The Challenge

Privileged accounts exist in every piece of hardware and software on a network, and they can provide anyone in possession of a privileged accounts with complete access to and control over sensitive information, business applications and critical IT infrastructure. When used properly, these accounts are used to 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. Yet, some organizations neglect to address these risks due to the perceived operational difficulty of finding and managing privileged accounts and their credentials.

To reduce the risks associated with unauthorized access to privileged accounts without over burdening IT teams, organizations should implement tools that proactively secure, automatically rotate and control access to privileged account credentials, which serve as the keys to the IT kingdom. Without such protections in place, organizations will face a number of challenges, including:

• **Increased risk of a successful attack.** Privileged accounts are a critical step in every attack lifecycle. When left unprotected, attackers can easily gain unauthorized access to these powerful accounts and use them to carry out damaging, costly attacks.

• **Audit failures and fines.** Compliance regulations often require organizations to control and audit access to privileged, and often shared, accounts. Without protections in place to control and audit this access at the individual level, organizations can face audit failures and punitive fines.

• **High operational costs.** Some IT teams are tasked with manually rotating and updating privileged account credentials to comply with regulations. These processes are extremely time-consuming and prone to human error. Without tools in place to automate and synchronize credential changes across systems, organizations can face high operational costs as well as lost productivity resulting from accidental account lockouts.

The Solution

CyberArk Enterprise Password Vault is designed to secure, rotate and control access to privileged account credentials based on organizational policies. A flexible architecture allows organizations to start small and scale to the largest, most complex IT environments. The solution protects privileged account credentials used to access the vast majority of systems. With CyberArk Enterprise Password Vault, organizations are able to:

• **Discover privileged accounts and both public and private SSH keys.** CyberArk Enterprise Password Vault automatically discovers and inventories privileged accounts and SSH keys both public and private throughout the entire IT environment. Administrators can select which accounts and authorized key pairs should be protected and automatically on-board them to the Digital Vault.
• **Secure privileged account credentials.** Once provisioned, privileged credentials are centrally secured in the CyberArk Digital Vault. The CyberArk Digital Vault includes multiple built-in security layers to provide the strongest level of protection for privileged account information.

• **Enforce granular access controls and workflows.** CyberArk Enterprise Password Vault enforces granular access controls in accordance with organizational policy. The solution enables authorized users to access privileged accounts needed for day-to-day responsibilities, and it supports automated workflows so that users may request access to accounts with elevated privileges as needed for legitimate business purposes.

• **Automatic password and key rotation.** The solution automatically rotates and synchronizes privileged account credentials in accordance with policy. Passwords and SSH keys can be automatically rotated after each use, at a regular cadence and on-demand.

• **Audit the use of privileged accounts.** CyberArk Enterprise Password Vault requires users to “check-out” credentials before accessing privileged or shared accounts, and it can require users to provide specific justifications when requesting access to accounts with elevated privileges.

• **Automatically invalidate potentially compromised credentials.** The solution is able to receive alerts from CyberArk Privileged Threat Analytics regarding potentially compromised privileged accounts. Upon receiving such an alert, the solution can immediately rotate the impacted password to invalidate the compromised credential.

**Benefits**

CyberArk Enterprise Password Vault proactively protects the keys to the IT kingdom, helping organizations keep sensitive systems and data safe from external attackers and malicious insiders. The solution enables organizations to:

• **Understand the scope of privileged accounts.** Understand what privileged accounts exist and who has access to those accounts to create effective privileged account security policies based on organizational risk tolerance.

• **Mitigate risks by strengthening privileged account security.** By better protecting access to privileged accounts and SSH keys, organizations can reduce the risk of unauthorized privileged access to Windows and *NIX systems, reducing the risk of malicious insider and external attacks.

• **Limit an attacker’s window of opportunity.** Minimize the useable life of credentials to significantly limit the timeframe during which an attacker can use stolen credentials to access privileged accounts.

• **Automatically contain privileged account threats.** Streamline incident response and automate threat containment by immediately invalidating potentially compromised privileged credentials.

• **Demonstrate compliance to auditors.** Clearly show auditors what privileged account policies and processes are in place, and easily report on which individual users accessed what, when and why.

• **Simplify the user experience for authorized privileged users.** Eliminate the need for users to manually manage several sets of credentials and instead enable single sign-on to privileged accounts throughout the organization.

• **Reduce the operational burden on IT teams.** Eliminate the time-consuming, tedious task of manually rotating credentials, and enable IT teams to focus on more strategic projects.

**Specifications**

**Encryption Algorithms:**
- AES-256, RSA-2048
- HSM integration
- FIPS 140-2 validated cryptography

**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), Korean, Portuguese (Brazil)

**Authentication Methods:**
- Username and Password, RSA SecurID, Web SSO, RADIUS, PKI and smartcards (for example PIV), LDAP, SAML

**Monitoring:**
- SIEM integration, SNMP traps, Email notifications

**Supported SSH Platforms:**
- **DNA Discovery:** RHEL 4-6; Solaris Intel and Solaris SPARC 9, 10, 11; SUSE 10; Fedora 18; Oracle Linux 5; CentOS 6; AIX 5.3, 6, 71, ESX/ESXi 5.0 and 5.1
- **SSH Key Security and Management:** RHEL 4-6; Solaris SPARC and Solaris Intel v9, v10, v11; CentOS 6; AIX 5.3, 6, 71, ESX, ESXi v5.1
- **Private Key Security:** Windows XP, Windows 7, Windows Vista, Windows 2008R2, Windows 2012R2

**Target SSH Servers:**
- OpenSSH

**Private Key Formats:**
- OpenSSH, Putty, Tectia

**SSH Key Lengths:**
- 1024, 2048, 4096, 8192

**Automation:**
- Support via REST APIs
• **Build security up front.** Support for REST APIs enable the automation of privileged account management tasks as well as easy integration with existing security tools and solutions.

• **Maximize the value of IT investments.** Leverage out-of-the-box integrations to make the most of complementary investments, such as strong authentication, ticketing, identity access and management, and SIEM solutions.

### A Comprehensive Solution

CyberArk Enterprise Password Vault is a component of the CyberArk Privileged Account Security Solution, a complete solution to proactively protect, isolate, control and continuously monitor privileged accounts on virtual and physical servers, databases, network devices, hypervisors, security appliances, SaaS and business applications and more.

All components of the CyberArk Privileged Account Security Solution share a single common infrastructure, enabling customers to expand the solution to meet changing business requirements. Products in the solution can be managed independently, or combined for a cohesive and comprehensive privileged account security solution.

### Specifications

#### Sample Supported Managed Devices:

- **Operating Systems:** Windows, "NIX, IBM iSeries, Z/OS, OVMS, HP Tandem", MAC OSX*, ESX/ESXi, XenServers
- **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
- **Applications:** CyberArk, SAP, WebSphere, WebLogic, JBOSS, Tomcat, Cisco, Oracle ERP*, Peoplesoft*, TIBCO*, ServiceNow*, BMC
- **Directories:** Microsoft, Oracle Sun, Novell, UNIX vendors, CA
- **Remote Control and Monitoring:** IBM, HP iLO, Sun, Dell DRAC, Digi*, Cyclades*, Fujitsu*
- **Virtual environments:** VMware vCenter and ESX
- **Storage:** IBM, HP iLO, Sun, Dell DRAC, Digi*, Cyclades*, Fujitsu*
- **Cloud-based Applications:** Facebook, Microsoft Azure Management, Amazon Web Services, Twitter*, SalesForce*, LinkedIn*, Microsoft 365*
- **OT/SCADA:** GE*, Industrial Defender*, RuggedCom*
- **Generic Interfaces:** any SSH/Telnet device, SNMPv3 (for credential storing), Windows registry, any web application e.g. Facebook, WMI remote command execution, passwords stored in database tables, Configuration files (flat, INI, XML)

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

©Cyber-Ark 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., 11.17. Doc. 104

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.