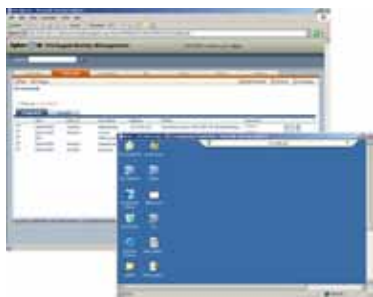


Enterprise Password Vault®



Enterprise Password Vault® (EPV) secures, manages, automatically changes and logs all activities associated with privileged and shared accounts.



Intuitive web access interface provides quick access to personalized views of your privileged accounts, with direct access to remote devices.

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 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 and Basel II) require organizations to provide accountability about who accessed shared accounts, when and whether the request was based on enterprise policy.
- **Insider Threats.** A major concern of large enterprises today is the insider threat. 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).
- **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), a two-time award winning (SC Magazine's 'Best Buy' and Network World's 'Clear Choice') part of Cyber-Ark's Privileged Identity Management (PIM) Suite enables organizations to secure, manage, automate and log all activities associated with privileged accounts by:

Protecting Privileged Accounts. PIM Suite utilizes the patented Cyber-Ark Vaulting Technology® to store, protect, control and log access to privileged accounts. The solution offers a simple access control interface that easily pinpoints who is entitled to use privileged accounts when and why.

Enforcing Enterprise Policy and Workflows. Policies are used to define and enforce access workflows to privileged accounts, including ticketing system integrations, scheduled password changes and more. EPV assures policy enforcement, while eliminating administrative overhead from the IT/IS teams.

Complying with Audit Regulations. EPV provides easy to use audit reports, as required by Sarbanes-Oxley, PCI and more, as well as proving adherence to regulatory requirements and security best practices related to access and usage of privileged accounts.

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

Authentication Methods:

- Username and Password
- RSA SecurID
- Web SSO
- RADIUS
- PKI and smartcards
- LDAP
- Windows-based Authentication

Monitoring:

- SIEM integration
- SNMP traps
- Email notifications

Supported Managed Devices:

- Operating System: Windows, Linux/UNIX, OS390, AS400, OVMS, HP Tandem, MAC OS
- Windows Applications: Service accounts, Scheduled Tasks, IIS Application Pools, COM+, IIS Anonymous Access
- Databases: Oracle, MSSQL, DB2, Informix, Sybase, any ODBC compliant
- Security Appliances: CheckPoint, Nokia, Juniper, Cisco, Blue Coat, Fortinet
- Network Devices: Cisco, Juniper, Nortel, F5, Alactel, Quintum
- Applications: SAP, WebSphere, WebLogic, JBOSS, Tomcat, Oracle ERP
- Directories: Microsoft, Sun, Novell
- Remote Control and/ Monitoring: IBM, HP iLO, Sun, Digi
- Generic Interfaces: any SSH/Telnet device, Windows registry



EPV delivers one central dashboard console for managing all types of privileged identities. Reports are available to auditors in self-service formats or exportable to Microsoft Excel.

FEATURES & BENEFITS

EPV utilizes Cyber-Ark's patented Digital Vault Technology™ that was designed to meet the highest security requirements for managing the "Keys to the Kingdom." The Digital Vault provides numerous underlying security capabilities for authentication, encryption, tamper-proof audit and data protection. Additionally, EPV offers a robust set of capabilities such as:

- **Extensive Amount of Supported Target Systems.** EPV supports the widest variety of platforms in the market, including over 50 operating systems, databases, fire walls, network devices, routers and key systems such as LDAP, Active Directory, SAP and more. EPV also allows easy extensibility to new devices, to meet enterprise-class unique requirements, allowing full scale implementation across the IT infrastructure.
- **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, to assure individual accountability. The system also assures privileged accounts will be available only for the requested time frame, and will be automatically checked-in and changed when this time frame elapses.
- **Web Interface 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. A unique dashboard presents important audit

statistics and an overview of activities in the system.

- **Direct Connection to Managed Devices.** To allow ease of use, EPV provides direct access ("Connect" or from a desktop shortcut) to the Windows/SSH devices, using the requested privileged account, with an option not to expose the credentials to end users.
- **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, EPV can automatically provision privileged accounts, as well as reflect any changes such as removed devices or new devices that joined the network.
- **Central Management with Distributed Reach.** Cyber-Ark's distributed architecture can locate multiple Central Policy Manager Servers for managing accounts on different network segments in a single product instance with centralized audit, access control and user management.
- **Enterprise Readiness.** Easily integrates with the enterprise infrastructure. This includes LDAP and IAM integration for user management and automatic account provisioning; use of Windows domain, RADIUS, PKI, SSO or RSA SecurID for authentication; monitoring and SEIM integration using SNMP, Syslog and SMTP; integration with ticketing and workflow systems; robust SDK, built-in HA/DR and much more!

THE POWER OF PIM

EPV is part of the market leading PIM Suite, a full life cycle solution for centrally managing privileged and shared identities, as well as embedded passwords found in applications and scripts. PIM enables organizations to secure, provision, manage, control and monitor all activities associated with all types of Privileged Identities and Accounts, by either human or unattended services. Furthermore, PIM allows monitoring privileged sessions and provides secure remote access to managed devices, using privileged SSO, without exposing powerful credentials to end users. ■