

Manaus, 09 de setembro de 2024.

**Ao**

**TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS – TJ/AM.**

Ref.:

Pregão Eletrônico SRP nº 40/2024.

**Objeto:** Contratação de empresa especializada no fornecimento de solução de gerenciamento de acessos privilegiados (PAM – Privileged Access Management).

A/C Sr. Pregoeiro(a),

Em complemento a proposta apresentada via sistema, confirmo nossos dados e ratifico as informações prestadas via sistema.

<b>Razão social</b>	IT PROTECT SERVIÇOS DE CONSULTORIA EM INFORMÁTICA LTDA.
<b>CNPJ</b>	23.378.923/0001-87.
<b>Endereço</b>	Trav. Alameda Mediterrâneo, nº 1000, Sala 302, Bairro Cidade Alpha, Cep. Eusébio/CE.
<b>CEP</b>	61.765-860
<b>Fones</b>	(91) 91981282388
<b>E-mail</b>	licitacoes@itprotect.com.br

Item	Descrição	Und.	Qnt.	Valor unitário	Valor total
1	Solução de Segurança para Identidades e seus Privilegios – Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI, com garantia pelo período de 12 (doze) meses.  Cyberark PAM Self Hosted .	unidades	75	R\$ 14.895,85	R\$ 1.117.188,75
	Solução de Segurança para Identidades e seus Privilegios –	unidades	40	R\$ 8.500,00	R\$ 340.000,00



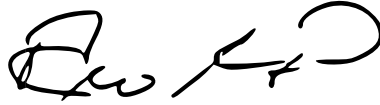
2	Proteção para Aplicações Tradicionais, com garantia pelo período de 12 (doze) meses.  Cyberark Credential Provider – Solução CCP ou Conjur.				
3	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para servidores Windows e Linux, com garantia pelo período de 12 (doze) meses.  Cyberark Endpoint Privilege Management e Cyberak On-Demand privileges manager.	unidades	400	R\$3.369,80	R\$ 1.347.920,00
4	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para Estações de Trabalho, com garantia pelo período de 12 (doze) meses.  Cyberark Endpoint Privilege Management.	unidades	3500	R\$ 500,00	R\$ 1.750.000,00
5	Serviço de instalação e configuração para Solução de Segurança para Identidades e seus Privilégios.	unidades	01	R\$ 120.000,00	R\$ 120.000,00
6	Transferência de Conhecimento para Solução de Segurança para Identidades e seus Privilégios (turma).	unidades	02	R\$ 47.250,00	R\$ 94.500,00
7	Serviço de Suporte Técnico Especializado.	mês	12	R\$ 21.000,00	R\$ 252.000,00
<b>VALOR TOTAL DA PROPOSTA</b>				<b>R\$ 5.021.608,75</b>	

Valor Total da proposta é de **R\$ 5.021.608,75 (cinco milhões vinte e um mil seiscentos e oito reais e setenta e cinco centavos)**, para a execução do objeto da contratação o pregão supracitado, de acordo com as condições, quantidade e prazos dispostos no edital, termo de referência e anexos.

Prazo de Validade da Proposta: **60 (sessenta) dias.**



**Observação: Estão inclusos nos preços supramencionados todos os custos diretos e indiretos, inclusive de embalagens, transportes ou fretes, e ainda os resultantes da incidência de quaisquer tributos, contribuições ou obrigações decorrentes da legislação trabalhista, fiscal e previdenciária a que estiver sujeito.**



**Theo Augusto Ramalho Costa**  
Diretor Executivo



## PLANILHA DE DADOS DA EMPRESA

<b>Dados da Empresa:</b>	
<b>Razão Social</b>	IT PROTECT SERVIÇOS DE CONSULTORIA EM INFORMÁTICA LTDA.
<b>Inscrição</b>	23.378.923/0001-87
<b>Endereço</b>	Trav. Alameda Mediterrâneo, nº 1000, Sala 302, Bairro Cidade Alpha, Cep. Eusébio/CE.
<b>CEP</b>	61.765-860
<b>Telefone</b>	+55 85 30480828
<b>E-mail</b>	licitacoes@itprotect.com.br
<b>Site internet</b>	www.itprotect.com.br
<b>Dados do Representante Legal da Empresa:</b>	
<b>Nome</b>	Theo Augusto Ramalho Costa
<b>Cargo</b>	Diretor Executivo
<b>Nacionalidade</b>	Brasileiro
<b>Estado Civil</b>	Solteiro
<b>Profissão</b>	Empresário
<b>Endereço</b>	Av. Golfinhos , 01641, Ap 414, 4º andar. Porto das Dunas, Aquiraz/CE.
<b>CEP</b>	61.700-000
<b>E-mail</b>	licitacoes@itprotect.com.br
<b>Identidade</b>	3708459
<b>Órgão Expedidor</b>	PC/PA
<b>CPF</b>	686.698.102-63
<b>Dados Bancários da Empresa:</b>	
<b>Banco</b>	Itaú Unibanco S/A – 34
<b>Agência</b>	Agência: 6540
<b>Conta</b>	Conta Corrente: 17078-1
<b>Dados do Contato com a Empresa:</b>	



<b>Nome</b>	Anders Willy Wissing Andersen Trindade Filho
<b>Cargo</b>	Gerente de Projetos
<b>Endereço</b>	Tv. Djalma Dutra 361. Apto 1701.
<b>CEP</b>	66.113-010
<b>Fone</b>	+55 91 99338-2295
<b>E-mail</b>	licitacoes@itprotect.com.br



# CYBERARK CONJUR® SECRETS MANAGER ENTERPRISE

## THE CHALLENGE

As enterprises adopt DevOps methodologies and automate their IT infrastructure, they recognize they must secure dynamic workloads, cloud native and automated IT environments without compromising developer velocity – any security solution must meet the needs of both the security team and developers.

Applications use secrets to securely access sensitive resources. While easy to hard-code secrets this practice poses an enormous risk – hard-coded secrets cannot be rotated, managed or audited and can be inadvertently made public in code repositories.

Additionally, configuration management and CI/CD tools use secrets to interact with other tools and access other resources. Access must also be managed for the DevOps admins, developers and other human users that administer them. These tools have become attractive targets for attackers, so not only must the secrets used by applications be secured, but also the credentials used by the tools themselves and by the humans managing them.

## THE SOLUTION

Conjur Enterprise is a secrets management solution tailored specifically to the unique infrastructure requirements of cloud native, container and DevOps environments. The solution helps developers and security organizations secure, rotate, audit and manage secrets and other credentials used by applications, automation scripts and other non-human identities.

Conjur Enterprise is specifically architected for containerized environments and can be deployed at massive scale. The solution integrates seamlessly with widely used DevOps tools and platforms. It also integrates with existing systems to help organizations extend established security models and practices. The solution enables organizations, regardless of where they are in their digital transformation journey, to secure applications and automated processes, and to integrate secrets management best practices into developer workflows.

Conjur Enterprise is a fully featured, enterprise-class solution fully backed by CyberArk's world-class support and services organization. Features include GUI access, rotation, audit and reporting, and HA/DR functionality. Additional resources for securing DevOps environments can be found at [www.cyberark.com/devops](http://www.cyberark.com/devops) and the open source version, Conjur Open Source and developer community are available at [www.conjur.org/blog](http://www.conjur.org/blog).

## BENEFITS

Reduce the risks in dynamic cloud native and DevOps environments without compromising security, business agility or velocity.

### For Security Teams

- Protect against breaches and software supply chain hacks by consistently managing and monitoring application credentials, and privilege across DevOps and automation environments by applying enterprise-wide security and compliance policies.
- Leverage CyberArk Identity Security Platform to give the DevOps administrators assigning privilege secure access.

### For Operations

- Reduce complexity and burden on IT by supporting massive scale and deployment flexibility to cloud, multi-cloud or hybrid environments while improving protection of the business.

### For Developers

- Simplify how applications securely access resources using native integrations with CI/CD tool sets, container platforms, and with Secretless Broker.
- Accelerate developer access with open source solutions.

Additionally, Conjur Enterprise 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. Elements in the solution can be combined to form a cohesive, end-to-end solution that delivers enterprise class privileged access security across hybrid, multi-cloud and containerized environments. The integrated solution helps organizations reduce the attack surface by applying consistent policies to both human users and non-human identities.

## KEY FEATURES

Key features and functions include:

- **Comprehensive secrets management** for privileged credentials such as API keys, certificates, passwords, SSH keys and tokens. Secrets are securely managed and automatically rotated based on policy.
- **Integration with DevOps toolchain** leverages native integrations to secure and manage secrets used by CI/CD tools such as Ansible, Jenkins and Azure DevOps and container orchestration software such as Kubernetes.
- **Integration with DevOps platforms** secures and manages secrets and credentials used by PaaS environments including Kubernetes, Red Hat OpenShift, VMware Tanzu and Cloud Foundry.
- **Role-based access controls (RBAC)** makes it easy to assign distinct privileges to different groups of non-human identities with different responsibilities. Administrators can define various roles (e.g. development, test, operations, administration) and grant each role unique privileges for specific resources (e.g. database password, web service endpoint).
- **Centralized audit records** for all authorization events and secrets operations.
- **Easy to use GUI** provides an overall view of users, machines, and secrets.
- **Innovative Secretless Broker capability** simplifies how applications connect securely to databases, SSH and HTTPS without having to fetch or manage secrets. This enhances security by isolating applications from being exposed to secrets.
- **Cloud scalability, performance and availability.** Leverages a distributed, high-availability architecture with Leader and Follower components. Leaders and Followers can be distributed across zones, regions and multi-cloud environments to minimize latency, support scalability and resistance and segregate data between environments (e.g., prod, dev, GCP, AWS).
- **Integration with CyberArk Identity Security Platform** enables organizations to use a centralized policy-based approach to consistently manage the credentials used by both human users as well as non-human identities. For example, integrations enable credentials to be managed, synced and monitored across DevOps environments, and isolate monitor and control privileged access by human users, including the DevOps admins managing the tool chain.
- **Support for integrations** with existing security systems including SIEM.

## OVERVIEW

### Deployment Options:

- Docker Image
- Amazon Machine Image (AMI)

### SDK and Development Libraries:

- Go, Java, Ruby, .NET
- REST API, CLI

### 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
- Container Security: Aqua
- Community Integrations (e.g., Azure DevOps, Concourse, TeamCity)

### CyberArk Vault Integrations:

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

### Other Native Integrations and Tools

- Secretless Broker: Red Hat OpenShift, Kubernetes
- Summon

### Security Solution:

- HSM integration
- SIEM tools

### Native Authenticators:

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

©CyberArk Software Ltd. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 02.21. Doc. 218042430

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.





## DATA SHEET

# CyberArk® Endpoint Privilege Manager

## The Challenge

When an attack evades your perimeter and endpoint security, you are reliant on detection technologies to react quickly to try and prevent it spreading. Attackers steal credentials or exploit vulnerabilities to elevate privileges and move laterally through your network to find valuable information. IT teams chose to give users local admin rights and to either not enforce least privilege whatsoever or maintain very relaxed policies, trying to prevent potential impact on user productivity and increased burden and associated costs for the desktop support team. As a result, organizations face these challenges:

- **Lost business productivity.** When organizations eliminate all privileges from business users, users may no longer be able to carry out certain tasks or use certain applications needed for their day-to-day roles. Inflexible privilege policies can bring the business to a halt.
- **High help desk costs.** When IT policies prevent business users from carrying out necessary, day-to-day tasks, users must call the help desk to restore necessary permissions. This can significantly drive up IT costs and overwhelm the support team.
- **Increased security risks due to 'privilege creep.'** Without the right tools, users tend to wrestle local admin rights back when there's a sporadic urgent need and rarely yield them back.
- **Increased risk of successful malware-based attacks.** Even if malware does not rely on elevated privileges, without comprehensive application control policies in place attackers still can achieve their goals, compromise credentials and exfiltrate sensitive data.

## The Solution

CyberArk Endpoint Privilege Manager helps remove the barriers to enforcing least privilege and allows organizations to block and contain attacks at the endpoint, reducing the risk of information being stolen or encrypted and held for ransom. A combination of Endpoint Privilege Management, Privilege Threat Protection and Application Control stops and contains damaging attacks at the point of entry. These critical protection technologies are deployed as a single agent to strengthen and harden all desktops, laptops and servers running Windows, Windows Server, macOS or Linux.

**CyberArk Endpoint Privilege Manager fences off cyberattacks by removing local admin rights, elevating applications Just-In-Time while creating an audit trail and protecting security controls from tampering.**

### PLATFORMS & DEPLOYMENT

#### Microsoft Windows

- Windows 7 x32, x64
- Windows 8/8.1 x32, x64
- Windows 10 x32, x64
- Windows 11 x32, x64

#### Microsoft Windows Server

- Windows Server 2008 x32, x64
- Windows Server 2008 R2 x64
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

#### Apple macOS

- macOS Monterey 12

#### Linux

- Red Hat Enterprise Linux 7.x, 8.x
- SUSE Linux Enterprise 12,15
- Amazon Linux 2
- CentOS 7
- Ubuntu 18.04, 20.04

#### Deployment Options

- Software-as-a-Service



# Benefits

With CyberArk Endpoint Privilege Manager, organizations are able to:

- **Remove local admin rights.** Endpoint Privilege Manager helps remove local admin rights while improving user experience and optimizing IT operations. Flexible policy-based management simplifies privilege orchestration and allows controlled Just-In-Time maintenance sessions.
- **Enforce least privilege.** Comprehensive conditional policy-based application control can help you create scenarios for every user group, from HR to DevOps. Endpoint Privilege Manager considers application context, parameters, and attributes to allow or block certain script, application or operation.
- **Allow quick adoption of least privilege by introducing JIT (Just In Time) elevation and access.** Add users to a local privilege group for a limited time, provide an audit trail on the endpoint throughout the temporary period the user had privilege rights, revoke and terminate access at the end of the session or before if required.
- **Securely manage local admin.** Protected credentials from CyberArk Enterprise Password Vault are managed locally on endpoints, on or off the network.
- **Detect and block credential theft attempts.** Credential theft plays a major part in any attack. Advanced protection helps an organization detect and block attempted theft of Windows credentials and those stored by popular web browsers.
- **Seamlessly elevate business user privileges as needed.** Once local administrator rights are removed from business users, CyberArk Endpoint Privilege Manager elevates privileges, based on policy, as required by trusted applications.
- **Quickly identify and block malicious applications.** Leveraging CyberArk's Application Risk Analysis to quickly determine risk associated with any application streamlines policy definitions and aids in preventing malicious applications from running in the environment.
- **Out of the box Ransomware Protection.** OOTB policy for protection against ransomware including comprehensive least privilege controls readily tested on hundreds of thousands of ransomware samples.
- **Linux policy-based sudo management** helps eliminate manually intensive, error-prone sudo administrative processes, allowing endpoint security managers to centrally configure sudo and enforce role-specific least privilege at scale.
- **Enable unknown applications to safely run in a restricted mode.** Unknown applications, which are neither trusted nor known to be malicious, are able to run in 'Restricted Mode' which prevents them from accessing corporate resources, sensitive data or the internet.
- **Leverage integrations with threat detection tools to analyze unknown applications.** CyberArk Endpoint Privilege Manager can send unknown applications to Check Point, FireEye and Palo Alto Networks threat detection solutions for automated file analysis.

## SPECIFICATIONS

### Flexible and Secure Application Rules:

- Executables, Dynamic-Link Libraries (dlls), Windows Applications, Scripts
- Exact, partial, wildcard and regexp matching
- File attributes, such as file name, checksum, owner, location and location type, source etc.
- Program attributes, such as product name, company name etc.
- Application context, such as launch parameters, parent process, etc.
- Granular application and child processes behavior control

### Credential Protection against:

- Tampering with Endpoint Privilege Manager agent
- Browser-stored credentials and credential stores compromise
- Credential theft from IT applications
- Credential theft from remote access tools
- Suspicious actions
- Windows Credentials Harvesting

Note: certain functionality is only available for selected platforms

## A Comprehensive Solution

CyberArk Endpoint Privilege Manager is part of the broader CyberArk Identity Security Platform, a complete solution designed to proactively protect against advanced attacks that exploit administrative privileges to gain access to the enterprise's heart, steal sensitive data, and damage critical systems. The solution helps organizations reduce the attack surface by eliminating unnecessary local administrator privileges and strengthening privileged accounts' security. Products in the solution can be managed independently, or combined for a cohesive and comprehensive privileged account security solution.



**SOC 2 Type 2  
compliant**

©Copyright 2022 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 10.22. Doc. TSK-2356 (TSK-1155)

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.

[www.cyberark.com](https://www.cyberark.com)



## DATA SHEET

# CyberArk Identity Technical Overview

November 2022\*

CyberArk, a leading Identity Security provider, empowers organizations to secure access to critical business data and infrastructure, protect a distributed workforce, and accelerate business in the cloud. With CyberArk Identity, CyberArk's Identity and Access Management solution, organizations can quickly achieve their workforce identity security goals while enhancing operational efficiency. CyberArk Identity is a SaaS-delivered solution designed for easy consumption and scalability. This technical overview deep dives into the stringent security measures CyberArk has taken to protect the data and privacy within CyberArk Identity.

## Built-in Security Measures

CyberArk Identity is engineered for enhanced data durability, integrity, and security and is SOC 2 Type 2 compliant. Furthermore, the service is hosted in premier Tier IV data center facilities that are highly secure, fully redundant, and certified for additional SOC 2 and ISO 27001 compliance. The service is built, managed, and secured according to industry standards. CyberArk encrypts data at rest and data in transit and is designed to avoid leakage and enable privacy. It hardens all components to reduce attack surfaces and implements multi-factor authentication and policy-based access controls to protect against unauthorized access and data disclosure.

### Data Center Locations

CyberArk currently runs SOC 2 Type 2 certified Identity-as-a-Service (IDaaS) on AWS datacenters in the USA, UK, Germany, Canada, Australia, India, Japan, Singapore, and other possible future locations. The Identity services can be accessed globally. For information on AWS security and compliance reports, please see [here](#).

AWS data centers are housed in nondescript facilities where physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, and other electronic means. Authorized staff uses multi-factor authentication mechanisms to access data centers, and all physical access by employees is logged and audited routinely.

Data center access and information are only provided to employees and contractors who have a legitimate business need for such privileges, and when an employee no longer requires these privileges, their access is immediately revoked—even if they continue to be an Amazon employee. All visitors and contractors are required to present identification before being signed in and continuously escorted by staff.

For more information, please refer to [AWS Data Center Controls](#).

## CyberArk Identity Certifications & Compliance

- GDPR
- ISO 27001:2013
- ISO 9001:2015
- SOC 2 Type II
- [CSA STAR Level 1](#)
- FedRAMP High: In Process

For more, please refer to the [CyberArk Trust Center](#).

## Hierarchical Encryption for Data at Rest

Tenant data is stored in Amazon Aurora and encrypted (AES 256) using unique Tenant Keys. Tenant Keys are stored in a POD Global database, encrypted using a Pod Master Key. The Pod Master Key is encrypted using Amazon Web Services Key Management Service (AWS KMS) and stored in a Vault with very limited DevOps access upon well-defined SOC 2 complaint processes. CyberArk leverages multi-layered hierarchical encryption algorithms to protect the database and its data. An AES-256 key is used for symmetric encryption, and an RSA-2048 key pair is used for asymmetric encryption.

## Encryption in Transit

All communications with the CyberArk Identity tenant use TLS 1.2 with strong encryption algorithms and keys (2048-bit RSA). Traffic between services inside AWS are encrypted using TLS 1.3 and each micro-service uses mutual TLS authentication.

## Encryption when Integrated with Self-hosted CyberArk Password Vault

When the CyberArk Cloud is integrated with a self-hosted CyberArk Password Vault, the encryption is at rest on self-hosted CorePAS vaults (AES-256 encryption).

When the CyberArk Cloud is integrated with a self-hosted CyberArk Password Vault, end-to-end encryption is implemented between an end user's browser and the CyberArk self-hosted PAM Vault. This ensures that the business user's credentials which are stored and fetched from the Vault, cannot be decrypted by CyberArk Identity during transit. With this additional security measure, only the end-user can view and manage their business credentials in the CyberArk self-hosted PAM Vault.

- SHA-256 hashing is used when users update a stored password
- All connections are over TLS 1.2
- Asymmetric RSA 2048 is used for the encryption of passwords between the Identity Connector and the Browser or Browser Extension
- Connector calls are all outbound via port 443. No inbound ports are required.

## CyberArk Connector Security

The CyberArk Identity Connector is required for integrating CyberArk Identity with on-premise directories, facilitating RADIUS authentication, or enabling access to internal web applications without the need for a VPN. The CyberArk Identity Connector is a lightweight Windows application that runs behind a customer's firewall to provide real-time authentication, policy, and access to user profiles without synchronizing directory passwords to the cloud. The CyberArk Identity Connector seamlessly integrates with Active Directory without opening extra ports in an organization's firewall or adding devices in their DMZ.

The CyberArk Identity Connector delivers the following security capabilities:

- For each tenant, a unique PKI Certificate is issued from the CyberArk Identity tenant to the CyberArk Identity Connector during registration
- All communications between the CyberArk Cloud and the CyberArk Identity Connector are encrypted and mutually authenticated for each tenant using these unique certificates
- All the traffic between the CyberArk Cloud and the CyberArk Identity Connector cannot be read by the AWS infrastructure
- All the traffic between the CyberArk Cloud and CyberArk Identity Connector is sent over TLS 1.2

## User and Admin Portal Security

CyberArk Identity authenticates users from either the built-in CyberArk Identity tenant Directory, an external directory service such as Active Directory, or an external Identity Provider.

Password compliance can be enforced through CyberArk's built-in password policies for CyberArk Cloud Directory users, password policies from external directory services, or SAML integration with an external Identity Provider.

CyberArk Identity additionally provides multiple built-in security layers for accessing the Admin Portal, including CAPTCHA, security image, adaptive multi-factor authentication (MFA), and various other login attack mitigations for improved security. CyberArk can also integrate with third-party MFA solutions.

Administrative rights can be limited through delegated administration roles, application-level permissions, or delegated administrators for Organizations.

## CyberArk Cloud Agent Security

CyberArk Cloud Agents connect to the Internet using corporate settings and communicate with the CyberArk Identity tenant over an SSL/TLS-encrypted tunnel for all types of communication (data sending and "keep alive" checks). The HTTPS connection to the service supports TLS 1.2 and above Cipher Suites. All data transferred between the agent and the CyberArk cloud over HTTPS is encrypted in transit.

## Stringent Access Control Mechanisms

CyberArk employs strict policy-based access controls to protect the CyberArk Identity cloud infrastructure. CyberArk employees, by default, do not have administrative access to customer tenants, but temporary read-only access can be granted by customers in support situations. Tenant databases are encrypted, so even when CyberArk employees are required to do maintenance, they are not able to access any of the data inside. CyberArk uses a privileged Identity management system to manage and audit CyberArk personnel's access to the Identity cloud environment. The session logs maintain a complete and accurate record of any action that has occurred in the system, such as a nefarious administration insider deleting or tampering with logs on a target system.

CyberArk performs background checks on all CyberArk employees who have access to operate and support the service, and they are required to attend security awareness training. Access to Identity Services networks and systems is managed in accordance with our access policy and is granted only to individuals who are responsible for operating and supporting the Identity Services, based on least privilege principles. CyberArk service administrators perform all functions through a VPN connection. Segregation of duty isolates personnel who approve access from personnel who provide access. Access to the Identity cloud is periodically reviewed. Access rights of individuals who leave CyberArk are promptly revoked. Security logs of access by CyberArk personnel are collected and stored for six months.

Additionally, audit reports that include logins and actions performed by CyberArk personnel in the console are generated where required.

Third-party contractors are not allowed to connect to Identity SaaS production servers and systems.

## Vulnerability Management

All Identity SaaS instances are scanned by an enterprise vulnerability management solution and handled according to [CyberArk's security vulnerability policy](#). In addition, all security updates for the Operating System and critical applications are applied.

For more information, please refer to [CyberArk's security vulnerability policy](#).

## Penetration testing

CyberArk uses an internal penetration testing team and an external vendor to run automatic and manual penetration testing on CyberArk Identity, including network and web app vulnerability, at least annually.

## Distributed Denial-of-Service (DDoS) Defense

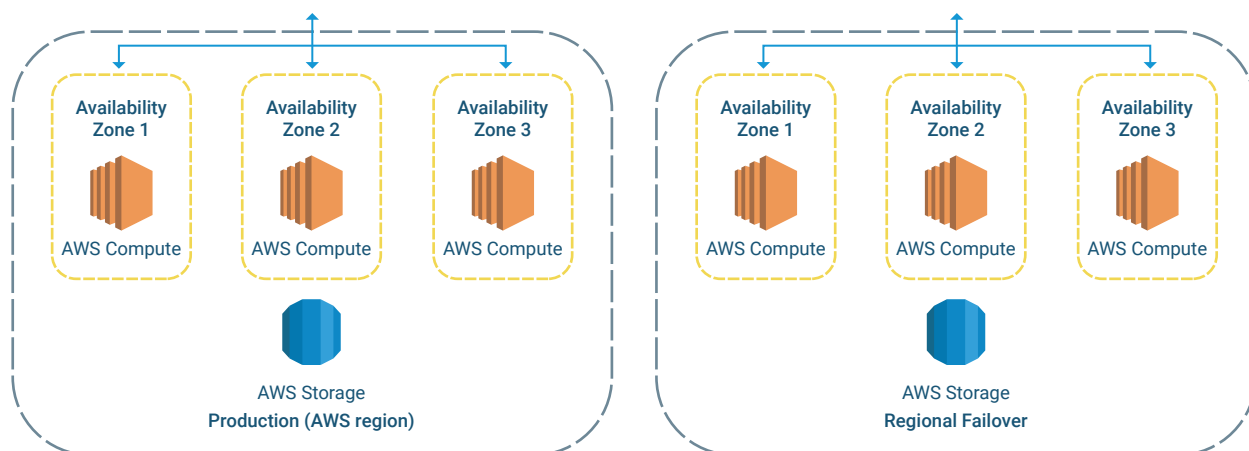
CyberArk utilizes technologies and platforms to detect, mitigate, and prevent DDoS attacks, such as Web Application Firewall (WAF).

# Service Availability

The Identity Services SLA is detailed in the Identity SaaS Service Level Agreement (Service Availability) document. The uptime service commitment for CyberArk Identity is 99.99%. This availability level is achieved by orchestrating multiple services and solutions to make sure that we have near-constant uptime for the Identity service. Identity has 24x7 monitoring tools that constantly monitor the availability and health of all components within the service. Any issues are promptly sent to the operations team, and swift resolution actions will be taken when needed. A team of Service Reliability Engineers are tasked with constantly improving Identity availability by building additional monitoring tools and enhancing the automated mitigation capabilities of the service.

CyberArk also has committed Service Maintenance, meaning (i) routine weekly maintenance performed by CyberArk during a pre-scheduled window; (ii) other system upgrades, enhancements or routine maintenance which is announced via email at least two days in advance; or (iii) emergency maintenance of the Services outside of the foregoing routine or pre-scheduled maintenance window that is reasonably required to complete the application of patches or fixes, or to undertake other urgent maintenance activities. CyberArk shall strive to limit the Service Maintenance window to the minimum possible to avoid service disruption. Please note that the Maintenance Window for upgrades typically occurs once every four months and requires up to 15 minutes of downtime. Security patches usually occur on a monthly basis which occasionally results in a downtime due to restart that can take up to 4 minutes.

CyberArk Identity is deployed on an AWS platform and replicated on three different Availability Zones (AZ), in case of outages in one of the AZ datacenters. Each Availability Zone includes the application and all the supported entities required for the solution's proper functionality, monitoring, and automatically triggered mitigations.



\*Each AZ is at least 100 miles from the other AZs in the same region.

The monitoring systems collect all the service elements (OS metrics, system and applications log, network data, audit, and components heartbeat), analyze them, and alert in case of availability issues or other suspicious indications.

A watchdog service triggers automatic procedures based on alerts the monitoring system generates. The watchdog eliminates the need for human intervention in mitigating issues with the service (e.g. spin up a new application server in one or more AZs and terminate the old one without any manual steps.)

Note: Achieving 99.99% availability is calculated by excluding scheduled maintenance of the service.

\* All uptime and availability commitments are subject to the terms and conditions set forth in CyberArk's Identity Service Level Agreement (Service Availability).

## Disaster recovery and business continuity

CyberArk maintains disaster recovery and business continuity policies for the Identity Services, in which backup files are stored in S3 on a per Region basis and then programmatically updated on a daily basis to a DR Region.

To view the list of tenant and DR locations, please refer to [CyberArk Identity component locations](#).

## Recovery Point Objective (RPO)

The RPO for CyberArk Identity, is up to 24 hours from the last working point in time.

## Recovery Time Objective (RTO)

The RTO for Identity SaaS is 24 hours, but recovery may occur between a few seconds and 24 hours, depending on the type of failure, although in most cases, it is much lower than 24 hours.

For more information, please refer to the [Identity cloud status page](#).

## Software Development Security

CyberArk Identity follows CyberArk's Secure Software Development Life Cycle, integrating security-related activities into the development cycle; this includes following industry security requirements, secure design practices, secure coding, security tests, code, and design reviews, etc. All security reviews are conducted against industry security standards (such as NIST and OWASP Top 10) and threat modeling (based on STRIDE methodology).

## CyberArk Corporate Security Standards and Practices

In compliance with ISO 27001 and SOC 2, CyberArk applies strict security controls and practices to the CyberArk cloud infrastructure and CyberArk's corporate environment, including:

- Personnel security
- Network, application and infrastructure security
- Physical security
- Risk management
- Business continuity plan and disaster recovery plan

For more information, please refer to the [CyberArk Corporate Security White Paper: Standards and Practices](#).

### About CyberArk

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.



©Copyright 2022 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 11.22. Doc. TSK-2569

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.

\* The information in this document is subject to change without notice.

[www.cyberark.com](https://www.cyberark.com)





## DATA SHEET

# CyberArk® Privileged Access Manager Self-Hosted

## The Challenge

Identity Security represents the largest security risk an organization faces today. When employed properly, privileged accounts maintain systems, facilitate automated processes, safeguard sensitive information and ensure business continuity. But in the wrong hands these accounts can be used to steal sensitive data and cause irreparable damage to the business. Privileged accounts are exploited in nearly every cyber attack. With privileged access, bad actors can disable systems, take control of IT infrastructure and gain access to sensitive data.

Organizations face a number of challenges when securing identities, namely protecting, controlling and monitoring privileged access, including:

- **Managing account credentials.** Many IT organizations rely on manually intensive, error-prone administrative processes to rotate and update privileged credentials—an inefficient, risky and costly approach.
- **Tracking privileged activity.** Many enterprises cannot centrally monitor and control privileged sessions, exposing the business to security risks and compliance violations.
- **Monitoring and analyzing threats.** Many organizations lack comprehensive threat analytics for privileged sessions.
- **Controlling privileged user access.** Organizations often struggle to effectively control privileged user access to critical infrastructure, cloud platforms (IaaS and PaaS), and SaaS applications.
- **Securing remote access.** It can be challenging with conventional user authentication and authorization approaches to make sure remote 3<sup>rd</sup> party users access only what they need (and only when they need it).

## The Solution

Privileged Access Manager (PAM) Self-Hosted is a part of the CyberArk Identity Security platform. PAM Self-Hosted provides intelligent controls to secure privileged access across hybrid cloud infrastructures. The solution helps organizations efficiently manage privileged credentials with strong authentication, proactively monitor and control privileged access, intelligently identify and quickly respond to suspicious activity.

**Efficiently protect, monitor and control privileged access across on-premises, cloud and hybrid infrastructure**

### SPECIFICATIONS

#### Encryption Algorithms:

- AES-256, RSA-2048
- HSM integration
- FIPS 140-2 validated cryptography

#### High Availability:

- Clustering support
- Multiple disaster recovery sites
- Integration with enterprise backup system

#### Access and Workflow Management:

- LDAP directories
- Identity and Access Management
- Ticketing and workflow systems

#### Multi-lingual Portal:

- English, French, German, Spanish, Russian, Japanese, Chinese (Simplified and traditional), Brazilian Portuguese, Korean

- **Enable privileged access with modern Single Sign-On (SSO) and adaptive Multifactor Authentication (MFA).** Access sensitive resources with a single set of credentials to reduce the risk of poor password practices. Provide risk-based authentication for each login leveraging user-specific contextual attributes.
- **Centrally secure and control access to privileged credentials based on organizationally defined security policies.** Automated privileged credential (password and SSH key) rotation eliminates manually intensive, time consuming and error-prone administrative tasks, safeguarding credentials used in on-premises, hybrid and cloud environments. Ensure Windows and macOS credentials that are not connected to the network are secured and rotated.
- **Isolate and monitor privileged sessions.** Establish secure, isolated sessions and record all activity. Credentials are retrieved by CyberArk and sent directly to target systems, preventing credential exposure to end users and machines. Meanwhile, session isolation prevents the spread of malware.
- **Detect, alert and respond to anomalous privileged activity.** Apply a complex combination of algorithms to identify malicious activity. A bi-directional data feed exchanges high-risk detections with SIEM tools.
- **Secure remote access.** Easily and securely authenticate external vendors and remote employees accessing CyberArk with biometric VPN-less MFA and no agents. Provision authorized users with Just-in-Time, passwordless access to critical resources and enable automatic session isolation and monitoring.

## Benefits

- **Deliver measurable cyber-risk reduction.** Protect access to privileged accounts and credentials. Defend systems against malware and attacks. Efficiently detect and respond to suspicious activity and malicious commands.
- **Enable operational efficiencies.** Eliminate manually intensive, time consuming and error prone administrative processes. Simplify operations and free up staff to focus on strategic tasks that support core business activities.
- **Satisfy audit and compliance.** Institute policy-based privileged access controls to ensure compliance with government and industry regulations. Easily demonstrate policies and processes to auditors. Produce detailed audit trails and access histories to exhibit compliance.
- **Secure digital transformation.** Balance security with a frictionless user experience. Enable seamless access for privileged users connecting to Tier0 assets, with centralized visibility and control.

CyberArk is the global leader in Identity Security. Centered on [privileged access management](#), CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.



©Copyright 2022 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 08.22. Doc. TSK-2064 (TSK-1409)

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.

## SPECIFICATIONS

### Authentication Methods:

- Username and Password, LDAP, Windows authentication, RSA SecurID, Web SSO, RADIUS, PKI, SAML, smart cards

### Monitoring:

- SIEM integration, SNMP traps, Email notifications

### Sample Supported Managed Devices:

- Operating Systems, Virtualization, and Containers: Windows, \*NIX, IBM iSeries, Z/OS, OVMS, ESX/ ESXi, XenServers, HP Tandem\*, MAC OSX\*, Docker
- Windows Applications: Service accounts including SQL server service accounts in cluster, Scheduled Tasks, IIS Application Pools, COM+, IIS Anonymous Access, Cluster Service
- Databases: Oracle, MSSQL, DB2, Informix, Sybase, MySQL and any ODBC compliant database
- Public Cloud Environments: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)
- Security Appliances: CheckPoint, Cisco, IBM, RSA Authentication Manager, Juniper, Blue Coat\*, TippingPoint\*, SourceFire\*, Fortinet\*, WatchGuard\*, Industrial Defender\*, Acme Packet\*, Critical Path\*, Symantec\*, Palo Alto\*
- Network Devices: Cisco, Juniper\*, Nortel\*, HP\*, 3com\*, F5\*, Nokia\*, Alcatel\*, Quintum\*, Brocade\*, Voltaire\*, RuggedCom\*, Avaya\*, BlueCoat\*, Radware\*, Yamaha\* McAfee NSM\*
- Applications: CyberArk, SAP, WebSphere, WebLogic, JBOSS, Tomcat, Cisco, Oracle ERP\*, Peoplesoft\*, TIBCO\*
- Directories: Microsoft, Oracle Sun, Novell, UNIX vendors, CA
- Remote Control and Monitoring: IBM, HP iLO, Sun, Dell DRAC, Digi\*, Cyclades\*, Fijitsu\* and ESX
- Configuration files (flat, INI, XML)

\* This plug-in may require customizations or on-site acceptance testing.



**CYBERARK®**  
The Identity Security Company™

## DATA SHEET

# CyberArk® Secrets Management

Enables organizations to centrally secure machine identities used by applications in cloud and hybrid environments

## The Challenge

Enterprises use DevOps methodologies and automation tools to improve business agility and also leverage a variety of commercial, internally developed and even legacy applications – each using credentials and machine (non-human) identities to access IT and other resources. While application, cloud and IT environments can vary significantly, the credentials need to be secured regardless of the app type and compute environment. This can be challenging for security, cloud operations and compliance teams:

- **Application credentials and machine identities are widespread** – they include credentials used by in-house developed apps, commercial off the shelf solutions (COTS), security tools such as vulnerability scanners, application servers, Robotic Process Automation (RPA) and CI/CD tool chains. Additionally, IoT devices are vulnerable unless their credentials are secured.
- **Machine identities need to be managed** – in addition to eliminating hard-coded credentials, requirements include strong authentication, least privilege, role-based access controls, secrets rotation or dynamic secrets, and audit.
- **Vault sprawl needs to be avoided** – when secrets are scattered across multiple vaults each vault becomes an “island of security”, preventing security teams from establishing a single centralized view of secrets, resulting in operational and security challenges.
- **Unmanaged secrets need to be identified** - when secrets are unknown and unmanaged, the level of risk and exposure can be impossible for security teams to determine.
- **Automated processes are incredibly powerful** – they can access protected data, scale at unparalleled rates, leverage cloud resources, and rapidly execute business processes. However, even simple scripts can contain powerful, unprotected (e.g., hard-coded) credentials that attackers can exploit.

## KEY BENEFITS

### For Security Teams

- Protect against breaches by managing credentials used by machine identities.
- Reduce vault sprawl by centrally managing secrets across multiple project teams and environments.
- Prevent credential theft by eliminating hard-coded secrets.
- Discover and gain insights on unmanaged secrets.
- Simplify securing identities with secrets management that's part of the most complete and extensible Identity Security Platform

### For Operations

- Improve efficiency with automated rotation, APIs and automation tools.
- Secure mission critical applications running at scale.

### For Developers

- Offer flexible solutions which do not require changes to dev workflows and provide option of rotated or dynamic secrets.
- Enable developers to use the CSP's built-in (native) secrets managers.
- Simplify how third party apps securely access resources by leveraging APIs and hundreds of certified out-of-the-box integrations.

### For Compliance and Audit

- Leverage a unified security solution to simplify meeting compliance and regulatory requirements.

It is critical that both human, machine and other non-human identities are consistently managed and secured across the enterprise, from cloud consoles, to databases, applications, and other sensitive assets.

## The Solution

CyberArk Secrets Management is designed to centrally manage, and secure secrets used by the broadest range of application identities in cloud-native and hybrid environments. The solution helps security teams offer developers solutions “that meet them where they are” for example by offering APIs for cloud portability, dynamic or rotated secrets, or for teams that have embraced a specific technology, transparent integrations with the Cloud Service Provider’s built-in secrets manager. Additionally, the platform helps security teams discover unmanaged secrets and gain visibility to secrets across the entire enterprise, apply consistent policies, simplify audit and reduce vault sprawl.

- **For cloud-native applications built using DevOps methodologies** – Several solutions are offered, each of which solve a unique set of use cases.
  - **For multi-cloud, cloud portability and DevOps environments** – [Conjur Cloud \(SaaS\)](#) and Conjur Secrets Manager Enterprise (Self-Hosted) provide secrets management solutions designed for the unique requirements of multi-cloud and multi-vendor DevOps environments. Conjur offers REST APIs and integrates with a wide range of DevOps tools, container platforms, and supports hybrid and multi-cloud environments. Developer resources and Conjur Open Source are also available at <https://developer.cyberark.com/>
  - **For teams that have embraced the CSP’s built-in (native) secrets stores** – [Secrets Hub](#) enables security teams to discover, centrally manage and rotate secrets in built-in (native) secrets stores without changing the developers experience. The SaaS solution provides security teams with visibility, helps reduce vault sprawl across multiple AWS and Azure project teams and simplifies securing hybrid environments.  
  
Conjur Cloud and Secrets Hub are part of the CyberArk Identity Security Platform which provides a comprehensive enterprise-wide platform for securing human and machine identities across the entire organization.
- **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. Now, instead of storing privilege credentials in COTS solutions, they are managed by CyberArk. And 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.

[CyberArk Secrets Management](#) provides robust enterprise-grade capabilities and integrates with existing systems to help organizations protect and extend established security models and practices.

# Capabilities

Secrets Management solutions are designed to help organizations:

- **Establish strong authentication** – by leveraging the native attributes of applications, containers, and other machine identities to eliminate the “secret zero bootstrapping” challenge and potential vulnerability.
- **Manage and rotate secrets** – by leveraging dual accounts and other techniques. Offer option of dynamic secrets as an alternative to rotation.
- **Secure unmanaged secrets** - by discovering and gaining insights on unmanaged secrets in the cloud provider’s built-in vaults.
- **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** – by tracking access and providing tamper-resistant audit.
- **Consistently apply access policies** – by applying role-based access controls on machine identities, leveraging integrations with other CyberArk and partner solutions to centralize policy management across the enterprise.
- **Reduce cyber debt** - by enabling automation (leveraging APIs, etc.) and using discovery and insights to help prioritize securing unmanaged secrets.
- **Ensure business continuity and other enterprise requirements** – by designing for scalability, availability, redundancy and resiliency. (including capabilities such as Conjur Cloud Edge).
- **Simplify deployment** – With both SaaS and self-hosted secrets managers and support for SaaS and Self-Hosted versions of the CyberArk Vault.

## OVERVIEW

### Cloud Native and DevOps Integrations:

- Tools/Toolchains: Ansible, Jenkins, Puppet, Terraform
- Public Clouds: AWS, Azure, GCP
- CSP Built-in Secrets Stores: AWS Secrets Manager, Azure Key Vault
- PaaS/Container Orchestration: Kubernetes, Red Hat OpenShift, Rancher, VMware Tanzu
- Container Security: Aqua, Twistlock

### Native Authenticators:

- Kubernetes
- Red Hat OpenShift
- AWS Secrets Manager (ASM)
- AWS IAM
- Azure Key Vault (AKV)
- Google Cloud Platform (GCP)
- JSON Web Token (JWT)
- OpenID Connect (OIDC)

### Discovery Capabilities

- AWS secrets stores

### COTS Application Integrations:

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

### Application Server Integrations:

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

### 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

### CyberArk Vault Integrations:

- CyberArk Privilege Access Manager (Self-hosted)
- CyberArk Privilege Cloud®



For more information about CyberArk Secrets Management or to request a demo, visit the CyberArk Secrets Management [product page](#).

If you're interested in more information regarding our full suite of solutions for securing cloud workloads and developer access visit the [Cloud Workloads Identities](#) Solution page, and to learn more about securing secrets for hybrid IT environments visit the [Secrets for Hybrid IT](#) Solutions page.

## CyberArk Identity Security Platform

[Secrets Management](#) 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 machine identities across the enterprise.



©Copyright 2024 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 01.24. Doc. TSK-5607

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.

[www.cyberark.com](https://www.cyberark.com)

# CyberArk Endpoint Privilege Manager for Linux

## The Challenge

Linux is ubiquitous — modern IT implementations, applications and DevOps pipelines are predominately Linux based. In fact, 43% of the top 1 million websites are powered by Linux, compared to just 23% for Windows.<sup>1</sup> Linux systems run business-critical applications and contain confidential data, and are a high-reward target for threat actors. Adversaries are increasingly setting their sights on Linux-powered assets, using privileged Linux accounts as means to get to them.

Many organizations allow users to work as superusers (using “su” or even working under root). IT administrators, application developers, database administrators and others have permanent superuser privileges. Threat actors routinely abuse privileged or over-privileged Linux accounts to launch attacks and exfiltrate data.

Linux offers a native way of reducing the risks associated with privileged accounts by enforcing least privilege. The Linux “sudo” command gives administrators and other entitled users the minimum set of privileges they need to perform their jobs. sudo is short for ‘superuser do’, as in a sudo

user can do what a superuser can do. It lets you temporarily elevate a user to run specific commands without logging in as root.

sudo is a powerful tool. But configuring sudo access control lists (ACLs), particularly on a large scale, is no easy matter. sudo configuration files (sudoers) are notoriously long and complex, and frequently misconfigured. Threat actors can take advantage of configuration mistakes to gain privileged access.

### In short, Linux’s sudo:

- Provides native least privilege capabilities
- Is often overprivileged
- Is difficult to manage at scale
- Can be circumvented
- Lacks central reporting necessary for audits
- Stores logs locally, subject to tampering

### HIGHLIGHTS

- Enforce least privilege and implement foundational security controls across Linux servers and workstations — at scale and with a native user experience
- Tightly control the commands and tasks each Linux user is permitted to execute based on role
- Strengthen security with advanced controls, such as enforcing policies on commands within scripts or restricted shells
- Centralize and unify privilege management for Windows, macOS and Linux endpoints across the enterprise
- Avoid manually intensive and error-prone administrative processes, and free up staff to focus on other tasks
- Simplify audits, improve compliance with government and industry regulations, and demonstrate cyber readiness for insurance underwriters
- Accelerate time to value with a SaaS solution that delivers cloud agility, economics and ease-of-operations

<sup>1</sup> World Wide Web Technology Surveys, February 2022



Moreover, most Linux distributions provide no native capabilities for provisioning, administering or auditing sudo configurations across systems. Many organizations usually rely on manual processes to manage privileges across Linux endpoints — a time-consuming, error-prone approach that squanders resources and is difficult to scale.

In addition, sudo provides no centralized event reporting capabilities to assist with compliance audits or security investigations. Events are logged locally on each machine. It is difficult for IT and security professionals to aggregate and correlate events across systems to isolate security incidents or examine compliance-related activity. In addition, system log files can be accidentally modified or intentionally tampered with by users with elevated privileges. Finally, there's no ability to enforce policy within restricted shells or scripts.

## The Solution

CyberArk Endpoint Privilege Manager™ for Linux provides foundational endpoint security controls and is designed to enforce the principle of least privilege for Linux servers and workstations. The solution eliminates manually intensive, error-prone sudo administrative processes, allowing endpoint security managers to centrally configure sudo and enforce least privilege across Linux systems, at scale, based on policy.

CyberArk Endpoint Privilege Manager for Linux is an integral component of CyberArk Endpoint Privilege Manager — a comprehensive endpoint security solution that provides single pane-of-glass administration and centralized, policy-based privilege management for Windows, macOS and Linux endpoints.<sup>2</sup> With Endpoint Privilege Manager, security professionals can centrally manage geographically dispersed, heterogeneous endpoints in a consistent manner from a single SaaS console.

Endpoint Privilege Manager can provide visibility and control over all enterprise endpoints, including remote endpoints that infrequently connect to the corporate network. A flexible reporting engine and detailed event journal make it easy to provide evidence for compliance audits, to support forensics investigations, and to demonstrate cyber readiness and proof of required security controls to insurance underwriters.

Endpoint Privilege Manager REST APIs allow you to tie activity and event auditing into your existing security information and event management (SIEM) platforms. And Endpoint Privilege Manager's policy engine is accessible via API for integration with external policy orchestration and automation tools.

Endpoint Privilege Manager is delivered as a SaaS solution for rapid deployment, simple operation and easy integration with other cloud-based services. A SaaS deployment model helps you accelerate time to value and reduce TCO by avoiding on-premises equipment expenses and operations hassles.

### CAPABILITIES

- Simple sudo policy management and enforcement (elevate or block individual specific commands and parameters based on policy)
- Configurable policy audit reports for compliance and forensics (determine when policies were triggered and by whom, and identify corresponding applications and endpoints, actions performed, etc.)
- Sudo with password prompt or passwordless
- Standard sudo command syntax for smooth adoption
- REST APIs for policy automation and external system integration
- Agent CLI for support and status monitoring
- Local logging with multiple verbosity options
- Integral agent downloader and installer
- Upgrade or uninstall agents directly from the EPM console

<sup>2</sup> CyberArk Endpoint Privilege Manager is available for workstations and for servers



# CYBERARK REMOTE ACCESS

SECURELY AND QUICKLY CONNECT EXTERNAL VENDORS AND EMPLOYEES MANAGING YOUR IT ASSETS—WITHOUT THE NEED FOR VPNS, AGENTS OR PASSWORDS

## THE CHALLENGE

Many businesses today rely on external vendors and remote employees to manage portions of their IT infrastructure. To successfully carry out their tasks these external service organizations require inherent privileged access to corporate IT systems. However, extending enterprise privileged access management solutions and practices to the remote workforce can be challenging when using conventional user authentication and authorization approaches.

Traditional enterprise identity management systems and access control solutions, designed to authenticate company employees and corporate-owned devices, aren't well suited for securing third-party staff and devices connecting to internal systems from outside the perimeter in today's modern world. Most businesses have little-to-no visibility or control over remote access to the enterprise network. Providing corporate workstations to every vendor is not a feasible strategy for a variety of reasons and deploying VPNs or agents on another company's laptops or desktops is often too much overhead for IT teams to manage. Alternatively, third-party staff and access requirements can change from day-to-day or week-to-week, making conventional identity management schemes based on user IDs and passwords impractical, and also adding them to the directory can be very costly both from a security and financial perspective.

With a dissolved perimeter, an increase in employees working remotely and a growing reliance on outsourced operations, enterprise IT operations and security teams alike must find innovative ways to grant external vendors secure access to privileged accounts without disrupting operations.

## THE SOLUTION

CyberArk Remote Access is specifically designed to provide fast, easy and secure privileged access for external vendors that need to access critical internal systems managed by CyberArk. With this solution, organizations can secure access to critical business data and infrastructure, support a distributed workforce, accelerate business in the cloud and drive customer experiences. The cloud-based, multifactor authentication provided with Remote Access leverages the biometric capabilities from smartphones or the combination of SMS and email for users without smartphones, which in turn allows authorized external vendors to securely and simply access privileged assets. Remote Access integrates with CyberArk Privilege Cloud for a full SaaS deployment to secure the remote privileged workforce (it also integrates with Privilege On-Premises if preferred).

Remote Access eliminates the need for VPN clients, security agents or passwords that can add risk, create administrative headaches and frustrate end-users. Instead, external vendors authenticate using native smartphone facial or fingerprint recognition functionality and are provisioned and authenticated for secure access to CyberArk. Remote Access combines Zero Trust access, biometric multi-factor authentication, just-in-time provisioning and full integration with CyberArk Privileged Access Manager (Cloud or On Premises), for full visibility and audit for administrators.

## HOW IT WORKS

When an external vendor attempts to log in to CyberArk's web portal, Remote Access displays a one-time, short-lived QR code on their workstation. Using the Remote Access mobile app the user scans the QR code and simultaneously authenticates their identity by means of facial or fingerprint recognition. If both the QR code and the biometric data are

## ONBOARDING

The Remote Access mobile app runs on iOS and Android phones. Once the app is downloaded, the remote user receives an email sent from the organization to access the Remote Access site. Remote users confirm their identity by verifying the email address and registered phone by entering a passcode received through SMS.

Biometric authorization is also used to verify and authenticate the user identification and can be mandated during the onboarding process to ensure successful first time log on. Biometric data is securely stored natively on the user's mobile device. The Client uses the hosted Remote Access console to manage external user accounts and audit activity. For remote users who cannot use or do not have smartphones, Remote Access can also provide multi-factor authentication via SMS and email tokens.

## WHY 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](http://www.cyberark.com).

approved, the remote user is granted secure access to the CyberArk web portal and authorized to access critical systems from their workstation. For remote users who cannot use or do not have smartphones, Remote Access can also provide multi-factor authentication via SMS and email tokens. The web browser session is isolated, and credentials are never shared to the end user's workstation when they enter into critical IT systems for regular work, maintenance or otherwise. The session is encrypted end-to-end.

CyberArk Privileged Access Manager, whether deployed in the cloud or on-premises, mitigates risks by helping enterprises efficiently manage privileged account access rights, proactively monitor and control privileged account activity, intelligently identify suspicious activity, and quickly and automatically respond to threats. Remote Access provides just-in-time user provisioning and access for external vendors, who are not part of the company directory service, to ensure critical assets are only accessed when necessary. The integration also provides enterprise operations and security teams full visibility and control over remote users' privileged access activities.

## BENEFITS

- **Mitigate security risks.** Implement Zero Trust access for remote workers connecting to sensitive systems managed by CyberArk Privileged Access Manager. Improve security posture with just-in-time provisioning to privileged accounts all while avoiding passwords, tokens and network-based access controls that can introduce vulnerabilities and expand attack surfaces.
- **Reduce operational expense and complexity.** SaaS solution streamlines operations by eliminating VPNs, agents and credentials needed for remote access. Temporarily authorize remote users in real-time within the application without administrator intervention and delete vendors by policy when access is no longer required.
- **Simplify remote access for external vendors.** Let authorized users securely authenticate to access privileged enterprise accounts with a simple glance or tap of a finger. Maintain biometric data on the mobile device separate from internal systems, for ultimate privacy and security.
- **Improve visibility and regulatory compliance.** Full integration with CyberArk provides the ability to record and monitor privileged access activity in real-time via isolated browser sessions. Detect in-progress and potential attacks before perpetrators gain access to critical systems and do irreversible harm.
- **REST API Support.** With full support of the CyberArk REST API, organizations are enabled to automatically provision and manage users as well as access audit data. Bulk actions like inviting multiple vendors at once, or deactivating / removing vendors automatically have never been easier.

# CyberArk Vendor PAM

Third-Party Privileged Access: Seamless. Efficient. Secure.

## The Challenge

Modern enterprises engage numerous external third parties, such as vendors, consultants, business partners, system integrators, and maintenance service providers for essential business functions. In fact, 41% of organizations surveyed by CyberArk work with over 100 third parties each. To successfully carry out their tasks, third-party users often require privileged access to IT infrastructure, internal and web-based applications with sensitive data, operational technology (OT), and industrial control systems (ICS).

In many cases, however, organizations struggle to properly secure and provision access for their vendors and contractors. Consequently, a third-party breach becomes a stepping stone for attackers targeting the harder-to-get-into enterprises. For example, 15% of the data breaches under investigation by the U.S. Department of Health and Human Services as of February 2022 involved "Business Associates" who had access to protected health information (PHI). According to SANS 2021 Survey: OT/ICS Cybersecurity, external remote services are the most frequent attack vector in OT incidents. So, it comes as no surprise that 77% of security leaders surveyed by CyberArk viewed third-party risk as a top 10 security concern.

Enterprises must, therefore, defend against attacks targeting third parties, while enabling them to provide the required services. Conventional approaches to achieving this goal include treating third-party identities like employees' and stitching together disparate agent and password-based products to protect external access. Such approaches are inefficient in terms of both the effort and time required to provision access. For example:

- **Processes and tools designed to authenticate company employees and corporate devices aren't well suited for third-party users, particularly those requiring short-term access.** Providing corporate workstations to every external user is not feasible. Adding external parties to the corporate directory can be costly and slow, as it takes days or weeks, to properly provision and de-provision access. Meanwhile, introducing new machines or identities in the directory also increases the attack surface
- **Deploying VPN clients on third-party laptops adds IT management overhead and holds back access provisioning.** Bolting token-based multi-factor authentication (MFA) on top of VPN exacerbates these issues. Identity management schemes based on user IDs and passwords are impractical in the context of frequently changing third-party personnel and access requirements. VPN and passwords also introduce security flaws like overprovisioning standing access with VPN and increasing risk of credential theft with passwords.

With growing reliance on remote working and outsourced operations, IT and security teams alike must find innovative ways to grant external parties secure access to critical systems without disrupting operations.

## The Solution

CyberArk Vendor PAM is a SOC 2 type 2 compliant and **SOC 3 certified** service that helps organizations defend against attacks targeting third-party access, while driving operational efficiencies and satisfying audit and compliance requirements. With this comprehensive, SaaS-based solution for third-party remote access, you can achieve the following:

- Enable third-party user productivity, while protecting critical systems and assets
- Ensure third-party remote access' inherent security and alignment with Zero Trust and least privilege principles
- Reduce the burden on IT related to secure remote access provisioning, maintenance, and deprovisioning
- Gain full visibility and record user activity to streamline compliance pertaining to third-party access.

96%

of organizations allow third parties to access critical systems.

86%

of organizations cited that onboarding third party vendors takes more than 1 business day.

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, just-in-time provisioning, and privileged credential and session management for security, visibility, and audit compliance. With Vendor PAM, authorized third parties can quickly authenticate using their existing smartphones' facial or fingerprint recognition and are provisioned just-in-time, least-privileged access to sensitive enterprise resources and web applications managed by CyberArk Privileged Access Manager (CyberArk PAM).

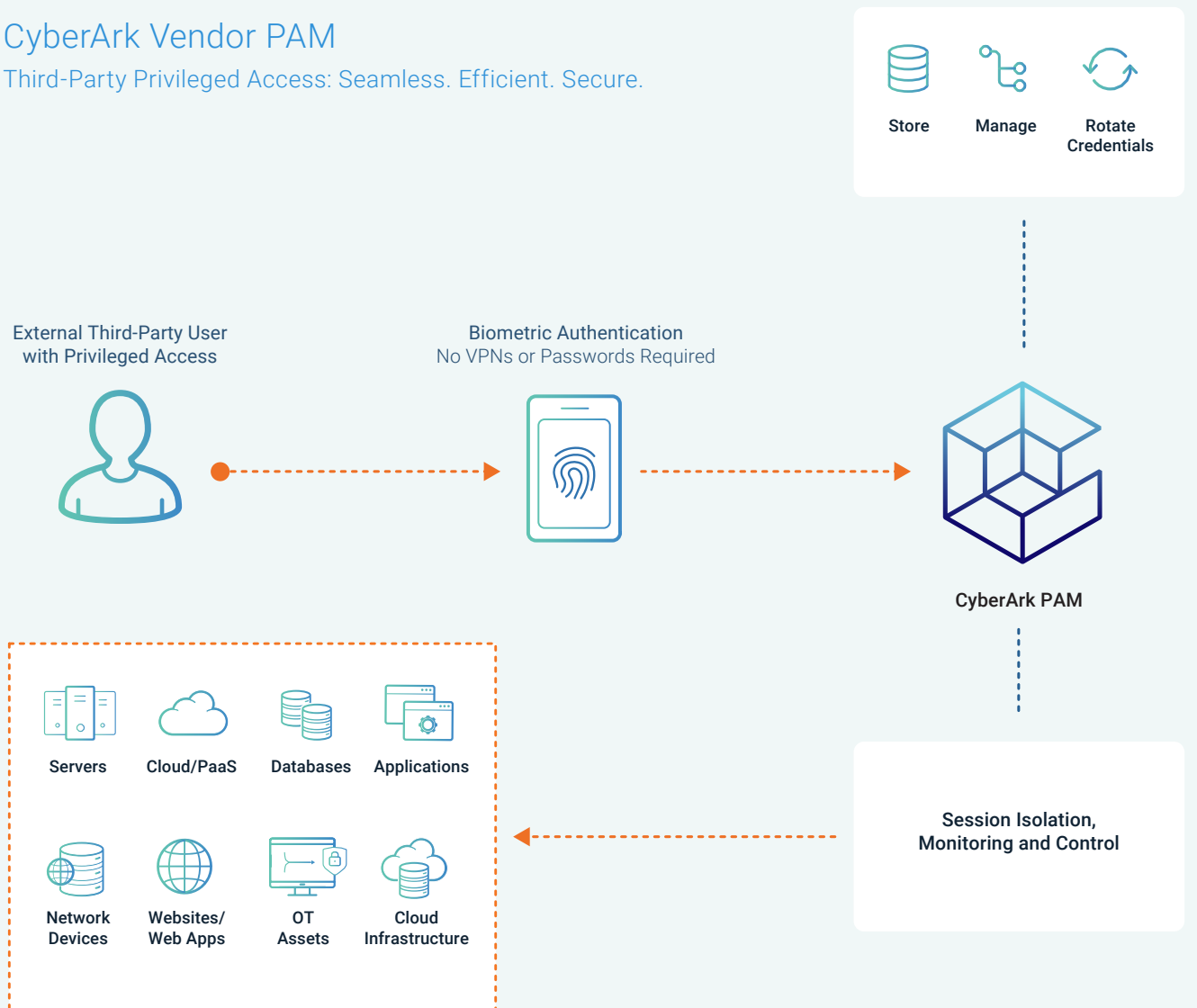
Vendor PAM's Offline Access capability provides authorized users the ability to securely obtain credentials during network or power outages, in air-gapped environments, and other situations in which they can't reach CyberArk PAM. Access credentials are securely stored on an authorized third-party's smartphone,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

## How It Works

When an authorized external third party attempts to log on to the CyberArk PAM's web portal, a one-time, ephemeral QR code is generated and displayed on their workstation. Utilizing the CyberArk Mobile app, the user scans the QR code and simultaneously verifies their identity via facial or fingerprint recognition. Once access has been granted, the third party enters the CyberArk web portal via an isolated, end-to-end encrypted, and monitored web-browser session. Credentials are never shared with the end user's workstation or visible to the end user during privileged sessions.

## CyberArk Vendor PAM

Third-Party Privileged Access: Seamless. Efficient. Secure.



Vendor PAM helps you mitigate risks by efficiently managing privileged account access rights and proactively monitoring and controlling privileged account activity. With Vendor PAM's REST APIs, your team can automatically provision and manage users, perform bulk actions like inviting multiple vendors at once or deactivating users automatically, and easily access data for audit and compliance reporting. Taking advantage of CyberArk PAM's core capabilities, your analysts can swiftly identify suspicious actions and respond to threats coming from 3rd parties.



# Benefits

- Defend against attacks by reducing the risk of privileged account compromise:
  - Leverage Vendor PAM in tandem with CyberArk PAM to securely authenticate external access, reduce risk of credential theft, isolate privileged sessions to prevent the spread of malware, and monitor them to swiftly detect and stop misuse
  - Implement just-in-time, least privilege access and utilize biometric authentication to validate identities in accordance with a Zero Trust security model
  - Automatically deprovision access once it is no longer needed
- Drive operational efficiencies by leveraging existing CyberArk PAM infrastructure and automating access-related IT workflows. Avoid the complexity and cost of shipping corporate devices, provisioning and deprovisioning directory accounts, managing passwords, and installing agents and VPN clients
- Enable the digital business by rapidly onboarding and simplifying access for authorized third parties. Onboard a new user in less than 2 minutes and make authentication as easy as taking a biometric reading on the user's existing smartphone
- Satisfy audit and compliance requirements, as mandated by FIPS 200, HIPAA, PCI DSS, NERC CIP, CFATS, and other regulations, by isolating, recording, and monitoring privileged access sessions in real time, while creating a comprehensive audit trail.

## About CyberArk

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.



©Copyright 2023 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 03.23. Doc. TSK-3570 (TSK-2479)

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.



ITEM	ESPECIFICAÇÃO
1	Solução de Segurança para Identidades e seus Privilégios – Monitoramento de comportamento e mitigação de riscos de usuários administradores da TI, com garantia pelo período de 12 (doze) meses.
2	Solução de Segurança para Identidades e seus Privilégios – Proteção para Aplicações Tradicionais, com garantia pelo período de 12 (doze) meses.
3	Solução de Segurança para Identidades e seus Privilégios – Proteção Local para servidores Windows e Linux, com garantia pelo período de 12 (doze) meses.
4	Privilégios – Proteção Local para Estações de Trabalho, com garantia pelo período de 12 (doze) meses.

## DOCUMENTAÇÃO ONLINE

[https://docs.cyberark.com/identity/latest/en/Content/Resources/\\_TopNav/cc\\_Home.htm](https://docs.cyberark.com/identity/latest/en/Content/Resources/_TopNav/cc_Home.htm) e  
[https://docs.cyberark.com/pam-self-hosted/latest/en/Content/Resources/\\_TopNav/cc\\_Home.htm](https://docs.cyberark.com/pam-self-hosted/latest/en/Content/Resources/_TopNav/cc_Home.htm)

[https://docs.cyberark.com/credential-providers/latest/en/Content/Resources/\\_TopNav/cc\\_Home.htm](https://docs.cyberark.com/credential-providers/latest/en/Content/Resources/_TopNav/cc_Home.htm) OU  
[https://docs.cyberark.com/conjur-enterprise/latest/en/Content/Resources/\\_TopNav/cc\\_Home.htm](https://docs.cyberark.com/conjur-enterprise/latest/en/Content/Resources/_TopNav/cc_Home.htm)

[https://docs.cyberark.com/epm/latest/en/Content/Resources/\\_TopNav/cc\\_Home.htm](https://docs.cyberark.com/epm/latest/en/Content/Resources/_TopNav/cc_Home.htm)

[https://docs.cyberark.com/epm/latest/en/Content/Resources/\\_TopNav/cc\\_Home.htm](https://docs.cyberark.com/epm/latest/en/Content/Resources/_TopNav/cc_Home.htm)

**COMPONENTES ENVOLVIDOS**

**SKU**

**(PAM + PTA) + IDENTITY**

**CCP OU CONJUR**

**EPM PARA SERVIDORES**

**EPM PARA DESKTOP**