International Journal of Leading Research Publication (IJLRP)
E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

The Benefits of Cyberark PAM (Privileged Access Management) Solution and How to Use It

Seema Kalwani

Independent contributor, IL, USA
seemakalwani@gmail.com

Abstract
The article provides CyberArk overview covering different job profiles in an organization, security threat and how employees can fall victim to the breach. How CyberArk Implementation can mitigate the threat and provide benefits to connect multiple servers by only entering credentials once in CyberArk. Connection to target servers is available via check-in/check-out password or through direct connect to the server from CyberArk. Feature of dual control is discussed to enforce two or more people being involved in the decision making for use of password. Native tools that users are comfortable using are also available to configure making it easier to connect without sacrificing security.

Keywords: PAM, CyberArk, Identity and Access Management, exclusive access, dual control

INTRODUCTION TO CYBERARK

CyberArk's Privileged Access Manager (PAM) is a full-lifecycle solution for managing the most privileged accounts and SSH Keys in the enterprise. It enables organizations to secure, provision, manage, control, and monitor all activities associated with all types of privileged identities. Looking at different aspects of CyberArk from end user perspective.

1. View and connect with privilege accounts
2. Connect to targets when check-out/check-in exclusive access is enforced
3. Connect to targets when dual control is enforced.
4. Connect to targets using native tools

As an end user one is required to log in and interact with different systems and software. One must provide and remember multiple passwords. In many cases the systems one logs in holds privilege information such as customer information or company information. When one has access to privilege information it makes one privilege user and unfortunately a prime target for attackers. Usually, the attacker goes behind the credential of a privilege user as that is what they need to access the IT infrastructure. Over the years companies have asked their privileged users to come up with strong passwords and to keep those passwords confidential. However, this is insufficient as it is hard for most of us to memorize complex passwords. And attackers these days can crack any password. This is where the PAM solutions can help. CyberArk provides Single Sign-on capabilities to all privileged applications, now one needs to memorize only one password, and it will connect one securely to the system that one needs. CyberArk also provides secured workflows against cyberattacks by validating the identity of the user using multi-factor authentication and limiting and monitoring access to sensitive data.

CONNECTING TO A SYSTEM USING CYBERARK SOLUTION – REVIEWING DIFFERENT JOB PROFILE IN AN ORGANIZATION

A. Windows administrator (WA)

An extremely qualified windows administrator knows the importance of security because he has access to so many critical systems. To be secure from bad actors one needs to be vigilant. Using complex, unique passwords for all the systems being accessed is important and routinely getting those passwords rotated is part of security policy. Memorizing complex passwords and changing them on a regular basis makes life tough. One may know the threat and take it upon oneself to do all that is needed to make the organization safe.

B. Developer

A developer needs to access explore different systems as part of their learning journey and finding solutions to the programming problems. They don't have access to any production system and may not be victims of a breach. There is a need for the role for accessing multiple online forums to share knowledge and ideas with many fellow developers.

C. Threat

A developer clicks on a link received in an email from an online forum not fully reviewing the message. By doing so, malware was introduced to the system. The malware harvests credentials sitting on the system including those of a desktop administrator who helped the developer to install a new printer driver. Using the stolen desktop administrator credential the malware spreads to many other workstations including a windows administrator (WA). The malware installs a key-logger on WA's system and captures the credential while he is doing his work. Suddenly several critical systems are vandalized using WA's credentials. WA who is ever careful is upset for being the victim of a breach. Because it is WA's credentials that were used management is looking at him for answers. In-spite of doing nothing wrong, the WA managed to become a victim. The developer had no ill intentions either. This can happen to any one of us in our day-to-day activities.

D. Solution

CyberArk Privilege Access Manager can be a solution to prevent such attacks. How will the day-to-day activities of Windows Administrator and the developer be different after the implementation of CyberArk PAM? May be layers of security and slow things down. Here are the benefits:

1. No longer need to remember long and complex passwords
2. Changing passwords is easy and can be done more often
3. Prevents one from being a victim of social engineering, one cannot reveal the password one does not know.

VIEW AND CONNECT WITH PRIVILEGE ACCOUNTS

A. Web Portal Access

Login with permissions to view and connect to the accounts.

Fig. 1. Login screen taken from CyberArk training module – Overview of CyberArk and How to use it.

B. Account View

User will see a list of all the accounts that he is authorized to access. Filters can be used to view the specific accounts. Users can see the recently used accounts by clicking on "Recently Used" button. The star icon in front of each account can be used to mark the favorites and click on the "Favorites" link to view all favorites. The filter section can be minimized and expanded by clicking on the 3 lines next to the "filter".

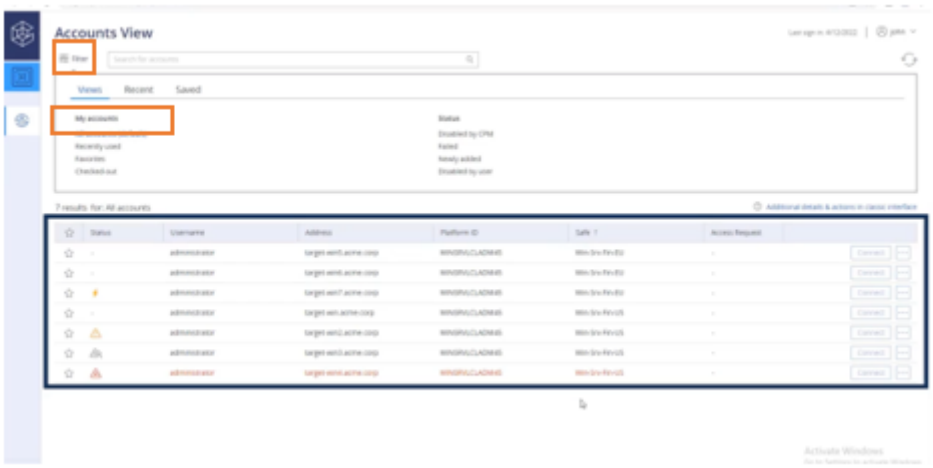

Fig. 2. Account View taken from CyberArk training module – Overview of CyberArk and How to use it.

C. Attributes in Account View

- Checked-out – Clicking on the link allows the user to view all accounts that
- Disabled by user – Clicking on the link allows the user to see all accounts which the user has manually disabled and opted out of password management.
- Disabled by CPM (Credential Privilege Manager) – Clicking on the link allows user to see all accounts that have been disabled by CPM and no longer being automatically managed.
- Failed – A list of accounts that could not be managed successfully by the CPM resulting in an error
- Newly Added – A list of newly added accounts in PAM

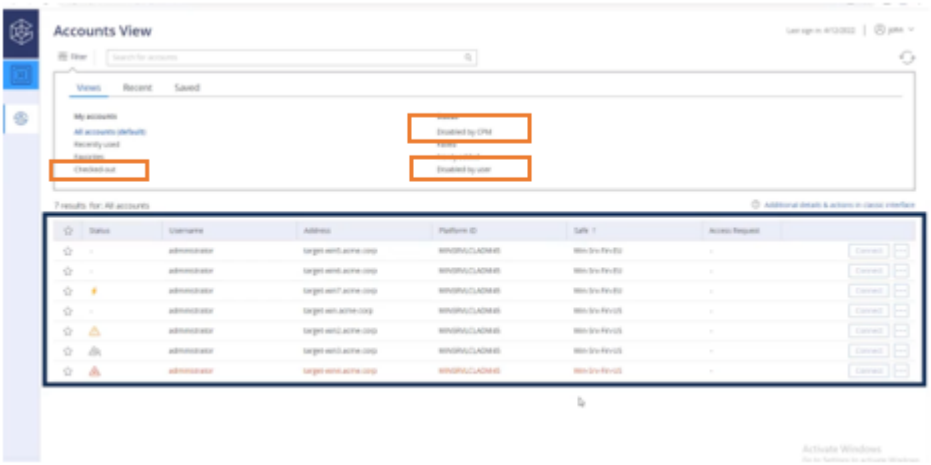

Fig. 3. Account View taken from CyberArk training module – Overview of CyberArk and How to use it.

D. Connect to Target

Click connect to securely connect to the target machine without being asked for a password. The connection to a windows box and multiple such boxes is established on a click from CyberArk.

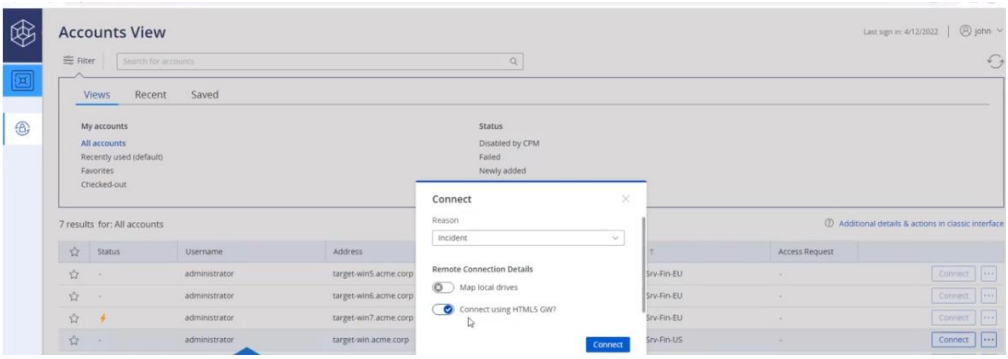

Fig. 4. Connect to target dialogue box taken from CyberArk training module – Overview of CyberArk and How to use it.

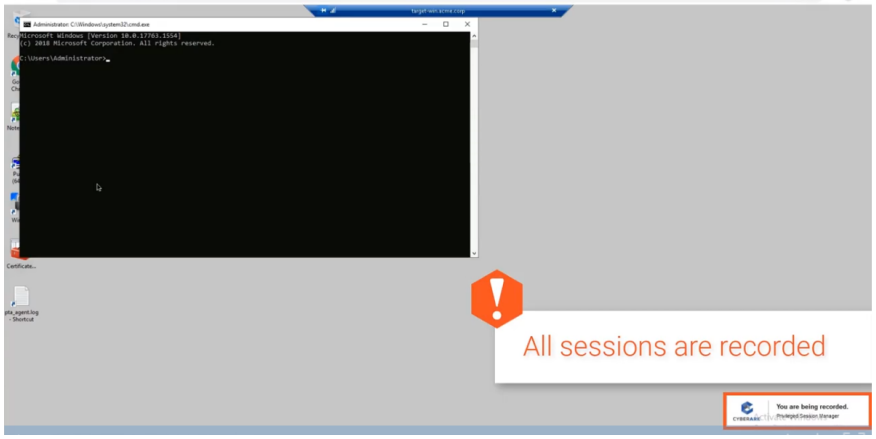

Fig. 5. Connect to target taken from CyberArk training module – Overview of CyberArk and How to use it.

CONNECT TO TARGETS WHEN CHECK-OUT/CHECK-IN EXCLUSIVE ACCESS IS ENFORCED

A. Exclusive access

Exclusive access allows check-out password of an account and have it locked to any other users attempting to check-out password. It allows any user to check-out password only after the initial user has checked-in the password. Which means only one user can have the password at any given point in time. Having full control of the password allows for monitoring who used the password and when. If this were in place the system would show WA not having access to the password.

The only way password can be checked out is if the following happens:

1. User manually checks-in the account
2. User disconnects from the session
3. Administrator manually checks-in the account
4. Automatic release by the system after a given period.

B. Login with a user with the privilege to view password

Click on the ellipse button on the right of the account to view the password. Along with check-out of the password user will see the time frame the password is accessible for. During this time frame the password is locked and accessible only for the user. When the time frame expires the password is automatically released and rotated unless the user checks the password back into the vault themselves.

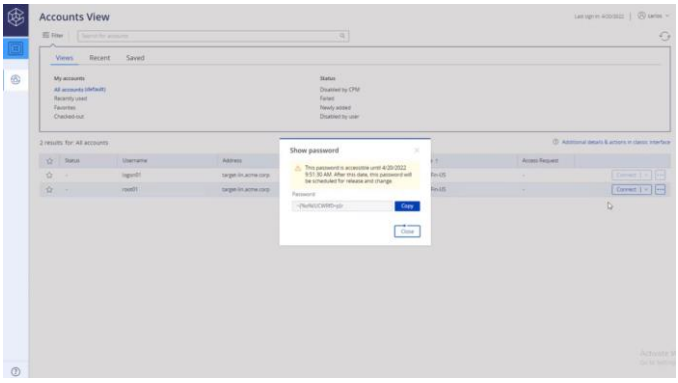

Fig. 6. View Password Screen taken from CyberArk training module – Overview of CyberArk and How to use it.

Other users who try to retrieve the password during the timeframe will see the following error.

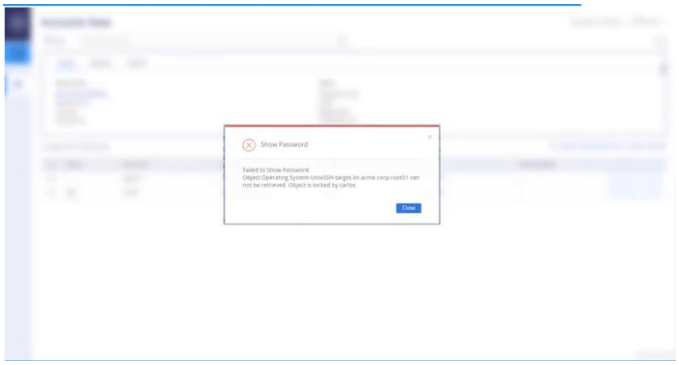

Fig. 7. Error Screen taken from CyberArk training module – Overview of CyberArk and How to use it.

C. Password Rotation

Once the user is done using the account, he checks-in the account to unlock it. The account is now marked for check-in. After a few minutes the system releases the account and changes the password. The same is

true when connected to a privilege machine using the connect button. The account is checked-out and inaccessible to other users just like when showing or copying the password. The account is automatically checked-in after the user disconnects from the session and the password will be rotated shortly after.

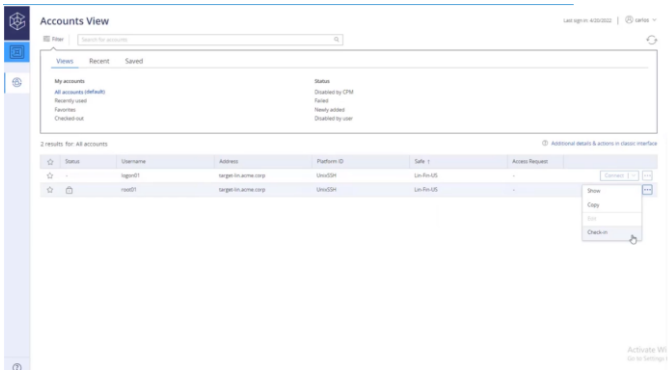

Fig. 8. Password rotation Screen taken from CyberArk training module – Overview of CyberArk and How to use it.

V. CONNET TO TARGET WITH DUAL CONTROL IS ENFORCED

A. Dealing with bad decisions

While CyberArk reduces the use of privileged accounts it does not reduce the bad decisions when used illegitimately. With dual control feature safeguard can be created. Dual control creates a request and approval process. Anytime a privileged account is used at least 2 people will have to agree that it is necessary. This creates a check against rash use of a privileged account.

B. Dual Control Workflow

Authorized safe members can either grant or deny requests to access accounts. This feature adds an additional measure of protection because it lets the organization see who wants to access the information in the safe when and for what purpose.

1. The user creates a request specifying the reason for accessing the account, whether they will access it once or multiple times and the time period during which they will access it.
2. A notification about the request is sent to users who are authorized to confirm this request
3. Request is confirmed or rejected by the authorized users. This can be done from the web portal or CyberArk Mobile app. The number of authorized users is defined in the master policy (4) Final step, the user connects to the account. Each time a user response to a request, the user who created it receives a notification. When the total number of confirmations are received for the request, the user receives a final notification.
4. The user can now activate the confirmation and access the account according to the request specifications.

C. Reduces Risk

Dual control diffuses the possible of using the password on one's own because it requires at least 2 people to access the password. There might be individuals who can be on both ends of the dual control 1) using the password 2) approving the password although this does not happen often. CyberArk has ensured that no one can approve their own request.

VI. CONNET TO TARGET USING NATIVE TOOLS

A. Native Tool Usage

There are windows administrators who use native tools and would like to combine the use of CyberArk with the use of native tools. CyberArk allows native tools to be used, it also has a remote desktop manager that is available to the user. On the Remote Desktop Manager select a device and right click to select properties. In the General tab of the Properties the host field can be populated with a CyberArk PSM (Privileged Session Manager) server. Username and password field can be left blank on this tab, that builds an additional layer of security. Under the Programs tab add a command to connect to the PSM server.

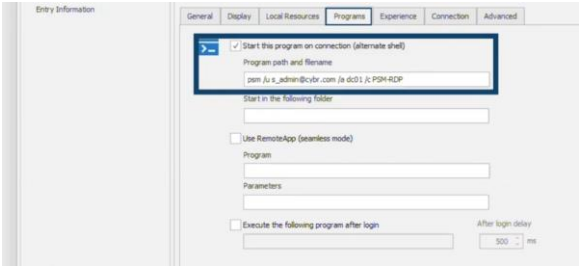

Fig. 9. Native tools Screen taken from CyberArk training module – Overview of CyberArk and How to use it.

B. Workflow

The session that would directly go the target now gets routed to the PSM and asks for CyberArk credentials to be connected to the target machine native tool the user is familiar with yet with the added security of CyberArk. A secure shell can also be used or any other application in place of the native tool.

C. PSM connection manager

PSM connection manager tool allows user to login using CyberArk credentials which then allows him to use the shortcuts directly. This will avoid the use of configuring the native tool as we discussed in the previous figure. CyberArk is making it easy to connect without sacrificing security.

D. Screen resolution

Screen resolutions – Administration -> Configuration options -> options -> Find and select the component to configure -> from the value column one can adjust the full screen, height and width options.

E. Multiple Monitor Support

Expand component -> Client settings -> Add an attribute -> multi-monitor and give it a value “Yes”.

Conclusion:

CyberArk has great features for an organization’s secure usage of privilege accounts. Digital vault software is the core of CyberArk’s solution. It is the secure repository of all sensitive information managing and controlling all access to the information, maintaining and providing tamperproof audit records. Privileged vault web access (PVWA) is the web-interface that allows user and administrators to access and manage privileged accounts. Privileged session manager (PSM) allows user to login to multiple servers using CyberArk credentials. Manages AWS accounts, secrets for multi-cloud, CI/CO pipelines and much more. This article is just scratching the surface of what CyberArk has to offer. A first glance at CyberArk’s offerings and various modules might be overwhelming.

REFERENCES

1. CyberArk, “Benefits of CyberArk Solution and how to use it”, https://training,.cyberark.com/pages/108/privilege-cloud-administrator (accessed November 21 2024)
2. CyberArk, “Breaking down the bussiness benefits and cost savings of CyberArk Privileged Access Management as a service”, https://www.cyberarlk.com/resources/blog/breaking-down-the-bussiness-benefits-and-cost-savings-of-cyberark-privileged-access-management-as-a-service (accessed November 21 2024)
3. LogicMonitor, “Best Practices What is CyberArk?”, https://www.logicmonitor.com/blog/what-is-cyberark, July 2024
4. InfosecTrain, “What is CyberArk”, https://www.infosectrain.com/blog/what-is-cyberark/, May 2022
5. Shreshtha, “What is CyberArk? A Brief intro on various CyberArk Architectures”, https://cloudfoundation.com/blog/what-is-cyberark-a-brief-intro-on-various-cyberark-architectures/, (accessed November 2024)