CYBERARK®
The Identity Security Company™

A Buyer's Guide to Securing Privileged Access

Table of Contents

Introduction

You see it every day. IT environments are evolving. New attack methods are emerging. But the primary security risk that teams like yours face — compromised identities and credentials — remain constant. And the powerful accounts and credentials IT administrators use are still the top targets.

Privileged credentials and access is the gateway to an organization's most valuable assets and a factor in nearly every major security breach. The adversaries attack path starts with attackers gaining initial access, performing reconnaissance, and then moving laterally and escalating privileges until they can exfiltrate data, disrupt operations or deploy ransomware. Failing to implement a proper identity security program can lead to failed audits or non-compliance, resulting in financial penalties, business delays and erosion of stakeholder trust. But that's nothing compared to the disruption a data breach can cause to business reputation, performance and continuity.

You need an effective solution for securing enterprise identities, protecting credentials and secrets and managing privileged access. This guide highlights key requirements to help you select a partner and accomplish this critical need.

Now let's explore what's changing and will likely evolve again (and again).

Privileged access management (PAM) is not just about admins, root accounts, and simply vaulting and rotating credentials anymore. Technology shifts have created new types of privileged identities, such as cloud engineers, developers, everyday business users and third-party vendors who may comprise your software supply chain. These identities can perform high-risk actions in your IT environment, such as creating, modifying or deleting resources. And they often have far more access than what's required to do their jobs.

Moreover, PAM programs now must address security risks around non-human identities, such as automation accounts, bots and applications that can access critical systems and data.

Equally important to understanding what constitutes privileged access in today's IT environment is recognizing where privilege now exists. PAM is not just about on-premises IT anymore. Organizations are increasingly moving to hybrid, cloud, and multi-cloud environments where the surge in new identities and increase in permissions sprawl have reached a point of chaos.

If you're evaluating your current PAM vendor, or seeking a new provider, these are the major trends impacting your ability to secure your organization and everything building. In the following pages, we'll review the exact capabilities a PAM vendor should provide, starting with foundational controls to secure IT admins' identities.

74%

of respondents are concerned about confidential information loss stemming from employees, ex-employees and third-party vendors.

Source: CyberArk, "2023 Identity Security Threat Landscape Report," June 2023.

Evaluation Criteria

1. Foundational PAM Controls

PAM solutions are designed to secure the most powerful IT users and accounts in your organization. These are the highly privileged identities that attackers target to gain access to sensitive data and systems. With the right PAM solutions, you can gain control over -- and visibility into -- who can access what, when, how and why.

Now, you might be thinking: "Yes, we know all of that." However, even though PAM is a cornerstone, many organizations are still not securing the identities of IT admins and accounts.

62% lack a complete picture of human and non-human access to sensitive resources.

63% admit that highest sensitivity access for employees is not adequately secured.

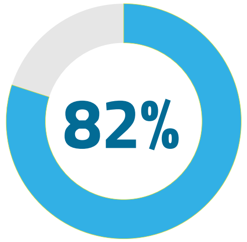
Here is a set of foundational PAM controls that all organizations, across industries, should look for when vetting providers.

1. Manage Privilege Credentials • Automatically discover and onboard privileged credentials. • Set policies for password complexity, frequency of password rotations, which users may access which safes, and more via centralized policy.	**3. Detect and Response to Threats** • Automatically discover and onboard unmanaged privileged accounts and credentials. • Detect anomalous behavior and indicators of compromise with policy-driven remediation capabilities.
2. Isolate and Monitor Sessions • Establish secure, isolated remote sessions and record all activity during that session. • Reduce risk of malware by not allowing end users to directly connect to target systems.	**4. Unify PAM with Access Management** • Use SSO to enable secure access to multiple applications with a single set of credentials and to eliminate password sprawl. • Implement adaptive multi-factor authentication (MFA) to validate every user, applying access controls and authentication factors that correspond to the user's risk profile.

Tip

As a best practice, adaptive MFA should be required to access all resources within an organization, including web apps, VPNs, endpoints, servers and privileged accounts.

2. Securing Privileged Access in Cloud Environments



The percentage of IT leaders now adopting the hybrid cloud. It's also the percentage of breaches involving data stored in public, private and/or multi-cloud environments.

The proliferation of identities in an organization's cloud environments adds another dimension to securing privileged access. Every human and non-human identity in a cloud environment can be configured with thousands of different permissions and entitlements to access workloads containing sensitive data.

Excessive, unused and misconfigured cloud permissions expose organizations to the risk of data breaches — and regulatory fines. The average cost of a data breach is $4.45 million. That cost increases when a breach involves data stored in the public cloud ($4.57 million) or across multiple environments ($4.75 million).

An attacker controlling an identity with excessive permissions can establish an easy path toward stealing data, installing ransomware and more. One way to mitigate these risks: apply Zero Standing Privileges (ZSP), which entails:

- Enforcing real-time least privilege in the cloud by granting only the relevant permissions a user needs — and only when needed — to accomplish a given task.
- In turn, reducing the impact of an attack: if a threat actor takes over an account, their options would be extremely limited without admin-level access.

Also prevalent in the cloud: non-human identities in the DevOps space that rely on secrets to access sensitive resources.

Your organization may have a solid program for reporting on privileged access among a defined group of IT admins. And you might be meeting requirements for on-prem environments. But now it's time to apply compliance best practices to the cloud.

99%

security decision-makers say they'll face an identity-related compromise in the year ahead.

40,000

Difference access controls users can access from the 1,400 native services offered by the three top cloud service providers.

$4.57 million

global average cost of a data breach in 2023.

45:1

ratio of non-human to human identities – at a time when all identities require protection.

Sources:

CyberArk, "2023 Identity Security Threat Landscape Report," June 2023.

IBM, "Cost of Data Breach Report 2023", July 2023.

Three areas for vetting security vendors for their ability to secure privileged access in cloud environments.

1. Meet Baseline Requirements

- Implement Zero Standing Privileges, replacing always-on access with configured policies based on roles, workload attributes and privileged access needs provisioned JIT.
- Maintain frictionless native access for users, by supporting existing developer workflows and integrating with existing tooling.
- Centralize secrets management and governance to a single hub, so developers can use their preferred tooling and the business can apply necessary industry and internal standards.

2. Standardize Audit and Reporting

- Build a proactive strategy to get ahead of auditors' required evidence, artifacts and reports—centered on continuous visibility for all identities' access.
- Define models permitting a "critical situation" level of access, to ensure on-call cloud engineering teams can quickly solve problems without waiting for approvals.
- Isolate and monitor high-risk access to cloud workloads and services, storing audit trails in the same place as web apps or on-premises session logs, to streamline processes.

3. Encourage Continuous Improvement

- Ensure all new cloud environments have secure access policies in place, with correctly configured roles and identity settings—offsetting the need to fix issues once they are provisioned.
- Use automation to enforce industry and internal standards for human and non-human access.
- Automate audit and reporting processes to reduce manual work and establish a proactive compliance program.

3. Consolidation of Privilege and Identity Controls

In today's enterprise organization, privilege is everywhere. Traditional distinctions between privileged and workforce identities are becoming increasingly blurry as any identity can become privileged under certain conditions. For example, employees or authorized third-parties may be accessing applications with sensitive data as part of their day-to-day activities. Therefore, organizations adopting Zero Trust — where each identity is verified and access to resources is based on least-privilege principles (PoLP) — must unify their identity and access management (IAM) and PAM programs.

In a unified identity environment, organizations can combine single sign-on (SSO), adaptive multi-factor authentication (MFA) and PAM solutions to build defense-in-depth strategies to secure all identities. Companies should leverage SSO to enable secure access to multiple applications with a single set of credentials and to reduce the attack surface by eliminating password sprawl and providing visibility into access activity.

At the same time, organizations should implement adaptive MFA to validate every user, applying access controls and authentication factors that correspond to the user's risk profile. As a best practice, adaptive MFA should be required to access all resources within an organization, including web apps, VPNs, endpoints, servers and privileged accounts.

Finally, organizations should integrate SSO and MFA with PAM solutions to lock down the highest risk and entitled accounts in an organization. PAM solutions can discover, onboard and centrally manage privileged accounts, credentials and identities while enforcing approval workflows governing access to those accounts. Session isolation and monitoring capabilities can prevent the spread of malware and create clear audit trails to satisfy compliance requirements. Recording those high-risk sessions adds an additional layer of visibility into the actions attempted or taken while in use.

Look for a PAM solution that can...

1. Integrate with IAM to unify privilege and identity controls like SSO and MFA.
2. Enforce strong authentication for access to sensitive resources.
3. Let you manage credentials for both privileged and workforce users.

4. Hybrid Infrastructure Support

Until recently, many enterprises either had in-house infrastructure or relied upon an external solution. As cloud offerings have become more pervasive, businesses need both types of infrastructure to coexist within the enterprise architecture.

Many organizations have established systems that are not designed for cloud environments, and they often use a 'lift-and-shift' approach to migrate them without re-architecting them. These systems, whether on-premises or in the cloud, require privileged credentials such as passwords or secure shell (SSH)keys to access and manage them. These credentials are essential for security and compliance and should be protected from credential theft and misuse.

PAM best practices, such as automated credential rotation and least privilege access, can reduce the risk of cyberattacks and improve the security posture. Additionally, these practices may also be required for IT security compliance or It's challenging to maintain identities and access control across such a diverse environment. There is risk in not supporting both traditional and enterprise identity security. Without an integrated and cohesive solution, customer needs could go unfulfilled, hackers could exploit a technical gap or critical services could be unsupported.

The right PAM solution enables an evolving set of hybrid technologies that drive operational efficiencies across all identities, infrastructure and applications for hybrid, multi-cloud and SaaS workloads — and does so cost-effectively.

Look for a PAM solution that can...

1. Provide a unified, automated and risk-aware platform across all identities and applications.
2. Seamlessly connect users to on-premises, multi-cloud and SaaS workloads efficiently.
3. Maximize your IT investment by enabling integration with existing applications and a new, evolving infrastructure.

5. Protection of All Identity Types

Businesses are adapting the way they conduct operations, including software design and creation. The integration of development, security and operations (DevSecOps) are changing the model; whereas human administrators once manually processed access control steps, activities are now increasingly done by automated systems — often at network speeds.

Businesses also use digital business. Applied to the right processes, software robot, or machine identities, can improve productivity, quality and accuracy of data and compliance with requirements. For example, robotic process automation (RPA) can manage an increasing suite of sensors, products and tools as part of the "Internet of Things (IoT)." Yet, RPA is different from traditional business automation, and these differences introduce a growing challenge of securing access and the protection of the credentials used by software robots. From traditional business automation these differences introduce a growing challenge of securing access and the protection of the credentials used by software robots.

Managing privileged access is critical to the scalability, efficient maintenance and the continued benefit afforded by software robots.

Your identity security solution must include an effective approach that integrates seamlessly with automation, scripts and workflow-oriented application program interfaces (APIs). These capabilities enable your enterprise to confidently take full advantage of the efficiency and productivity benefits automation technology offers without jeopardizing cybersecurity.

Look for a PAM solution that can...

1. Enable secure vaulting and management of privileged account credentials used by software robots and RPA administrators.
2. Enable just-in-time access through shared accounts and break glass approach.
3. Consistently manage embedded credentials in DevSecOps, cloud and traditional applications.
4. Support automated application lifecycle management, ensuring immediate productivity and reducing IT delays.

6. Secure Experience for All Identities

People are a critical part of securing the enterprise. Any procedure adding complexity or burden to privileged identity and access management brings additional risk, reduces productivity and impedes effectiveness. In contrast, the right solution increases user satisfaction and makes it easy for them to be secure, supporting the right balance of usability and risk management. The customer experience must be frictionless.

Select the PAM vendor that offers identity access and management solutions providing adaptive multi-factor authentication support for both privileged and non-privileged users. As MFA is part of the Zero Trust strategy it strengthens security and streamlines user experiences by selecting the right authentication factors for a particular user based on real-time conditions, behavioral analytics and policies.

IT Team

- Digital vault for access credentials to securely store passwords, secrets, SSH keys and other credentials used by people, applications and machines.
- Credential management and rotation to automatically update and rotate credentials based on policy, reducing the risk of unauthorized access.
- Privileged session isolation, monitoring and recording to to contain threats, prevent malware spread and simplify audits. It also includes threat analytics capabilities to automatically detect suspicious behavior and anomalous activity.
- Protection for on-premises and cloud-based resources from unauthorized access.

Security Team

- Privileged accounts and credentials that employees use to administer systems, Windows domains, applications, CI/CD tools, etc.
- Privileged accounts and credentials that third-party IT service vendors use to remotely administer and support systems and infrastructure.
- Secrets that applications, bots, machines and automation scripts use to access and configure IT resources.
- Endpoint security by removing local administrative rights from endpoints and escalating privileges on-demand.
- Entitlements and identity and access management configurations in public cloud environments.

The right solution experience is one that maximizes self-service capability and allows users to utilize native tools to enhance productivity. It also makes it easy for an increasingly remote workforce to be securely identified, authenticated and authorized as part of a cost-effective and efficient life cycle.

Look for a PAM solution that can...

1. Strike the right balance between frictionless access and effective identity security.
2. Monitor and secure remote access to maximize effectiveness while enforcing least privilege requirements.
3. Support self-service capabilities and automated workflows to enable users to be efficient and productive.

7. Continuous Innovation

While PAM needs are not new, the environments being secured are continually changing. As technology evolves in new and exciting ways, to keep pace with these evolutionary realities you need an identity security partner that is continually innovating. A vendor with a product that only meets today's immediate needs — but that isn't already planning for tomorrow — may not be the most effective partner in the long run.

You are innovating, too, and doing so faster than ever. Today's agile and rapid development processes depend upon effective system integration and access. Without it, continuous integration and deployment pipelines shut down, resulting in delays or disruptions to critical business applications and services for the business and its customers. Your PAM solution must be one that enables interoperability while securing your infrastructure.

PAM solutions at a minimum, should continuously discover, onboard, manage and rotate the credentials of new devices and accounts on the network. PAM programs should isolate sessions accessing devices and accounts, while monitoring and recording sessions, enhancing controls to achieve continuous compliance and oversight. Operational technology (OT) environments and IoT devices pose challenges for PAM programs due to their complexity and lack of visibility. Best-in-class PAM solutions can work with the gateway controlling the devices and industrial control systems in OT environments to access, secure, rotate and centrally manage their credentials. Leading PAM solutions offer identity threat detection and response (ITDR) capabilities such as real-time monitoring, anomaly detection, security event and integrity monitoring, user behavior analytics and regulation compliance monitoring.

Look for a PAM vendor that can...

1. Show a proven track record of continual innovation and technical advances.
2. Consistently address emerging threats and use cases.
3. Make sufficient investment in research and development to improve identity security solutions.
4. Draw upon industry-leading threat researchers dedicated to examining emerging attack techniques to drive improvement for the security community.

8. Safeguards Against Advanced and Evolving Threats

The right solution needs to stay a step ahead of the attackers. As cybercrime becomes smarter, more profitable and organized, your solution needs to help you stay informed and prepared. The U. S. National Security Agency recommends that you consciously operate and defend resources as if the adversary already has a presence within your environment.

Modern businesses are adopting a security-first culture as a best practice, educating users about security risks and tactics adversaries often use to steal credentials and install ransomware and other advanced malware programs. They are weaving security into DevOps processes and making it easier for developers to secure their applications to reduce supply chain vulnerabilities and other risks. They are instituting the principle of least privilege to isolate attacks and contain blast radiuses. And they are conducting Red Team/Blue Team exercises to continuously test and hone their detection and response skills.

In this "assume breach" model, the right PAM solution must assume every identity is untrusted and must apply PoLP practices through dynamic security policies. Many solutions are built to protect inside information and thwart attackers on the outside. The reality is that there is no more "inside" and "outside." The PAM solution must originate with engineers and analysts who understand threat actors' tactics, techniques and procedures (TTPs), staying abreast of new methods that provide effective Identity Security and protect the avenues that an adversary would exploit.

Today's enterprise business needs a technically excellent suite of products backed by proven research into incident prevention, detection and response. As product engineers gain intelligence about hackers' tactics and methods, that understanding should be baked into the solution. That suite will also provide measurable risk reduction to demonstrate an effective return on a solid product and service investment.

Look for a PAM solution that can...

1. Demonstrate success in thwarting millions of ransomware variants.
2. Reduce cost and risk to your enterprise through a successful and continually improving identity security program framework.
3. Enable a Zero Trust approach that leverages adaptive authentication and authorization, supported by a tamperproof audit trail of all activity.

9. Broad Ecosystem

An effective PAM solution should be able to demonstrate that it can draw upon an extensive portfolio of partnerships and alliances. Those relationships enable effective integration and cooperation that protect the business's investment in technology. Integration helps each component do what it does best, while ensuring that the whole system provides security in harmony.

Because identity is the thread that binds every facet of an enterprise's information and technology, the right solution can demonstrate the ability to interoperate with a broad array of applications, services and providers. As systems become increasingly interdependent and as a Zero Trust approach drives increased authentication needs, that integration becomes mission-critical.

Look for a mature product with specific features that include a scalable and resilient architecture, a comprehensive feature set, protection for human and non-human identities, support for hybrid and multi-cloud environments, and integration with other security products as part of a multi-layer defense-in-depth security framework.

Business leaders should be cautious of solutions that may initially seem less costly, yet don't provide sufficient integration or support alliances with other product offerings. Skimping on proven integration techniques or failing to take advantage of experienced service experts can result in stranded technologies and technical debt. A solution without effective integration can introduce system and security risk add complexity and increase development costs.

Look for a PAM solution that can…

1. Deliver certified and supported bi-directional third-party integrations to help maximize the value of your existing assets and services.
2. Help your organization maximize the return on your investment in existing IT infrastructure.
3. Support integration through an extensible platform for everything from homegrown applications to external services.
4. Easily integrate via trusted industry standards and protocols like SAML, REST and OAUTH.

10. Proven Dependability

One of your business's most critical assets is your data, yet that data is likely spread across a wide area of in-house, online and external partner systems. The right solution needs to protect that data against threats to confidentiality, integrity and availability. The right PAM solution partner needs to be one with a proven track record for a visionary product approach, leading-edge customer service and a stable corporate presence.

PAM solutions should also isolate privileged sessions to prevent session hijacking, lateral movement and provide a clear reporting trail for compliance audits and inquiries. Leading PAM solutions provide a common framework and unified administrative tools for managing privileged credentials used by all identities — human and non-human.

As requirements increase regarding privacy and security controls for customers and systems around the globe, regulators and auditors will expect to see a solution that fulfills (or exceeds) data protection requirements.

- Maintain strict governance over access to privileged accounts to defend against cyberattacks and protect against data theft and abuse.
- Provide detailed reporting on privileged account information and usage, simplifying compliance audits and risk assessment exercises.
- Automatically detect anomalous behavior to identify in-progress attacks in real-time, accelerate incident response and simplify incident reporting.
- Mitigate the fact that many users can see and/or take actions with sensitive data but shouldn't be able to. These identities are prime targets for attackers.

When deployed in conjunction with other security systems and best practices, PAM solutions help you satisfy audit and compliance requirements for government and industry regulations. Effective PAM programs can help improve your bottom line and help you avoid costly financial penalties.

Look for a PAM vendor that can...

1. Demonstrate years of industry experience resulting in proven success with numerous customers in your industry.
2. Demonstrate industry leadership and recognition by leading industry analysis firms like Gartner and Forrester.
3. Help you ensure conformance and compliance through tools and services that are recognized and trusted by regulators, auditors and cyber insurers.

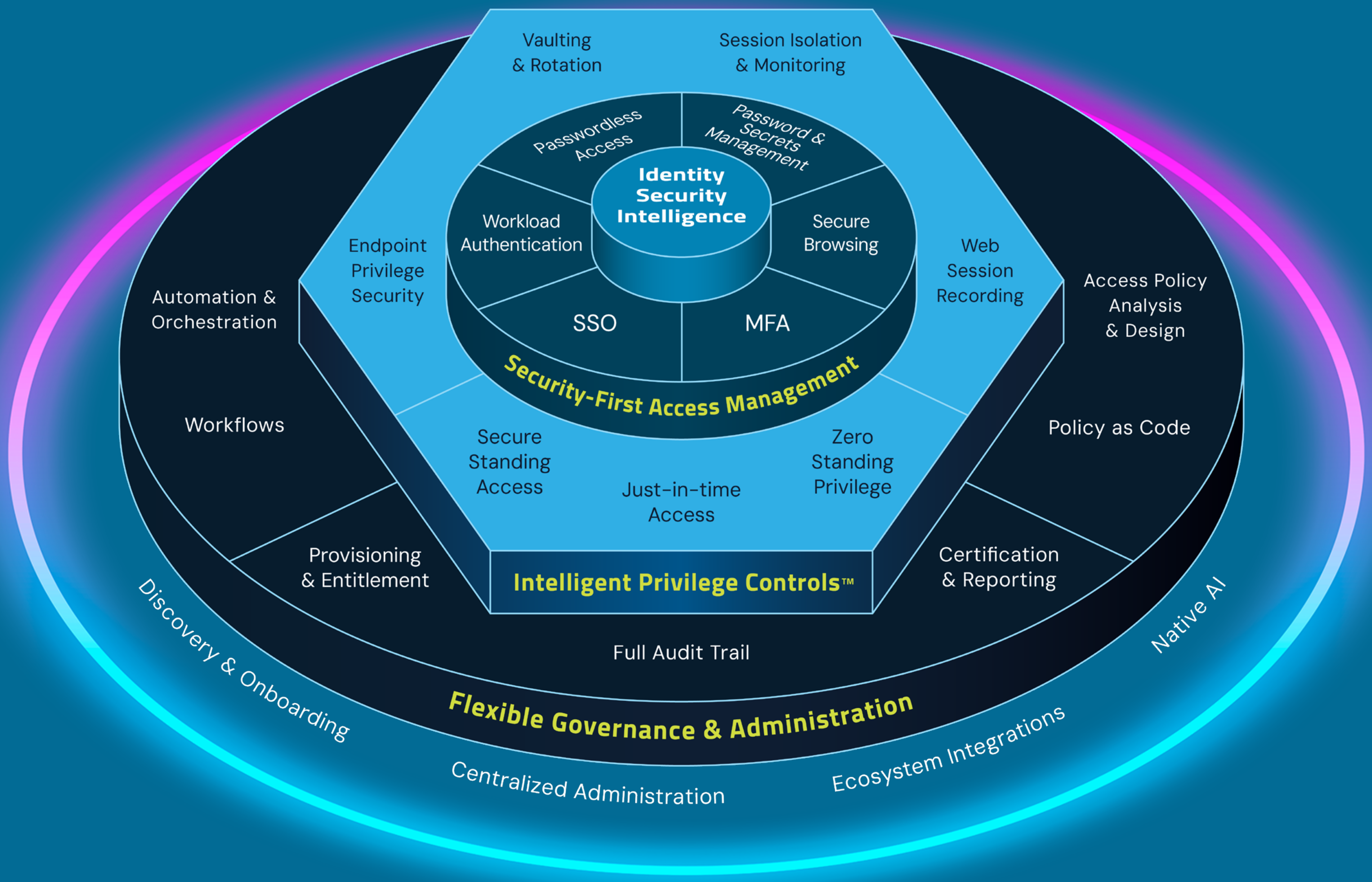
The CyberArk Identity Security Platform is centered on intelligent privilege controls and threat protection across all human and machine identities for enhanced security and operational efficiency. CyberArk is the only vendor with an identity security platform that can offer customers the flexibility to provide standing access, just-in-time access (JIT) or Zero Standing Privileges depending on the identity type and the specific targets needed to be accessed. The platform is based on a set of foundational shared services, including AI-powered Identity Security Intelligence, that delivers a unified user experience through a single admin portal and enhances value with robust automation and analytics. Through our vast partner network and out-of-the-box integrations, CyberArk supports each organization along every step of their identity security journey, while helping them maximize existing security investment.

Identity security offers organizations the peace of mind that their most critical assets are secure while accelerating business agility. But putting a plan in place that effectively secures the expanding number and types of identities and their access can feel daunting. The CyberArk Blueprint was designed with this in mind, allowing organizations to better understand the attack chain, assess their own security, educate themselves on Identity security best practices, and ultimately help them build a plan to measurably reduce risk. You don't have to go it alone, and the CyberArk Blueprint is here to be your companion for the journey ahead.

Accelerate your security with the CyberArk Blueprint:

1. Understand the attack chain.
2. Assess your security posture.
3. Build your identity security plan.
4. Learn use case best practices.

CyberArk Identity Security Platform


Vaulting & Rotation
Session Isolation & Monitoring
Passwordless Access
Password & Secrets Management
Identity Security Intelligence
Workload Authentication
Secure Browsing
Endpoint Privilege Security
Web Session Recording
SSO
MFA
Security-First Access Management
Automation & Orchestration
Access Policy Analysis & Design
Workflows
Policy as Code
Secure Standing Access
Just-in-time Access
Zero Standing Privilege
Provisioning & Entitlement
Certification & Reporting
Intelligent Privilege Controls™
Full Audit Trail
Flexible Governance & Administration
Discovery & Onboarding
Centralized Administration
Ecosystem Integrations
Native AI

Conclusion

The threat landscape changes so quickly that organizations must have confidence both in the product as is and the vendor's ability to innovate and shape the PAM solution as changes necessitate. Today's PAM programs face an increasingly vast and dynamic threat landscape, upended by innovation such as AI, and reshaped by new identities, environments and attack methods. Preventing cyberattacks targeting your most valuable assets and data has become critical to any enterprise. Protecting your credentials and secrets, and managing privileged access is a requirement. Adopt the CyberArk PAM solution to secure privileged credentials and secrets wherever they exist: on-premises, in the cloud, and anywhere in between to help thwart security breaches and reduce the risk of financial and reputational damage to your organization.

Are you ready to build your roadmap to PAM success? Visit www.cyberark.com to learn more and schedule your personalized demo today!

REQUEST A DEMO

CyberArk is the global leader in identity security. Centered on intelligent privilege controls, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow us on Twitter via @CyberArk, LinkedIn or Facebook.

©Copyright 2024 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.

THIS PUBLICATION IS FOR INFORMATIONAL PURPOSES ONLY AND IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER WHETHER EXPRESSED OR IMPLIED, INCLUDING WARRANTY OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT OR OTHERWISE. IN NO EVENT SHALL CYBERARK BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND IN PARTICULAR CYBERARK SHALL NOT BE LIABLE FOR DIRECT, SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE OR LOSS OF USE, COST OF REPLACEMENT GOODS, LOSS OR DAMAGE TO DATA ARISING FROM USE OF OR IN RELIANCE ON THIS PUBLICATION, EVEN IF CYBERARK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. | U.S., 04.24 Doc: TSK-6983(6210)

CYBERARK®
The Identity Security Company™