud Apps, then click Insights.
- On the insights page select SharePoint. 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 comprehensive file information, including user, filename, share status, and file type.

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

SharePoint 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.

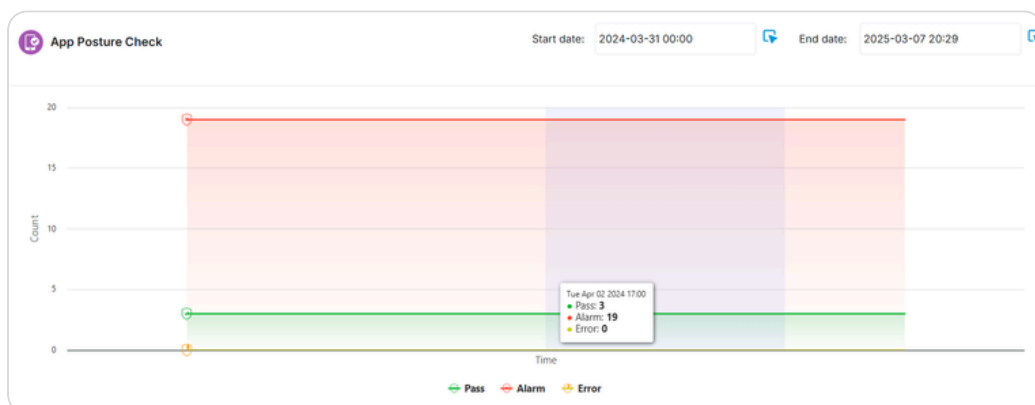
SITE	FILE NAME	SHARED	CATEGORY COUNT	TOP CATEGORIES	LAST MODIFIED
Shehroze	CP IOS Version_ 1.1.0 Build 0.docx	[User Icon]	--	KIP	04/25/2024 06:52
Usman.Nazir	cloud-apps.txt	[User Icon]	--	KIP	07/31/2024 13:21
Usman.Ali	ACB-Meezy.postman_collection1 (1).json	[User Icon]	--	KIP	09/26/2023 13:26
Usman.Nazir	Screenshot from 2024-07-19 19-10-14.png	[User Icon]	--	KIP	07/19/2024 14:12
Usman.Ali	ACB-Meezy.postman_collection1.json	[User Icon]	--	KIP	09/26/2023 13:25
hr.ops	23 Dec Bilawal salary slip.pdf	[User Icon]	1	[Category Icon]	03/12/2024 05:36
hr.ops	Abdullah Zulfiquar (Python).pdf	[User Icon]	--	KIP	08/07/2023 11:15
hr.ops	Abdullah_Naseem's_resume 1.pdf	[User Icon]	1	[Category Icon]	05/27/2024 08:43
Usman.Ali	active users.txt	[User Icon]	--	KIP	08/26/2024 10:56
hr.ops	Abdullah_Naseem's_resume.pdf	[User Icon]	1	[Category Icon]	05/15/2024 11:18

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.

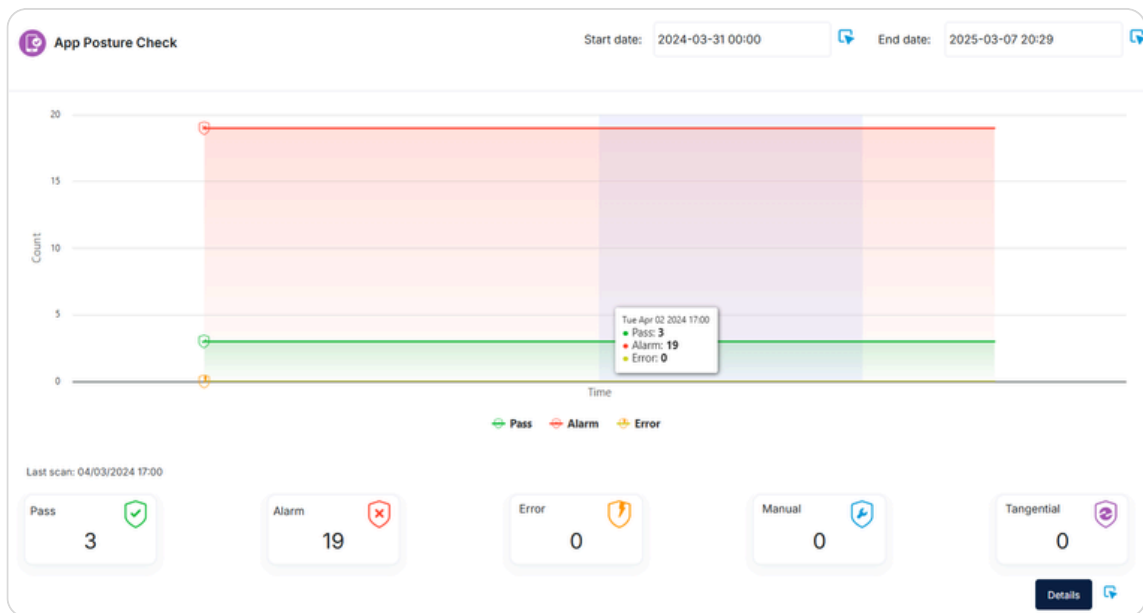
- On the cloud apps insights page select SharePoint to display all the integrated accounts below.
- Click on the account name to expand and scroll down to the App Posture Check section.



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 SharePoint security, as evaluated against security best practices.

Cloud Apps > Insights > Best Practices

SharePoint

Account name: demo-sharepoint | Last updated: 04/03/2024 17:00 | Scanned results: 04/03/2024 17:00

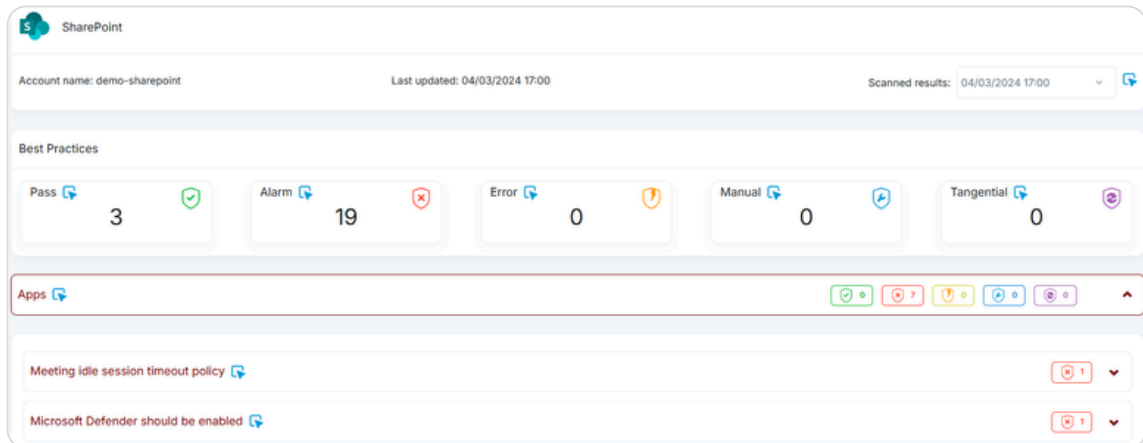
Pass	3	Alarm	19	Error	0	Manual	0	Tangential	0
------	---	-------	----	-------	---	--------	---	------------	---

Apps

- Meeting idle session timeout policy (Alarm: 1)
- Microsoft Defender should be enabled (Alarm: 1)
- Calendar sharing policy (Alarm: 1)
- Microsoft Defender safe document policy (Alarm: 1)
- Customer lockbox feature setting (Alarm: 1)
- Check if modern authentication in Microsoft 365 is enabled (Alarm: 1)
- Check Microsoft 365 audit log search setting (Alarm: 1)

4 Strengthening SharePoint Security Posture with Cytex: Your Action Plan

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



5 Cytex's Action Plan

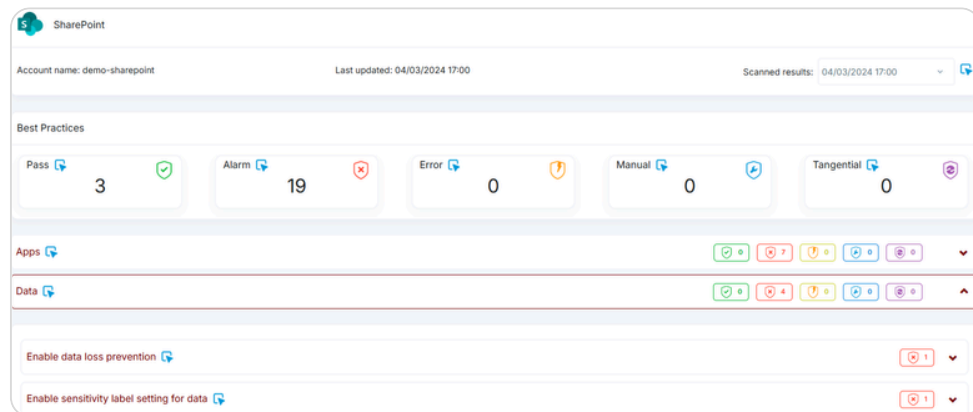
Identity:

- ▶ 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.



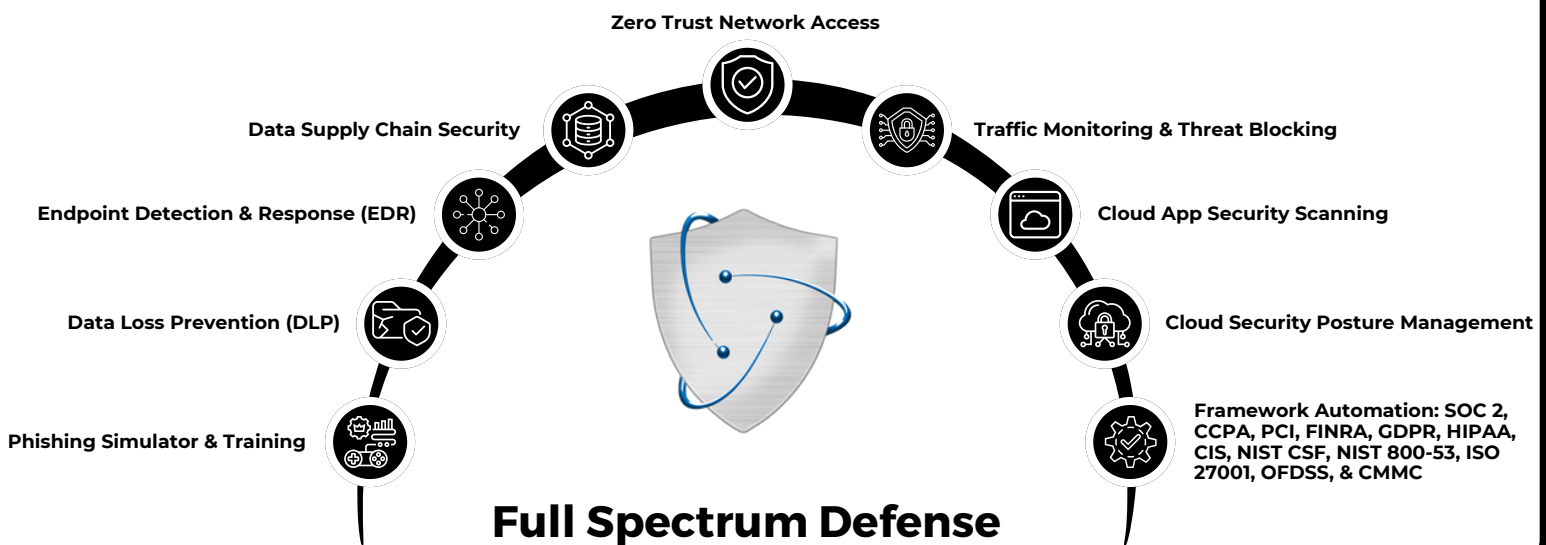
Applications:

- ▶ Microsoft Defender should be enabled for SharePoint, OneDrive, Office 365 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



[@cytextsmb](https://twitter.com/cytextsmb)



[@cytexsecure](https://www.youtube.com/cytexsecure)