PeerPaper Report

Top 10 Considerations When Choosing a Privileged Access Management Solution

Based on real user reviews of CyberArk PAS

IT Central Station
Unbiased reviews from the tech community

CSO
FROM IDG

ABSTRACT

Privileged Access Management (PAM) is a critical element of any organization's security strategy. PAM is all about governing the access rights of highly privileged users, both human and non-human, who can administer key systems and applications—and potentially wreak havoc on a company's security posture if they are impersonated by attackers or malicious insiders. A number of powerful PAM solutions are now on the market. Which one is right for your organization? To answer this question, IT Central Station members offer their top 10 considerations when choosing a PAM solution. Their insights are based on their experiences with the CyberArk Privileged Access Security (PAS) solution.

CONTENTS

INTRODUCTION

Privileged Access Management (PAM) is essential for robust cybersecurity and effective regulatory compliance. PAM involves governing the privileged access rights of users, both human and non-human, who can administer key systems. Such "privileged users" expose an organization to risks. These include impersonation by hackers as well as malicious insider attacks and abuse of systems by former employees.

PAM offers a countermeasure. A number of powerful PAM solutions are now on the market. Which one is right for your organization? To answer this question, IT Central Station members offer their top 10 considerations when choosing a PAM solution. Their insights are based on their experiences with the CyberArk Privileged Access Security (PAS) Solution.

A Brief Overview of PAM

PAM comprises policies, processes and tools that seek to control who has administrative privileges in an IT environment for sensitive on-premises and cloud-based workloads. PAM is necessary due to the risk organizations face from improper administrative access. For example, a privileged (admin) user might be able to set up, modify or delete user accounts on a company's email server. A "super admin" has even greater rights, as shown in Figure 1. He or she often has what is known as "root" access and the ability to modify or delete the entire application or underlying infrastructure. Even a regular user who has complete "local admin" rights to their own workstation could click on a phishing link and install malware that provides an entry way to attackers.

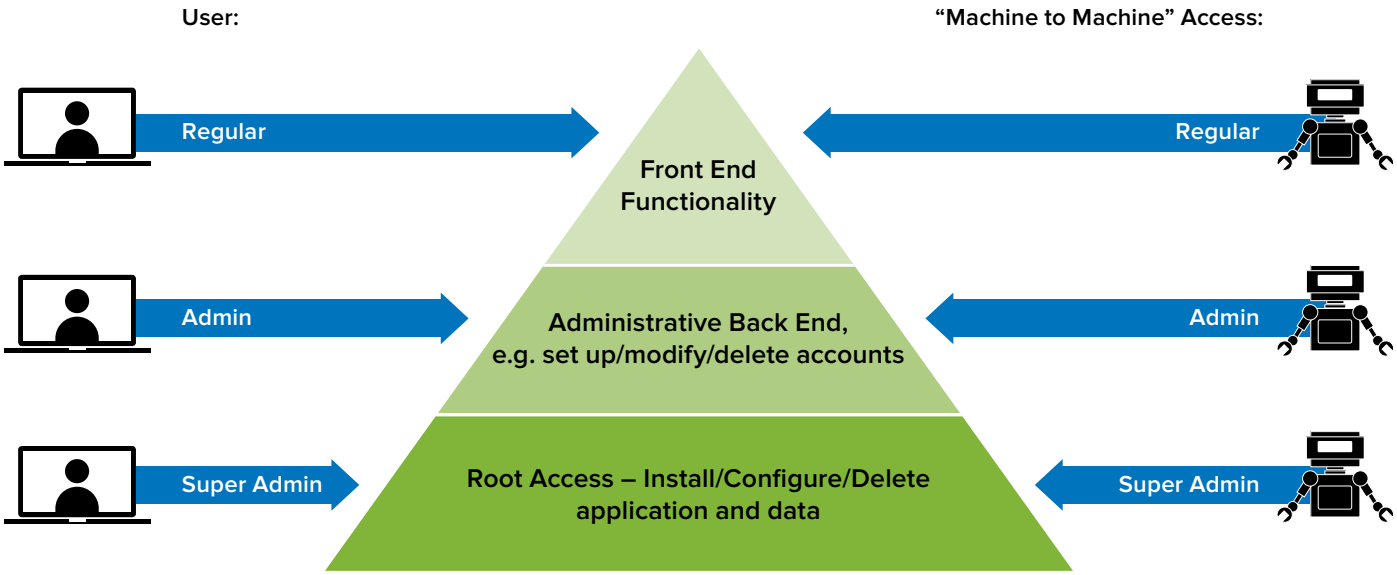

Figure 1 - The different types of access, ranging from a regular user to a super admin as well as machine-to-machine access

If a hacker can impersonate a privileged user (or create a new privileged user identity), he or she can disrupt operations or steal confidential information. PAM is therefore an important element of an organization's cyber defenses. PAM solutions are designed to mitigate privileged account risk by managing administrative credentials and levels of access privilege.

PAM solutions also secure highly privileged non-human "machine to machine" credentials. This includes credentials and secrets for internal applications, security software such as vulnerability scanners, application servers and IT management software, Robotic Process Automation (RPA) platforms, and the CI/ CD (Continuous Integration/ Continuous Deployment) tool chain.

Top 10 Considerations When Choosing a PAM solution

IT Central Station members who use CyberArk for PAM offer 10 top considerations for the selection of a PAM solution. These include factors like ease of implementation, cloud readiness, ease of use, session management, ease of integration, automation and more. They also recommend paying attention to audit and reporting features as well as password management and credential securing features.

1. Ease of implementation

A PAM solution should be relatively easy to deploy. It's a serious enterprise technology, so it won't be a push-button implementation. However, solutions that are overly complex are not ideal either. In this context, a Senior System Engineer at a transportation company with over 10,000 employees praised CyberArk's ease of implementation. He remarked that the solution did not require a lot of customization, noting, "You can get it right out-of-the-box and run with it." A Lead Consultant at a large tech services company similarly shared, "I have an affinity towards CyberArk. I find that it works out-of-the-box, as a product."

Other observations about implementation of use included:

- "[It's an] agentless solution which is easy to customize to any platform having network connectivity. [It is] easy to configure HA and DR options [and] a wide range of devices are supported out-of-the-box." - Technical Director at a small tech services company
- "The initial setup was pretty straightforward. I think the implementation only took a couple of days." - Senior Security Engineer at a financial services firm with over 1,000 employees

Ideally, a PAM solution will enable more than one approach to implementation. For instance,

> **You can get it right out-of-the-box and run with it.**

some IT departments may prefer a gradual deployment. As a Senior Consultant - Information Security Engineering at a major financial services firm explained. "You can gradually implement CyberArk, starting with more easily attainable goals, such as basic vaulting and password rotation and build on that with additional modules, such as Privileged Session Manager and Application Access Manager."

2. Cloud readiness

Many CyberArk users on IT Central Station expressed an interest in either applying PAM to cloud-hosted applications or putting their PAM solution itself in the cloud. One user, a Security Analyst at a 10,000+ employee retailer is currently using CyberArk for applications running in the cloud. For others, it's a plan. Cloud readiness, therefore, emerges as a consideration for selecting a PAM solution. An Associate Engineer at an insurance company with more than 5,000 employees shared, "We utilize CyberArk's secure infrastructure. We are moving towards applications in the cloud, but we do not currently have that."

> **I love how we can make a policy that affects everybody instantly, which is great.**

A Technical Consultant at a healthcare company explained how his team uses CyberArk for all application IDs to onboard into CyberArk. It's been a big job. He said, "So far, the performance is good because we have onboarded more than 40,000 accounts, and it's growing every day." He added, "We plan to utilize CyberArk's secure infrastructure application running in the cloud. We are conducting workshops with CyberArk on this."

A Security Specialist I at a healthcare company with over 1,000 employees similarly commented, "Our company is not in the cloud yet. We are not that big. We are looking to move to it soon, as it is on our roadmap. By the end of the year or early next year, we are hoping to move CyberArk to the cloud." A Security Analyst at a mid-sized financial services firm said, "We plan to utilize CyberArk's secure infrastructure and applications running in the cloud. We have AWS now. That is our next avenue: To get in there and have that taken care of."

3. Ease of use

Like any security solution, PAM should be easy to use, whether from the user interface or via an application programming interface (API) like REST. If it's overly complicated or burdensome, it may get circumvented or ignored. This was a problem in earlier generations of PAM technology. Customers therefore prefer solutions that are intuitive to use. Comments about ease of use for PAM included:

- "I love how we can make a policy that affects everybody instantly, which is great. I love the interface because it is colorful, easy to read, easy to see, and how easy it is to make policies." - Information Security Analyst III at a healthcare company with over 10,000 employees
- "Allows users to self-provision access to the accounts that they need." - Senior Security Engineer at a financial services firm with over 1,000 employees
- "You can write different types of policies for custom business needs or any developer needs. If they need certain functions allocated, they can be customized easily." - IT Security Specialist I at a healthcare company with over 1,000 employees

- "It is very simple to use." - Project Manager at a major tech services company

4. Session management and recording features

Security analysts almost always turn to the PAM solution when there is a security incident. They want to know who accessed the system that was targeted in an attack. Who did what, and when? These are the big questions. Forensic capabilities like session management and recording are quite helpful in this regard. A Security Team Lead at a tech services company with over 10,000 employees put it this way: "The most valuable feature to me is the recording feature. I can track all of the records, the commands, the server, any misguidance, etc."

A Global Privileged Access Management Technical Architect at a large consultancy echoed this view, saying, "We can track down not only who made a change, but exactly what they changed or did." So, too, did the Technical Director at the small tech services company, who said, "It also provides DVR-like recording for all privileged access and text-based recording to easily audit all privilege activities."

Even without the need for a post-incident investigation, security managers like to have tight control over privileged access sessions. A Systems Admin Analyst III at an energy/utilities company with over 1,000 employees, for example, uses CyberArk's Privileged Session Manager for SSH [Secure Shell], which, in his view, "makes it extremely convenient for UNIX Administrators to utilize their favorite SSH client software (i.e., SecureCRT or Putty) to connect to a privileged target without having to go through the Password Vault Web Access (PVWA) web login." A CyberArk Consultant at a large hospitality company uses CyberArk's Privileged Session

Manager for provisioning, securing, and recording sessions.

5. Password management

Maintaining strong administrative passwords is crucial to preventing unauthorized privileged account access. Indeed, some of the biggest cybersecurity and compliance disasters had a root cause of shared or infrequently changed admin passwords. CyberArk users want effective password management in a PAM solution. As the hospitality industry CyberArk Consultant said, "CyberArk's Central Policy Manager is useful for agentless automated password management through AD [Active Directory] integration as well as endpoints for different devices."

An IT Analyst at a tech services company with over 10,000 employees discussed how the process works. He said, "When the accounts have been used, its password is changed (to

something a user would have had to write down) before being made available for reuse. The passwords, which are hidden from the users are not known, and thus can be long and complex, while only being used for a session before being changed."

Other users shared the following observations about password management:

- "The most valuable feature is the ability to manage many accounts and broker connections between devices without needing to know passwords." - Security Analyst at a retailer with over 10,000 employees
- "The Central Policy Manager is the most valuable feature because the password is constantly changing. If an outsider threat came in and gained access to one of those passwords, they would not have access for long. That is critical and very important for the stability of our company." - Data Security Analyst II at a financial services firm with more than 5,000 employees

> **The Central Policy Manager is the most valuable feature because the password is constantly changing.**

- "We use it to harden our passwords for privileged users. We also utilize CyberArk to secure application server credentials." - Security Analyst at a financial services firm with more than 5,000 employees
- "I love the ability to customize the passwords: the forbidden characters, the length of the password, the number of capital, lowercase, and special characters. You can customize the password so that it tailor fits, for example, mainframes which can't have more than eight characters. You can say, 'I want a random password that doesn't have these special characters, but it is exactly eight characters,' so that it doesn't throw errors." - Information security engineer/ business owner
- "I had a fair number of systems where the passwords were not fully managed by CyberArk yet, and they were expiring every 30 or 45 days. I was able to get management turned on for those accounts. From an administrator perspective, I didn't have to go back into those systems and manually change those passwords anymore. CyberArk was taking that administrator task away from me and handling it, so it lightened the load on our administrative work." - Core Analyst/ Server Admin at a comms service provider with over 1,000 employees

A highly secure and available vault that can easily manage a large number of credentials is also extremely important in terms of controlling access. The hospitality industry CyberArk Consultant remarked, "The Enterprise Password Vault offers great capabilities for structuring and accessing data." The Senior Consultant - Information Security Engineering proactively vaults and manages all elevated accounts across multiple platforms. For a Security Architect at a 10,000+ employee healthcare company, the value came from the disaster recovery functionality they have with CyberArk Enterprise Password Vault. He said, "We test it frequently, and it is stable for us. We have been very pleased with the stability of the solution."

6. Audit and reporting features

Security and compliance audits usually look closely at privileged account management policies and the solutions that enforce them. PAM is a fundamental part of the identity and access controls of common compliance

frameworks such as HIPAA, PCI, ISO, and GDPR, to name a few examples. A PAM user at a financial services firm with over 10,000 employees spoke to this need, saying, "For audit and risk purposes, CyberArk Enterprise Password Vault has helped us meet our standards and requirements to help us comply with industry standards and banking regulations. Reports and other quick audit checks make this possible."

Internal audits may also review PAM solutions and privileged account activity. For example, a Senior Identity and Access Management System Administrator at a mid-sized financial services firm said, "CyberArk PAS is our go-to solution for securing against the pass the hash attack vector and auditing privileged account usage." A Director Information Security at a small insurance company added, "It has helped from an auditing perspective identify who has access to privileged accounts. We are able to now track who is accessing systems. It provides accountability to the individuals who are using it, knowing that it is audited and tracked. The auditing and recording are incredible."

7. Ease of integration

PAM solutions almost never function on a standalone basis. They must integrate with infrastructure and applications for which they govern privileged access, whether on-premises, cloud or hybrid. They also have to integrate with other IT management, security and compliance solutions such as ticketing systems, vulnerability scanners, and identity governance solutions to cite a few examples. Several CyberArk users shared their experiences using the CyberArk Marketplace, which offers plugins and proven integrations for a wide variety of external systems and applications. Figure 2 offers a simple view of a PAM solution's potential integrations. To this point, the insurance company Associate Engineer I noted, "Each new product that our company buys, we turn to CyberArk, and they are say,

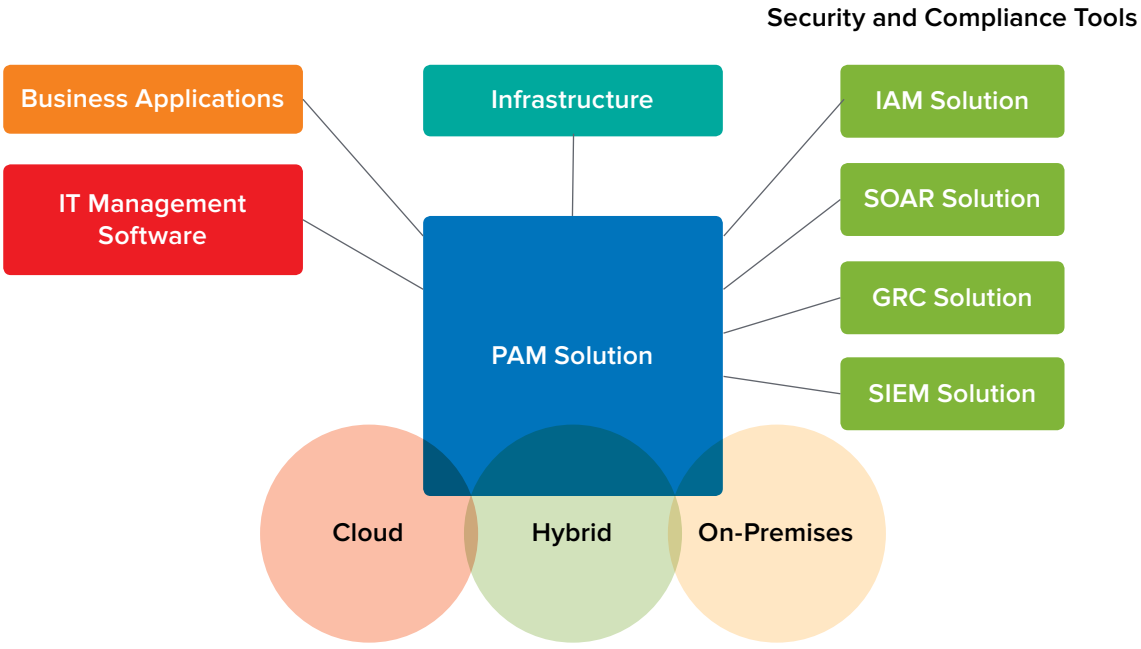

Figure 2 - Reference architecture reflecting PAM's need to integrate with both business applications and security and compliance systems as well as infrastructure and IT Management Software—in cloud-based, on-premises and hybrid architectures

'Yes, we integrate with that.'" For him, the most important criteria when selecting a vendor is whether they integrate with CyberArk.

The healthcare Technical Consultant praised CyberArk for integration, saying, "The flexibility of integrating with other technologies is important because of a lot of applications - a lot of COTS [commercial off-the-shelf] products - are not supported when we are bringing the application IDs. The CyberArk platform provides a lot of opportunities to do customization."
The healthcare Security Architect said, "We have never had any issues with deploying additional things."

He then explained, "We have tightly integrated CyberArk into a lot of our different processes. Our security organization is massive. We have a lot of different teams and different things moving. Not only have we integrated this into our identity access management team, so onboarding and offboarding, but we also have integrated it into our threat management side where they do security configuration reviews before we have applications go live."

8. Automation

IT Central Station members place value on automation as a PAM solution feature. Automation makes security operations more efficient while reducing the potential for human error in managing privileged accounts. Review highlights for automation include:

- "The most valuable [feature] would be the REST API on top of [Privileged Threat Analytics] PTA, which we do not have installed yet, but we are looking to install it moving forward in the future. What it enables us to do is if someone takes a privileged account and logs into a machine that we do not know about, it will alert us and log that they have logged in. It allows us to take that identity back and rotate the credentials, so we now own it instead of the intruder going out and using a rogue account." - Associate Engineer I at an insurance company with over 5,000 employees
- "It has an automatic password rotation. We have so many accounts, and being such a large organization, it helps take a lot of maintenance off of our plates, as well as automating a lot of those features to help increase our security. Having this automation in place, it has really been beneficial for us." - Security Architect at a healthcare company with over 10,000 employees

> **"...it helps take a lot of maintenance off of our plates as well as automating a lot of those features to help increase our security.**

- "We're auto-discovering our new Windows servers." - Identity and Access Management Analyst at a financial services firm with over 1,000 employees

9. Securing application credentials

As part of CyberArk's PAS offering, Application Access Manager secures the credentials used by applications, scripts, automation tools and other non-human identities to access internal and external resources, such as, databases, cloud and IT resources, third party applications, tools and container platforms.

While customers typically initiate their PAM program to secure the privileged credentials

used by humans, a critical next step is to remove hard-code passwords and credentials from applications, scripts and other non-human identities. For example, according to a Consultant at a large hospitality company, “CyberArk is managing our privileged accounts: most of the service accounts, admin accounts, and all other privileged accounts on different platforms including Windows and Linux. A lot of databases have already been onboarded. At the moment we are working towards integrating, or implementing, the AIM [Application Identity manager, which is now called Application Access Manager (AAM)] product to make sure those hard-coded credentials are being managed by CyberArk, instead of being directly coded in.”

According to a security analyst at a mid-sized insurance company, it’s also valuable to use the same platform to secure privileged credentials for both human and non-human credentials, “We use it for all of our privileged accounts, local admin, domain admin, and application accounts. We use several of the product suites. We are using the [Enterprise Password Vault] EPV suite along with AIM [AAM], and we are looking into using Conjur right now. Overall, it has been a great product and helped out a lot with being able to manage privileged accounts.”

10. Price and value

The decision to purchase a PAM solution is not usually the result of a quick and simple evaluation process. Many factors deserve attention and discussion. These will naturally include the solution’s price, total cost of ownership and overall value to the enterprise. To this end, a Senior Technologist at a retailer with over 1,000 employees advised, “Understand your needs prior to purchasing,” then added, “the CyberArk team will advise as well which is a plus.”

With specific needs in mind, it’s possible to make an informed decision about the various licensing options that are usually available. For instance, as the insurance company Associate Engineer I explained about CyberArk, “Check out the unlimited model as it can save money and make for a more scalable solution depending on the size and needs of your organization.” A Senior Manager - Privileged Access Management at a tech services company with over 10,000 employees recommended, “Standardized offerings that allow for customer-specific flexibility.” IT Support Specialist / Project Lead at a similar-sized energy/utilities company commented, “Setup, costs, and licensing are fairly straightforward and easy to navigate.”

CONCLUSION

Selecting the right PAM solution requires a balanced process of evaluation. Many factors are worthy of consideration. According to CyberArk users on IT Central Station, the most important aspects of a PAM solution to consider include ease of implementation and ease of use. A PAM solution should be cloud-ready, given the seemingly inevitable migration of enterprise IT in that direction. The strength of the solution's session management, credential rotation, and the ability to secure application credentials are also relevant features. A PAM solution should provide robust auditing and automation. By taking these selection criteria into consideration within a specific organizational context, it is possible to find a PAM solution that forms a good fit in terms of security, compliance and cost of operations.

ABOUT IT CENTRAL STATION

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. However, in the world of enterprise technology, most of the information online and in your inbox comes from vendors when what you really want is objective information from other users. IT Central Station provides technology professionals with a community platform to share information about enterprise solutions.

IT Central Station is committed to offering user-contributed information that is valuable, objective and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.itcentralstation.com

IT Central Station does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, IT Central Station websites, and IT Central Station materials do not reflect the opinions of IT Central Station.

ABOUT CYBERARK

CyberArk (NASDAQ: CYBR) is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 500, to protect against external attackers and malicious insiders.