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 — a Real, Pervasive, Threat

Attackers are wreaking havoc across the globe with advanced cyberattacks that directly target the most valuable assets of an enterprise. Modern organizations are digitally transforming their businesses with cloud-first strategies, increasing consumption of SaaS applications and implementing DevOps methodologies. While critical for business productivity, these initiatives widen the attack surface by creating additional human and machine identities that can gain privileged access under certain conditions, establishing new pathways for attackers to target. Forrester estimates that 80 percent of security breaches involve privileged credentials.[1] Once attackers get in, they seek access to an organization's most sensitive data with the intent to cause costly harm. The compromise of 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.

Privileged identities and the accounts they use to access critical resources represent one of the largest security risks an organization faces today. Privileged identities continue to grow across organizations, and privileged access is provisioned to employees and external vendors in all departments, not just IT administrators. 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's 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 accounts used by both human users and non-human/machine identities have all-powerful access to confidential data and systems.
- Privileged accounts have shared administrative access, making their users anonymous.
- Privileged accounts grant sweeping access, 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 the cloud.
- Privileged accounts go unmonitored and unreported – and therefore unsecured.

Privilege must be secured wherever it exists, whether in explicitly labeled privileged accounts or for accounts used by workforce or machine identities that have select 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 spreads across hybrid and multi-cloud deployments, all predictions 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 Credentials – The Keys to the IT Kingdom

Privileged credentials are the keys to the IT kingdom. They are required to unlock privileged accounts and they are 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.

[1] The Forrester Wave™: Privileged Identity Management, Q4 2020

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 of 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.

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

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 privilege, and powered by artificial intelligence-based behavior and risk analytics, the CyberArk Identity Security Platform helps organizations secure access to critical business data and infrastructure, protect a distributed workforce, and accelerate business in the cloud.

CyberArk's Identity Security Platform is built on the pillars of management for Access, Privilege and DevSecOps to deliver authentication, authorization, access and audit in an integrated, seamless manner—enabling security at every step in the Identity Security lifecycle. Our intelligent approach balances the need for better security with end user productivity. CyberArk solutions leverage real-time intelligence and analytics to create a context-based, adaptive approach to the Identity Security lifecycle – for all identities, across all systems and apps, using any device. To mitigate the risk of a serious breach, enterprises need to adopt a security solution with consistent controls that specifically address their privileged access exposure.

Are You Underestimating Your Level of Risk?

In our CyberArk 2022 Identity Security Threat Landscape report[2], we discovered that credential access was the number one area of risk, cited by 40% of respondents. Respondents reported that more than 50% of workforce identities in the enterprise have access to sensitive data. Privileged access for machine identities is even more of a risk - respondents reported 68% of non-humans or bots have access to sensitive data.

If not properly secured, these identities with privileged access 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, NERC- CIP, HIPAA, GDPR, CCPA and SWIFT CSCF, have increased their requirements to control, manage and monitor privileged access.

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.

[2] CyberArk 2022 Identity Security Threat Landscape Report, April 2022

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 actually 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.

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.

Cloud administrators and shadow admins. Business processes, such as finance, HR, and procurement, are increasingly moving critical workloads to the public cloud. The human and machine identities with access to these workloads must be protected and continuously reviewed to implement least privilege access.

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.

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 cyber attacks. But as organizations enable a remote workforce and store more of their sensitive data in cloud services and applications, 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. This privileged access can’t be overlooked. In the hands of the attacker, workforce user credentials could put sensitive information like corporate financial data and intellectual property at risk.

End users. Far too many companies *still* allow their end users to run with local admin access to do menial things like install software and setup a printer. Any IAM user with access to their organization’s public cloud workspaces can be provisioned with thousands of permissions, opening the door to major misconfigurations. In the hands of the wrong person, end user privileged credentials provide the first place for incoming attackers to persist as they begin their journey toward corporate financial data, intellectual property, and other sensitive data.

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. 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

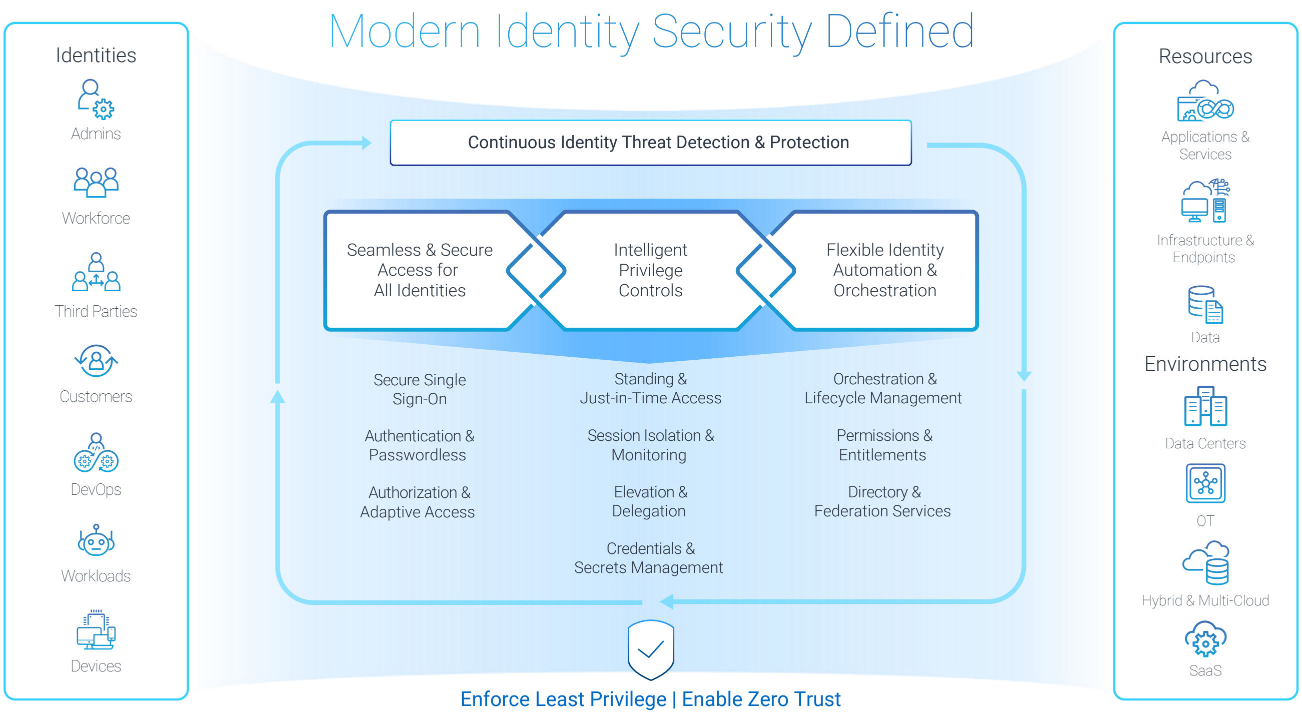
Best practices dictate that organizations create, implement and enforce PAM policies to reduce the risk of a serious breach. Effective enterprise security and compliance begins with well executed business policy. A policy first approach ensures that the exposure to external threats, insider threats and 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 securing standing and just-in-time privileged access to critical systems. These systems include: CyberArk PAM solutions span on-premises, cloud, industrial control systems (ICS) environments as well as the DevOps pipeline.

Recommended steps in protecting your organization's privileged access:

- Set policy first.
- Discover all of your privileged identities, accounts and credentials.
- Protect and manage privileged credentials used by users and applications.
- 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.


Modern Identity Security Defined
Identities
Admins
Workforce
Third Parties
Customers
DevOps
Workloads
Devices
Continuous Identity Threat Detection & Protection
Seamless & Secure Access for All Identities
Intelligent Privilege Controls
Flexible Identity Automation & Orchestration
Secure Single Sign-On
Authentication & Passwordless
Authorization & Adaptive Access
Standing & Just-in-Time Access
Session Isolation & Monitoring
Elevation & Delegation
Credentials & Secrets Management
Orchestration & Lifecycle Management
Permissions & Entitlements
Directory & Federation Services
Resources
Applications & Services
Infrastructure & Endpoints
Data
Environments
Data Centers
OT
Hybrid & Multi-Cloud
SaaS
Enforce Least Privilege | Enable Zero Trust

Privileged Access Manager

Privilege Cloud® | Privileged Access Manager Self-Hosted

Discover, manage and protect privileged accounts and credentials

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.
- Enable users to automate and simplify PAM tasks via REST APIs such as account workflow, onboarding rules, permissions granting, and more.
- Provide security and audit teams with a clear view of which individual users accessed which privileged or shared accounts, when and why.

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.

- Helps prevent the spread of malware using privileged session isolation.
- Helps protect privileged passwords and SSH keys from advanced attack techniques such as key-stroke logging and pass-the- hash attacks.
- Create an indexed, tamper-resistant recordings 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.

Detect, alert and respond to privileged threats and malicious activity

Threat intelligence capabilities in CyberArk PAM solutions allow organizations to detect, alert, and respond to anomalous privileged activity indicating an in-progress attack. PAM Self-Hosted 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.

Privilege Cloud integrates with Identity Security Intelligence – one of the CyberArk Identity Security Platform Shared Services – 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, including bi-directional integration with leading SIEM solutions. The service provides real-time alerts and recommends actions to accelerate identification, analysis, and response to high-risk events.

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.

Vendor Privileged Access Manager

Securely and quickly connect remote vendors to CyberArk. No VPNs, agents or passwords needed

CyberArk® Vendor Privileged Access Manager is a SOC 2 Type 2 compliant service that combines Zero Trust access, biometric multifactor authentication and just-in-time (JIT) provisioning to secure external vendors that require privileged access to critical internal resources. The solution enables security teams to provide external vendors with only the access they need. Vendor PAM fully integrates with the CyberArk Privileged Access Manager solution for full audit, session isolation and remediation capabilities. Vendor Privileged Access Manager is designed to provide fast, easy and secure privileged access to external vendors who need access to critical internal systems.

By not requiring VPNs, agents or passwords Vendor Privileged Access Manager removes operational overheard for administrators and makes organizations more secure.

- Integrates with CyberArk Privilege Cloud and PAM Self-Hosted to provide additional layer of security for critical systems.
- Introduces a more secure solution than traditional token-based or VPN approaches.
- Enables administrators to onboard external vendors Just-in-Time without the need to add them to Active Directory.
- Removes operational overhead associated with managing VPNs, agents and passwords.
- Offers offline access to authorized users to obtain credentials in case of network and power outage, air gapped environments and more.

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

Dynamic Privileged Access

Reduce risk of standing access with Just-in-Time elevation

CyberArk Dynamic Privileged Access is a non-intrusive, agentless solution that provisions JIT access to cloud-hosted Virtual Machines (VMs) as well as on-premises servers, reducing the risk of standing access rights. The service brokers ephemeral sessions based on attribute-based access control policies, enabling organizations to intelligently provision access based on business requirements.

The service provides Just-in-Time (JIT), privileged access to Linux and Windows virtual machines hosted in AWS and Azure lcoud environments, as well as Windows servers on-premises. Ephemeral sessions are fully isolated to prevent the spread of malware, and provisioned according to attribute-based access control (ABAC) policies to drive measurable risk reduction.

Leveraging Dynamic Privileged Access and Privileged Access Manager together allows organizations to holistically secure Just-in-Time and standing privileged access across public cloud and on-premises systems. This enables operational efficiencies for security teams, audit and compliance processes, also advancing Zero Standing Privileges (ZSP) and Zero Trust initiatives.

Cloud Entitlements Manager™

Analyze and remove excessive privileges and permissions across cloud environments

CyberArk Cloud Entitlements Manager is a SOC 2 Type 2 compliant service that reduces risk by implementing Least Privilege across cloud environments. From a centralized dashboard, Cloud Entitlements Manager provides visibility and control of Identity and Access Management (IAM) permissions across an organization's cloud estate. Within this single display, Cloud Entitlements Manager leverages Artificial Intelligence to detect and remediate risky permissions, helping organizations strategically reduce risk without disrupting necessary access for cloud operations. Key benefits include:

- Gain cloud-agnostic visibility of permissions and act swiftly to reduce risk.
- Implement Least Privilege for all human and machine identities throughout the cloud estate.
- Operate cloud permissions securely and efficiently.
- Proactively reduce risk and measure progress.
- Discover shared admin accounts with high privileges and onboard them for management with Privilege Cloud.

Cloud Entitlements Manager requires no dedicated infrastructure and offers unprecedented time to value. Within an hour of registration, users can leverage intelligent recommendations to remediate excessive permissions across their AWS, AWS EKS, Azure, and GCP environments.

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

Endpoint Privilege Manager™

Enforce least privilege on the endpoint

Endpoint Privilege Manager is a SOC 2 Type 2 compliant service 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 through the Application Control feature, 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 Endpoint Privilege Manager's 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.

Endpoint Privilege Manager helps organizations protect against threats that take advantage of unmanaged local admin access. The solution reduces security risk and configuration drift, while reducing help desk calls from end users.

- Enables organizations to remove administrative rights from everyday business users without halting productivity, and seamlessly elevating privileges based on policy when needed to run authorized applications or commands.
- Protects 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.
- Detects and blocks attempted theft of Windows credentials and other popular credential stores, thus preventing propagation through the environment.
- Completely integrated to the CyberArk Application Risk Analysis service to enable automated analysis and timely policy decisions for unknown applications.
- Comprehensive ransomware protection with the ability to detect ransomware with certainty and respond before the attack can cause significant damage.
- Seamless integration with partner technologies improves threat intelligence by integrating third-party data into the endpoint privilege manager platform, including threat intelligence, asset data and other security health indicators.
- Privilege Deception capabilities detect an insider threat or an attacker impersonating to an insider who is trying to remain undetected.

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

Access Management and Identity Management Solutions

Workforce Identity | Customer Identity

Secure access to the entire enterprise, including cloud and on-premises applications, endpoints and VPNs
CyberArk Identity is a SOC 2 Type 2 compliant suite of services designed to help organizations securely manage identity and access for their employees, partners, and customers. CyberArk Identity enables organizations to improve employee productivity, enhance customer and partner experiences, and reduce the risk of weak or default passwords – the primary cause of security breaches.

To expand the value of PAM, CyberArk offers the following Identity Management and Access Management capabilities:

- **CyberArk Identity Single Sign-On:** CyberArk SSO is an easy-to-manage service for one-click access to your cloud, mobile, and legacy apps. CyberArk SSO enables a secure and frictionless sign-in experience for internal and external users that adjusts based on risk. Users simply sign in to a web portal using their existing corporate credentials to access all their assigned applications from one place.
- **CyberArk Identity Adaptive Multifactor Authentication:** CyberArk Adaptive MFA adds an extra layer of protection before access to corporate applications is granted. Leveraging device, network, and user behavior context, CyberArk MFA intelligently assigns risk to each access event and allows you to create dynamic access policies that are triggered when anomalous behavior is detected.
- **CyberArk Identity Flows** is an identity orchestration solution that improves security, efficiency and productivity by automating identity data and events. With Identity Flows, organizations can automate complex identity management workflows and synchronize identity data across diverse applications, directory stores and repositories.
- **CyberArk Identity Lifecycle Management:** CyberArk LCM simplifies routing of application access requests, creation of application accounts, management of entitlements for those accounts, and revoking of access when necessary. With CyberArk LCM, you can enable users to request access to applications from the CyberArk Identity App Catalog, provide specific users the ability to approve or reject these access requests, and automatically create, update and deactivate accounts based on user roles.

- **CyberArk Secure Web Sessions** is a cloud-based service that enables organizations to monitor, record, and audit end-user activity within high-risk and high-value web applications. Security and compliance specialists can use Secure Web Sessions to search recorded sessions using free text input and quickly filter events by users, dates, and actions.
- **CyberArk Workforce Password Management** is an enterprise-focused password manager providing a user-friendly solution to store business application credentials in a centralized vault and securely share them with other users in the organization.

CyberArk Identity is available for a **30-day free trial**.

DevSecOps Solutions

Secrets Manager

Protect, manage and audit the widest range of application credentials across hybrid, containerized and cloud environments

CyberArk Secrets Manager enables organizations to centrally secure and manage, secrets and credentials used by the broadest range of applications, including internally developer applications, COTS, BOTS, automation platforms and CI/CD tools, running in hybrid, cloud-native and containerized environments. Mission critical applications running at scale can securely access high-value resources, including databases and IT infrastructure, to improve business agility while reducing operational complexity.

Loved by security teams and developers, Secrets Manager offers the most out-of-the-box integrations which helps developers simplify securing applications and DevOps environments. Secrets Manager provides organizations with a critical capability to help secure applications and tools across the software supply chain. Additionally, with the CyberArk Identity Security Platform organizations can consistently manage credentials used by human and non-human identities across the entire enterprise.

Secrets Manager is designed to provide a strong security solution that enables organizations to control, manage and audit all non- human privileged access for the broadest range of application types, across the broadest range of environments.

- **For cloud-native applications built using DevOps methodologies:** Conjur Secrets Manager Enterprise provides a secrets management solution tailored specifically to the unique requirements of cloud native and DevOps environments. The solution integrates with a wide range of DevOps tools, PaaS/Container orchestration platforms, and supports hybrid and multi-cloud environments, including native integrations with Jenkins, Ansible, OpenShift, Kubernetes, AWS, Azure and GCP. The solution integrates with the CyberArk Identity Security Platform to provide a single enterprise-wide platform for securing privileged credentials. An open source, developer version is available at **www.conjur.org**.
- **For securing commercial off-the-shelf solutions (COTS):** Credential Providers can rotate and manage the credentials that third-party tools and solutions such as security tools, RPA, automation tools, IT management, etc. need to complete their jobs. For example, a vulnerability scanner typically needs high levels of privilege to scan systems across the enterprise's infrastructure. Instead of storing privilege credentials in COTS solutions, they are managed by CyberArk. To simplify how an enterprise allows third party solutions to access privileged credentials, CyberArk offers the most validated out-of-the-box COTS integrations for solving identity security challenges.

- **For internally-developed traditional applications:** Credential providers help protect high volume, mission critical applications, sensitive business data and simplify operations by eliminating hard-coded credentials from internally developed static applications. The solution provides a comprehensive set of features for managing application passwords and SSH keys, and supports a broad range of static application environments, including application servers, Java, .NET Core, and scripting running on a variety of platforms and operating systems including Unix/Linux, Windows and zOS.

With CyberArk Secrets Manager, enterprises can reduce the attack surface by extending their established security models and practices to secure applications across the organization's entire application portfolio and software supply chain.

- Ensures a comprehensive audit on any access by tracking all access and providing tamper-resistant audit.
- Consistently applies access policies by applying role-based access controls on non-human identities, leveraging integrations with other CyberArk and partner solutions to centralize policy management across the enterprise and other policy-based controls.
- Ensures business continuity and other enterprise requirements including scalability, availability, redundancy and resiliency, alerting, policy-based rotation and other enterprise requirements.

Get started with **Conjur Open Source**.

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 CyberArk Blueprint

CyberArk has developed a prescriptive blueprint to help organizations establish and evolve an effective PAM program. The CyberArk Identity Security Blueprint is designed to defend against three common attack chain stages used to steal data and wreak havoc. Simple, yet comprehensive, the CyberArk Blueprint provides a prioritized, phased security framework that closely aligns PAM initiatives with potential risk reduction, helping organizations address their greatest liabilities as quickly as possible.

The CyberArk Blueprint was built with contemporary organizations and extensibility in mind. It prescribes PAM controls and best practices for organizations using conventional on-premises infrastructure and software development methods, as well as for organizations embarking on digital transformation projects such as migrating infrastructure to the cloud, adopting CI/CD practices, optimizing processes through robotic process automation or implementing SaaS solutions for business-critical applications.

The CyberArk Blueprint reflects the combined knowledge and experience of CyberArk's global sales, sales engineering, security services and customer success organizations. As the undisputed leader in Identity Security, CyberArk is uniquely positioned to deliver a thorough and effective PAM blueprint:

- CyberArk solutions are trusted by 7,500 customers, including more than 50% of the Fortune 500, across a wide range of industries including financial services, insurance, manufacturing, healthcare and tech.
- CyberArk's Incident Response and Red Team have been front and center in helping companies recover from some of the largest breaches of the 21st century. Additionally, CyberArk draws on the insights of its Threat Research and Innovation Lab.
- 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 is widely recognized as a leader in both PAM and access management in all major industry analyst reports.
- Learn more by visiting www.cyberark.com/blueprint.

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.

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.

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., 12.22 Doc. TSK-2625 (TSK-1602, 208101)

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.