



Your Cloud App Security Playbook

Securing Entra ID with Cytex



hello@cytex.io

cytex.io



Securing Your Identity Perimeter: Entra ID with Cytex

In the age of cloud-first strategies, your identity infrastructure is your security perimeter. Entra ID, as the gateway to your Microsoft ecosystem, demands unwavering vigilance. This playbook unveils how Cytex transforms Entra ID security from a reactive checklist to a dynamic, automated defense, ensuring that your digital identities remain fortified against evolving threats.

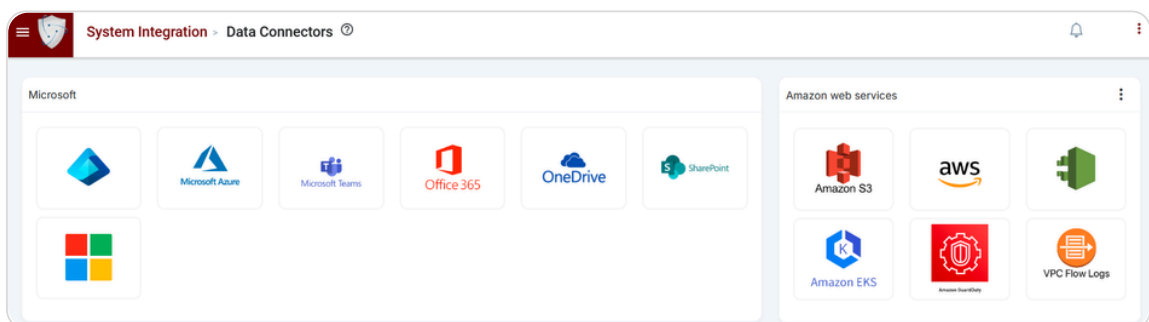


1

Seamless Entra ID Integration with Cytex

Cytex's connects seamlessly with Entra ID services, allowing you to onboard and manage Entra accounts for security and data monitoring purposes. The integration also supports advanced features such as event-based scans and log visibility, ensuring real-time updates and streamlined account monitoring.

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



Account Integration Wizard

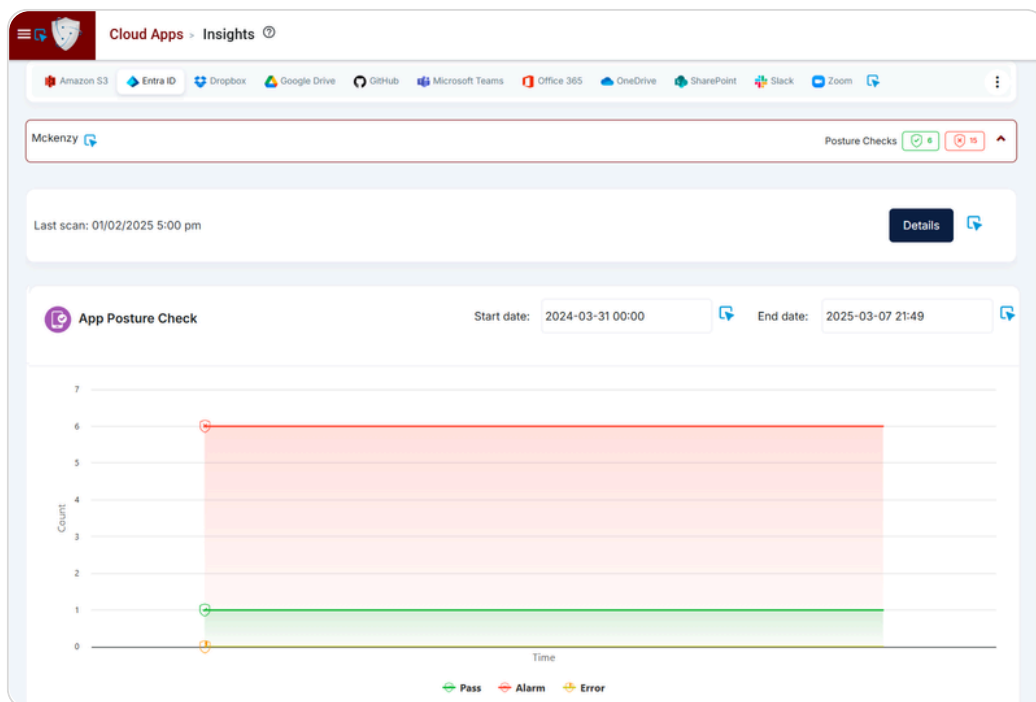
- Choose Account Type, create Account Name, and click Next.
 - Click the hyperlink *"Click to get the access code"* to get the access code from SharePoint by signing in with an admin account.
 - Enter the access code and click Next.
- Now select data collection frequency from the dropdown.
- Choose a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

Entra ID 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 Entra ID 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 Entra ID. 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

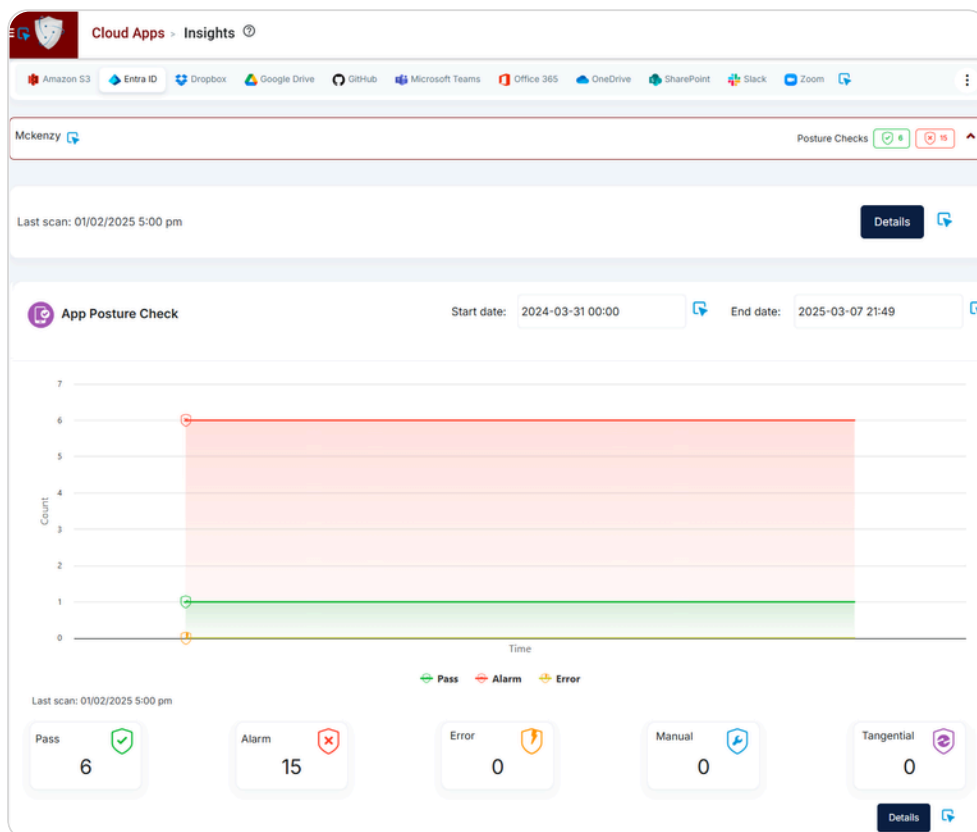
The Cytex App Posture Check module provides a detailed view of the security and compliance status of your cloud applications, giving you insights into their overall risk posture.

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

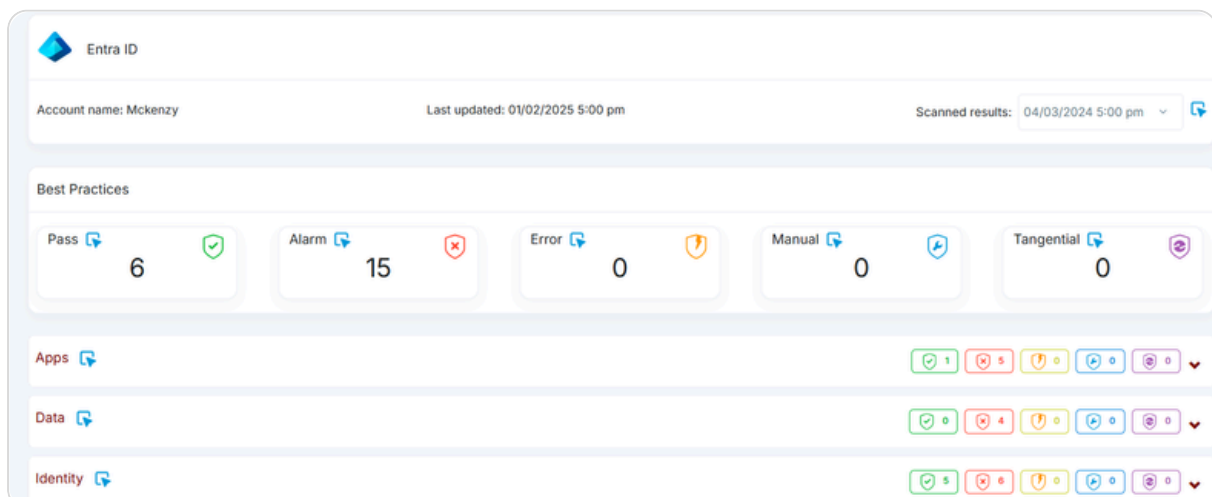
3 App posture check: Assessing your cloud app risk posture

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.

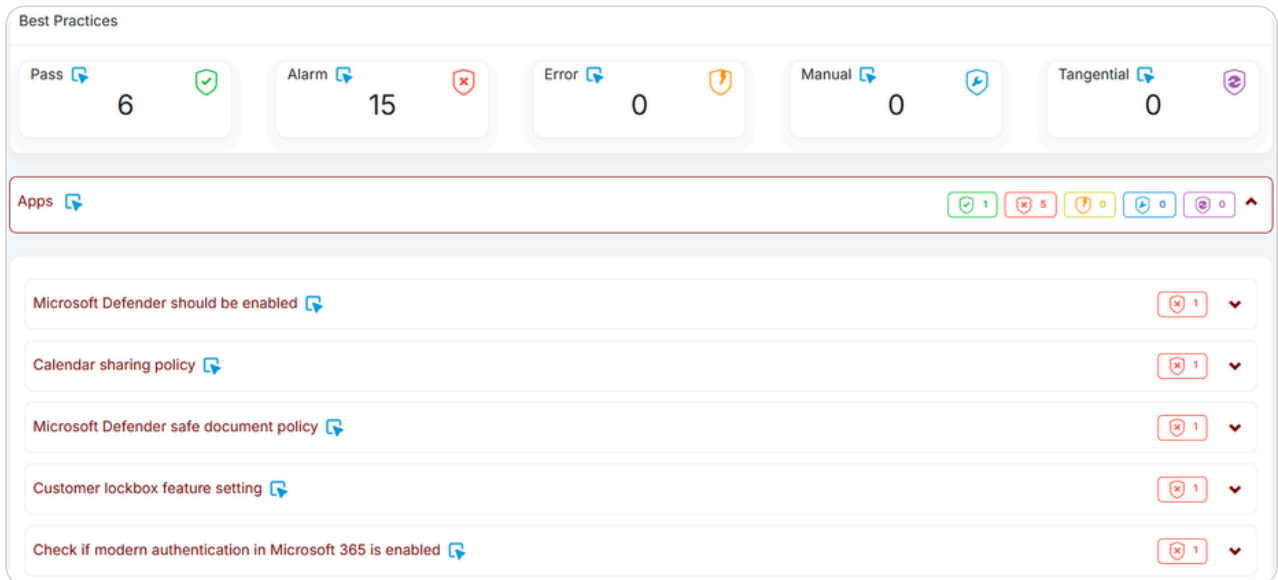


In the App Posture Check section, click the Details button to explore and assess the identified gaps in your Entra ID’s security, as evaluated against security best practices.



4 Strengthening Entra ID Security Posture with Cytex: Your Action Plan

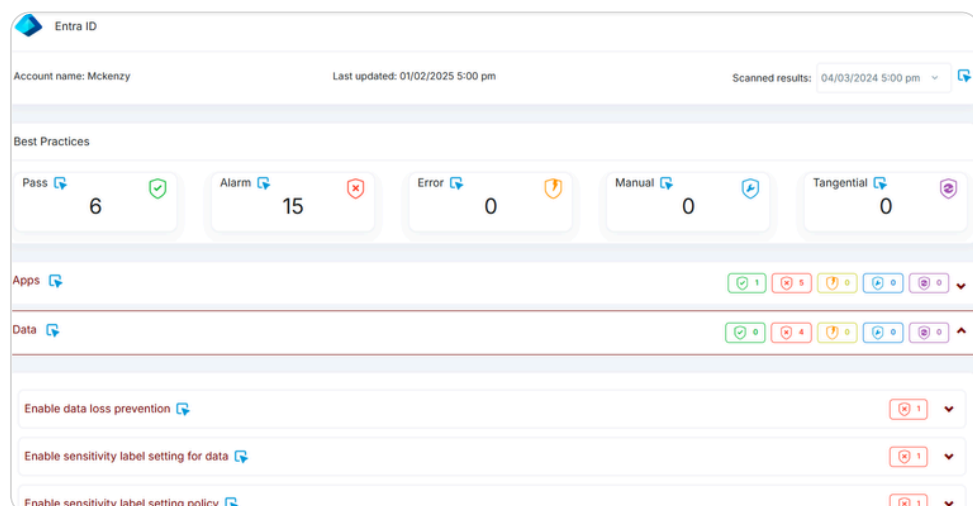
Following Cytex's evaluation, you'll find a customized action plan with best practices specifically for your Entra ID environment, highlighting the gaps. The comprehensive guidance empowers you to elevate your Zoom security.



5 Cytex's Action Plan

Data Loss Prevention:

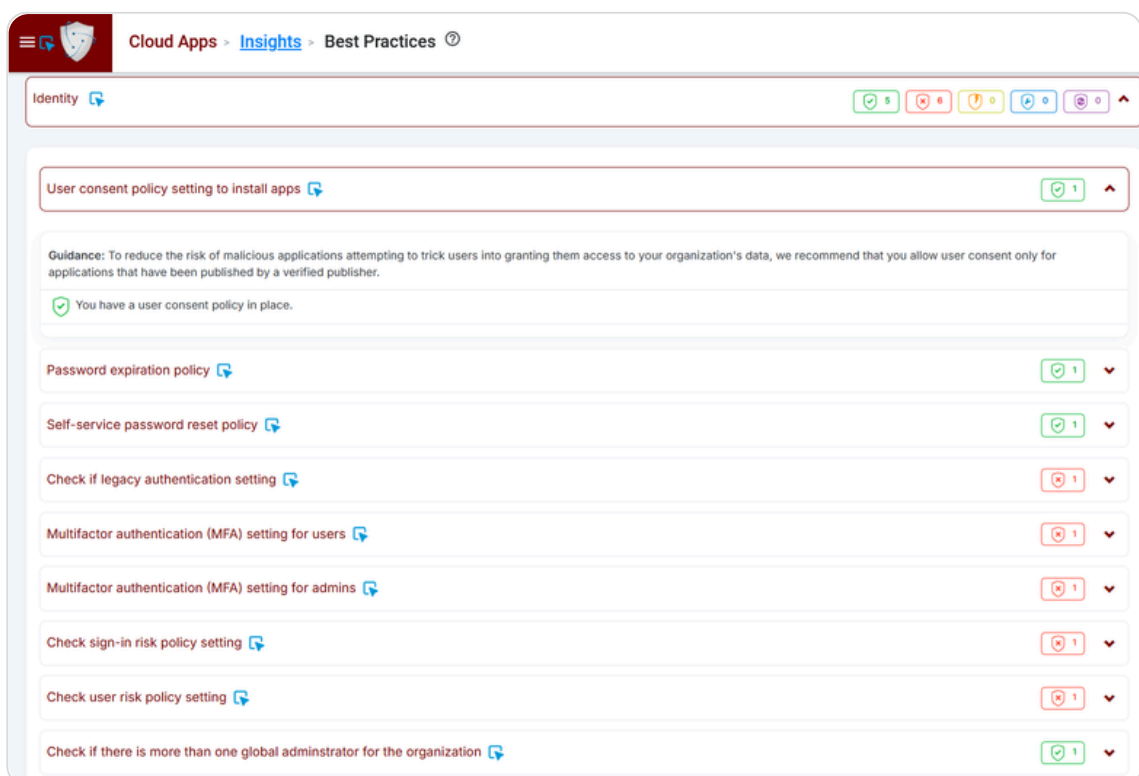
- ▶ Enable data loss prevention policy.
- ▶ Enable sensitivity labels for your data in order to track the data type without exposing sensitive data on other platforms.
- ▶ Setup and use data classification policies for data stored in your apps like Outlook, Word, SharePoint sites, and Office 365 groups.
- ▶ 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.



5 Cytex's Action Plan

Identity:

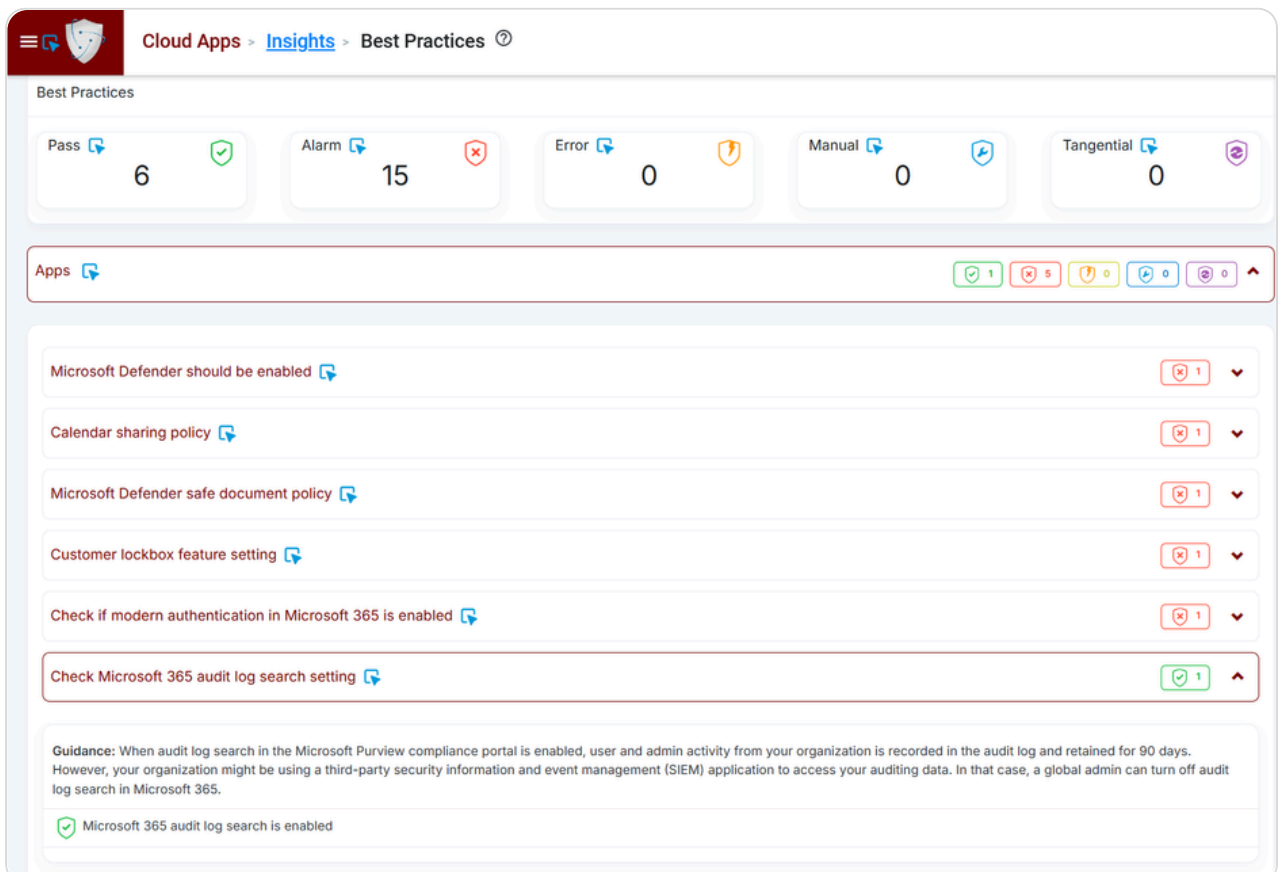
- ▶ Enable security default Multi-factor authentication (MFA) for everyone: admins and users.
- ▶ Make sure to have more than one global administrator for the organization. According to CIS O365 Benchmark 2.0.0, the suggestion is to have between two to four global admins.
- ▶ Enforce a password expiration 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

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 a Calendar Sharing policy to restrict users from sharing their detailed calendars with external users.



The screenshot displays the 'Best Practices' section of the Microsoft 365 compliance dashboard. At the top, the navigation path is 'Cloud Apps > Insights > Best Practices'. Below this, there are five summary cards for different alert types: Pass (6), Alarm (15), Error (0), Manual (0), and Tangential (0). A table below lists specific best practices with their status and counts:

Best Practice	Status	Count
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	Pass	1

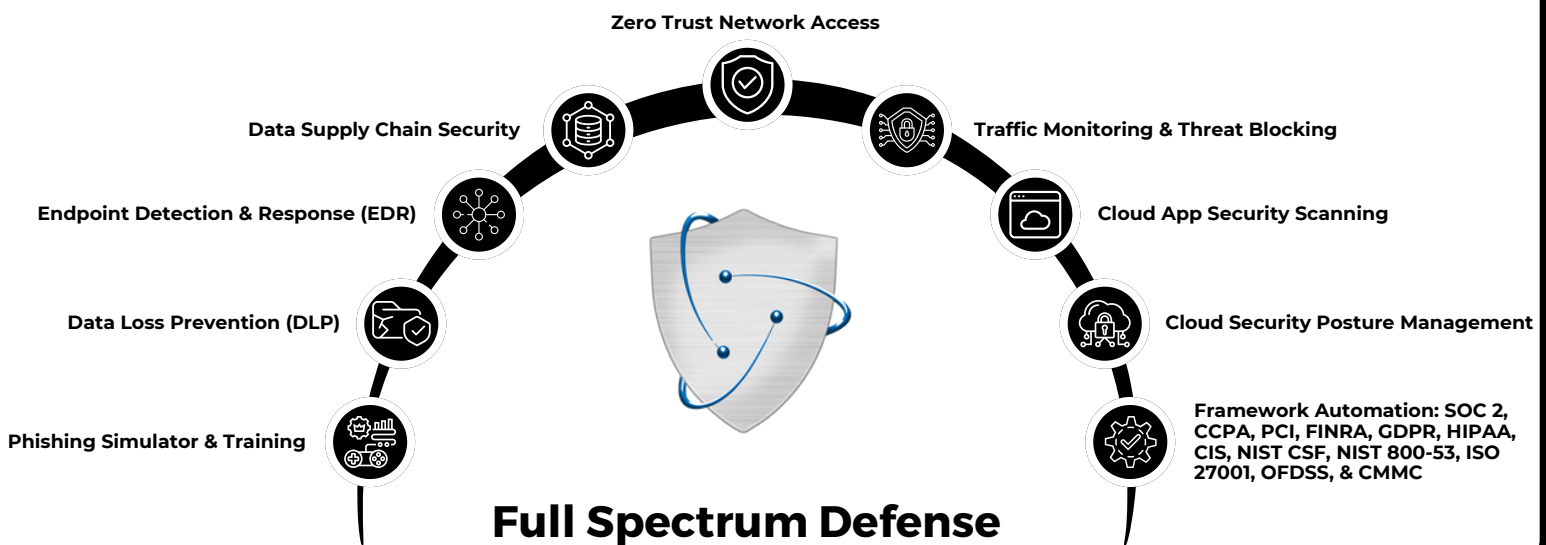
Guidance: When audit log search in the Microsoft Purview compliance portal is enabled, user and admin activity from your organization is recorded in the audit log and retained for 90 days. However, your organization might be using a third-party security information and event management (SIEM) application to access your auditing data. In that case, a global admin can turn off audit log search in Microsoft 365.

Microsoft 365 audit log search is enabled



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)