CYBERARK

DATA SHEET

CYBERARK® PRIVILEGED ACCESS MANAGER SELF-HOSTED

THE CHALLENGE

Privileged accounts and the access they provide represent the largest security vulnerability 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. Bad actors can use privileged accounts to disable systems, take control of critical IT infrastructure and gain access to confidential business data and personal information.

Organizations face a number of challenges 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 threats and compliance violations.
- **Monitoring and analyzing threats.** Many organizations lack comprehensive threat analysis tools and are unable to proactively identify suspicious activities and remediate security incidents.
- **Controlling privileged user access.** Organizations often struggle to effectively control privileged user access to critical infrastructure, cloud platforms (IaaS and PaaS), SaaS applications, creating compliance risks and operational complexity.
- **Securing remote vendors.** Most organizations have little-to-no visibility or control over remote access to privileged corporate IT systems and infrastructure.

THE SOLUTION

CyberArk Privileged Access Manager Self-Hosted is a part of the CyberArk Identity Security Platform, providing foundational controls for protecting, controlling, and monitoring privileged access across on-premises, cloud and hybrid infrastructure. The solution helps organizations efficiently manage privileged credentials with strong authentication methods, proactively monitor and control privileged account activity, intelligently identify suspicious activity and quickly respond to threats.

- **Enable privileged access with modern Single Sign-On (SSO) and adaptive Multifactor Authentication (MFA).** Access privileged (or corporate) resources with a single set of credentials to enforce stronger password policies, reduce the risk of poor password practices and gain visibility into the access activities across the enterprise. Provide an extra layer of protection with adaptive MFA that leverages user-specific contextual attributes such as location, device and network information to assign risk to each user login attempt and create dynamic access policies.

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

Authentication Methods:

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

Monitoring:

- SIEM integration, SNMP traps, Email notifications

Continued on the next page...

SPECIFICATIONS

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
- 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)
- Public Cloud Environments: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)

* This plug-in may require customizations or on-site acceptance testing. Please consult CyberArk Sales Engineering for more details.

- **Centrally secure and control access to privileged credentials based on administratively 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 remote sessions and record all activity during that session. Credentials are retrieved by the solution and sent directly to the target system, so neither the end user nor their machine is exposed to the credential. End users never directly connect to target systems, reducing the risk of movement from potential malware on an endpoint to a target system.
- **Manage Nomadic Devices.** Enforce security policies and rotate credentials of accounts on endpoints that are not always connected to the enterprise network with the Loosely Connected Devices capability.
- **Detect, alert and respond to anomalous privileged activity.** The solution collects data from multiple sources and applies a complex combination of statistical and deterministic algorithms to identify malicious privileged access activity. A bi-directional data feed enables the exchange of high-risk privileged access findings with common SIEM tools.
- **Secure remote access.** Easily and securely authenticate external vendors and remote employees accessing CyberArk with biometric multifactor authentication that is VPN-less, agentless and passwordless. Simply provision authorized users with just-in-time access to critical internal resources and enable automatic session isolation, monitoring and recording.

BENEFITS

- **Defend against attacks.** Strengthen privileged access security. Protect the access to privileged account passwords and SSH keys. Defend systems against malware and attacks. Efficiently detect and respond to suspicious activity and malicious actions. Protect against unauthorized privileged account access, impersonation, fraud and theft.
- **Drive operational efficiency.** Eliminate manually intensive, time consuming and error prone administrative processes. Simplify operations and improve the efficiency of IT security teams. Free up valuable IT staff to focus on strategic tasks to 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.
- **Enable the digital business.** Balance security with a frictionless user experience. Consistently enable seamless access for privileged users connecting to Tier0 assets, with centralized visibility and controls for privileged access management.

©Copyright 2021 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., 11.21. Doc. WRQ-161

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.