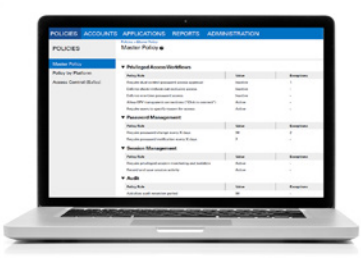
Enterprise Password Vault®

Proactively secure, rotate and control access to privileged account passwords used throughout the enterprise IT environment.



Centrally manage privileged account identities and policies from a single location.

Why CyberArk?

CyberArk is the trusted expert in helping organizations stop the most critical cyber-attacks before they stop business.

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 password 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 places, 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 password 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 passwords based on organizational policies. The solution is proven to scale in the largest, most complex enterprise IT environments, and it can protect privileged account passwords used to access the vast majority of systems. With CyberArk Enterprise Password Vault, organizations are able to:

- **Discover privileged accounts.** CyberArk Enterprise Password Vault automatically discovers and inventories accounts throughout the IT environment. Administrators can select which accounts or groups of accounts should be protected and automatically provision them to the Digital Vault.
- **Secure privileged account passwords.** Once provisioned, privileged passwords 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.
- **Automatically rotate passwords.** The solution automatically rotates and synchronizes privileged account passwords in accordance with policy. Passwords 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" passwords before accessing privileged or shared accounts, and it can require users to provide specific justifications when requesting access to accounts with elevated privileges. This creates a detailed audit trail and enables security and audit teams to easily report on who accessed what, when and why.
- **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 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.
- **Reduce the risk of unauthorized access to privileged accounts.** Centrally secure privileged passwords to prevent the loss, theft or unauthorized sharing of privileged credentials and mitigate the risk of unauthorized privileged account access.
- **Mitigate the risk of an inside attack.** Proactively prevent unauthorized insiders from gaining access to privileged account credentials, and track all privileged account access at the individual level to deter authorized insiders from abusing privileges to cause damage.
- **Limit an attacker's window of opportunity.** Minimize the useable life of passwords 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 passwords.
- **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 passwords, and enable IT teams to focus on more strategic projects.
- **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. The solution includes CyberArk SSH Key Manager, a solution for securing and managing SSH keys, another type of powerful privileged credential. 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

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

Authentication Methods:

- Username and Password, RSA SecurID, Web SSO, RADIUS , PKI and smartcards, LDAP

Windows-based Authentication Monitoring:

- SIEM integration, SNMP traps, Email notifications

Sample Supported Managed Devices:

- Operating Systems: Windows, NIX, IBM iSeries, Z/OS, OVMS, HP Tandem, MAC OS, 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
- Security Appliances: CheckPoint, Nokia, Juniper, Cisco, Blue Coat, IBM, TippingPoint, SourceFire, Fortinet, WatchGuard , Industrial Defender, Acme Packet, Critical Path, Symantec, Palo Alto
- Network Devices: Cisco, Juniper, Nortel, HP, 3com, F5, Alactel, Quintum, Brocade, Voltaire, RuggedCom, Avaya, BlueCoat, Radware, Yamaha
- Applications: SAP, WebSphere, WebLogic, JBOSS, Tomcat, Oracle ERP, Peoplesoft, TIBCO, Cisco
- Directories: Microsoft, Sun, Novell, UNIX vendors, RSA, CA
- Remote Control and/ Monitoring: IBM, HP iLO, Sun, Dell DRAC, Digi, Cyclades, Fijitsu
- Virtual environments: VMware vCenter and ESX
- Storage: NetApp
- Generic Interfaces: any SSH/Telnet device, Windows registry, any web application e.g. Facebook, WMI remote command execution, passwords stored in database tables, Configuration files (flat, INI, XML)