CYBERARK®

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 3rd 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.

CYBERARK®

©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.