



Your Cloud App Security Playbook

# Securing Amazon S3 with Cytex



[hello@cytex.io](mailto:hello@cytex.io)

[cytex.io](https://cytex.io)



# Amazon S3 security best practices

Secure your Amazon S3 buckets effectively with Cytex. This guide demonstrates how our platform automates critical security configurations, preventing data leaks, unauthorized access, and ensuring robust data protection.

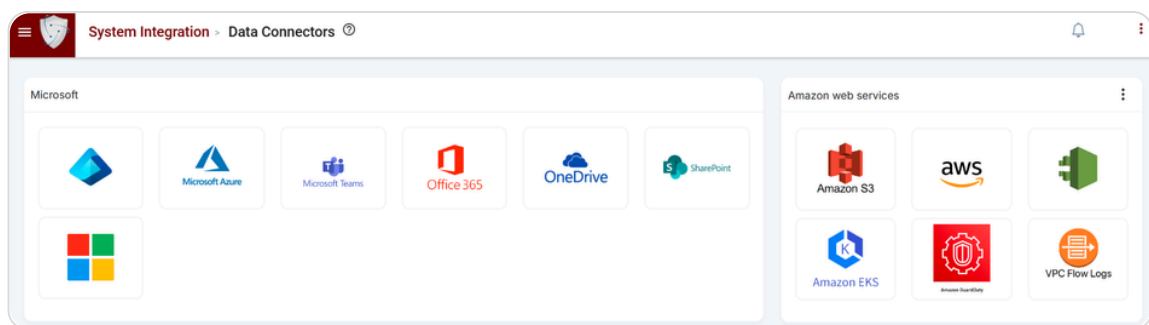


1

## Seamless Amazon S3 Integration with Cytex

Cytex's integration provides seamless connection with Amazon S3 services, enabling secure storage and management of data with advanced compliance features.

- Log in to Cytex and open the main menu.
- Expand System Integration, then Integration Manager, and click on Data Connectors.
- Select Amazon S3 as the cloud asset on the Data Connectors page.



### Account Integration Wizard

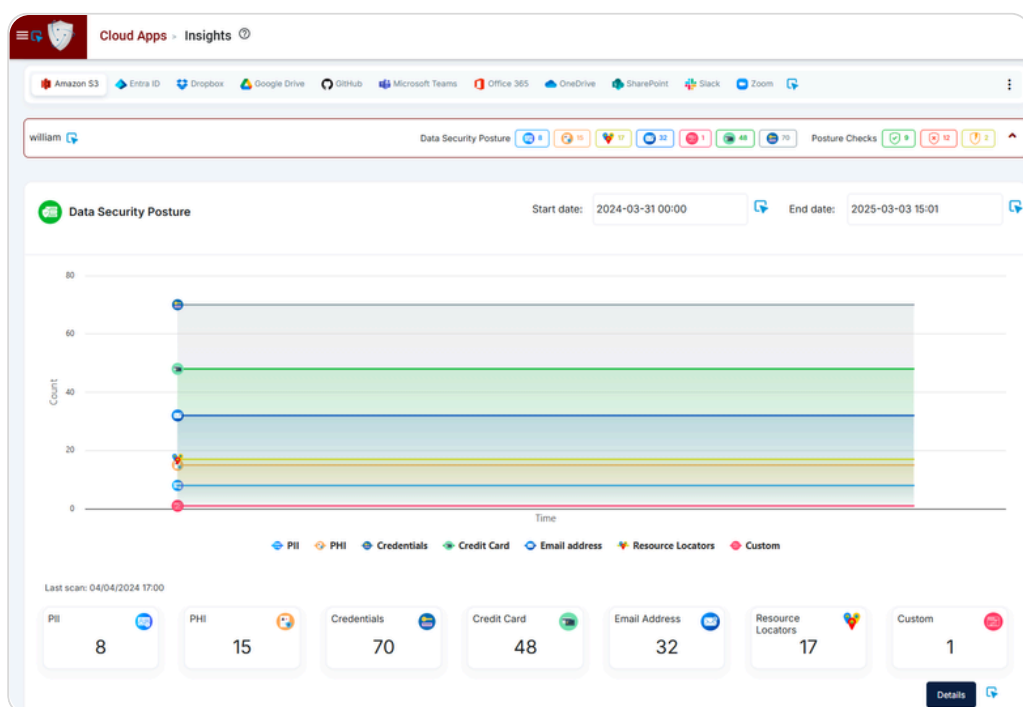
- Choose Account Type, create Account Name, and click Next.
  - Click the hyperlink *"Click to get the access code"* to get the access code from Amazon S3 by signing in with an admin account.
  - Enter the access code and click Next.
- Now select data collection frequency from the dropdown.
- Choose 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 Amazon S3 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

## Amazon S3 security scan and insights : visualizing your cloud app security posture with Cytex

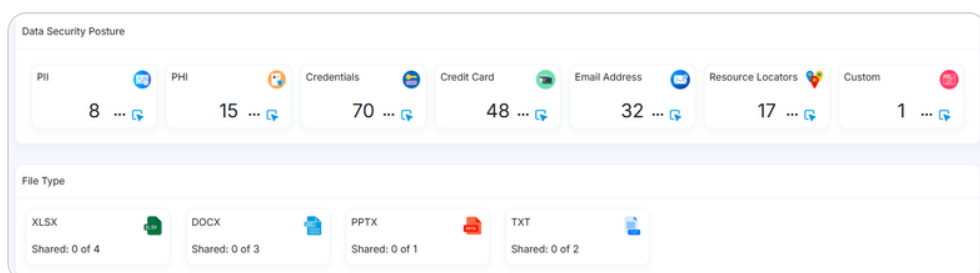
The Cytex Insights module offers both visual and numerical indicators to evaluate cloud application security and compliance. This ensures real-time monitoring and secure management of your Amazon S3 buckets and resources. It also includes App Posture Checks to quickly view pass, fail, and alarm statuses.

- In the Cytex main menu expand Cloud Apps, then click Insights.
- On the insights page select Amazon S3 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.

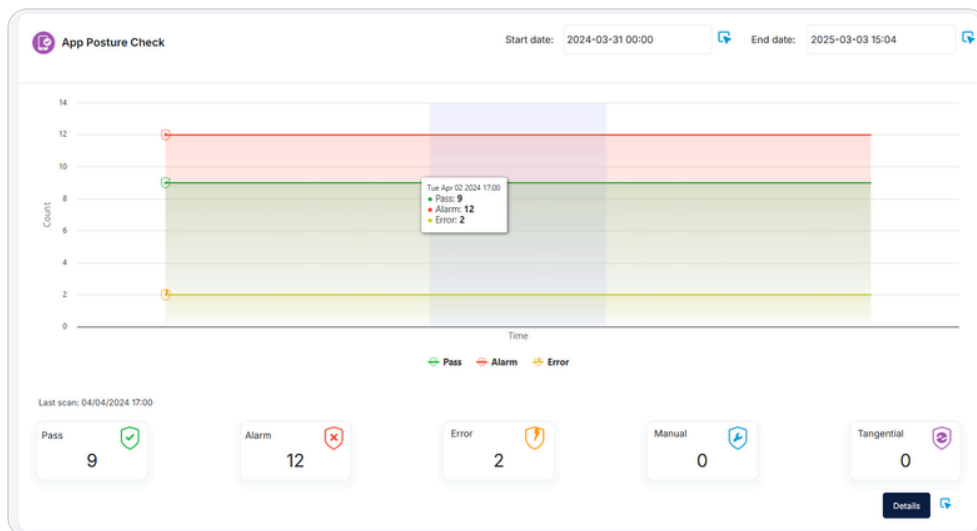
### 3 App posture check: Assessing your cloud app risk posture

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 Amazon S3 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 Amazon S3 security, as evaluated against security best practices.

Account name: william | Last updated: 04/04/2024 17:00 | Scanned results: 04/04/2024 17:00

**Best Practices Summary:**

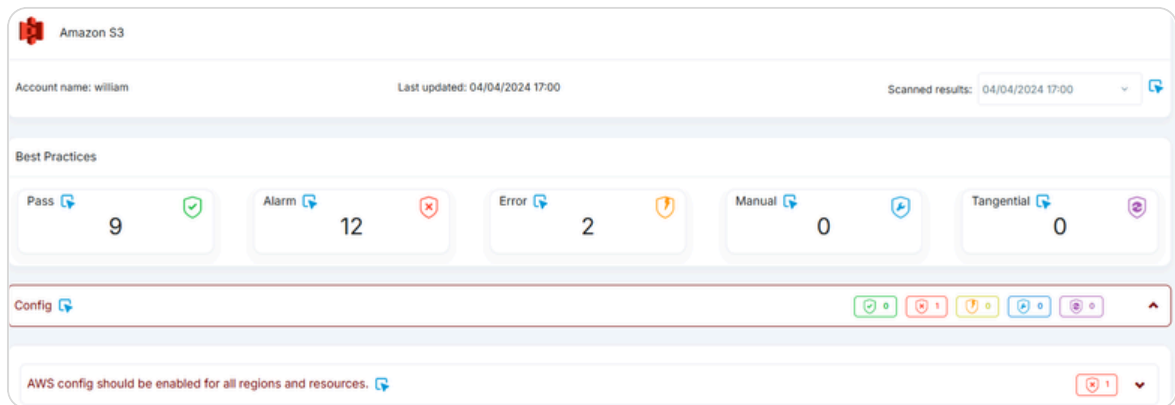
Status	Count
Pass	9
Alarm	12
Error	2
Manual	0
Tangential	0

**Category Breakdown:**

Category	Pass	Alarm	Error	Manual	Tangential
Config	0	1	0	0	0
GuardDuty	0	1	0	0	0
IAM	4	3	2	0	0
S3	5	7	0	0	0

## 4 Strengthening Amazon S3 Security Posture with Cytex: Your Action Plan

Following Cytex's evaluation, you'll find a customized action plan with best practices specifically for your Amazon S3 environment, highlighting the gaps. The comprehensive guidance empowers you to elevate your Amazon S3 security.



## 5 Cytex's Action Plan

### Identity Access Management (IAM) Policies:

- ▶ Multi-factor authentication (MFA) should be enabled for all users with a console password.
- ▶ IAM users should inherit permissions and policies from groups or roles.
- ▶ Active access IAM keys should be rotated at least every 90 days.
- ▶ Access keys and users who have been inactive for  $\geq 90$  days should be removed.
- ▶ IAM root user access key should exist.
- ▶ Hardware MFA should be enabled for the root user to sign in with root user credentials.
- ▶ Password policies for IAM users should use all the recommended configurations.
- ▶ Identity-based policies should not include '\*' for services in Allow statements that use the \* wildcard to grant permissions for all actions on any service.
- ▶ Ensure that administrative privileges should not be assigned to all users, the default version of IAM policies should not have the administrator access statement with 'Allow' with 'Action': over 'Resource': '\*'

### Security configurations:

- ▶ AWS config should be enabled for all regions and is recording all resources.

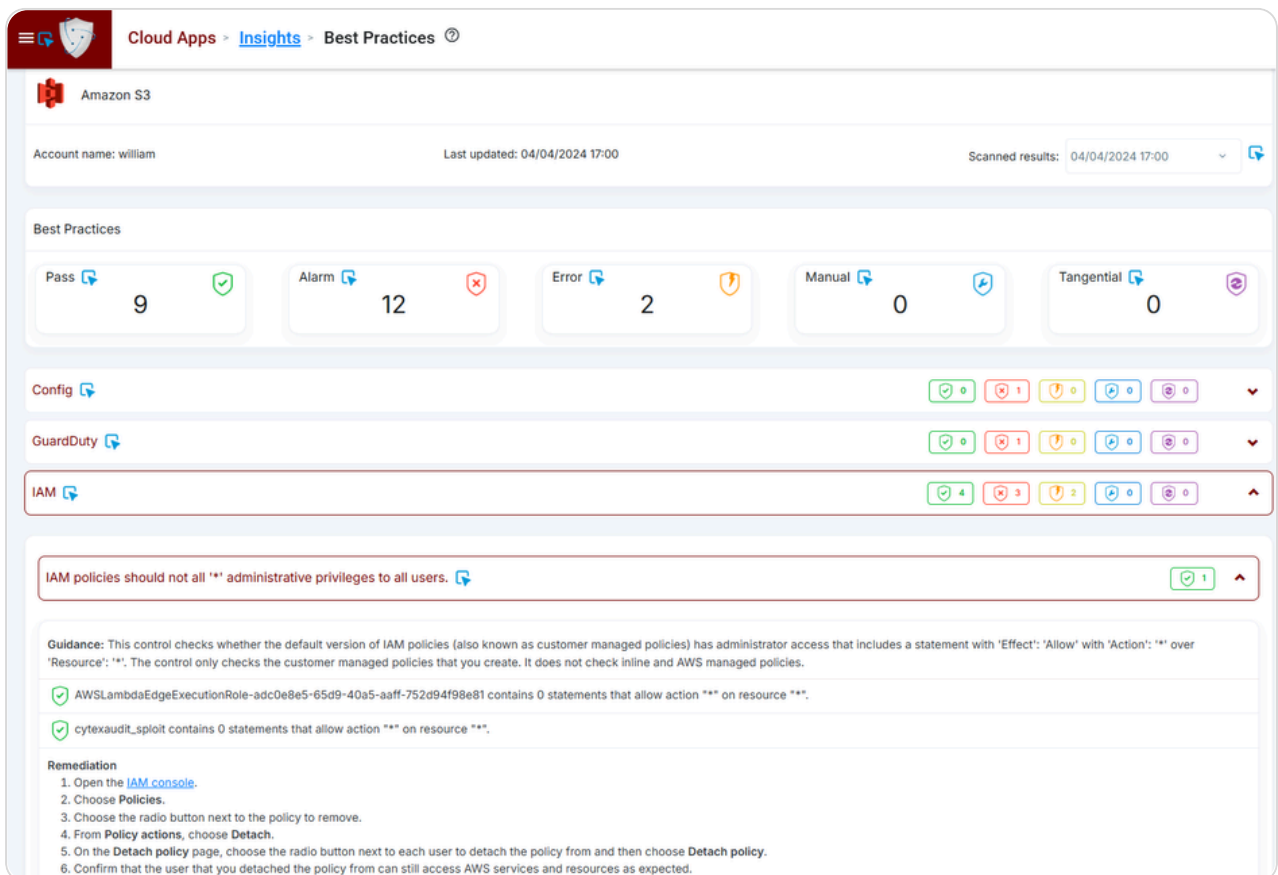
### S3 Bucket configurations and access settings:

- ▶ All the Amazon S3 public access settings should be configured.
- ▶ S3 buckets should block public access settings, the bucket policy, and the bucket access control list (ACL).
- ▶ S3 buckets should restrict public read, and write access.

## 5 Cytex's Action Plan

### S3 Bucket configurations and access settings:

- ▶ S3 buckets should have the default server-side encryption enabled.
- ▶ S3 buckets should require TLS, and have policies that require all requests to use Secure Socket Layer (SSL) and only accept transmission of data over HTTPS in the S3 resource policy, indicated by the condition key `AWS: SecureTransport`.
- ▶ S3 permissions should be restrictive and prevent other AWS accounts from performing denied actions on resources in the S3 bucket.
- ▶ S3 public access setting should have bucket-level public access blocks applied.
- ▶ S3 bucket server access logging should be enabled.
- ▶ S3 buckets with versioning should have lifecycle policies configured.
- ▶ S3 buckets should have event notifications enabled.
- ▶ S3 access control lists (ACL) should not be used to manage user access to buckets.



Cloud Apps > Insights > Best Practices

Amazon S3

Account name: william Last updated: 04/04/2024 17:00 Scanned results: 04/04/2024 17:00

Best Practices

Pass	9	Alarm	12	Error	2	Manual	0	Tangential	0
------	---	-------	----	-------	---	--------	---	------------	---

Config

GuardDuty

IAM

**IAM policies should not all "\*" administrative privileges to all users.**

Guidance: This control checks whether the default version of IAM policies (also known as customer managed policies) has administrator access that includes a statement with 'Effect': 'Allow' with 'Action': '\*' over 'Resource': '\*'. The control only checks the customer managed policies that you create. It does not check inline and AWS managed policies.

- ✓ AWSLambdaEdgeExecutionRole-adc0e8e5-65d9-40a5-aaff-752d94f98e81 contains 0 statements that allow action "\*" on resource "\*\*".
- ✓ cytexaudit\_spl0it contains 0 statements that allow action "\*" on resource "\*\*".

Remediation

1. Open the [IAM console](#).
2. Choose **Policies**.
3. Choose the radio button next to the policy to remove.
4. From **Policy actions**, choose **Detach**.
5. On the **Detach policy** page, choose the radio button next to each user to detach the policy from and then choose **Detach policy**.
6. Confirm that the user that you detached the policy from can still access AWS services and resources as expected.

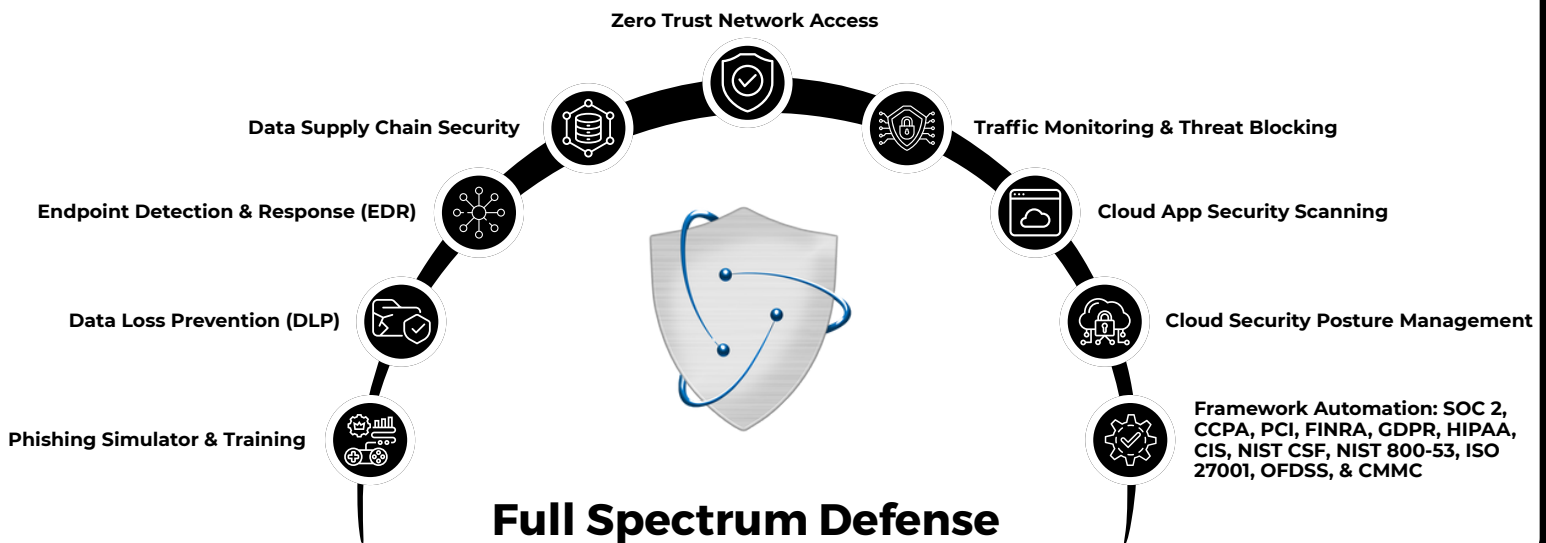
### Amazon Guard Duty:

- ▶ Amazon GuardDuty should be enabled for supported regions and accounts to track unauthorized or unusual activity.



# Explore **Cytex Unified Resilience Platform** today

[Schedule demo](#)



<https://cytex.io>



[hello@cytex.io](mailto:hello@cytex.io)



[@cytexsmb](#)



[@cytexsecure](#)