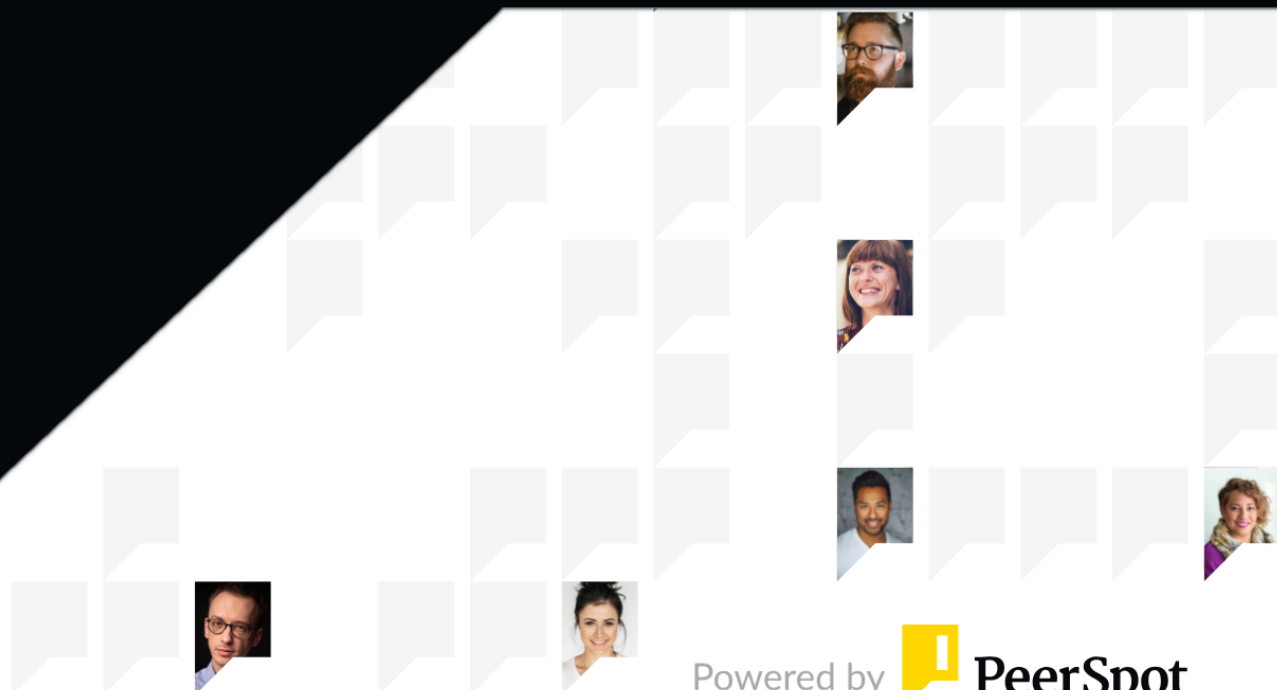




Idira Privileged Access Manager

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 13

Other Solutions Considered..... 14 - 16

ROI..... 17 - 19

Use Case..... 20 - 24

Setup..... 25 - 28

Customer Service and Support..... 29 - 31

Other Advice..... 32 - 36

Trends..... 37 - 38

About PeerSpot..... 39 - 40

Product Recap



Idira Privileged Access Manager

Idira Privileged Access Manager Recap

CyberArk Privileged Access Manager safeguards privileged accounts through password management, credential rotation, and session recording. With seamless integration and real-time monitoring, it ensures robust security across platforms.

CyberArk Privileged Access Manager is recognized for its extensive capabilities in managing and securing privileged accounts. It offers vital functionalities such as automatic password rotation, real-time session monitoring, and cross-platform integration through APIs and custom connectors. Users find the flexibility in workflows and granular access controls beneficial, particularly in protecting access across cloud and on-prem infrastructures. However, improvements in its interface, installation process, plugin support, and integration with third-party tools are often suggested. Pricing is a concern for many, along with the need for better dashboard reporting, user provisioning, and enhanced documentation. Organizations leverage this tool for encrypting and monitoring critical account activities and automating password management to bolster security.

What are the key features of CyberArk Privileged Access Manager?

- **Enterprise Password Vault:** Provides secure storage and management of enterprise credentials.
- **Privilege Session Manager:** Offers comprehensive session recording and monitoring.
- **Privileged Threat Analytics:** Detects and alerts on potential credential threats.
- **Integration Capabilities:** Easily integrates with multiple systems using APIs and custom connectors.

What benefits or ROI should users expect?

- **Enhanced Security:** Automates and centralizes password management, reducing risk of account misuse.
- **Compliance Support:** Ensures alignment with compliance policies through automated processes.
- **Operational Efficiency:** Streamlines security operations with real-time monitoring and integration.
- **Adaptability:** Protects privileged access across diverse infrastructure setups including cloud and on-prem.

CyberArk Privileged Access Manager finds substantial use in industries such as finance, healthcare, and technology, where the protection of privileged accounts is critical. These sectors rely on its capabilities to manage application credentials securely and provide safe access for developers, administrators, and vendors across various infrastructures.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “What I appreciate about CyberArk Privileged Access Manager is that it is not only for password security; we can also manage their applications and platforms, and whenever a user logs in, end-to-end protection is handled, including monitoring user activity through PSM servers and reacting to threats with Privileged Threat Analysis.”



Singaravelu C

CyberArk Engineer at Tata Consultancy

- ✓ “CyberArk Privileged Access Manager assists in meeting compliance and regulatory requirements such as HIPAA and SOX, ensuring I adhere to necessary standards in my operations.”



RaoB

Senior CyberArk architect at a consultancy with 11-50 employees

- ✓ “CyberArk Privileged Access Manager provides granularity. You can break things down into individual safes. You have specific access to safes by individual or group. The interface is with AD, with LDAP, or with local CyberArk passwords. You also have the ability to establish policies for your individual credentials.”



Sean Izor

Senior PAM Consultant at iC Consult GmbH



“One additional thought is that Idira Privileged Access Manager has become a crucial part of our daily Linux administration and security work.”



Mahmudul Hoque Khan

Lead Engineer at a engineering company with 201-500 employees



“The session recording and monitoring capabilities are valuable. We have real-time session management ability to record, audit, and monitor any privileged user activities. That is a big deal.”



Verified user

IT Cyber Security Lead at a mining and metals company with 1,001-5,000 employees



“CyberArk Privileged Access Manager has been helpful in managing over 125,000 privileged accounts in a single environment for our client, and we have multiple CyberArk environments for different clients with different numbers of accounts.”



Atul-Gujar

CyberArk manager at a comms service provider with 10,001+ employees



“Overall, I think CyberArk Privileged Access Manager is very good and can be considered a market leader in this space.”



Mohamed Fouad

Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

What users had to say about valuable features:

“CyberArk Privileged Access Manager provides security and video recording of user sessions for audit purposes. This feature is critical in financial sectors where auditing who performed specific actions is essential. Having video records adds a layer of proof and ensures compliance with audit requirements.

The key feature of CyberArk Privileged Access Manager is that it's a comprehensive package rather than just dependent on components such as Vault or Privileged Session Manager. Each component is necessary, and the Vault is the heart of CyberArk; everything connects via PSM and PSMP. I particularly appreciate PSM and PSMP because they simplify troubleshooting and charging..”

Atul-Gujar

CyberArk manager at a comms service provider with 10,001+ employees

[Read full review](#) 

“CyberArk Privileged Access Manager is very good on stability as a PAM solution. You can consider that if you do not have a stable PAM solution and the PAM solution always has issues with many maintenance windows, your entire organization cannot access the systems. It is very critical to rely on a stable system as a PAM solution.

“The most valuable features are integrations with ticketing systems, recording sessions, and running with compliance. We also have another feature from CyberArk Privileged Access Manager, especially SSH key lifecycle management, which performs excellently in this area.

“CyberArk Privileged Access Manager does not interrupt the sessions or administration sessions. Our professional services team implemented it, and we deployed full PAM features and the complete CyberArk Privileged Access Manager product in just three weeks across our larger organization. I think this is a strong point for CyberArk Privileged Access Manager..”

Mohamed Fouad

Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

[Read full review](#) 

“CyberArk Privileged Access Manager's best features include password rotation and an excellent monitoring solution, with the additional benefit of monitoring for Enterprise Password Management (EPM) where I provision privileged access.

“Delving deeper into the solution reveals many valuable features, but I particularly find password rotation and monitoring capabilities highly effective for auditing purposes. These features restrict users from unauthorized communications outside of CyberArk.

“CyberArk Privileged Access Manager has helped reduce privileged accounts in my healthcare organization, where I generate reports for approximately 500,000 accounts. This reporting capability allows me to analyze and restrict based on the reports tab effectively. I note that there are limitations with supporting the pass reporter feature, although I still find it valuable for generating comprehensive account and safe level reports.

“CyberArk Privileged Access Manager assists in meeting compliance and regulatory requirements such as HIPAA and SOX, ensuring I adhere to necessary standards in my operations..”

RaoB

Senior CyberArk architect at a consultancy with 11-50 employees

[Read full review](#) 

“I think the best features Idira Privileged Access Manager offers include centralized privileged access management. If I rank these features, I would give access control the best feature rating for me, as the ability to control hybrid access without relying on permanently active users or shared credentials is particularly valuable in reducing the risk of data breaches. The session visibility is also useful for troubleshooting because we can see who accessed the server and what administrative activity was performed. In my opinion, the centralized approach makes it easier for operations and security teams, allowing them to do their job without needing deep technical knowledge.

“The strongest feature for us is access control in Idira Privileged Access Manager. I have noticed that giving people administrative access to our servers improves management, especially when providing temporary credentials for policy access. This makes it easier to manage privileged access among team members, and we can simply revoke the authentication license after they finish their work.

“I can recall details about the features, particularly the granularity of access in Idira Privileged Access Manager, which allows us to define access based on specific servers or resources rather than providing broad pseudo access. That is quite practical, as I do not have to give my team members full administrative access to a specific server; I can grant them limited access to only what they need, so they can perform their tasks without interrupting the operations of other resources..”

Mahmudul Hoque Khan

Lead Engineer at a engineering company with 201-500 employees

[Read full review](#) 

“CyberArk Privileged Access Manager has improved how my organization functions as we have 24 PSM servers, four CPM servers, one primary Vault, and one DR Vault. We are in the process of upgrading from version 11.3 to 14.6 and maybe next month, we are going to update our servers.

“The best features of CyberArk Privileged Access Manager include that it is normally used for securing passwords because nowadays, most of the breaches happen due to leaking passwords. So we actually manage the passwords in a secured way. In a Vault, there is end-to-end security, with seven layers of security that we are maintaining. That is called session encryption, firewalls, authentication, authorization, and auditing. At the end of the day, we are doing the file encryption. Through this, we are actually managing the passwords in a very secure way. We can explain this architecture to the vendor to convince them to come to CyberArk Privileged Access Manager.

“What I appreciate about CyberArk Privileged Access Manager is that it is not only for password security; we can also manage their applications and platforms. Each and every thing, whenever a user is coming to CyberArk Privileged Access Manager or logging in to CyberArk Privileged Access Manager, end-to-end protection will be handled by CyberArk Privileged Access Manager. Whenever they connect to their target servers, each and every thing will be monitored and reviewed by CyberArk Privileged Access Manager administrators such as us. We see whatever incidents happen and whatever is going to happen. Whatever the user does from the target system, we can monitor everything through the PSM servers. We also have PTA, Privileged Threat Analysis. Whenever a user is doing unwanted things such as running unwanted scripts in their target system, the PTA incident automatically closes their target system. For example, if a user is working beyond their scope and is running some scripts, it will show that and raise an incident. We get the tickets and we can monitor it and have a call with the user. We are giving end-to-end security from the user to the platform level..”

Singaravelu C

CyberArk Engineer at Tata Consultancy

[Read full review](#) 

“The most beneficial feature in Idira Privileged Access Manager is its simple user interface. It is definitely advantageous. I also appreciate the enhancements that come along with the continual updates that are provided.

It has improved the organization by making it simpler to gain access to privileged credentials. There are so many accounts needed by most people now, and having a tool that can not only store those credentials for you but also manage them and give you easy access has made life a lot easier. The tool manages credential cycling, which is typically a pain for anybody, while providing a simple means to use them.

The solution is very good for protecting full levels of data privacy. We silo out different parts of the solution for access to different types of infrastructure in the same way we would to our customers so that we can restrict who can get to something. In combination with our IM processes, we can be quite granular about who has access to what.

We can stay updated on regulations. The updates that are coming through help to keep the product secure and also add in updates and enhancements that give greater functionality and keep it relevant in terms of requirements.

The controls are fairly granular. We can control who can administrate it and who can use it and what they can use when they're using it. It has positively impacted visibility. As we leverage the product for administration of the product, we're able to be much more granular in how we provide the access. The audit controls allow us to see who is doing what, and when, it should be required.

It safeguards credentials. This is very important. The ability to have the product manage and maintain credentials and only provide them to authorized individuals, whilst not actually allowing them to retrieve those credentials, has become more paramount as we look to increase the security based on sort of ongoing real-world threats.

It's helping with compliance, specifically around securing and hardening of infrastructure. It allows us to harden while still maintaining usability.

In terms of operational efficiency, it depends on where you're coming from. Some things are more efficient, some things are a little less efficient yet more secure. It's that ongoing balancing act between operation efficiency and security that we must deal with.

We've been able to reduce the number of privileged accounts in the organization with the ability to have shared accounts. Since the credentials are not specific to a user and they're made available to a user for the duration of their session, we can reduce the number of privileged accounts we have within the organization. We've reduced the accounts by a half to a third between ourselves and our customers. .”

Shad Smith

[Read full review](#) 

Technical Architect at a tech vendor with 10,001+ employees

Other Solutions Considered

“About a year ago, we started looking at potential alternatives. There were two others that were considered and were ruled out for various reasons before looking at additional proof of concepts to see what other features could be leveraged from Idira Privileged Access Manager that we weren't using. It managed to pass all of the requirements..”

Shad Smith

Technical Architect at a tech vendor with 10,001+ employees

[Read full review](#) 

“In comparison to other PAM solutions like Delinea and BeyondTrust, I find CyberArk Privileged Access Manager continues to lead in effectiveness. With over nine years of experience, I believe CyberArk is superior in its password rotation capabilities and overall management, despite competitors having similar functionalities under different names..”

RaoB

Senior CyberArk architect at a consultancy with 11-50 employees

[Read full review](#) 

“I have used other PAM solutions, and I find that when it comes to CyberArk Privileged Access Manager, it is a company that has a long history of trust with users and vendors, which provides a more secure way of doing things for their platforms and their work. So in my opinion, CyberArk Privileged Access Manager is the best solution we can give to vendors for PAM solutions..”

Singaravelu C

CyberArk Engineer at Tata Consultancy

[Read full review](#) 

“Before choosing Idira Privileged Access Manager, I evaluated other options such as BeyondTrust and Dalina. We compared them mainly based on access control capabilities, Linux support, deployment requirements, overall cost, and licensing. Ultimately, we selected Idira Privileged Access Manager because it fits our existing environment and requirements effectively..”

Mahmudul Hoque Khan

Lead Engineer at a engineering company with 201-500 employees

[Read full review](#) 

“We previously used a different solution before Idira Privileged Access Manager, but it was not enterprise-grade; we relied on native SSH access. As developers and engineers, we understood SSH well and managed tasks manually. However, we switched to Idira Privileged Access Manager because not all team members were tech-oriented. While the previous approach worked for basic administration, it offered limited centralized access and made it harder to maintain consistent audit trails..”

Mahmudul Hoque Khan

[Read full review](#) 

Lead Engineer at a engineering company with 201-500 employees

“Before Idira Privileged Access Manager, we didn't have a PAM product itself. We were using Citrix to provide remote access, but the need to move into the PAM space arose to provide extra security and audit control.

Although I wasn't involved with the process, there was a competition to define which product would be used, and the Idira Privileged Access Manager product came out on top..”

Shad Smith

[Read full review](#) 

Technical Architect at a tech vendor with 10,001+ employees

ROI

Real user quotes about their ROI:

“CyberArk Privileged Access Manager has been very effective in helping my company meet compliance and regulatory requirements. Implementing CyberArk Privileged Access Manager saved time on compliance requirements in finance, typically around one hour..”

Surajit-Sutradhar

Operation Specialists at a tech vendor with 10,001+ employees

[Read full review](#) 

“The pricing compared to other solutions, particularly Fortinet, is favorable. Fortinet overall has excellent pricing. However, CyberArk Privileged Access Manager has good return on investment. The pricing is affordable compared to the features and the stability of the product..”

Mohamed Fouad

Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

[Read full review](#) 

“CyberArk Privileged Access Manager has helped our organization save on costs. CyberArk Privileged Access Manager is expensive, but it helps protect us from losing money.

Its benefits are visible immediately after the deployment, but in Brazil, people generally implement CyberArk Privileged Access Manager after an incident. .”

LZ LZ

[Read full review](#) 

Coordenador at a computer software company with 1,001-5,000 employees

“From a security perspective, we started seeing value right away because we didn't have a PAM solution at the time. Over the next sort of months and years, we settled into the product and started to look at how we could make it work for us. This has been an ongoing process over the years, particularly with product enhancements and new features, which provide additional benefits against the incurred costs..”

Shad Smith

[Read full review](#) 

Technical Architect at a tech vendor with 10,001+ employees

“We are starting to see a return on investment with Idira Privileged Access Manager. As it has been eight months since implementation, we estimate that access administration and troubleshooting take roughly fifteen to twenty percent less time. Centralized access and the audit trail make it easier to identify who performed administrative actions, allowing us to reduce headcount while saving time to allow our IT and security operational teams to focus on other tasks..”

Mahmudul Hoque Khan

[Read full review](#) 

Lead Engineer at a engineering company with 201-500 employees

“Regarding measurable benefits after deploying CyberArk Privileged Access Manager, customers often ask about return on investment. One measurable benefit is the reduction of engineering resources in the IT staff since they do not need as many administrators to manage numerous services.

Additionally, they reduce the number of personnel in the information security team, as fewer controllers or auditors are needed to oversee the activities of IT staff. These benefits can certainly be measured.

CyberArk Privileged Access Manager has helped customers save on costs primarily by reducing the number of engineering and information security personnel. This includes salaries and bonuses; although they do not fire these individuals, they reallocate them to other activities..”

Verified user

[Read full review](#) 

Head of Sales Services Department at a comms service provider with 51-200 employees

Use Case

“We are working with CyberArk solutions such as PAM on-premises. We are working with CyberArk Privileged Access Manager, including AIM, PSM, and PSMP components. .”

Atul-Gujar

CyberArk manager at a comms service provider with 10,001+ employees

[Read full review](#) 

“We use Idira Privileged Access Manager to provide a protective layer for our infrastructure, as well as for our customers.

Additionally, the audit functionality that it provides is used as protection for our employees. It offers evidence, so if there's any question about wrongdoing, there's proof that the job was done correctly..”

Shad Smith

Technical Architect at a tech vendor with 10,001+ employees

[Read full review](#) 

“In the healthcare sector, my use case involves securing privileged accounts across the entire organization. Although this is not specific to any sector, I also work for banking and financial services. As a PAM solution, I secure privileged accounts while provisioning access.

“With nine plus years of experience, I can develop and suggest solutions for various infrastructures, install, build, onboard, upgrade, patch, reboot, and maintain backup and restore solutions, as well as handle disaster recovery activities. I address troubleshooting of infrastructure issues and end-user requests, effectively managing onboarding and deboarding, and access provisioning for end-users. This allows me to provide end-to-end support in CyberArk Privileged Access Manager..”

RaoB

Senior CyberArk architect at a consultancy with 11-50 employees

[Read full review](#) 

“My main use case for Idira Privileged Access Manager is securing and controlling privileged access to critical servers and infrastructure. We use many servers, such as virtual machines for our institution to run software development. One specific use case I can share is how we manage these resources effectively.

“Additionally, we have to maintain our Linux servers, which sometimes requires hiring third-party or outsourced people to access them. Idira Privileged Access Manager helped us by providing a more controlled way to handle elevated SSH access without relying on shared or permanently active privileged credentials. The session visibility and audit trail are particularly useful when multiple engineers work on the same production environment. This is another use case of our administrative activity linked to specific users and maintenance tasks..”

Mahmudul Hoque Khan

Lead Engineer at a engineering company with 201-500 employees

[Read full review](#) 

“My use case for CyberArk Privileged Access Manager is that I work as an administrator where I can configure and integrate all those CyberArk Privileged Access Manager components such as PSM, CPM, hardening the CPMs, checking the services of the PVWA and Vaults, and making sure everything is operational. I am responsible for creating safes and managing the accounts. I onboard the accounts on the platform based on their vendor requirement.

“We also provide the SIEM integration to check the logs and we are responsible for Splunk integration too, but it is not related to CyberArk Privileged Access Manager. We actually implement all those application logs to Splunk for the dashboard monitoring and the alert-based system through ITSI..”

Singaravelu C

CyberArk Engineer at Tata Consultancy

[Read full review](#) 

“As an implementation engineer, I have extensive experience with CyberArk Privileged Access Manager and its implementation this year at our customer site. We have been acting as a resident engineer for one of our customers for the past six months.

“CyberArk Privileged Access Manager provides a repository and management system for our administrators to have sessions on our systems. For example, we require any administration access to our firewalls to be conducted through the PAM solution first. CyberArk Privileged Access Manager allows our administrators to access the firewalls and record the sessions.

“Another use case is user offboarding. If an employee like Muhammad leaves our company, we can simply delete this user from the entire organization. We also have excellent compliance capabilities to review what occurs during administration sessions because we have them already recorded..”

Mohamed Fouad

[Read full review](#) 

Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

The deployment of CyberArk Privileged Access Manager is straightforward, similar to installing any application on a PC. For those familiar with CyberArk, the installation process is very simple. Thoroughness is essential, but it is generally an easy process.

RaoB

[Read full review](#) 

Senior CyberArk architect at a consultancy with 11-50 employees

“The initial setup is relatively straightforward once you've done it. It is certainly a lot easier to repeat. We have multiple instances of the on-prem deployed, so we've done it a few times now..”

Shad Smith

[Read full review](#) 

Technical Architect at a tech vendor with 10,001+ employees

“After implementing CyberArk Privileged Access Manager, it typically takes about four to five months for a company to realize time to value, assuming they have a strong implementation team and infrastructure in place..”

Atul-Gujar

[Read full review](#) 

CyberArk manager at a comms service provider with 10,001+ employees

“The initial setup required careful planning around our Oracle Linux infrastructure, privileged accounts, and access points, with licensing evaluated based on the number of users and systems needing privileged access..”

Mahmudul Hoque Khan

[Read full review](#) 

Lead Engineer at a engineering company with 201-500 employees

“The time it takes to deploy CyberArk Privileged Access Manager is actually based on the architecture of their requirement, such as the number of users, accounts, and the platforms they are onboarding into CyberArk Privileged Access Manager. If it is less than ten users and four platforms, it will take one or two days. If the communication between our servers and the platforms is already good, it will normally take one to two days. If their requirement is more, such as at the platform level where they have both Windows and Linux operating systems and database operating systems and they want to segregate multiple users based on their OS, at that time we just need some time to create the SOPs and we have to proceed based on that requirement..”

Singaravelu C

CyberArk Engineer at Tata Consultancy

[Read full review](#) 

“The typical deployment process for CyberArk Privileged Access Manager starts with ensuring organizational prerequisites are met. We begin by sending prerequisites required for the environment, and the customer provides feedback that the environment is ready.

After we establish remote connection capabilities, we initiate the installation process following the agreed scope of work. This process includes integrating with Active Directories, second-factor authorization services, and email systems.

Next, we configure role-based access control, set up reporting, and automate email notifications for predefined activities.

Finally, we utilize a Threat Intelligence system to establish a baseline of regular behavior for administrative users..”

Verified user

[Read full review](#) 

Head of Sales Services Department at a comms service provider with 51-200 employees

Customer Service and Support

“CyberArk customer support is professional. We contacted them on only one case and resolved it in time. Based on our experience, we resolved the issue in just five minutes. I can say the support team is very professional and very technical with strong technical capabilities..”

Mohamed Fouad

Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

[Read full review](#) 

“Regarding technical support from CyberArk, while L2 and L3 teams are effective, L1 support requires improvement due to longer response times in critical situations. Coordination with higher support levels sometimes takes longer than expected, which should be addressed..”

Atul-Gujar

CyberArk manager at a comms service provider with 10,001+ employees

[Read full review](#) 

“I had a generally positive experience with Idira Privileged Access Manager's customer support. I reached out a couple of times, and the support team was responsive and helpful. Our initial inquiries involved configuration and troubleshooting questions about access control, as specific answers were not found in documentation. While some complex issues required additional communication, overall, the support met our day-to-day needs effectively..”

Mahmudul Hoque Khan

Lead Engineer at a engineering company with 201-500 employees

[Read full review](#) 

“The customer service is generally quite good, although if it's more complicated, you have to wait for it to be passed back to their dev support, which can take more time. For simpler issues, the turnaround is relatively quick. If more complicated, it can take longer to get the right level of support.

However, the support they provide is usually good, particularly their dev guys, who certainly know what they're talking about..”

Shad Smith

Technical Architect at a tech vendor with 10,001+ employees

[Read full review](#) 

“I rate the technical support for CyberArk Privileged Access Manager as the main thing in any environment. It can be a production environment such as CyberArk Privileged Access Manager or any production environment with any project. Because of technical support, we have continuous deployment and continuous monitoring. Whenever they are doing their work best, and at that time, when something is going down, they are the first point of contact to check what the issue is. After that, it will come to the developers to check that issue. So I will rate the monitoring team, the operations team, a ten..”

Singaravelu C

CyberArk Engineer at Tata Consultancy

[Read full review](#) 

“Regarding my relationship with the vendor, I am currently a customer. Previously, I was a partner while working in the banking and financial sector, but now in healthcare solutions, I associate as a customer. I reach out to the vendor whenever I encounter issues, seek information, or require assistance with upgrades. I maintain consistent communication on a weekly or biweekly basis through calls, emails, or tickets.

“I rate CyberArk's technical support as an eight. The vendor provides solid support when needed..”

RaoB

Senior CyberArk architect at a consultancy with 11-50 employees

[Read full review](#) 

Other Advice

“We have customers for various industries and use the product internally ourselves. We are in the IT sector and provide services to organizations in a variety of sectors.

It's definitely worth looking at as a PAM tool. I would steer towards the SaaS version since everything suggests that it is potentially a better way to go than on-prem. However, on-prem would still be suitable for those who must control and own their data.

It's still worthwhile implementing, and overall, I'd probably give it an eight out of ten..”

Shad Smith

Technical Architect at a tech vendor with 10,001+ employees

[Read full review](#) 

“CyberArk Privileged Access Manager requires upgrading and maintenance. We have scheduled the upgrade, and we have detailed and informative documentation for upgrading. There is an integration matrix, or rather a compatibility matrix, between the newer versions of CyberArk Privileged Access Manager with other systems. Before upgrading, we study the compatibility matrix and the upgrade process is very smooth.

“My overall rating for CyberArk Privileged Access Manager is ten..”

Mohamed Fouad

Cybersecurity Team Leader at EMAK For Computer Manufacturing (ECM)

[Read full review](#) 

“My advice for others considering Idira Privileged Access Manager would be to start with clearly defined privileged access, such as controlling access to Linux production servers, and then expand from there. Before deployment, it is vital to map out existing privileged accounts, policies, and audit requirements to understand your system, which will facilitate implementation. Integrating with your identity provider and [SIEM](#) early is crucial as it can significantly impact overall deployment. I suggest piloting the access workflows with a small group of users before fully rolling them out in a production environment.

“One additional thought is that Idira Privileged Access Manager has become a crucial part of our daily Linux administration and security work. The implementation of session visibility and auditing provides better accountability without introducing excessive complexity for administration. I hope to see further improvements in integrations and reporting, and while the AI implementation is good, it needs additional work. Overall, it delivers a practical foundation for managing privileged access in our operations, which aligns with our goals. I would rate this solution seven out of ten..”

Mahmudul Hoque Khan

Lead Engineer at a engineering company with 201-500 employees

[Read full review](#) 

“The requirements for CyberArk, particularly in India, have evolved significantly since the company acquired several businesses in 2014. Every organization needs an identity and access management (IAM) and privileged access management (PAM) solution. CyberArk stands out as the leading product in this category. While there are other protocols available in the market, CyberArk is known for its security, reliability, and user-friendly access.

In my experience working with multiple companies and clients using CyberArk, I have not encountered any cases of breaches or malicious activity associated with the platform. This track record provides a strong sense of security and assurance regarding CyberArk’s capabilities. Although the privileged access management solution can be costly, it offers extensive security features, including multi-factor authentication (MFA). Overall, CyberArk is an excellent product for organizations seeking robust security solutions.

Regarding granularity of PAM controls in CyberArk Privileged Access Manager, it means having centralized control in the Vault. Standalone CyberArk Vaults perform best compared to cluster systems, which present challenges during maintenance or network connectivity issues.

Overall, I would rate CyberArk Privileged Access Manager a nine out of ten..”

Atul-Gujar

CyberArk manager at a comms service provider with 10,001+ employees

[Read full review](#) 

“CyberArk Privileged Access Manager solution requires maintenance, and definitely, we are actually doing rotations 24/7 to make sure every system is active 24/7 so a user will not get interrupted when accessing their platforms.

“My clients use CyberArk Privileged Access Manager for around 12,000 accounts.

“The vendor can contact me if they have any questions or comments about my

review.

“I'm interested in being a reference for CyberArk Privileged Access Manager.

“I definitely recommend CyberArk Privileged Access Manager to other users because it gives more security to their platforms and users to store their passwords and provides end-to-end security. If they do not want to breach their platforms, I would recommend CyberArk Privileged Access Manager 100 to 200 percent to keep it secure. My overall rating for this product is a ten..”

Singaravelu C

CyberArk Engineer at Tata Consultancy

[Read full review](#) 

“I recommend CyberArk Privileged Access Manager to small and mid-level organizations needing a PAM solution. I assert that it has been a reliable tool for me for over nine years. Even a proof of concept might be beneficial initially, with an emphasis on understanding the budget aspect. I would rate this product a nine overall.

“I find CyberArk to be expensive in general. Many organizations have considered alternatives due to budget constraints, even though CyberArk is a leading product in the PAM industry, recognized for its quality and long-standing presence. However, the high cost can drive some customers away.

“Integrating CyberArk Privileged Access Manager with existing [EHR](#) systems and healthcare workflows, such as SailPoint, presents challenges. SailPoint integration often hinges on third-party tools, making the process complicated and critical for many organizations. I endeavor to manage this necessity.

“In terms of mean time to respond, I acknowledge variable response time. The L1 team is proactive, yet the vendor often pushes to close incidents swiftly, even when issues remain unresolved. This can extend the resolution timeline significantly.

“When assessing CyberArk Privileged Access Manager for protecting against ransomware attacks, I find that it effectively isolates components such as the primary vault, DR vault, PVWA, [CPM](#), PSM, and PSMP, ensuring communication is limited to internal only. This isolation prevents any interaction with the external world, including AD, thereby safeguarding my systems. The feature of maintaining a DMZ for the vault, which ensures that attackers cannot reach it, is critical in protecting against ransomware threats targeting Active Directory.

“Every infrastructure requires maintenance, including upkeep and patching. I find managing CyberArk Privileged Access Manager's infrastructure is straightforward. It can run effectively in physical or virtual environments, whether on cloud machines or VMware systems. Overall, maintenance is not overly complex.

“If deploying in a lab environment, setting up the primary and DR vaults, PVWA, and [CPM](#) can usually be completed within one and a half to two hours. Organization-wide implementations may require more time due to necessary approvals and hardware availability, but the actual installation process itself remains swift.

“I assess the granular controls provided by CyberArk Privileged Access Manager as robust because they enable tailored access at the individual user level or through AD groups. This includes detailed role definitions such as safe reader, safe auditor, safe approver, and safe manager. As an administrator, I can manage all access. By provisioning least privileged access and allowing users to connect and view their accounts without exposing passwords, I uphold the principle of least privilege at the safe level..”

RaoB

Senior CyberArk architect at a consultancy with 11-50 employees

[Read full review](#) 

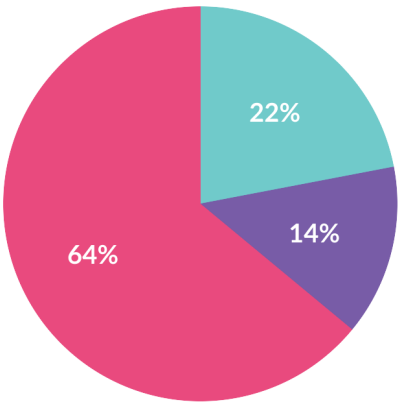
Top Industries

by visitors reading reviews

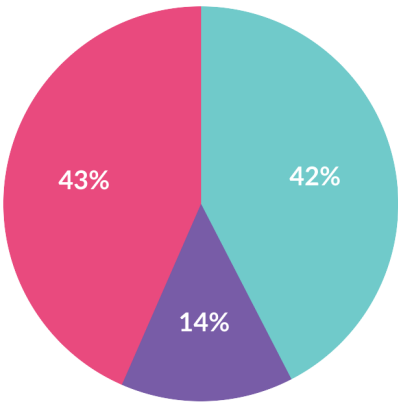


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944