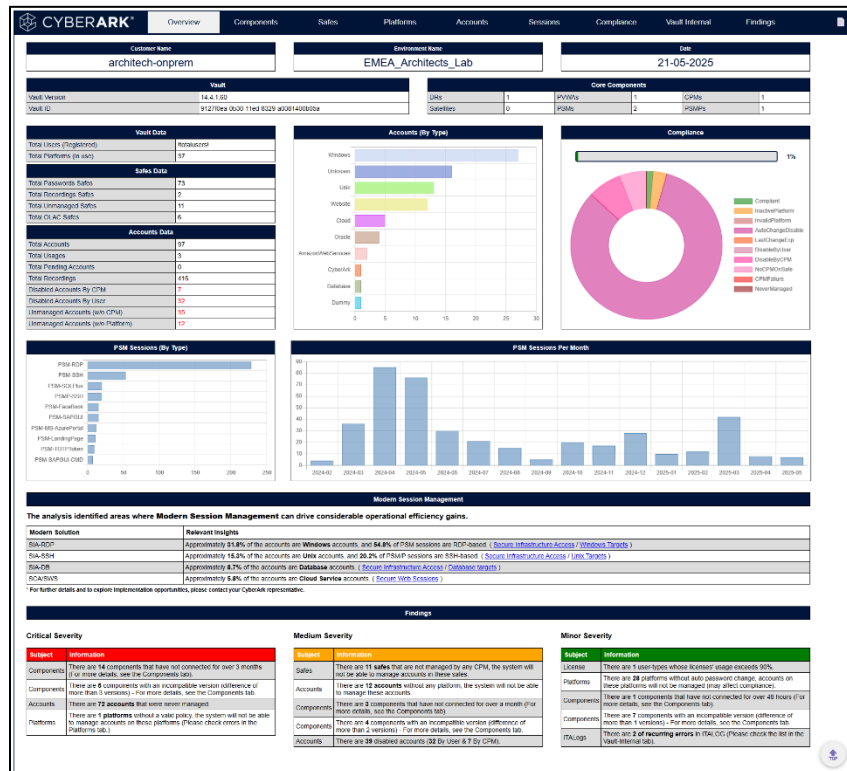


CyberArk Vault Analysis Tool

Introduction

The CyberArk Vault Analysis Tool (VAT) helps you assess the health of your CyberArk Self-Hosted or Privilege Cloud environment, and if you're preparing for or evaluating a PAM Self-Hosted Upgrade or a migration from PAM Self-Hosted to SaaS, it can help with planning.

Running this tool provides a detailed report on your vault's operational status, supporting ongoing health checks, migrations, and best-practice alignment.



Prerequisites

Before you begin, ensure you have:

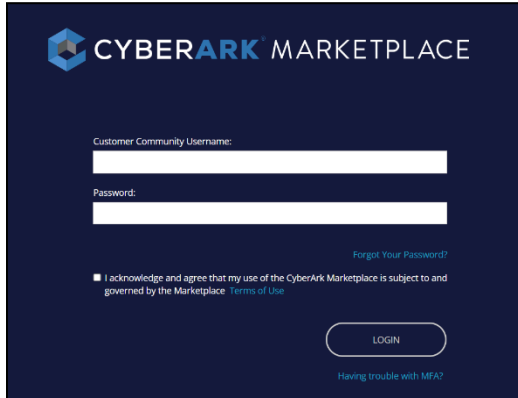
- Access to the CyberArk Community Portal (Advanced or Admin level)
- A system with network access to the Vault on port 1858
- The ability to send and receive files (for tool download and data upload)
- For PAM Self-Hosted:
 - Vault administrator credentials (must be a Vault user, not LDAP/external)
 - o Running the collector on a component server, such as PVWA or CPM, ensures it has the required access
- For Privilege Cloud:
 - o (Shared Services) The ability to activate and reset the password for the “installeruser”
 - o (Standard) The credentials for your “subdomain_admin” user
 - o Running the collector on a Privilege Cloud Connector server ensures it has the required access

Collecting Data

The first step is to run the Vault Analysis Tool Collector to collect data about your environment. Later, this will be submitted to CyberArk for analysis.

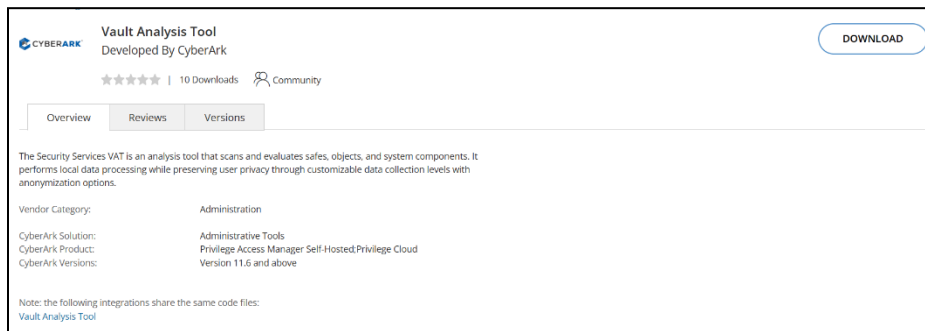
Download the Collector

1. Go to the CyberArk Marketplace and **log in** with your CyberArk Community account.



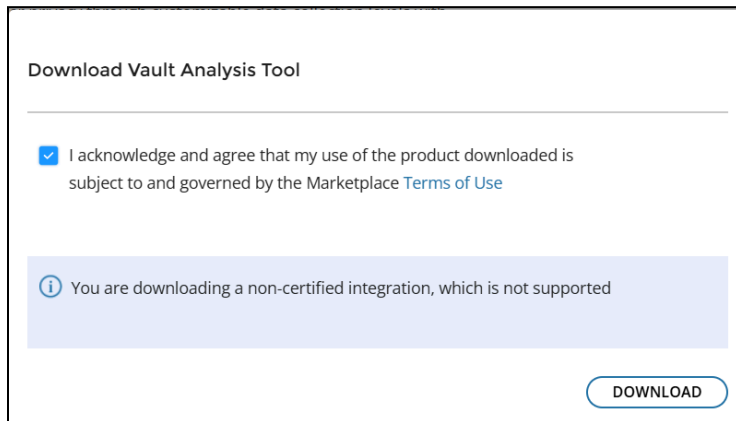
The image shows the CyberArk Marketplace login page. It has a dark blue background with the CyberArk logo and 'MARKETPLACE' text at the top. Below the logo are two input fields for 'Customer Community Username' and 'Password'. There is a 'Forgot Your Password?' link next to the password field. Below the input fields is a checkbox with the text 'I acknowledge and agree that my use of the CyberArk Marketplace is subject to and governed by the Marketplace Terms of Use'. A 'LOGIN' button is at the bottom right, and a link 'Having trouble with MFA?' is at the bottom center.

2. A link to the marketplace listing will be provided by a CyberArk representative.



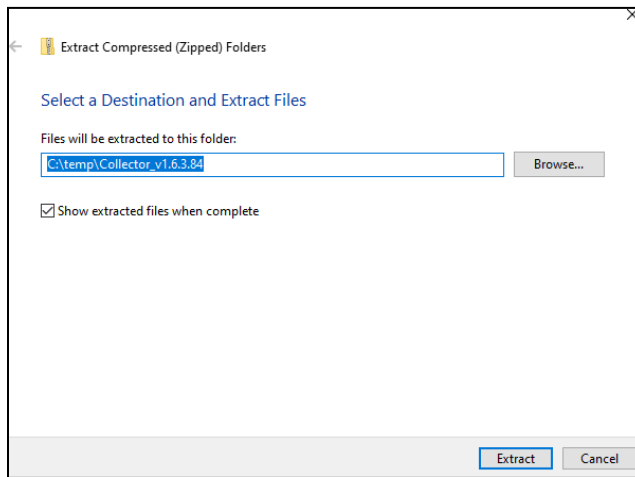
The image shows the marketplace listing for the 'Vault Analysis Tool'. It includes the CyberArk logo, the product name 'Vault Analysis Tool', and 'Developed By CyberArk'. There is a 'DOWNLOAD' button in the top right corner. Below the product name are five stars and '10 Downloads'. There are tabs for 'Overview', 'Reviews', and 'Versions'. The 'Overview' tab is selected. The description states: 'The Security Services VAT is an analysis tool that scans and evaluates safes, objects, and system components. It performs local data processing while preserving user privacy through customizable data collection levels with anonymization options.' Below the description is a table with two columns: 'Vendor Category' and 'Administration'. The table contains the following information: 'CyberArk Solution: Administrative Tools', 'CyberArk Product: Privilege Access Manager Self-Hosted Privilege Cloud', and 'CyberArk Versions: Version 11.6 and above'. At the bottom, there is a note: 'Note: the following integrations share the same code files: Vault Analysis Tool'.

3. Download the Vault Analysis Tool Collector.



The image shows the 'Download Vault Analysis Tool' confirmation page. It has a title 'Download Vault Analysis Tool' at the top. Below the title is a checkbox with a checkmark and the text 'I acknowledge and agree that my use of the product downloaded is subject to and governed by the Marketplace Terms of Use'. Below this is a light blue box with an information icon and the text 'You are downloading a non-certified integration, which is not supported'. At the bottom right is a 'DOWNLOAD' button.

4. Extract the downloaded ZIP file to your chosen location.



Execute the Collector

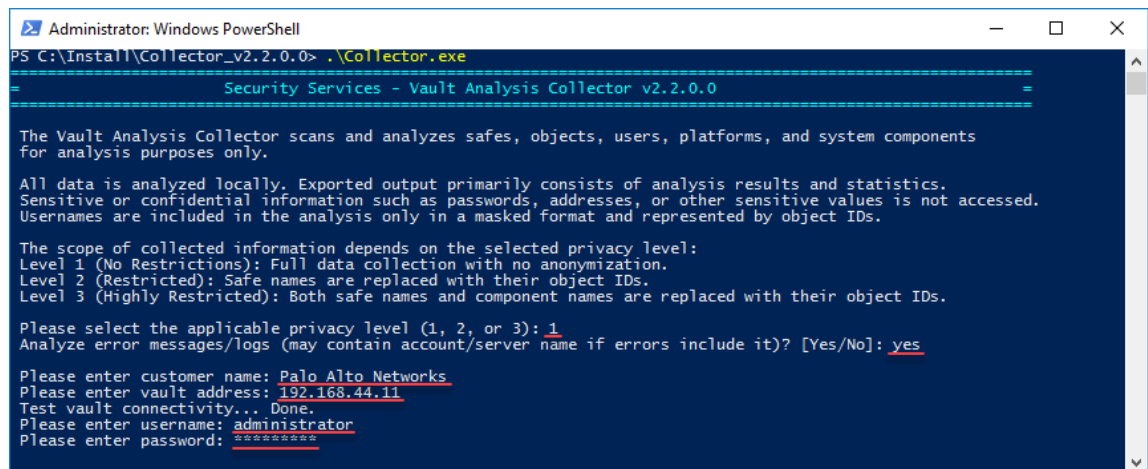
1. Run Collector.exe

Name	Date modified	Type	Size
Logs	10/16/2025 10:01 AM	File folder	
Temp	10/16/2025 6:01 AM	File folder	
calibey64102u-2013.dll	10/16/2025 3:51 AM	Application exten...	2,265 KB
cassley64102u-2013.dll	10/16/2025 3:51 AM	Application exten...	346 KB
Collector	10/16/2025 9:56 AM	Application	195 KB
CyberArk.Casos.dll	10/16/2025 3:51 AM	Application exten...	15,322 KB
CyberArk.Services.Exceptions.dll	10/16/2025 3:51 AM	Application exten...	159 KB
icudt58l.dat	10/16/2025 3:51 AM	DAT File	25,598 KB
msvc120.dll	10/16/2025 3:51 AM	Application exten...	645 KB
msvc120.dll	10/16/2025 3:51 AM	Application exten...	942 KB
ReadME	10/16/2025 3:51 AM	Text Document	1 KB

2. When prompted, enter the following details:

Field	Value/Description
Privacy level*	Level 1 (No Restrictions): Obfuscate usernames. Level 2 (Restricted): Also obfuscate safe names. Level 3 (Highly Restricted): Also obfuscate component names.
Analyze error messages	Recommended
Customer name	Your company name
Vault address	Your vault address <i>For ISPSS environments only: Vault address is vault-{tenant-id}.privilegecloud.cyberark.cloud</i>
Username	Vault administrator user (e.g. Administrator, installeruser or subdomain_admin depending on environment type)
Password	Password for the vault administrator user

**CyberArk recommends privacy level 1 for most situations.*



```
Administrator: Windows PowerShell
PS C:\Install\Collector_v2.2.0.0> .\Collector.exe

=====
Security Services - Vault Analysis Collector v2.2.0.0
=====

The Vault Analysis Collector scans and analyzes safes, objects, users, platforms, and system components
for analysis purposes only.

All data is analyzed locally. Exported output primarily consists of analysis results and statistics.
Sensitive or confidential information such as passwords, addresses, or other sensitive values is not accessed.
Usernames are included in the analysis only in a masked format and represented by object IDs.

The scope of collected information depends on the selected privacy level:
Level 1 (No Restrictions): Full data collection with no anonymization.
Level 2 (Restricted): Safe names are replaced with their object IDs.
Level 3 (Highly Restricted): Both safe names and component names are replaced with their object IDs.

Please select the applicable privacy level (1, 2, or 3): 1
Analyze error messages/logs (may contain account/server name if errors include it)? [Yes/No]: yes

Please enter customer name: Palo Alto Networks
Please enter vault address: 192.168.44.11
Test vault connectivity... Done.
Please enter username: administrator
Please enter password: *****
```

3. Allow the collector to run. It will:
 - Log in to the vault as the administrator
 - Create a temporary user and add it to the Auditors group
 - Collect and encrypt the required data
 - Remove the temporary user
4. When the collector is complete it will report “Vault scan completed successfully.”
5. Note the name of the output file reported by the collector. You will use it in the next step.

Submit Data for Analysis

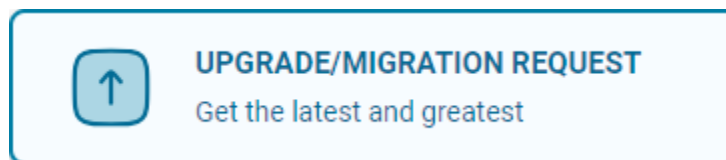
The submission process varies depending on the purpose of the report. If you are planning or considering a migration to PAM SaaS, follow the steps in the PAM SaaS Migration Planning section. Otherwise, follow the “Health Check” section.

You will receive a copy of the report in both cases.

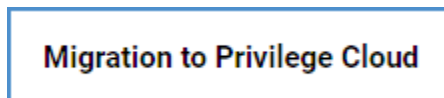
PAM SaaS Migration Planning

Submit the Data on the Migration Planning Portal

1. Log on to the CyberArk Community Portal (<https://community.cyberark.com>).
2. Navigate to the *Services Hub*, either by clicking on the Services Hub tile, or by using the Services Hub link at the top of the site.
3. In the *Create Requests and Review Cases* section, click on *Upgrade/Migration Request*.



4. Click on the *Migration to Privilege Cloud* button.



5. Upload the output file created by the Collector, and answer the questions in the form.
6. Submit the form.

What Happens Next?

Once the file has been processed, your Account Executive will contact you to review the results and discuss next steps.

Health Checks and Other Purposes

Upload the Collected Data for Processing

1. Log on to the CyberArk Community Portal (<https://community.cyberark.com>).
2. Navigate to *My Company Files*
3. Upload the VA_Report-*.vhc_ file.
 - For **File Classification**, select “Log.”
 - In **Description**, enter “Vault Analysis Data.”
4. Notify your CyberArk representative when the file is uploaded
5. Your CyberArk representative will notify you when the report is available for download.

Additional Notes

- The Vault Analysis Tool supports both Self-Hosted and Privilege Cloud environments.
- Scan time is typically 5–15 minutes and can vary for larger environments with many safes & accounts.
- The tool provides actionable insights and prioritizes findings for remediation.