Cyber-Ark®
Security That Empowers People™

Privileged Identity Management 6.0

The Privileged Identity Management Suite is an enterprise-class, unified policy-based solution that secures, manages and tracks all privileged accounts and activities associated with datacenter management whether on-premise or in the cloud.

Approach Compliance with Confidence

Superior security that protects the 'Keys to the Kingdom' with a proven detailed audit trail to meet regulatory requirements.

Eliminate Insider Threats

Out-of-the-box best practices for defining and enforcing a unified policy for privileged identity management across your IT infrastructure whether on-premise or in the cloud.

Do Business Better

Improve workforce productivity with a single access point for handling privileged credentials.

THE CHALLENGE

In today's environment, organizations spend a great deal of resources building an infrastructure for securing their enterprise, assuring business continuity and meeting compliance requirements. Typical enterprise IT environments are comprised of hundreds or thousands of servers, databases, network devices and applications, all controlled and managed by a variety of privileged and shared administrative identities—some forms of which are known as breakglass, emergency or fire IDs—which are the most powerful in any organization. This includes the "root" or "oracle" accounts on UNIX/Linux, Administrator in Windows, Cisco Enable, Oracle database system/sys, MSSQL sa and many more. Ironically, the security, control and auditability of these privileged identities is often neglected, their usage difficult to monitor, and their passwords less frequently changed than personal non-privileged accounts, if at all. In some cases, these identities are required not only by the internal IT personnel but also by external 3rd party vendors and thus require extra care, such as secure remote access and secure session initiation without exposing the credentials. Powerful passwords are also often found hard coded inside applications, scripts and parameter files, leaving them unsecured, rarely changed and visible to the world. Whether your datacenter is on premise, managed, hosted or in the cloud, mismanagement of the "Keys to the Kingdom", impose great risks to organizations:

- **Insider Threat**
  One of the biggest concerns today is the risk of insider threat. In many organizations, the same root or Administrator password is used across the organization, making it easier for a disgruntled insider to abruptly take down core systems, access or steal sensitive information, or even take control of key business systems.

Facts & Figures:

Cyber-Ark secures 8 of the 10 largest banks in the world.

1 in every 3 Fortune 50 companies have selected Cyber-Ark.

Privileged Identity Management Suite delivers one central console for managing, monitoring and viewing all the forms of privileged accounts that access your most sensitive systems across your organization's IT infrastructure and the privileged commands that are run on them.

- **Loss of Sensitive Information**
  Privileged accounts typically have unlimited access to back end systems. Compromising such accounts may lead to uncontrolled access, bypassing the normal system operation. For instance, this can result in loss of money, regulatory penalties and severe reputational damage.
- **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. Moreover, inaccessibility of such a password by an on-call administrator may cause hours of delay in recovering from system failure.
- **Audit and Accountability**
  Regulations (such as Sarbanes Oxley, PCI and Basel II) require organizations to provide accountability about who accessed shared accounts, what was done, and whether passwords are protected and updated according to policy.

THE SOLUTION

Cyber-Ark's Privileged Identity Management (PIM) Suite is an enterprise-class, unified policy-based solution that secures, manages and logs all privileged accounts and activities associated with datacenter management, from on premises to off-site, hosted environments and all the way to the cloud.

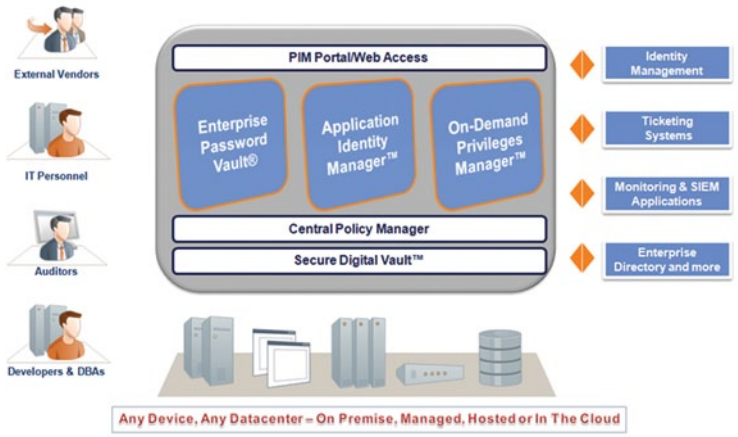
It protects your critical business systems from multiple parties anonymously accessing them on a daily basis, creating a complete, tamper-proof audit trail while concurrently automating all of the processes associated with privileged account management. Moreover, the PIM suite seamlessly integrates with the full range of systems and assets in your organization for more holistic accountability and operational efficiency.

The PIM Suite also complements Cyber-Ark's Privileged Session Management Suite which controls, records and monitors all privileged session connections to servers, databases and virtual environments. By enabling continuous protection, risk management and compliance of these sensitive systems, the extent to which privileged accounts can potentially damage your business is dramatically minimized.

The Cyber-Ark PIM Suite includes the following products:

Enterprise Password Vault®

Cyber-Ark's award-winning Enterprise Password Vault (EPV) enables organizations to secure, manage, automatically change and log all activities associated with all types



of Privileged Accounts. EPV offers industry leading implementation, integration, scalability and robustness for managing hundreds of thousands of servers, databases, network devices and more.

Application Identity Manager™
Cyber-Ark's market-leading Application Identity Manager (AIM) provides the only robust, complete solution to fully address the challenges of hard-coded, embedded credentials and encryption keys. The solution eliminates the need to store embedded credentials in applications, scripts or configuration files, and allows these highly sensitive passwords to be centrally stored, audited and managed within Cyber-Ark's patented Digital Vault.

On-Demand Privileges Manager™
On-Demand Privileges Manager (OPM) is the first unified solution for managing and monitoring superusers and privileged accounts under one roof. Usage of accounts such as 'root' users on UNIX is no longer anonymous and can now be controlled by pre-defined granular access control, where both the command itself and the output are recorded.

Encompassing these products are:
PIM Portal/Web Access
A single multi-lingual web-based access point manages and defines policies for shared and application accounts, allows you to search for recorded sessions and set root permissions in order to execute specific commands on-demand. The PIM Portal is also accessible from mobile phones to securely retrieve credentials or request/approve use of a privileged credential.

Central Policy Manager
A revolutionary engine for privileged account management which automatically manages and enforces enterprise policy on local or remote networks across the enterprise with no human intervention.

Secure Digital Vault
Cyber-Ark's award-winning patented Digital Vault Technology™ protects access control and policy information, stores session recordings and information required for audits. The secure infrastructure ensures that account privileges and recordings cannot be tampered with in transit and at rest.

BENEFITS

With Cyber-Ark's Privileged Identity Management Suite (PIM), enterprises can easily:

Eliminate Insider Threats
PIM manages, protects and controls access to all privileged accounts and makes hard-coded application credentials invisible to developers, database administrators and IT staff.

Meet Compliance and Audit Requirements with Confidence
The PIM Suite creates easy to use, unified audit reports required by Sarbanes-Oxley, PCI and more. It allows enterprises to enforce corporate security policies to ensure compliance with regulatory needs and security best practices related to access and usage of privileged accounts for both human and application (unattended) access.

"We now have a fully-automated, 24/7 system that streamlines operations, lowers enterprise risk, and improves reporting and audit processes"

Burak Öztürk,
Finansbank

Reduce IT Overhead with More Efficient Control and Less Human Error
PIM eliminates manual administration with extremely reliable and uninterrupted service. Minimal administrator overhead results in increased productivity and is less prone to human errors.

Fast and Easy Adoption Means Short Time to Value
PIM is quick to deploy with a proven track record of improving IT productivity. Our experience spans hundreds of enterprise customers in all verticals, providing immediate ROI.

Enterprise-ready
With industry leading performance, scalability and robustness, PIM can protect and manage up to hundreds of thousands of privileged accounts across a highly heterogeneous IT environment, with complex and distributed network architectures. PIM can leverage existing enterprise infrastructure and integrate with core corporate systems.

FEATURES

From streamlining privileged account management to delivering the rock-solid security of a Digital Vault, the many benefits of the Privileged Identity Management Suite are powered by a robust set of system capabilities, such as:

Security and Audit
- Highly secure storage for controlling the "Keys to the Kingdom" utilizing FIPS 140-2 validated cryptography
- Centralized audit management through built-in audit-ready reports as well as self-serve access for auditors and scheduled reports sent directly to the auditor's inbox for periodic reviews
- Sophisticated and flexible web portal for creating personalized views of privileged account access
- Tamper-proof storage for critical corporate PIM-related information, such as audit records, session recordings, policies, and more

Managing Shared and Administrative Accounts
- Out-of-the-box policy based automation and management for a heterogeneous IT environment with over 70 types of managed devices, including most operating systems, databases, firewalls, network devices, routers and more
- Extensible device management architecture with flexibility to introduce support to additional systems and devices as needed
- Self recovery solutions such as automatic reconciliation of out-of-synch passwords
- Automatic discovery and provisioning of accounts ensures that even accounts hidden in services, scheduled tasks, application pools as well as local administrator groups etc are discovered and managed securely, according to enterprise policies
- Direct access to target device without exposing the password to end users as well as a generic interface to transparently connect to any device

On-Demand Privileges
- Granular access control to manage who can run which commands on a personal basis
- Replaces siloed SUDO solutions with enterprise-ready unparalleled security, centralized easy management, and enhanced audit capabilities

Enterprise Readiness
- Integration with enterprise infrastructure, including Directories and User Provisioning integration for user management, authentication products (2-factor, RSA, Radius, PKI, LDAP and more), monitoring and SIEM integration, SNMP, Syslog and SMTP, built-in HA/DR architecture and much more
- Full Software Development Kit (SDK) to integrate with a myriad of enterprise systems
- Distributed architecture with central management and storage that is ideal for multi-network and multi-site environments and benefits from a single administration, audit and monitoring interface with full performance load balancing of password management

2010 Computing Security Awards WINNER

Cyber-Ark wins "Enterprise Security Solution of the Year" for its Privileged Identity Management Suite, Computing Security Awards 2010

"Cyber-Ark PIM suite is among the leading-edge products in the emerging PIM market, providing one of the most comprehensive feature sets in the market."

Martin Kuppinger,
Cyber-Ark Privileged Identity Management Suite (PIM) Product Report

Cyber-Ark®
Security That Empowers People™