



Your Cloud App Security Playbook

Securing Google Drive ● with Cytex



hello@cytex.io

cytex.io



Securing Google Drive with Cytex

Maintaining compliance while managing Google Drive security can be a complex balancing act. This playbook explores how Cytex seamlessly integrates compliance checks and automates policy enforcement, ensuring that your data adheres to regulatory requirements and industry best practices without hindering collaboration.

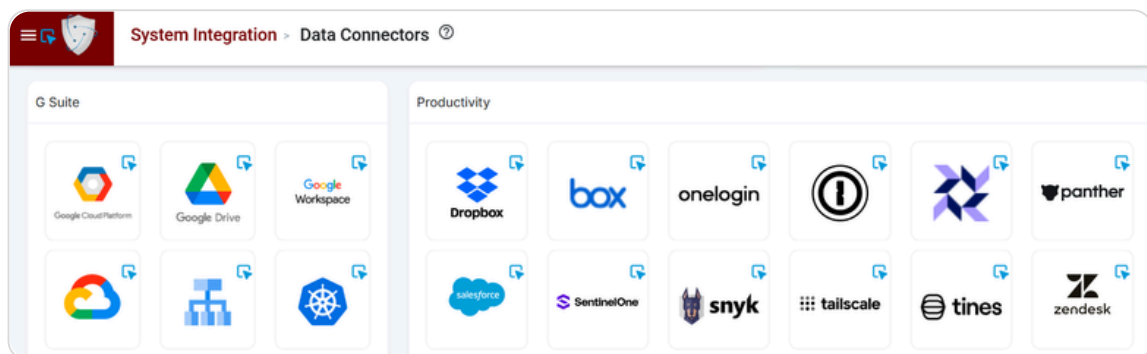


1

Seamless Google Drive Integration with Cytex

Cytex's integration connects seamlessly with Google Drive services, offering secure file storage and sharing with advanced compliance features, including Data Loss Prevention.

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



Account Integration Wizard

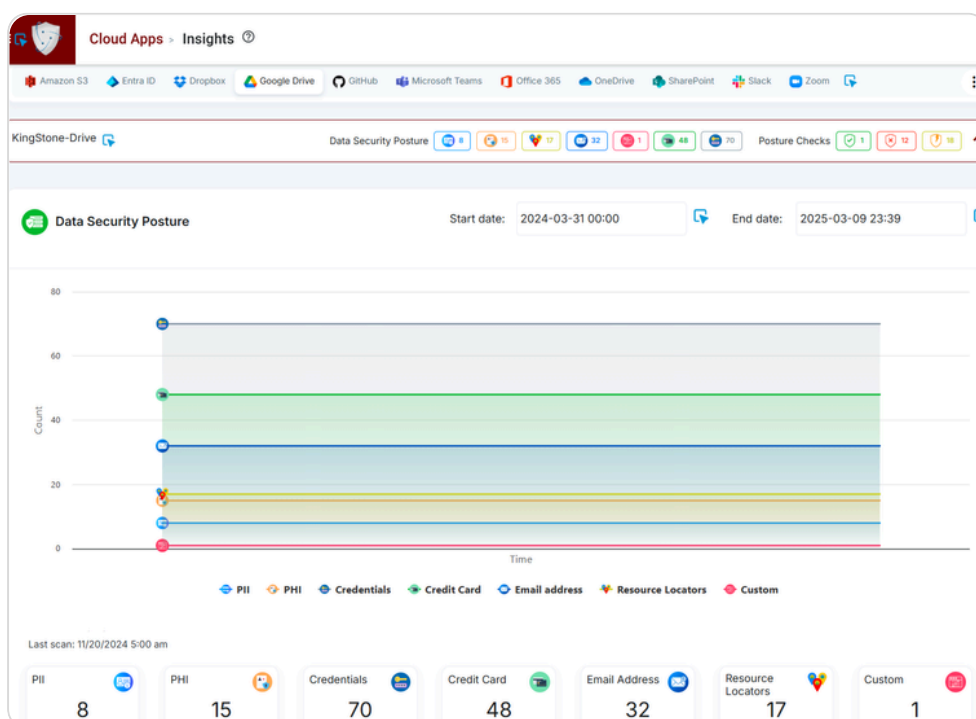
- Choose Account Type, create Account Name, and click Next.
 - Click the hyperlink *"Click to get the access code"* to get the access code from Google Drive by signing in with an admin account.
 - Enter the access code and click Next.
- Now select data collection frequency from the dropdown.
- Choose 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 Google Drive accounts and data. When real-time events and log option is selected:
 - Select Log Frequency. Set log frequency to align with your organization's monitoring needs.
 - 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

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

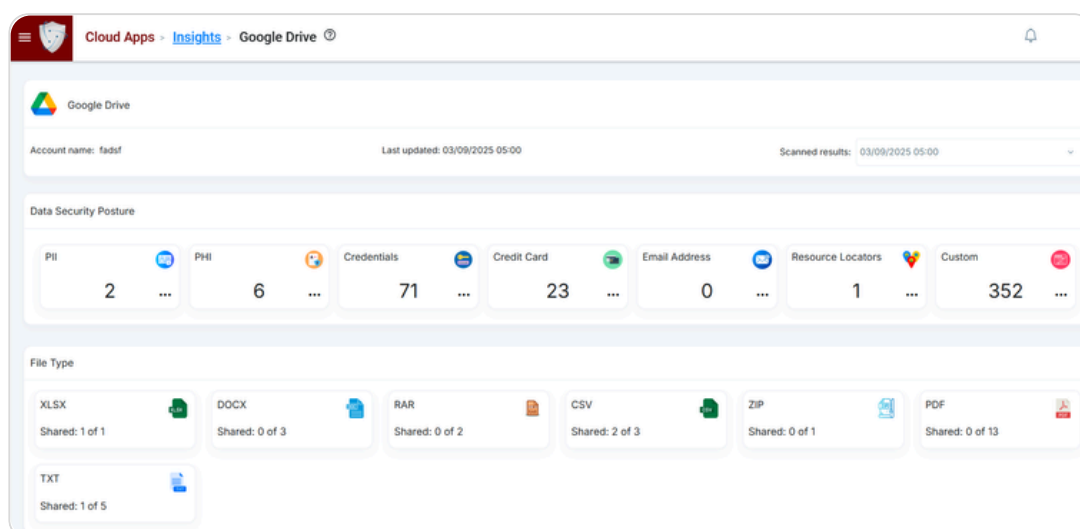
The Cytex Insights module offers both visual and numerical indicators to evaluate cloud application security and compliance. This ensures real-time monitoring and secure management of your Google Drive environment and resources. It also includes App Posture Checks to quickly view pass, fail, and alarm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

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

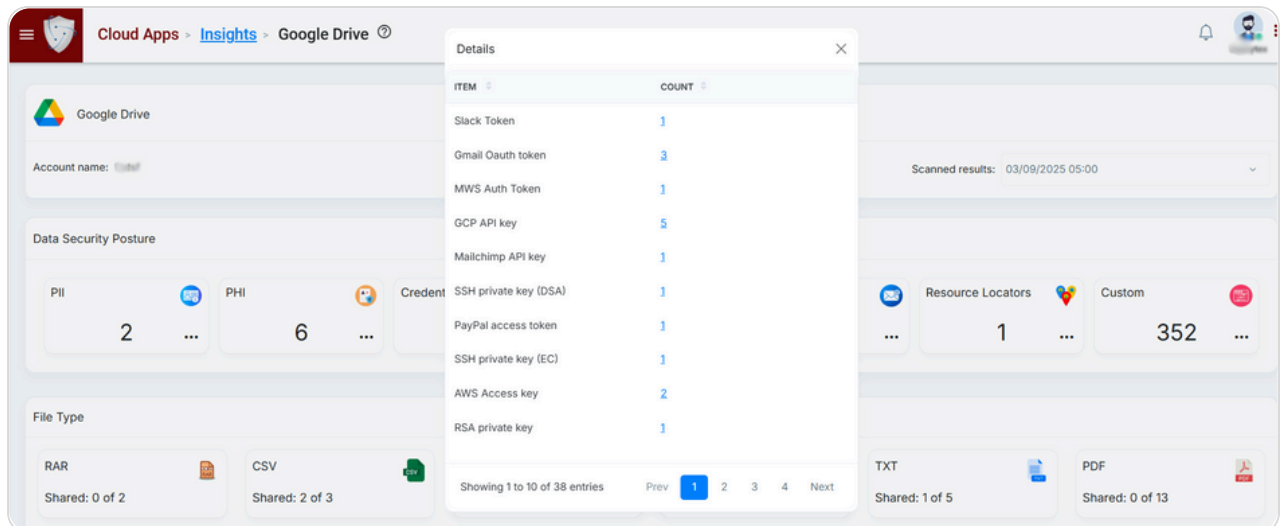
The Data Security Posture insights organize data into seven categories.



2

Google Drive 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.



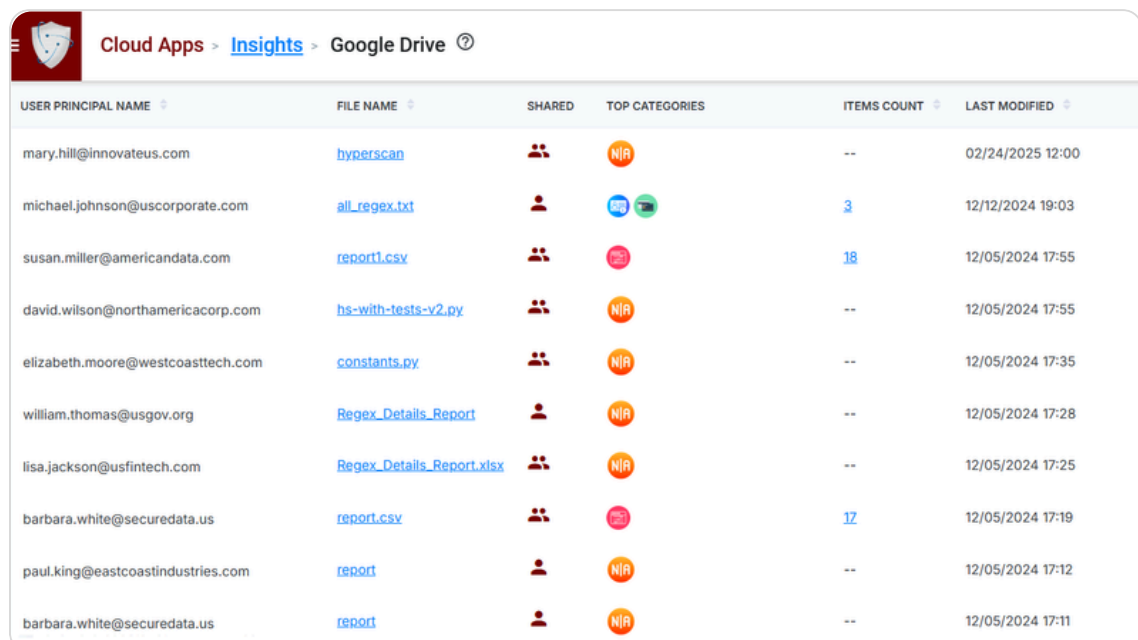
The screenshot shows the 'Cloud Apps > Insights > Google Drive' interface. A 'Details' pop-up window is open, displaying a list of sensitive items and their counts:

ITEM	COUNT
Slack Token	1
Gmail OAuth token	3
MWS Auth Token	1
GCP API key	5
Mailchimp API key	1
SSH private key (DSA)	1
PayPal access token	1
SSH private key (EC)	1
AWS Access key	2
RSA private key	1

The background interface shows the 'Data Security Posture' section with categories: PII (2), PHI (6), and Credentials (3). The 'File Type' section shows RAR (0 of 2) and CSV (2 of 3). The 'Scanned results' section shows '03/09/2025 05:00'. The 'Resource Locators' section shows 1 item, and the 'Custom' section shows 352 items.

The Data Security Posture insights organize data into seven categories, classifying it by patterns while precisely identifying sensitive information according to the chosen policy.

- PII: Ensures the safety of Personally Identifiable Information.
- PHI: Provides secure storage for Protected Health Information.
- Credentials: Stores login credentials securely.
- Credit Card: Categorizes and secures sensitive credit card information.
- Email Address: Protects and organizes email data.
- Resource Locators: Tracks resource locations effectively.
- Custom: Allows custom categorization for specific needs.



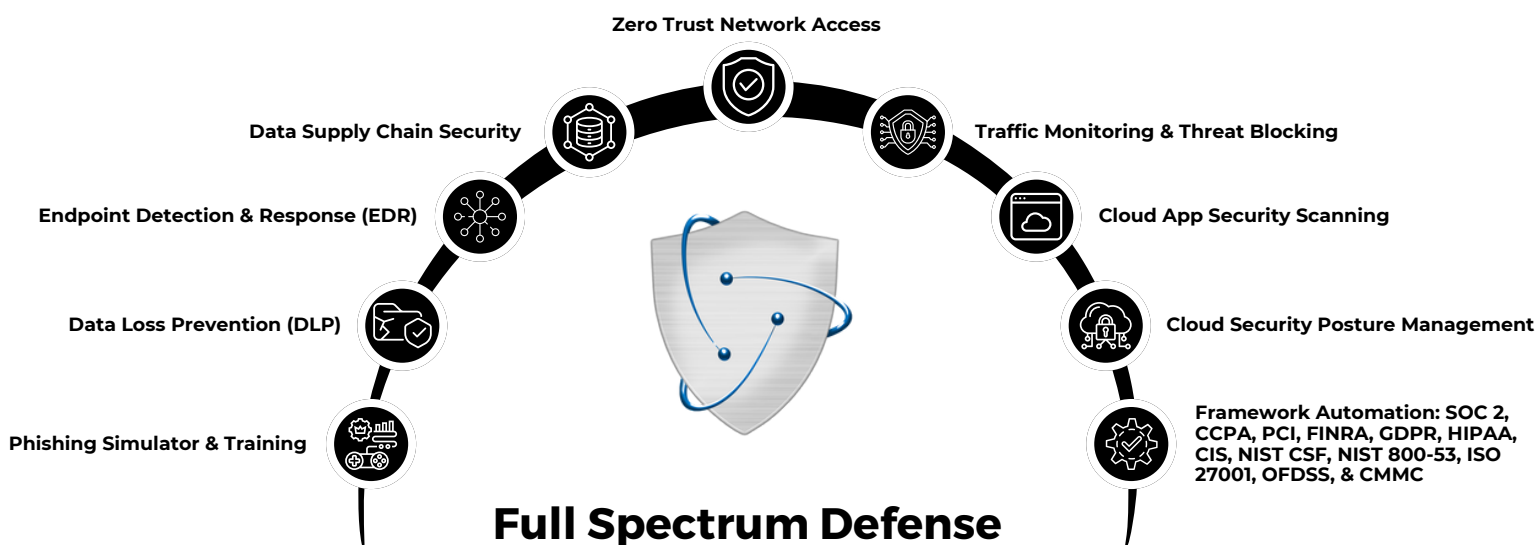
The screenshot shows the 'Cloud Apps > Insights > Google Drive' interface. The 'Detailed View' section displays a table of sensitive records:

USER PRINCIPAL NAME	FILE NAME	SHARED	TOP CATEGORIES	ITEMS COUNT	LAST MODIFIED
mary.hill@innovateus.com	hyperscan		PII	--	02/24/2025 12:00
michael.johnson@uscorporate.com	all_regex.txt		PII, PHI	3	12/12/2024 19:03
susan.miller@americadata.com	report.csv		PII	18	12/05/2024 17:55
david.wilson@northamericacorp.com	hs-with-tests-v2.py		PII	--	12/05/2024 17:55
elizabeth.moore@westcoasttech.com	constants.py		PII	--	12/05/2024 17:35
william.thomas@usgov.org	Regex_Details_Report		PII	--	12/05/2024 17:28
lisa.jackson@usfintech.com	Regex_Details_Report.xlsx		PII	--	12/05/2024 17:25
barbara.white@securedata.us	report.csv		PII	17	12/05/2024 17:19
paul.king@eastcoastindustries.com	report		PII	--	12/05/2024 17:12
barbara.white@securedata.us	report		PII	--	12/05/2024 17:11



Explore **Cytex Unified Resilience Platform** today

[Schedule demo](#)



<https://cytex.io>



hello@cytex.io



[@cytexsmb](#)



[@cytexsecure](#)