CYBERARK®

SOLUTIONS BRIEF

CyberArk Workforce Identity

BENEFITS

Defend Against Attacks

Protect against data breaches or malicious attacks from lost, stolen, or compromised credentials. Defend against impersonation, phishing, spear-phishing, social-engineering and other exploits.

Improve User Experiences

Provide fast, frictionless access for remote workers and on-the-go users. Eliminate password sprawl and fatigue, and VPN hassles.

Drive Operational Efficiencies

Automate lifecycle management. Provide self-service tools for users and approval flows. Free up administrative staff to focus on core business tasks.

Satisfy Audit and Compliance

Increase visibility and streamline audits. Avoid regulatory fines and reputational damage.

Enterprises are adopting cloud-based applications and infrastructure to accelerate business agility and simplify operations. The cloud fundamentally transforms the way businesses deliver and access applications, creating new opportunities for adversaries and new challenges for security organizations.

CyberArk Identity is designed from the ground up to protect today's cloud-centric digital enterprises. The solution portfolio lets organizations securely extend all their business applications and IT services to remote workers and on-the-go users while delivering exceptional end-user experience. CyberArk Identity helps enterprises defend against attacks, drive operational efficiencies, and improve compliance.

CHALLENGES

Digital transformation poses a variety of challenges for IT security organizations including:

- **Securing the perimeterless enterprise.** Traditional perimeter-based security models, designed to protect conventional on-premises IT infrastructure and office-based workers, aren't well suited for the digital era. Organizations must introduce new systems and practices, such as Zero Trust, to safeguard cloud infrastructure, protect SaaS applications, while providing secure access to existing on-premises resources to remote workers and mobile users..
- **Managing accounts and passwords.** Today's businesses are powered by dozens or even hundreds of different applications. Managing accounts and passwords is a challenge for IT administrators and end-users alike. Enterprises must find ways to eliminate password fatigue, prevent risky behavior, and streamline the administration of user accounts, credentials, and privileges.
- **Enabling remote workforce.** Today's workers conduct business from any place, at any time, using any device. To be fully productive they need fast, frictionless access to all their applications and services whether working from home, the office, or the road. Businesses must find ways to secure remote workers and safeguard on-premises and cloud-based IT systems and data without hindering user satisfaction.

SOLUTION

CyberArk Identity helps today's businesses overcome the unique user authentication, authorization, and auditing challenges accompanying digital transformation. The services included in CyberArk Identity solution streamline operations and gives workers simple and secure access to all their enterprise resources—on-premises, cloud, hybrid—from any location, using any device.

The integrated CyberArk Identity solution includes:

CyberArk Identity Single Sign-On

CyberArk Identity Single Sign-On (SSO) gives workers convenient one-click access to all their enterprise applications using a single set of credentials. The solution helps eliminate password sprawl and fatigue, improve user experiences, and avoid risky workarounds like using common credentials, or recording passwords on paper or spreadsheets. The solution also centralizes, unifies, and simplifies access administration, reducing help desk interactions and operations expenses.

CyberArk Identity Adaptive Multi-Factor Authentication

CyberArk Identity Adaptive Multi-Factor Authentication (MFA) helps businesses avoid data loss and other risks posed by compromised or stolen credentials. The solution supports a variety of authentication mechanisms, including passwordless factors, and protects a range of enterprise identities and resources, such as applications, infrastructure, and endpoints. Unlike traditional MFA solutions, CyberArk Identity Adaptive MFA uses AI-powered behavioral analytics and contextual information to determine which authentication factors to apply to a particular user in a specific situation, improving end-user satisfaction and productivity.

CyberArk Identity Lifecycle Management

CyberArk Identity Lifecycle Management (LCM) lets administrators efficiently onboard and offboard users, and manage their access privileges throughout their course of employment. The solution includes self-service tools for users and approving managers, as well as administrative reports to help security teams track access activity, investigate incidents, and support compliance audits. Integration with leading HR systems, Identity Governance and Administration solutions, and directory services simplifies new-hire provisioning and eliminates manually-intensive, error-prone processes.

CyberArk Identity App Gateway

CyberArk Identity App Gateway lets users securely access traditional applications hosted in corporate data centers using the same credentials and authentication methods they use to access cloud apps. The solution provides strong security and easy access without VPN hassles, expenses, or support burdens. Easy to implement, CyberArk Identity App Gateway can be deployed without modifying application code or reconfiguring firewall rules.

CyberArk Identity Directory Services

CyberArk Identity Directory Services lets organizations centrally manage enterprise IT directories at scale. The solution integrates with a variety of popular on-premises and cloud-based directory services including Microsoft Active Directory, Azure Active Directory, and LDAP Directories. An extensible schema makes it easy to maintain information related to users, computers, endpoints, mobile and server objects, and other elements using a unified data store and common administrative tools.

CyberArk Identity User Behavior Analytics

CyberArk Identity User Behavior Analytics uses AI and Machine Learning to collect, analyze, and visualize user behavior and threat data in real-time. The solution includes interactive dashboards to help administrators easily assess risk, reporting tools to help administrators investigate security incidents and support audits, and real-time alerts to notify administrators of suspicious activity. It also provides webhooks to feed alerts to third-party tools like ServiceNow.

WHY CYBERARK

CyberArk is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. To learn more, visit www.cyberark.com.

CYBERARK®

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.

CYBERARK®

WHITE PAPER

CYBERARK® PRIVILEGED ACCESS MANAGEMENT SOLUTIONS

The industry's most complete solution to reduce risk created by privileged identities, credentials and secrets

www.cyberark.com

Table of Contents

Privileged Access — a Real, Pervasive, Threat

Attackers are wreaking havoc across the globe with advanced cyber attacks 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.

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

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

credentials should be additionally authenticated for each use with Multi-Factor 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 Threat Landscape 2019 Report[2], we discovered that 84% of IT security professionals recognized that infrastructure and critical data are not fully protected unless privileged accounts, credentials and secrets are secured and protected. If not properly secured, infrastructure and data can be easily fall prey to popular attack methods like malware, DDoS and brute force attacks. Yet, many organizations indicate that their organization has not done enough to protect themselves against malware and advanced attacks: fewer than 40% of respondents indicated that their organization had implemented strict access policies for users with access to critical infrastructure and applications. Malware requires admin access to gain persistence; privileged access without vigilant management creates an ever-growing attack surface around privileged accounts.

Additionally, DevOps security has not yet reached the necessary maturity levels of traditional enterprise IT: only 35% of respondents belong to organizations that have implemented a PAM security strategy for cloud or DevOps. Perhaps even more surprising is the revelation that only 46% of organizations have a strategy in place for protecting their mission critical servers—the compromise of which would represent a total loss of control of the network to a hacker. When you consider the massive risks associated with the typical enterprise coupled with a general lack of strong privileged security measures across many organizations—and then face the reality that the majority of security breaches executed in the last 10 years have involved the abuse of privileged access—it becomes very clear where IT security professionals need to have a focused plan of attack.

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, "CyberArk Global Advanced Threat Landscape Report 2019," 2019

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 privileged 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.

Business users. Senior-level executives and IT personnel with sensitive information have long been targets of cyber attacks. But as organizations grow their footprint, enable a remote workforce and store more of their sensitive business data in cloud services and applications, the lines between traditionally privileged users and the workforce have blurred. Traditionally non-privileged 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 wrong person, business 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.

Social media. Privileged access is granted to administer the corporate internal and external social networks. Employees and contractors are granted privileged access to write to those social media accounts. Misuse of these credentials can lead to a public takeover causing harm for an organization’s brand or an executive’s reputation.

Applications. Applications use privileged accounts 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, each of which is managed by an admin console which is accessed using privileged credentials which 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

Each PAM solution within the CyberArk Identity Security Platform addresses a different requirement for securing privilege, and are all are designed to work together to provide a complete, secure solution for operating systems, endpoints, cloud infrastructure and workloads, servers, databases, applications, hypervisors, network devices, security appliances, and more. 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, websites, 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.

Privileged Access Manager

Privilege Cloud® | Privilege On-Premises

Discover, manage and protect privileged accounts and credentials

CyberArk® Privileged Access Manager, which can be deployed as a Service or on-premises, 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 meet 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.

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

The solution 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.

DVR-like recordings provide a complete picture of a session with search, locate, and alert capabilities on sensitive events without having 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.

- Isolates privileged sessions to help prevent the spread of malware from a user's endpoint to a critical system.
- Helps protect privileged passwords and SSH keys from advanced attack techniques such as key-stroke logging and pass-the-hash attacks.
- Secures and controls privileged sessions to guard against malware or zero-day exploit from bypassing controls.
- Creates an indexed, tamper-resistant record of privileged sessions and provides searchable metadata.
- Offers command line control and native SSH access while still providing secure access to privileged users using either passwords or SSH keys.
- Provides AD Bridge capabilities that enable organizations to centrally manage Unix users and accounts that are linked to AD through the CyberArk platform.

Detect, alert and respond to privileged threats and malicious activity

CyberArk provides a security intelligence solution that allows organizations to detect, alert, and respond to anomalous privileged activity indicating an in-progress attack. The solution collects a targeted set of data from multiple sources, including the CyberArk Digital Vault, SIEM, and the network. Then, the solution applies a complex combination of statistical and deterministic algorithms, enabling organizations to detect indications of compromise early in the attack lifecycle by identifying malicious privileged activity.

- Detects and alerts in real-time with automatic response to detected incidents.
- Identifies privileged access related anomalies and malicious activities with the ability to detect in-progress attacks.
- Adapts threat detection to a changing risk environment with self-learning algorithms.
- Correlates incidents and assigns threat levels.
- Enhances the value of existing SIEM solutions with out-of-the-box integrations.
- Improves 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 SaaS solution that combines Zero Trust access, biometric multi-factor 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 Privileged Access Manager 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

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

Cloud Entitlements Manager™

Artificial intelligence-powered removal of excessive privileges and permissions across cloud environments

CyberArk Cloud Entitlements Manager is a SaaS solution 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

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 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 Solutions

Workforce Identity | Customer Identity

Secure access to the entire enterprise, including cloud and on-premises applications, endpoints and VPNs

CyberArk Identity is a SaaS-delivered 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.

CyberArk Identity suite includes all fundamental pillars of Identity and Access Management (IAM) – Single Sign-On (SSO), Adaptive Multi-Factor Authentication (MFA), Identity Lifecycle Management (LCM) and User Behavior Analytics (UBA).

- **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 Multi-Factor 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 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 Identity User Behavior Analytics:** CyberArk UBA enables you to determine the risk of every user and access request by collecting and analyze a rich set of contextual factors. Leveraging Machine Learning, User Behavior Analytics engine builds user profiles that model standard behavior and automatically flags anomalous activity. With UBA, you can generate access-related insights, investigate security incidents, and define remediation actions when potential breach attempts are detected.

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

DevSecOps Solutions

Secrets Manager: Conjur® Enterprise, Conjur® Open Source and Credential Providers

Protection, management, and audit for 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.

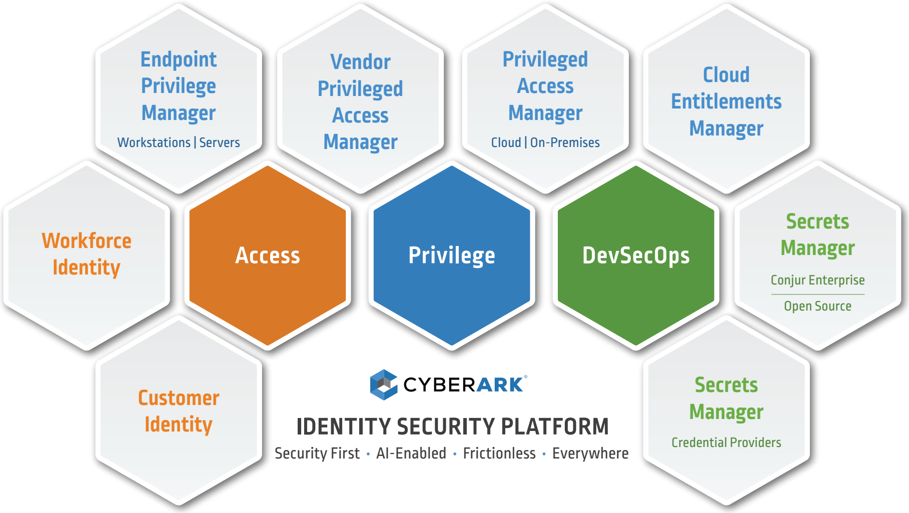
- **For cloud-native applications built using DevOps methodologies:** Conjur Secrets Manager Enterprise provides a secrets management solution tailored specifically to the unique requirements of cloud native and DevOps environments. The solution integrates with a wide range of DevOps tools, PaaS/Container 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.


Endpoint Privilege Manager
Workstations | Servers
Vendor Privileged Access Manager
Privileged Access Manager
Cloud | On-Premises
Cloud Entitlements Manager
Workforce Identity
Access
Privilege
DevSecOps
Secrets Manager
Conjur Enterprise
Open Source
Customer Identity
CYBERARK
IDENTITY SECURITY PLATFORM
Security First • AI-Enabled • Frictionless • Everywhere
Secrets Manager
Credential Providers

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 there is a preference for deploying software on-premises, 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 6,600+ 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 PAM in all major industry analyst reports.
- Learn more by visiting www.cyberark.com/blueprint.

WHY CYBERARK

- **Most Complete and Extensible Identity Security Platform.** Solving the full range of hybrid to multi-cloud identity challenges with a security-first approach.
- **Architected for the Modern Enterprise.** Built and ready platform that enables digital business and supports dynamic infrastructure and the new normal workforce.
- **Broadest Integration Support.** Most out-of-the-box integrations to solve identity security across the organization.
- **Identity Security Innovator.** Pioneered the key solution to solve the hardest IT security problem. Continuing to lead the market with dynamic solutions to address new and emerging threats.
- **Proven Expertise in Securing Identities.** Long-tail of experience and tenure with the world's largest enterprises provides the deepest and widest 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 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., 02.21 Doc. 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.

CYBERARK®

DATA SHEET

CYBERARK® SECRETS MANAGER

THE CHALLENGE

Enterprises are increasingly adopting DevOps methodologies and automation to improve business agility while also leveraging commercial and internally developed applications. However, each application, automation tool and other non-human identity relies on some form of privileged credential to access sensitive resources. Application and IT environments can vary significantly within the same organization — from highly dynamic, cloud native to largely static and even mainframe based. The credentials used by applications need to be secured regardless of the application type and compute environment. Securing these credentials poses challenges for IT security, operations, and compliance teams:

- **Application and other non-human credentials are widespread –** they include embedded hard-coded credentials in business-critical applications including internally developed and commercial off-the- shelf solutions (COTS), security software such as vulnerability scanners, application servers, IT management software, Robotic Process Automation (RPA) platforms, and the CI/CD tool chain.
- **Application and other non-human credentials need to be managed –** in addition to eliminating hard-coded credentials in code and scripts, recommended approaches and techniques including strong authentication, least privilege, role-based access controls, credential rotation, and audit.
- **Automated processes are incredibly powerful –** they can access protected data, scale at unparalleled rates, leverage cloud resources, and rapidly execute business processes to drive tremendous value. However, as well-publicized security breaches demonstrate, automated processes are susceptible to sophisticated cyberattacks, which can occur suddenly and spread rapidly.

Businesses must protect privileged credentials assigned to non-human identities to defend against attacks. Additionally, these credentials are typically assigned and managed by people such as IT admins, developers and DevOps admins. Consequently, it is critical that human access to admin consoles are also consistently managed and secured across the enterprise.

KEY BENEFITS

For Security Teams

- Protect against breaches by consistently managing and monitoring credentials used by almost all application types and non-human identities.
- Prevent inadvertent exposure of credentials by eliminating hard-coded credentials.
- Part of the most complete and extensible Identity Security Platform

For Operations

- Reduce complexity and burden on IT by automating the management and rotation of application credentials.
- Secure mission critical applications running at scale.

For Developers

- Simplify how applications securely access sensitive resources with the most of out-of-the-box integrations and flexible APIs.
- Avoid impacting velocity.

For Compliance and Audit

- Leverage a unified security solution to ease the burden of meeting extensive compliance and regulatory requirements.

THE SOLUTION

CyberArk Secrets Manager is designed to secure secrets and credentials used by the broadest range of application types in hybrid, cloud native and containerized environments. Secrets Manager comprises Conjur® Secrets Manager Enterprise (and Open Source) and the Credential Providers.

- **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. The solution integrates with the CyberArk Identity Security Platform to provide a single enterprise-wide platform for securing privileged credentials. Developer resources and Conjur Open Source are available at www.conjur.org.

- **For securing commercial off-the-shelf solutions** – 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 enterprises allow third party solutions to access privileged credentials, CyberArk offers the most validated COTS integrations for solving identity security challenges.
- **For internally-developed traditional applications** – Credential Providers can protect business-system data and simplify operations by eliminating hard-coded credentials from internally developed applications. The solution provides a comprehensive set of features for managing application passwords and SSH keys, and supports a broad range of application environments, including application servers, Java, .Net, and scripting running on a variety of platforms and operating systems including Unix/Linux, Windows and zOS.

Secrets Manager provides robust enterprise-grade capabilities and integrates with existing systems to help organizations protect and extend established security models and practices.

CAPABILITIES

The Secrets Manager solutions are designed to help organizations:

- **Establish strong authentication** – by leveraging the native attributes of applications, containers, and other non-human identities to eliminate the "secret zero bootstrapping" challenge and potential vulnerability.
- **Manage and rotate secrets** – by leveraging dual accounts and other techniques.
- **Simplify integrations** – by supporting validated integrations with CI/CD toolsets, and container platforms, and a wide range of commercial software platforms, applications and tools, such as business applications, security tools and RPA.
- **Accelerate deployment and usage** – by providing developers with easy to-use solutions to secure secrets in application and DevOps environments.
- **Ensure a comprehensive audit on any access** – by tracking all access and providing tamper-resistant audit.
- **Consistently apply 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.
- **Ensure business continuity and other enterprise requirements** – including scalability, availability, redundancy and resiliency.
- **Flexible deployment options** – Secrets Manager supports both SaaS and on-prem versions of the CyberArk Vault to simplify deployments and increase flexibility, while also strengthening security by centrally managing credentials and secrets across the enterprise.

OVERVIEW

COTS Application Integrations

- Security Software: Vulnerability Management, Discovery Solutions, etc.
- IT Management Software
- Robot Process Automation and other Automation Solutions

Application Server Integrations:

- IBM WebSphere Application Server, WebSphere Liberty, JBoss, Oracle WebLogic Server, Tomcat

Cloud Native and DevOps Integrations:

- Tools/Toolchains: Ansible, Jenkins, Puppet, Terraform
- Public Clouds: AWS, Azure, GCP
- PaaS/Container Orchestration: Kubernetes, Red Hat OpenShift, VMware Tanzu, Cloud Foundry
- Secretless Broker: OpenShift, Kubernetes
- Container Security: Aqua, Twistlock

Enterprise Grade:

- HSM integration, SIEM Tools
- AES-256, RSA-2048, SHA2

SDK and Development Libraries:

- DevOps: Go, Java, Ruby, .NET
- Application SDK: C/C++, CLI, Java, .NET, .NET Core, / .NET Standard, Web Service/REST

Native Authenticators:

- Kubernetes
- Red Hat OpenShift
- AWS IAM
- Azure
- Google Cloud Platform
- OpenID Connect (OIDC)

CyberArk Vault Integrations:

- CyberArk Privilege Access Manager (Privilege On-Premises)
- CyberArk Privilege Cloud®

CYBERARK IDENTITY SECURITY PLATFORM

Secrets Manager is part of the CyberArk Identity Security Platform which helps organizations secure access to critical business data and infrastructure, protect a distributed workforce, and accelerate business in the cloud. The integrated solution helps organizations reduce the attack surface by applying consistent policies to human and non-human identities across the enterprise.

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.