CYBERARK®
The Identity Security Company™

WHITEPAPER

CyberArk Privileged Access Management Solutions

The industry’s most complete platform reduces risk created by privileged identities, credentials and secrets.

Table of Contents

Privileged Access Management — an Identity Security Cornerstone

IT runs on privileged access. Organizations rely on identities with powerful access rights — known as privileged access — to set up, maintain and run the infrastructure and services powering their digital initiatives. Examples include accounts used to access domain controllers, databases, virtual machines (VMs) in cloud environments, admin consoles for cloud services and even web applications that host sensitive data.

And identities beyond administrators also have high-risk privileged access. Developers that build applications, third-party vendors working on IT projects and even workforce employees with access to sensitive data or systems all have privileged access.

As attackers wreak havoc with advanced cyberattacks around the world, they're targeting valuable enterprise assets. At the same time, modern organizations are digitally transforming their businesses with cloud-first strategies, increasing consumption of SaaS apps and investing heavily in developing their own customer-facing apps.

While critical for business productivity, these initiatives widen the attack surface. Each new environment and digital initiative create new human and machine identities that can gain privileged access under certain conditions, establishing new pathways for attackers to target.

Once attackers get in, they seek access to an organization's most sensitive data with the intent to cause costly harm. Compromising privileged identities can lead to damaged reputations, financial losses and stolen intellectual property. Malicious insiders within an organization can also divulge sensitive information to the public or plant seeds to cause internal damage.

Virtually all **(99%)** respondents agree they'll face an identity-related compromise in the year ahead, and **58%** say this will happen as part of a digital transformation initiative such as cloud adoption or legacy app migration.[1]

Privileged identities and the accounts they use to access critical resources represent one of the largest security risks an organization faces today. Identities with privileged access continue to grow across organizations, for both employees and external vendors in all departments, not just IT admins. Under certain circumstances, every member of the workforce (employees and vendors), and/or machine identity can become a privileged user and ultimately gain access to sensitive business applications, systems and internal resources. It's clear that privileged identities are top targets for attackers. Here are a few reasons why:

- Privileged accounts and credentials exist in nearly every networked device, database, application and server on-premises, in the cloud and throughout the DevOps pipeline.
- Privileged access used by both human users and machine identities enables all-powerful access to confidential data and systems.

[1] CyberArk 2023 Identity Security Threat Landscape Report, April 2023

- Many privileged accounts have shared administrative access, making their users anonymous.
- Privileged accounts have sweeping entitlements, far beyond what is needed for the everyday user to perform their job function. It is especially challenging to restrict unnecessary privileges on endpoints and in cloud-based development environments, where fast software delivery is the top priority.
- Privileged accounts go unmonitored and unreported — and therefore unsecured.
- Privileged accounts best practices differ hugely between cloud service providers (CSP). This places a huge burden on the identity security teams responsible for building and enforcing access control policies.
- Privileged access to today's environments such as public cloud services is a comparatively new challenge with limited established best practice. This in many cases results in cybersecurity debt.

Privilege must be secured wherever it exists, whether in explicitly labeled privileged accounts or for permissions used by workforce or machine identities that grant access to sensitive information. Anyone, or anything, in possession of a privileged account could control an organization's resources, disable security systems and access vast amounts of sensitive data. As IT infrastructures grow more dynamic and spread across hybrid and multi-cloud deployments, all signs point to privilege misuse worsening in the future unless organizations take action now.

Best practices dictate that organizations should incorporate securing all identities – particularly those with explicit privileged access – into the core of their security strategy. Managing and securing privileged access is an enterprise-wide security challenge that requires consistent controls to protect, monitor, detect, alert and respond to all privileged activity that presents material risk.

Privileged Access: The Keys to the IT Kingdom

Privileged credentials are the keys to the IT kingdom. They are required to unlock privileged accounts and sought out by external attackers and malicious insiders as the primary way to gain direct access to the heart of the enterprise. As such, an organization's critical systems and sensitive data are only as secure as the privileged credentials required to access these assets.

Most organizations today rely on a mix of privileged credentials such as passwords, API keys, certificates, tokens and SSH keys to authenticate users and systems to privileged accounts. All these credential types must be securely stored and rotated. All use of credentials should be additionally authenticated for each use with multifactor authentication (MFA). If left unsecured, attackers can compromise these valuable secrets and credentials to gain possession of privileged accounts and advance attacks or use them to exfiltrate data. As some organizations begin to protect passwords, attackers, in their constant journey to find the path of least resistance, have shifted their attack methods to SSH keys, which are often overlooked.

Privileged credentials evolve quickly to privileged access when faced with cloud workloads and services. The expectation of cloud developers is that of federated access – where their identity, defined in the enterprise's IDaaS platform is federated into every CSP the enterprise uses and matched with entitlements. Some of these entitlements may come with higher risk. Attackers understand that a user's SSO credentials now might represent access to near unlimited opportunity within an enterprise's cloud accounts. Identity is the first route into a cloud breach as reflected in IBM's Cloud Threat Landscape report where security researchers identified that 36% of attacks responded to by IBM's incident response teams with valid credentials.

Organizations must adopt a privileged access management (PAM) strategy that includes proactive protection and monitoring of all use of privileged secrets, credentials and roles.

Guidance from the Trusted Advisor in Privileged Access Management

CyberArk is the leading identity security provider and recognized creator of the PAM market. Built on a foundation of securing privileged access, the CyberArk Identity Security Platform helps organizations secure all identities with high-risk access to critical business data and infrastructure with the right level of privilege controls. As a global organization, CyberArk combines over 20 years of knowledge and experience and is uniquely positioned to deliver the CyberArk Blueprint to the market.

CyberArk solutions are trusted by over 8,000 customers, including more than 50% of the Fortune 500, across a wide range of industries including financial services, insurance, manufacturing, healthcare and tech.

CyberArk is widely recognized as a leader in identity security by leading industry analysts.

CyberArk security services and customer success organizations have decades of real-world implementation and support experience, and have a detailed, first-hand understanding of PAM risks and best practices.

CyberArk Red Teams can help organizations prepare against cyberattacks by emulating threat actors attacking their networks and trying to gain access to their most valuable assets. They also help customers strengthen security and improve response time against Cyberattacks.

Additionally, CyberArk draws on the insights of its CyberArk Labs, its threat research and innovation lab. CyberArk Labs produces groundbreaking research that examines emerging attack techniques, driving greater awareness and industry collaboration while helping to improve the overall security posture of companies everywhere. The team is made up of an elite group of white hat hackers, intelligence experts and security leaders that examine post-exploit methods to understand the attack chain and the movement of attackers so they can more effectively defend against them.

Are You Underestimating Your Level of Risk?

In our CyberArk 2023 Identity Security Threat Landscape report[2], we discovered 63% of respondents admit that the highest sensitivity access for employees is not adequately secured. In the same vein, 74% of respondents are concerned with confidential information loss stemming from employees, ex-employees and third-party workforce. Privileged access for machine identities is even more of a risk — respondents reported 68% of non-human identities or bots have access to sensitive data.

If not properly secured, these identities can easily fall prey to popular attack methods like malware, DDoS and brute force attacks. Malware requires admin access to gain persistence; privileged access without vigilant management and session isolation creates an ever-growing attack surface around privileged accounts.

Compliance: To Meet or Not to Meet

As the risk of advanced threats increases, compliance regulations, standards and frameworks such as PCI DSS, SOX, NIST, NIS 2, NERC CIP, HIPAA, GDPR, CCPA and SWIFT CSCF, have increased their requirements to control, manage and monitor privileged access. Requirements differ across these frameworks, but nearly all require implementation of least privilege access, defense-in-depth authentication, risk-based credential management, session monitoring and identity threat detection measures.

Organizations that do not fully understand their privileged landscape face the prospect of audit failure resulting in steep fines and penalties and more importantly, remaining vulnerable to a serious breach without a PAM strategy.

Who Are Your Privileged Users?

Enterprises tend to overlook the vast array of identities with access to privileged information. The truth is that there are not enough policies set to ensure that identities have only the right level of access to the systems and information they need to perform their jobs. This results in anonymous, unchecked access to privileged accounts and sensitive information which leaves the enterprise open to potential compromise that could cripple an organization.

- **IT / Systems administrators**. For almost every device in an IT environment (every endpoint and server), there are shared and built-in privileged accounts with elevated privileges and unfettered access to its operating systems, networks, servers and databases. Teams of systems administrators and cloud operations professionals that build and maintain IT infrastructure are the primary users of these privileged accounts, which grant the most powerful (and highest-risk) access in the enterprise.
- **External vendors.** Nowadays, every organization relies on a network of trusted third-party vendors to complete critical business tasks and maintain business operations. Due to the complexities of managing and provisioning access to workers that are not a part of the organization, privileged access is often granted to perform a job function allowing contractors to work under a cloak of anonymity. Once inside, remote vendors have unrestricted access similar to any "standard" privileged user and can elevate privileges to access sensitive data throughout the organization.

[2] CyberArk 2023 Identity Security Threat Landscape Report, April 2023

- **Developers**. Developers are challenged to build the software that drives the customer experience for every business. Trends like platform or site reliability engineering have pushed developers into being responsible for their hard work as it runs in production. Developers collect privileged access to numerous environments and platforms in a quest to preserve their productivity and velocity. Any attempt to control this privileged access without careful consideration to the impact will be met with resistance from developers, who are empowered to move as fast as possible. According to the 2023 CyberArk Threat Landscape report, 77% of respondents say developers have too many privileges — making these human identities highly attractive targets.
- **Application or database administrators**. Application and database administrators are granted broad access to administer the systems to which they are assigned. This access allows them to also connect with virtually any other database or application found in the enterprise.
- **Workforce users**. Senior-level executives and IT personnel with sensitive information have long been targets of cyberattacks. But as organizations store more of their sensitive data in cloud services and SaaS apps, the lines between traditionally privileged users and the workforce have blurred. Workforce users now often require selective privileged access to cloud-hosted resources or sensitive records within SaaS applications. In some teams, marketing, HR or finance professionals own their applications. This privileged access can't be overlooked. In the hands of the attacker, workforce user credentials could put sensitive information like corporate financial data, intellectual property and regulated customer data at risk.
- **Local admin accounts on endpoints and servers**. Endpoint privilege security solutions help enforce role-specific least privilege for Windows, macOS and Linux workstations and server. Far too many companies still privilege end users with local admin access to run menial tasks like install software on their laptops or setup a printer. Removal of local admin rights results in users operating under standard user accounts while applications are elevated just-In-time. Security controls are protected from tampering by users while applications are controlled and monitored to create an audit trail and significantly reduce the attack surface.
- **Applications and machine identities**. Machine identities like applications require privileged credentials, known as secrets, to communicate with other applications, scripts, databases, web services and more. These accounts are often overlooked and pose significant risk, as their credentials are often hard-coded and static. A hacker can use these credentials as attack points to escalate privileged access throughout the organization.
- **DevOps and automation tools**. DevOps pipelines enable organizations to achieve high levels of agility by automatically building and deploying services and applications. To access data and other applications and services, these services require secrets and other credentials which must be secured. Additionally, a typical DevOps pipeline is supported by several powerful tools. Credentials granting access to these admin consoles must also be protected.

Policy First: Aligning Risk Management with Business Objectives

Best practices dictate that organizations create, implement and enforce PAM policies to reduce the risk of a serious breach. Effective enterprise security and compliance begins with well executed business policy. A policy first approach ensures that the exposure to external threats, insider threats and privilege misuse is reduced, and the organization can meet strict government and industry compliance regulations.

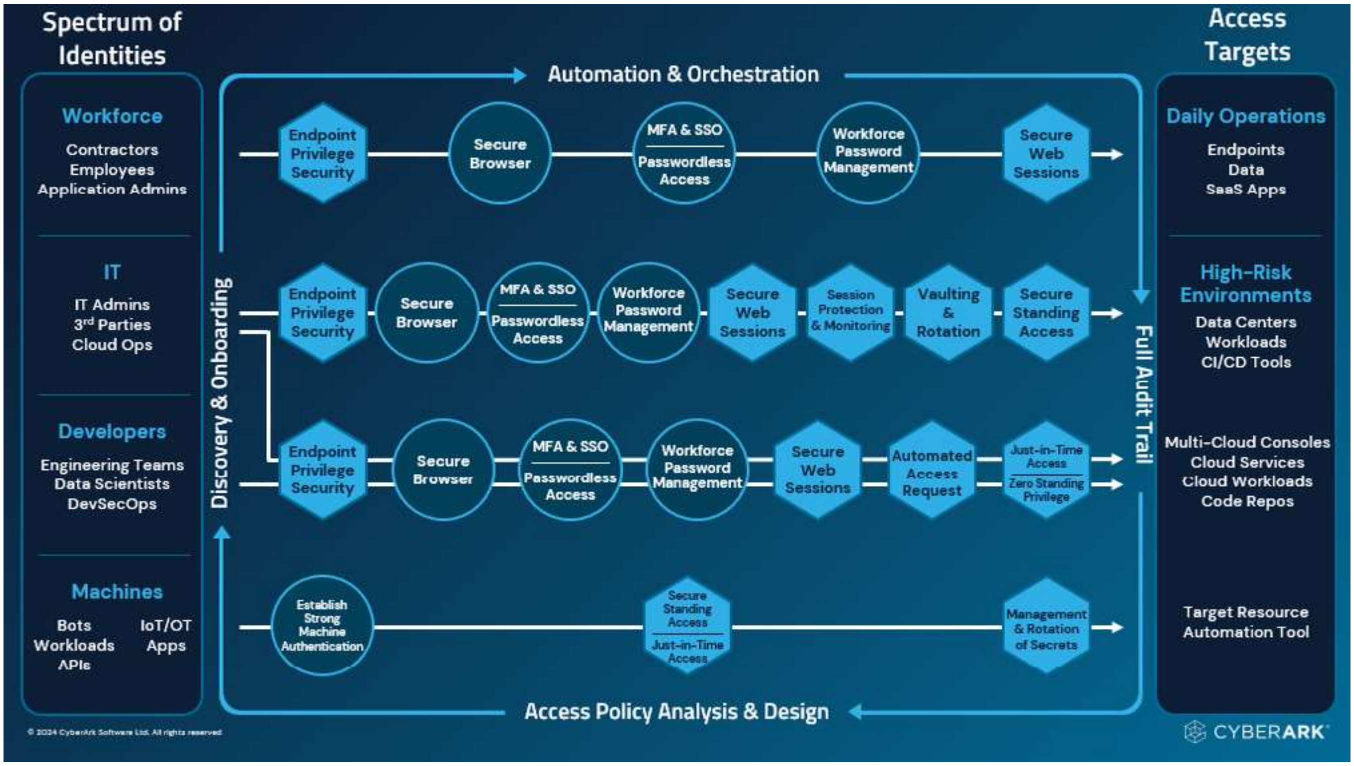
CyberArk PAM Solutions

CyberArk offers a complete set of capabilities for ZSP to secure standing and just-in-time (JIT) privileged access to critical systems and assets by applying the right level of privilege controls. These systems include CyberArk PAM solutions which span on-premises, cloud or multi-cloud, hybrid infrastructure, operational technology (OT) and industrial control systems (ICS) environments as well as the DevOps pipeline.

The following are recommended steps to protect your organization's privileged access:

- Discover all of your privileged identities, accounts and credentials.
- Protect and manage privileged credentials and secrets used by human and machine identities.
- Control, secure and monitor privileged access to servers and databases, SaaS applications and cloud consoles.
- Provide least privilege access on workstations and in the cloud for business users and IT administrators.
- Control applications on endpoints and servers.
- Use real-time privileged access intelligence to detect and respond to in-progress attacks.

CyberArk PAM solutions also enable users to automate and simplify PAM tasks via REST APIs such as account workflow, onboarding rules, permissions granting, and more. Low-code and no-code automation of lifecycle management tasks also helps improve efficiency of PAM efforts, especially for resource-strained teams.



The CyberArk Identity Security Platform delivers capabilities tailored for the needs and risk-levels of all identities.

CyberArk Privileged Access Manager

CyberArk Privilege Cloud® | CyberArk Privileged Access Manager Self-Hosted

CyberArk Privileged Access Manager, which can be deployed as a service or as self-hosted software, helps prevent the malicious use of privileged credentials such as passwords and SSH keys and brings order and protection to vulnerable accounts. The solution secures privileged credentials based on defined PAM policy and controls who can access which credentials and when. This automated process reduces the time-consuming and error-prone task of manually tracking and updating privileged credentials to easily satisfy audit and compliance standards.

- Guard against unauthorized users accessing privileged account credentials and ensure authorized users have the necessary access for legitimate business purposes.
- Update and synchronize privileged passwords and SSH keys at regular intervals or on-demand, based on policy.
- Discover and protect privileged credentials used in hybrid and cloud environments, as well as throughout the DevOps pipeline and on loosely connected endpoints off-network.
- CyberArk PAM solutions provide advanced capabilities for just-in-time privileged access and implementing Zero Standing Privileges.

Providing access with ZSP advocates for the removal of persistent access privileges for users within an enterprise network. It leverages the same concept of just-in-time access, requiring users to obtain access as and when needed instead of granting continuous access rights, but extends past that using the principle of least privilege.

Access with Zero Standing Privileges helps solve the challenges of account takeover, credential theft and identity compromise, both by removing standing privileges to limit implicit trust and providing several levels of control to verify access.

Rather than elevating the requested user to an administrative role, security teams can instead allocate just the permissions the user needs to accomplish the task required. By elevating access just in time with zero standing privileges, we can reduce the risk of lateral movement as there is no credential with always-on access and there are no permissions that could be exploited if that credential falls into the wrong hands.

Isolation, control and real-time monitoring and recording for privileged sessions

The service secures, isolates, controls and monitors privileged user access and activities to critical Unix, Linux, and Windows-based systems, databases, virtual machines, network devices, mainframes, websites, SaaS applications, cloud consoles and more. It provides a single-access control point, helps prevent malware from jumping to a target system through the isolation of end users, and records every keystroke and mouse click for continuous monitoring.

Video recording of user sessions provides a complete picture of behavior with search, locate and alert capabilities on sensitive events that eliminate the need to filter through logs. Real-time monitoring helps provide continuous protection for privileged access as well as automatic suspension and termination of privileged sessions if any activity is deemed suspicious. The solution also provides full integration with third-party SIEM solutions with alerts on unusual activity.

Session Isolation + Monitoring

- Helps protect privileged passwords and SSH keys from advanced attack techniques such as key-stroke logging and pass-the- hash attacks.
- Creates an indexed, tamper-resistant recording of privileged sessions for audit and compliance.
- Offers command line control and native SSH access while still providing secure access to privileged users using either passwords or SSH keys.
- Provides Active Directory bridge capabilities that enable organizations to centrally manage Unix users and accounts linked to AD through the CyberArk platform.

CyberArk Privilege Cloud now enhances support of secure, VPN-less, native access with either vaulted credentials or with zero standing privileges to target systems, including: databases, Windows, *NIX and Kubernetes systems. These enhancements enable increased security and reduced Total Cost of Ownership (TCO).

Detect, alert and respond to privileged threats and malicious activity

Identity threat detection and response (ITDR) capabilities in CyberArk PAM solutions allow organizations to detect, alert and respond to anomalous privileged activity indicating an in-progress attack. Both through direct capabilities and bi-directional integrations with XDR and SIEM solutions, CyberArk helps organizations detect and respond to a wide variety of identity-centric attacks.

CyberArk PAM solutions collects a targeted set of data from multiple sources, including the CyberArk Vault, SIEM solutions, and the network to apply statistical and deterministic algorithms to identify and terminate early indications of compromised privileged access.

CyberArk Privilege Cloud uses the CyberArk Identity Security Intelligence services, part of the CyberArk Identity Security Platform, to automatically detect multi-contextual anomalous user behavior and privileged access misuse. Detection algorithms cover both workforce access and privileged access attempts for an organization's employees, allowing organizations to centrally correlate access attempts to analyze risk. The service provides real-time alerts and recommends actions to accelerate identification, analysis and response to high-risk events.

Identity Threat Detection and Response capabilities in CyberArk PAM solutions:

- Detect and alert in real-time with automatic response to detected incidents.
- Identify privileged access related anomalies and malicious activities with the ability to detect in-progress attacks.
- Adapt threat detection to a changing risk environment with data correlation and highly customizable risk scoring.
- Enhance the value of existing SIEM solutions with out-of-the-box integrations.
- Improve auditing processes with informative data on user patterns and activities.

CyberArk Vendor Privileged Access Manager

CyberArk Vendor PAM is a solution that provides just-in-time VPN-less, passwordless privileged access for third-party vendors. Vendor PAM is a SOC 2 Type 2 compliant and SOC 3 certified service. With this comprehensive, SaaS-based solution, customers can achieve the following:

- Securely connect third-party vendors to vaulted infrastructure and cloud consoles just-in-time with ZSP.
- Ensure third-party remote access is inherently secure and aligned with Zero Trust and least privilege principles.
- Reduce the burden on IT related to provisioning, maintaining, and deprovisioning access for third-party vendors and contractors.
- Gain full visibility of third-party activity and record user activity to streamline compliance pertaining to third-party access.

Vendor PAM eliminates the need for legacy approaches to securing third-party access, such as VPN clients, passwords, and agents that can add risk, create administrative complexity, and frustrate end-users. The solution combines Zero Trust access, biometric MFA, JIT provisioning, session management and recording for security and security and audit and compliance. Vendor PAM enables JIT provisioning of authorized third parties as well as secure access to web applications that are managed by CyberArk PAM or CyberArk Identity.

CyberArk Vendor PAM includes an offline access capability providing authorized users the ability to securely obtain credentials during network or power outages, in air-gapped environments, and other situations in which they can't reach CyberArk PAM. With the CyberArk mobile app, credentials are securely stored on an authorized third-party's smartphone, so the user can get a hold of them immediately after completing the biometric authentication, with credential usage recorded for audit and compliance purposes.

The solution is available to CyberArk PAM customers for a **30-day free trial**.

CyberArk Secure Cloud Access

CyberArk Secure Cloud Access is a CyberArk Identity Security Platform service that provisions access just-in-time with ZSP to cloud management consoles and services running in Amazon Web Services (AWS), Azure and Google Cloud Platform (GCP) environments. CyberArk Secure Cloud Access elevates access just-in-time to roles scoped with just enough permissions to adhere to the principle of least privilege and meet the risk reduction benefits of having zero standing privileges.

By elevating access just-in-time, CyberArk Secure Cloud Access enables technical teams with the permissions to do their job while reducing the risks of credential theft and excessive access. CyberArk Secure Cloud Access allows users to launch sessions that are protected and monitored natively removing the need to go through a jump server. This enables seamless access while reducing risk and keeping visibility of end user behavior to satisfy audit. In the event of a critical situation, Engineers can request on-demand elevation of access, enabling them to securely request and rapidly receive the elevated entitlements needed to save the day.

CyberArk Endpoint Privilege Manager

CyberArk Endpoint Privilege Manager (EPM) is a SOC 2 Type 2 compliant solution designed to prevent attacks that originate on the endpoint by removing local administrative rights on the endpoint (Windows and Mac desktops/laptops). The solution allows for JIT elevation and access on a “by request” basis for a pre-defined period of time, with full audit of privileged activities. Full administrative rights or application-level access can be granted, with access being time limited and revoked as needed.

The solution reduces configuration drift on endpoints with minimal impact to the end user, enabling IT operations and security teams to allow approved applications to run, and restrict the ones that are not approved. These unknown applications can run in a 'Restricted Mode' which prevents them from accessing corporate resources, sensitive data or the Internet. These applications can be sent to the CyberArk Endpoint Privilege Manager cloud-based application analysis service, which in turn can integrate with data feeds from technology partners including Checkpoint, FireEye, Palo Alto Network, as well as other services for additional analysis.

CyberArk EPM also secures the browser and credentials with 50 different credential and security token protection rules. CyberArk Endpoint Privilege Manager helps prevent cookie stealing, web session hijacking, browser password dumping and operating system and third-party application **credential compromise**. When deployed on a server, especially a domain controller, CyberArk EPM defends against high-impact token manipulation and compromise attacks, such as Golden Ticket, Golden SAML and others.

CyberArk Endpoint Privilege Manager reduces security risk and protects against threats by:

- Enabling organizations to remove administrative rights from everyday business users without halting productivity, help protect against threats that take advantage of local admin access and seamlessly elevate privileges based on policy when needed to run authorized applications or commands.
- Protecting against malicious applications entering and propagating throughout the environment, enabling users to run unknown applications in a "Restricted Mode" to help the workforce stay productive and safe.
- Detecting and blocking attempted theft of Windows credentials and other popular credential stores, thus preventing propagation through the environment.
- Detecting and responding to ransomware before the attack can cause significant damage.
- Integrating seamlesslly with partner technologies to improve threat intelligence by integrating third-party data into an endpoint privilege manager platform, including threat intelligence, asset data and other security health indicators.
- Detecting an insider threat or an attacker impersonating an insider who is trying to remain undetected with privilege deception capabilities.

The solution is available for a **30-day free trial**.

Take Your PAM Program Further with Integrated Access and Secrets Management

It's not just IT and developer teams that have high-risk access. Integrating CyberArk access management and secrets management capabilities can help organizations centrally and efficiently protect the workforce and machine identities that pose the greatest risk to the enterprise.

Integrated Access Management and Identity Management

CyberArk Identity is a suite of solutions designed to simplify identity and access management in enterprises, providing Workforce and Customer Access and Identity Management solutions in a single offering. Businesses can use CyberArk Identity to authenticate, authorize and audit access to applications and IT systems with a security-first mindset. Benefits of integrating CyberArk Identity include:

- Reducing risk by protecting workforce and customer credentials.
- Applying extra layers of authentication to high-risk access.
- Automating the management of digital identities across enterprise IT environments.
- Centrally granting, maintaining and analyzing access to right-size permissions on the journey to least privilege.
- Automating access certification and reporting for all identities across the enterprise.

CyberArk Secure Browser

The CyberArk Secure Browser safeguards your organization's most valuable resources by extending market-leading identity security protections to the web browsing experience. CyberArk Secure Browser is hardened to protect sensitive resources from attacks all while offering end users a familiar and productive experience. It is designed for the enterprise and takes an identity-centric approach to securing access to all resources and data, for all identities from all devices.

The CyberArk Secure Browser provides users with secure, one-click access to privileged infrastructure targets or web applications with "launchpad" style widgets. The CyberArk Secure Browser helps eliminate existing security gaps between consumer-focused browsers and SaaS applications, endpoint-based controls and identity providers. CyberArk Secure Browser helps reduce risk and connect to target systems, adding strong data loss prevention, oversight, auditing and privacy capabilities to the browsing experience.

DevSecOps Solutions

CyberArk Secrets Management is an essential part of the CyberArk Identity Security Platform, and provides robust enterprise-grade capabilities for centrally managing and securing non-human credentials for almost all application types. The solution integrates with existing systems to help organizations protect and extend established security models and practices.

The solution enables organizations to centrally secure, manage and rotate identities for the broadest range of application types from cloud native containerized apps to commercial-off-the-shelf (COTS) applications robotic process automation (RPA), statics (N-tier) and mainframe apps. CyberArk Secrets Management secures credentials used across:

Cloud environments and cloud-native applications	Contemporary, dynamic and ephemeral applications leveraging containers, serverless compute functions, cloud-native secret stores (Amazon Web Services, Azure, Google Cloud Platform) and microservices architecture.
DevOps tools, CI/CD pipelines and the software supply chain	Agile software development and delivery tools, CI/CD automation platforms, configuration management tools and service orchestration solutions.
Automation tools and scripts	Various scripts and tools that automate IT and other administrative functions, such as onboarding new identities into an enterprise's privileged access management solution.
Commercial off-the-shelf (COTS) and ISV Applications	Third-party software products like business intelligence solutions, RPA tools and vulnerability scanners that can be hosted internally or consumed as SaaS solutions.
Internally developed app	Homegrown static or cloud-native apps used for internal or customer-facing purposes, including conventional apps hosted on physical or virtual machines, legacy mainframe applications and application servers and cloud-native apps running on microservices.
IoT and OT device identities	Securely manages the credentials managed by off-the shelf third party IoT management gateway platforms.

Get started with **CyberArk Secrets Management solutions.**

SaaS and Subscription: Flexible Deployment and Consumption Models

To meet each organization's preference, CyberArk offers a variety of flexible consumption and deployment models for both SaaS or on-premises subscription. The CyberArk SaaS portfolio provides secure solutions managed by CyberArk that provide an agile and consistent code train with minimal resource allocation needed to perform upgrades, patches and more. If organizations prefer to self-host and self-manage their software, subscription consumption models provide flexible, short-term licensing that is geared towards optimizing license adoption and consumption. All options provide robust security and make it easy to deploy and expand the security footprint, with the added benefit of consumption models preferred by so many modern organizations.

Establishing PAM Success with the CyberArk Blueprint

To equip customers for success, CyberArk has developed a prescriptive framework to help organizations establish and evolve an effective identity security program to accelerate their success. The CyberArk Blueprint framework guides organizations through their identity security journey by helping security teams understand the identity attack chain, assessing their security posture, learning best practices and building their roadmap.

The CyberArk Blueprint's prescriptive recommendations are designed to defend against the three common identity attack chain stages used to steal data and wreak havoc. The phased security framework closely aligns PAM initiatives with potential risk reduction, helping organizations address their greatest liabilities as quickly as possible.

The CyberArk Blueprint was built with today's IT environment in mind. It prescribes intelligent privilege controls and best practices for organizations across the full spectrum of identities including IT admins, developers, workforce users and machines, as well as the full scope of today's IT environment, including cloud service providers, CI/CD tools, high-risk web applications, infrastructure-as-code and machine workloads.

The CyberArk Blueprint is not just a singular resource; it consists of a broad ecosystem of self-service educational resources and collateral, including videos, whitepapers, toolkits and success knowledge articles. Each component provides best practice guidance across the people, process and technology domains — all designed to help you accelerate your identity security journey.

Learn more about the CyberArk Blueprint.

WHY CYBERARK

- **Most complete identity security platform:** Solves the full range of hybrid to multi-cloud identity security challenges with a security-first approach.
- **Built for the dynamic enterprise:** Enables dynamic enterprises that increasingly rely on cloud-based services and the "new normal" workforce.
- **Broadest integration support:** Offers the most out-of-the-box integrations to solve identity security challenges across the organization.
- **Identity security innovator:** Pioneered the key solution to solve the hardest IT security problem: securing privileged access. Continues to lead the market with dynamic solutions to address new and emerging threats.
- **Proven expertise in securing identities:** Extensive experience and tenure with the world's largest enterprises provides deep and wide institutional knowledge of identity security challenges.

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security solutions for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads, and throughout DevOps pipelines. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com.

CYBERARK®
The Identity Security Company™

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. U.S., 03.24 Doc. TSK-6095

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.