Enterprise Password Vault®

Enforce an enterprise policy that protects your most critical systems, managing the entire lifecycle of shared and privileged accounts across data centers.

Retrieve privileged credentials and approve access directly from your mobile device for secure anytime, anywhere access to your privileged accounts.

EPV delivers one central dashboard console for managing all types of privileged identities.

Why CyberArk?

CyberArk is the trusted expert in stopping cyber attacks before they stop business.

The Challenge

One of today's biggest IT security risk and compliance challenge is the mismanagement of privileged identities and their passwords. Privileged and shared accounts exist in virtually every device or software application in an enterprise, such as 'root' on a UNIX/ESX server, Administrator on a Windows workstation, dedicated break-glass accounts, fire IDs, SAP shared accounts, Cisco Enable, Oracle system/sys, MSSQL SA and many more. As an organization's most critical "Keys to the Kingdom," privileged accounts require extra care. Ironically, these accounts are often neglected, rarely changed, and almost impossible to track or control who used them and when. If mismanaged, privileged accounts impose great risk to organizations, including:

- **Audit Failures.** Compliance regulations (such as Sarbanes Oxley, PCI, Basel III and others) require organizations to provide accountability about who accessed shared accounts, when and whether the request was based on enterprise policy.
- **Internal and External Threats.** Insider threats still remain a major concern for large enterprises today. 86% of insider incidents are perpetrated by people with system administrator access; on average half are no longer supposed to have privileged access (CERT/Secret Service Studies). External targeted attacks are also making headlines where perpetrators are going after privileged accounts to access the organization's most sensitive systems and data.
- **Downtime.** Inaccessibility of a critical password by an on-call administrator may cause hours of delay in recovering from system failure, resulting in loss of business to organizations and costly outages.
- **Administrative Overhead.** With hundreds of network devices, privileged identities can be extremely time-consuming to manually update and report on, and more prone to human errors.

The Solution

Enterprise Password Vault (EPV) allows organizations to secure, manage, automate and log all activities associated with privileged accounts. With Password Vault®, you can:

Minimize Threats. With CyberArk's unique Digital Vault, privileged credentials are secured and pre-defined policies enforce workflows to access privileged accounts, including integration with ticketing systems, scheduled password changes, managerial approval and more.

Approach Compliance with Confidence. Improve the day-to-day operations as well as the audit compliancy process with easy to use audit reports, as required by Sarbanes-Oxley, PCI and others.

Do Business Better. Enable enterprises to automatically provision, secure and manage access to hundreds of thousands of privileged accounts via a central repository.

CyberArk's Password Vault offers you unique value:

- Minimize loss of business and costly outages by enforcing an enterprise policy that protects your most critical systems
- Ensure accountability of every access to your most sensitive data with advanced out-of-the-box monitoring and reporting tools
- Improve workforce productivity with a simple access control interface for managing privileged identities and automatic discovery capabilities for new or removed machines
- Protect your sensitive assets when working with third parties by enabling direct connection to the target device, without disclosing the privileged credential or enable automatic connection to local/remote systems

- Automate privileged account management in the Private Cloud and improve VMware admin efficiency to discover and manage ESX hypervisors and all guest machines

Benefits

Enterprise Password Vault (EPV) utilizes CyberArk's award-winning Digital Vault Technology to store, protect and log access to privileged accounts with the utmost security. The Digital Vault provides numerous underlying security capabilities for authentication, encryption, tamper-proof audit and data protection. Additionally, the Password Vault offers a robust set of capabilities such as:

- **Extensive Amount of Supported Target Systems.** Password Vault supports the widest variety of platforms in the market and allows for easy extensibility to new devices, to meet enterprise-class unique requirements, allowing full scale implementation across the IT infrastructure. You can also extend privileged access control to sensitive web applications such as Salesforce, the Corporate Facebook account or any web-based ERP/ CRM applications.
- **Customizable Request Workflows.** With EPV enterprises can easily integrate with their help desk and ticketing systems, to enforce entering a valid ticket when requesting access to privileged accounts. The solution offers powerful dual control approval process, as well as exclusive check-out/check-in for limited times, automatically changing the password thereafter. Request and approval workflows are also supported from mobile devices.
- **Web Interface & Built-in Reports for Users and Auditors.** EPV offers a flexible access control mechanism to create personalized views of managed devices. Auditors can have direct access to a reporting web application and schedule reports as needed. A unique dashboard presents important audit statistics and an overview of activities in the system.
- **Direct Connection to Managed Devices.** For ease of use and improved efficiency, EPV provides direct access to Windows, Unix/ Linux and other SSH devices, using the requested privileged account, with an option of not exposing the credentials to end users. This capability is also extended to websites and web applications where it is particularly important to replace or not expose the password as when employees leave the organization, they still have access to the website.
- **Self Recovery Capabilities.** EPV can automatically reconcile passwords, with no human intervention when a password is detected as 'non-synchronized'.
- **Automatic Provisioning of Accounts.** Using the enterprise directory or the vCenter environment, EPV can automatically provision privileged accounts, as well as reflect any changes such as new or removed devices on the network, including new administrator accounts created in the local Administrators group and ESX hypervisor root accounts. With our unique auto discovery capability, an automatic notification will be sent if an unmanaged service account is detected within the policy and reports can be retrieved for an overall picture of unmanaged accounts.
- **Central Management with Distributed Reach.** CyberArk's distributed architecture can locate multiple Central Policy Manager Servers for managing accounts on different network segments utilizing a single Password Vault for secure storage enabling unparallel scalability, centralized audit, access control and user management.
- **Enterprise Readiness.** Easily integrates with the enterprise infrastructure offering additional value to an existing solution.

A Comprehensive Solution

CyberArk Enteprise Password Vault is a component of the CyberArk Privileged Account Security Solution, a complete solution to protect, monitor, detect, alert, and respond to privileged accounts. Products in the solution can be managed independently, or combined for a cohesive and complete solution for operating systems, databases, applications, hypervisors, network devices, security appliances and more. The solution is based on the CyberArk Shared Technology Platform which delivers enterprise-class security and allows customers to deploy a single infrastructure and expand the solution to meet changing business requirements.

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)*