Standing Cloud Access Discovery and Onboarding

Name of Company: Wiz.io
Website: https://www.wiz.io/
Name of Product:
Version: V3.0
Date: January 2025

Table of Contents

1 SOLUTION OVERVIEW

The integration between Wiz and CyberArk empowers organizations to seamlessly detect and manage standing cloud user accounts, thereby enhancing access control and fortifying security measures while ensuring compliance in dynamic cloud environments. By harnessing Wiz's extensive cloud visibility and CyberArk's intelligent privilege controls, this integration automates the identification of unmanaged cloud user accounts, reducing deployment times for remediations, and enhancing user experience through streamlined onboarding processes. It represents a strategic move towards fostering a healthier, more secure cloud environment, poised to deliver tangible benefits and drive organizational success.

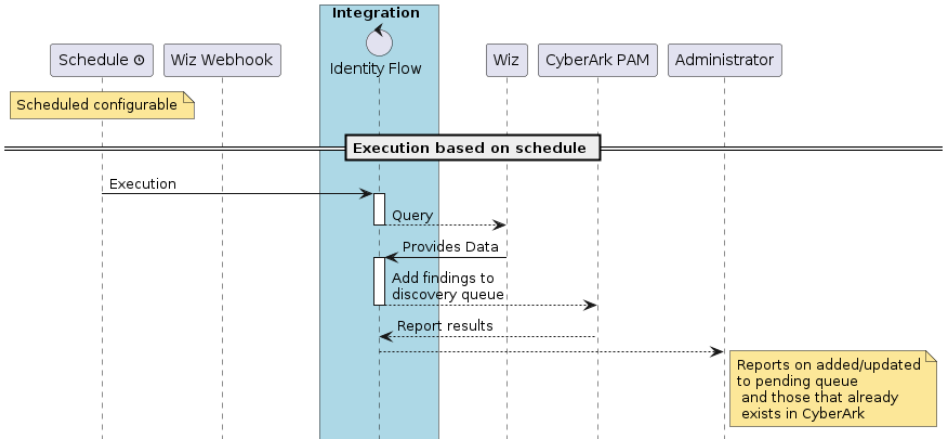
2 KEY BENEFITS

Enhanced Security: Proactively identify and manage standing cloud accounts through CyberArk's PAM solutions, significantly reducing the risk of unauthorized access, data breaches, and compliance violations.

Operational Efficiency: Streamline the account management process, minimizing manual effort, and eliminating the risk of human error associated with manual account identification and management.

Compliance Assurance: Meet stringent regulatory compliance requirements by effectively managing and monitoring privileged accounts in the cloud environment, demonstrating a commitment to data security and governance.

3 INTEGRATION DESCRIPTION AND DIAGRAM



The integration is planned to run in a predefined cadence, executed via a schedule.

Schedule: Set up the Identity Flow to run at regular intervals. We recommend on daily or weekly cadence. During each execution, it retrieves Issues from Wiz using the Wiz GraphQL for Issues marked as OPEN or IN PROGRESS. For every relevant Issue from supported cloud platforms, it uses Privilege Cloud's Account Discovery RestAPI to add them to a pending queue. The flow then notifies administrators with execution status of the discovered cloud users and the pending queue. Built-in functionality from CyberArk can be used to onboard the accounts.

Upon execution completion, an email will be sent with following information:

- Count of newly and previously discovered accounts
- Detailed information on discovered accounts that can be downloaded as CSV file.

Integration has 2 execution profiles to note:

- **First** run: Fetching All relevant Issues, therefore expected to run significantly longer than following runs
- **Subsequent** runs: Will fetch only the delta information from the last successful execution

4 REQUIREMENTS

- CyberArk Privilege Cloud on Shared Services
- Wiz.io

5 INSTALLATION

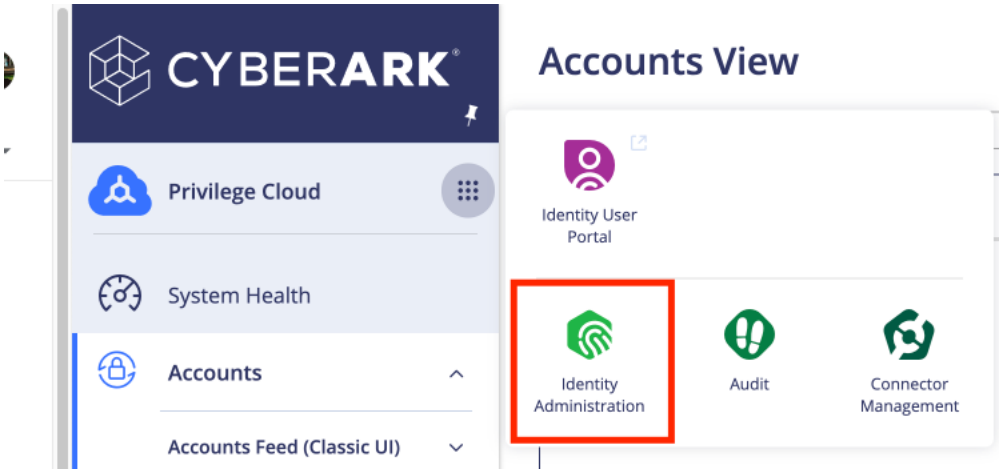
1. Go to the CyberArk Marketplace
2. Download the Standing Cloud Access Discovery and Onboarding Integration on the marketplace.
3. Store the file locally for later use.

6 CONFIGURATION

6.1 CyberArk Privilege Cloud Configuration

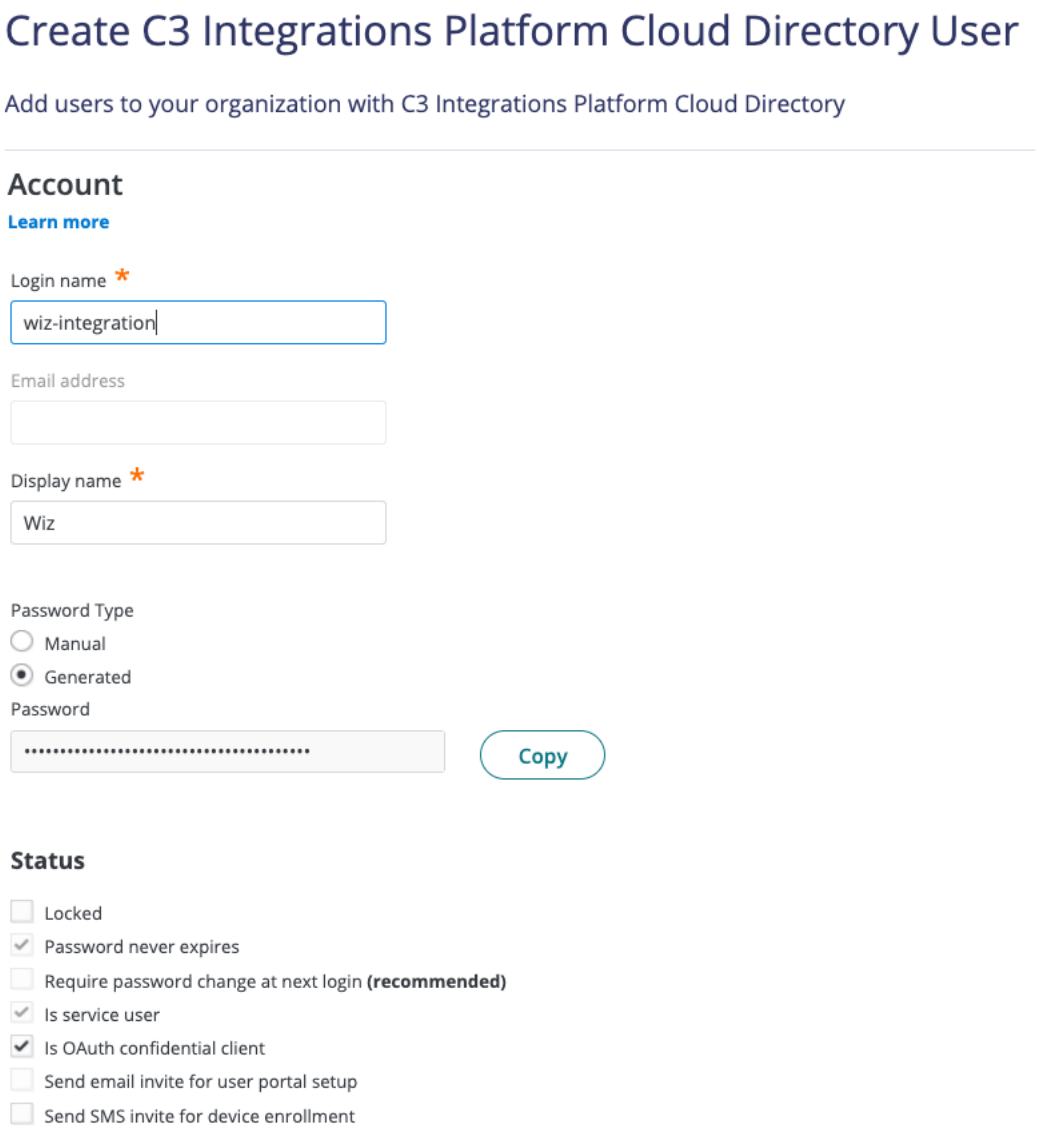
The Integration requires an OAuth service user for authentication to CyberArk Privilege Cloud.
Following are the steps to create a new OAuth service user in CyberArk Identity.

1. Log into CyberArk Identity Security Platform Shared Services (ISPSS) with a user that has permissions to manage users in CyberArk Identity.
2. From the service picker, choose **Identity Administration**.



3. In the left-hand menu, expand **Core Services**, click on **Users**.
4. In the Users screen, click the **Add User** button.
5. Fill in the required fields for:
    a. Login name.
    b. Display name.
    c. Password + Confirm password.
        i. Make sure to remember the password.

6. Under **Status** mark the checkbox next to **Is OAuth confidential client**.
7. Click the **Create User** button.



8. Assign the new user to the Privilege Cloud Discovery Source role:
    a. In the left-hand menu, click on **Roles**.
    b. Find the **Privilege Cloud Discovery Source** role and click on it.
    c. Navigate to the **Members** tab.
    d. Click the **Add** button.
    e. Search for the new service user, select it, and click on **Add**.
    f. Click **Save**.

6.2 CyberArk Identity Flows Configuration

1. Import the Flow into CyberArk Identity Flows
    a. Login to the CyberArk Identity Security Platform with a user that has permissions to access Identity Flows.
    b. Go to Identity Administration.
    c. Within Identity Administration, open Flows.
    d. Click “import”, “Import from Computer" and select the JSON files that was downloaded:
        i. Wiz-OnboardUsers-V3.json
        ii. Wiz-OnboardUsers-Report-V3.json
2. Configure the Authorization for Privilege Cloud
    a. Open Settings at the bottom-left corner.
    b. Click Authorization and select New Authorizations.
    c. Configure the following parameters:
        i. Type: OAuth2
        ii. Flow: Client Credentials
        iii. Content Type: application/x-www-urlencoded
        iv. ClientID: {Username that was configured in Privilege Cloud e.g. wiz-integration}
        v. Client Secrets: {Generated Password}
        vi. Token URL: {https://[Identity Tenant ID].id.cyberark.cloud/oauth2/platformtoken }
    d. Click Authorize and Save.
3. Configure the Authorization for Wiz API (The Service Account can be created according to step 6.4)
    a. Open Settings at the bottom-left corner.
    b. Click Authorization and select New Authorizations.
    c. Configure the following parameters:
        i. Type: OAuth2
        ii. Flow: Client Credentials
        iii. Content Type: application/x-www-urlencoded
        iv. ClientID: {Username that was configured in Wiz for the service account to access Wiz API}
        v. Client Secrets: {Generated Password}
        vi. Token URL: https://auth.app.wiz.io/oauth/token
        vii. Audience: wiz-api
        viii. Add a scope with read:issues
    d. Click Authorize and Save.
4. Configure Custom Variables for the Flow:

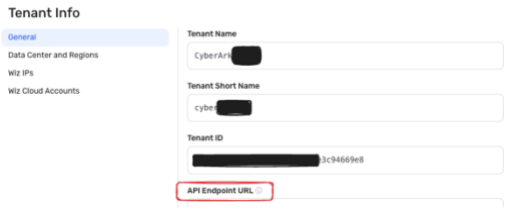
a. *email-recipients:* Comma-separated list of email addresses to receive reports/results of Wiz findings and CyberArk PAM discovery account statuses.

b. *email-subject:* Subject line for the email sent by the integration. Default value: "Cloud Access Discovery Report: Insights and Recommendations".

c. *report*-key: a GUID string token of your choosing to be used as apiKey in Report-Data-File flow.

d. *wizapihostname:* i.e. api.us17.app.wiz.io. Can be found in Tenant Info section in on Wiz Platform

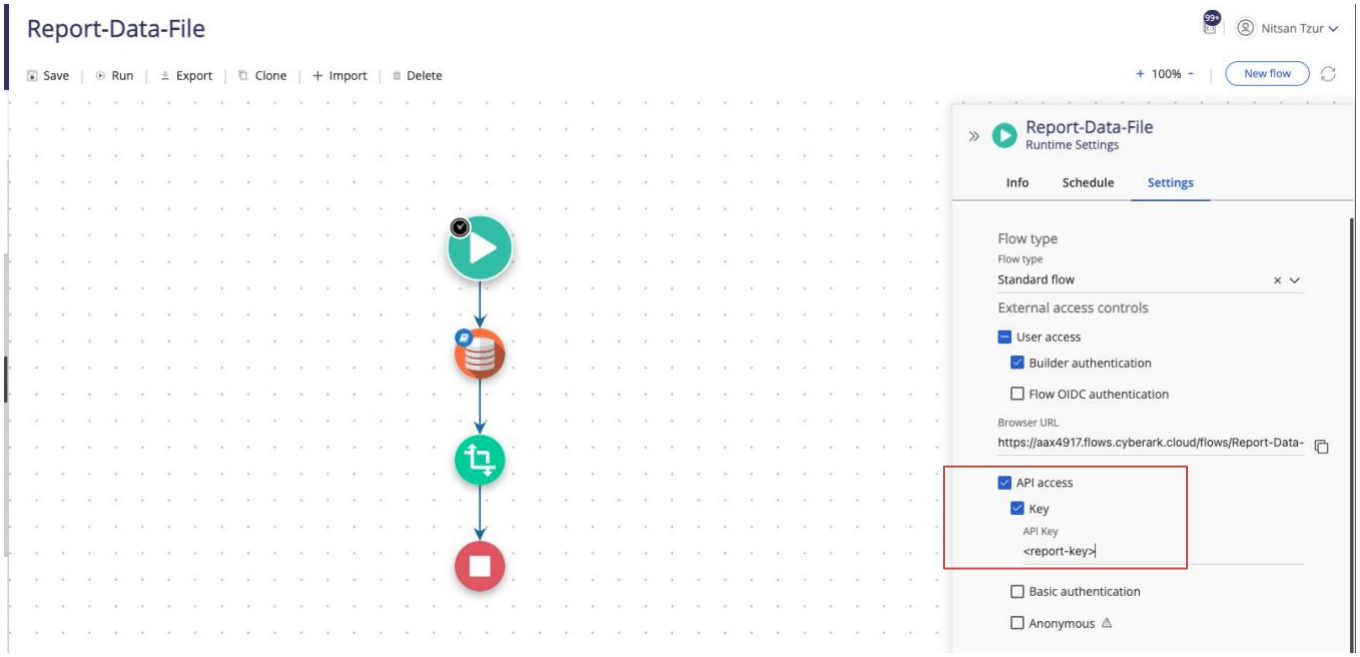
e. *pcloudtenant:* your CyberArk tenant name



5. For the 2 nodes with the CyberArk logo and labeled “Discovered Accounts Add Discovered”, in the Settings > Authorizations, select the authorization for Privileged Cloud created in step 2 above.

6. For the 2 nodes with the Wiz logo and labeled “Graphql”, in the Settings > Authorization, select the authorization for Wiz API created in step 3 above.

7. Open Report-Data-File flow and in the top node navigate to **Settings** tab. Check **API Access** and in **API Key** insert the **Custom Variable** value defined in 4c



8. To test the integration, Save the Flow at the top, and click Run.

6.3 Configure the integration in Wiz

Configure the integration within Wiz

1. Login to the Wiz portal
2. Navigate to **Settings, Integrations.**
3. Click **Add Integration** and select **CyberArk.**
4. Paste the **Flow URL** that we copied earlier from CyberArk Identity Flows.
5. Select **Basic Authentication**

6. **Paste the username/password** that you've created within Identity Flows in the previous step.
7. Click **Add Integration.**
8. Copy the **Service Accounts Credentials.**

7 DATA FETCHING CRITERIA

7.1 Default Standing Cloud Access Filtering

Issues are the risks that Wiz has identified in the cloud environment, as defined by Controls, according to their severity. By default, the integration uses the “Pull Issues” query to retrieve high-risk cloud user access from Wiz. Query example:

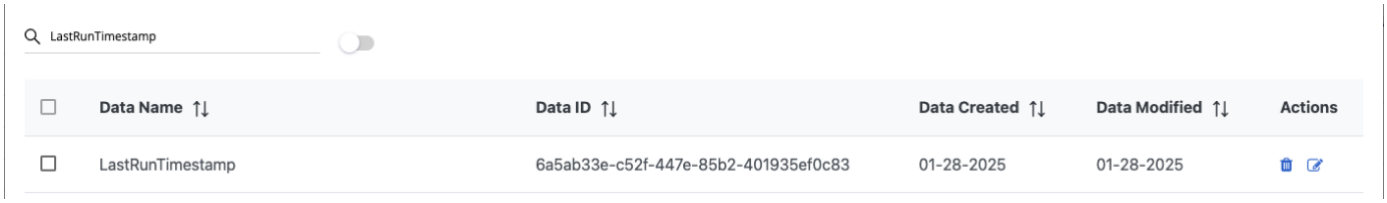
```
{
 "first" : 500,
 "filterBy" : {
  "status" : [
   "OPEN",
   "IN_PROGRESS"
  ],
  "relatedEntity" : {
   "type" : [
    "USER_ACCOUNT"
   ],
   "cloudPlatform" : [
    "AWS",
    "Azure",
    "GCP"
   ],
            "frameworkCategory" : [
    "wf-id-165"
   ]

  },
 "orderBy" : {
  "field" : "STATUS_CHANGED_AT",
  "direction" : "ASC"
 }
}
}
```

These criteria will pull issues currently OPEN or IN_PROGRESS for “USER_ACCOUNT” related entities for the following Cloud Platforms: AWS, Azure, or GCP. We are limiting the fetched Issues to framework: “Wiz for CIEM” to focus on the most relevant records.

7.2 Last run watermark

By default, after the first run, only delta of newly created issues will be fetched. To override this behavior, clear the last run data store On Identity Flows left hand panel, navigate to Data section.

1. Click on **Manage** and type**: LastRunTimesptamp** in search text



2. Click on pencil icon to edit Datastore value. Change value to **YYYY-MM-DDTHH:MM:SSZ** date/time format or delete entire the Datastore to force all data rerun on next execution cycle

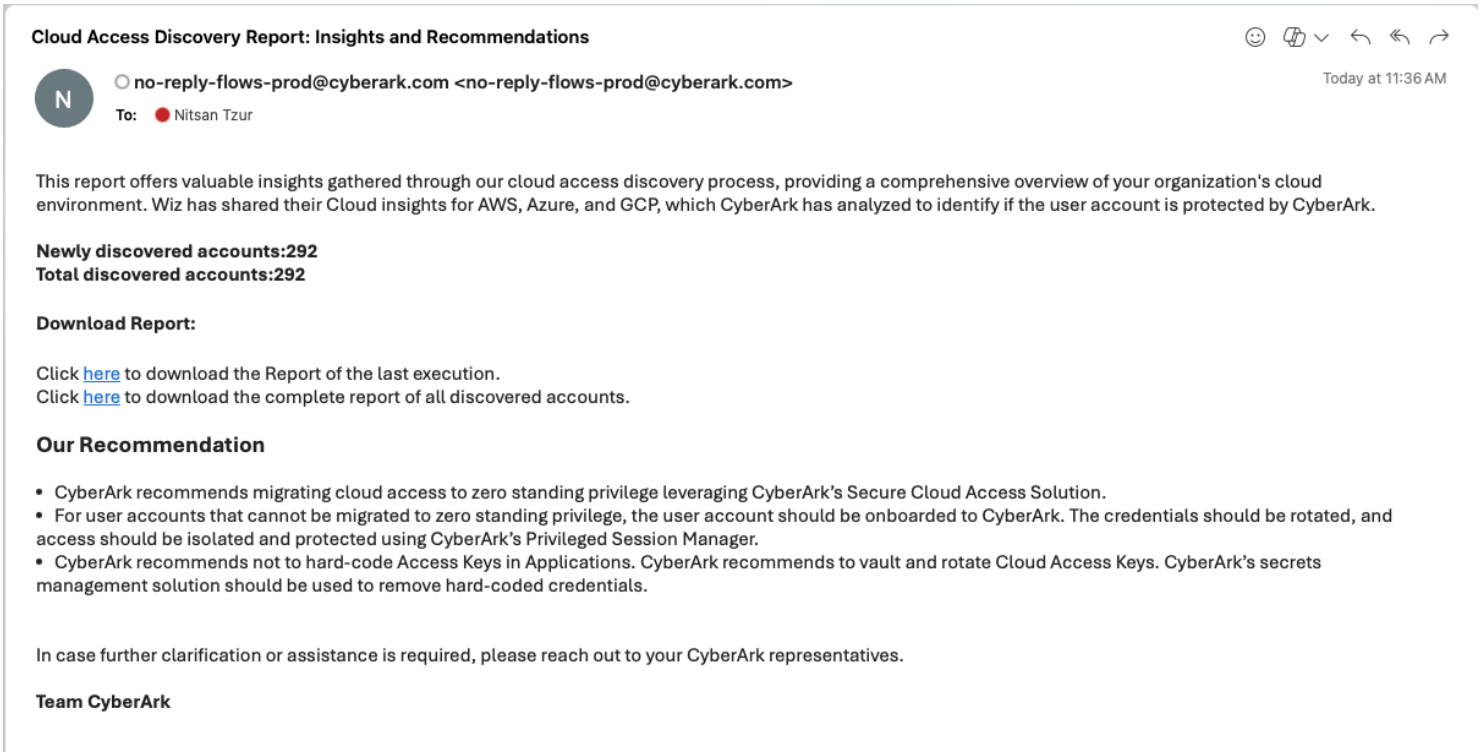
8 HOW TO USE THE INTEGRATION

By running the Integration, the discovered accounts will be stored in a persistent data stores within Identity Flows. There 2 types of reports saved:

a. Full report of all accumulated discovered accounts

b. Report for the last run – the incremental discovered accounts from latest execution

Those two reports are available to download in CSV format upon execution completion. A notification email will be sent once reports are ready. Links to download reports are embedded in the email. Example of such email presented below:



Cloud Access Discovery Report: Insights and Recommendations

N

no-reply-flows-prod@cyberark.com <no-reply-flows-prod@cyberark.com>

Today at 11:36 AM

To: Nitsan Tzur

This report offers valuable insights gathered through our cloud access discovery process, providing a comprehensive overview of your organization's cloud environment. Wiz has shared their Cloud insights for AWS, Azure, and GCP, which CyberArk has analyzed to identify if the user account is protected by CyberArk.

Newly discovered accounts:292
Total discovered accounts:292

Download Report:

Click here to download the Report of the last execution.
Click here to download the complete report of all discovered accounts.

Our Recommendation

- CyberArk recommends migrating cloud access to zero standing privilege leveraging CyberArk's Secure Cloud Access Solution.
- For user accounts that cannot be migrated to zero standing privilege, the user account should be onboarded to CyberArk. The credentials should be rotated, and access should be isolated and protected using CyberArk's Privileged Session Manager.
- CyberArk recommends not to hard-code Access Keys in Applications. CyberArk recommends to vault and rotate Cloud Access Keys. CyberArk's secrets management solution should be used to remove hard-coded credentials.

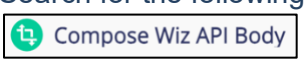
In case further clarification or assistance is required, please reach out to your CyberArk representatives.

Team CyberArk

9 TROUBLESHOOTING

What if you face an error fetching Issues from Wiz

1. Validate proper input compose on Data Transformation node named: “Compose Wiz API Body”
    - Open the Wiz Onboading Flow in Identity Flows.
    - Search for the following Node, it can be found above the first node with the Wiz Logo.



2. Verify that the response from the Wiz GraphSQL node is as expected.
    - Navigate to Identity Flows, Logs
    - Open the last executed flow, Search for the GraphQL Node
    - Search for unexpected data formats or any error messages.

How to rerun the discovery scan on all cloud accounts

1. By default, only newly created issues are fetched after the first run. To fetch all issues again, clear the last run data store:
    - Navigate to the Data Section on the Identity Flows left-hand panel.
    - Click on Manage and type “LastRunTimestamp” in the search text.
    - Clock on the pencil icon to edit the Datastore value. Change the value to the desired date/time format (YYYY—MM-DDTHH:SSZ) or delete the entire datastore to force a full data rerun on the next execution cycle.

10 PARTNER CONTACT INFO

Business Contact	Name	Joanne Wu
	Email	Joanne.wu@cyberark.com
Support Contact	Name	Business Development Technology
	Email	bizdevtech@cyberark.com