CYBERARK®

# Privileged Account Security Solution

Best practices dictate that privileged accounts should be incorporated into an organization's core security strategy. Privileged accounts are a security problem and need singular controls put in place to protect, monitor, detect and respond to all privileged account activity.

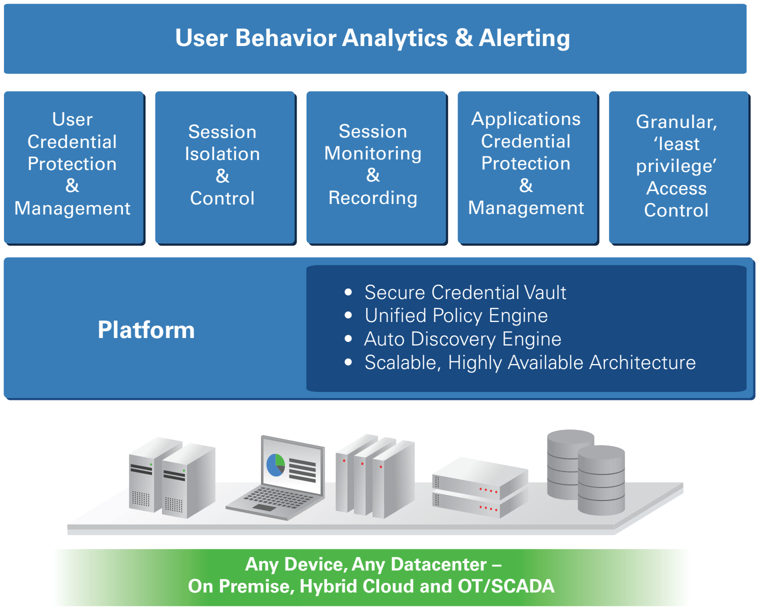
## Why CyberArk?

CyberArk is the only company that can provide full protection from advanced and insider threats to mitigate your risks and meet high stakes compliance requirements. CyberArk has more deployments in large-scale distributed and virtual environments, solving more privileged account security challenges than any other vendor.

Privileged accounts represent the largest security vulnerability an organization faces today. These powerful accounts are used in nearly every cyber-attack, and they allow anyone who gains possession of them to control organization resources, disable security systems, and access vast amounts of sensitive data.

To protect these accounts and the critical resources they provide access to, organizations need comprehensive controls in place to protect, monitor, detect and respond to all privileged account activity.

CyberArk is the trusted expert in privileged account security. Designed from the ground up for security, the CyberArk Privileged Account Security Solution provides the most comprehensive solution for on-premise, cloud and OT/SCADA environments. This complete enterprise-ready Privileged Account Security Solution is tamper-proof, scalable and built for complex distributed environments to provide the utmost protection from advanced external and insider threats.



**User Behavior Analytics & Alerting**

User Credential Protection & Management

Session Isolation & Control

Session Monitoring & Recording

Applications Credential Protection & Management

Granular, 'least privilege' Access Control

**Platform**

- Secure Credential Vault
- Unified Policy Engine
- Auto Discovery Engine
- Scalable, Highly Available Architecture

**Any Device, Any Datacenter –
On Premise, Hybrid Cloud and OT/SCADA**

## CyberArk Shared Technology Platform:

Digital Vault™ : The award-winning, patented Digital Vault is an isolated and bastion hardened server with FIPS 140-2 encryption that only responds to the vault protocols for unmatched security.

Master Policy™ : Master Policy is an innovative policy engine that enables customers to set, manage and monitor privileged account security policy in a single, simple, natural language interface.

Discovery Engine: Designed to continually discover changes to your IT environment, the discovery engine enables constant up-to-date protection and ensures that all privileged account activity is accounted for and secure.

Scalable, Flexible, Low-Impact Architecture: CyberArk's Privileged Account Security Solution was architected for minimal impact and protects your existing investment in your current IT environment.

Enterprise-Class Integration: CyberArk's Privileged Account Security Solution enables organizations to leverage existing investments with out-of-the-box support for numerous devices, networks, servers and applications, including websites and social media.

## Privileged Account Security Products

Every product in the CyberArk privileged account security solution is stand-alone and can be managed independently while still sharing resources and data from the common infrastructure. Working together the products provide a complete, secure solution.

### Enterprise Password Vault™

*Protection, management and audit of privileged credentials*

Enterprise Password Vault prevents malicious use of privileged user passwords, and brings order and protection to vulnerable accounts. Enterprise Password Vault secures privileged passwords based on your privileged account security policy and controls who can access which passwords and when. Automated password rotation reduces the time-consuming and error-prone task of manually tracking and updating privileged passwords to easily meet audit and compliance standards.

### SSH Key Manager™

*Management, rotation and protection of privileged SSH keys*

SSH Key Manager is designed to prevent unauthorized access to privileged accounts protected by SSH keys. SSH Key Manager securely stores and controls access to private SSH keys, manages trust relationships with public SSH keys on systems, and enables organizations to report on who used what keys and when. The product automatically rotates key pairs in accordance with security policies, enabling organizations to strengthen security without burdening the IT team.

### Privileged Session Manager™

*Monitoring, control and isolation of privileged sessions*

Privileged Session Manager enables security teams to rapidly detect and respond to threats inside the network. Real-time monitoring enables organizations to instantly spot suspicious activity, and remote session termination enables security teams to disrupt attacks in process. Searchable DVR-like recordings enable security and audit teams to easily locate events without sorting through any logs. By monitoring, controlling and isolating privileged sessions, the product helps organizations strengthen security, accelerate incident response and meet compliance requirements.

### Privileged Threat Analytics™

*Analytics and alerting on malicious privileged account activity*

As the industry's only targeted privileged threat analytics solution, CyberArk Privileged Threat Analytics identifies previously undetectable malicious privileged user activity. By applying patented algorithms to a rich set of privileged account behavioral data, the solution produces accurate, actionable intelligence, allowing incident responders to disrupt and directly respond to attacks.

### Application Identity Manager™

*Protection, management and audit of embedded application credentials*

Application Identity Manager eliminates hard-coded application credentials including passwords and SSH keys from applications and scripts. The product meets and exceeds high-end enterprise requirements for availability and business continuity, even within complex and distributed network environments. The product eliminates embedded application accounts often without requiring code changes and with zero impact on application performance.

### On-Demand Privileges Manager™

*Least privilege access control for UNIX, Linux and Windows*

On-Demand Privileges Manager allows privileged users to use administrative commands from their native UNIX session while eliminating unneeded root or admin rights. This secure and enterprise ready sudo-like solution provides unified and correlated logging of all super-user activity linking it to a personal username while providing the freedom needed to perform job function. The product continuously monitors all administrative commands super users run based on their role and task.

### Start Assessing Your Privileged Account Risk Today With CyberArk DNA™

CyberArk DNA™ (Discovery and Audit) is a free assessment tool that helps organizations discover where privileged accounts are throughout the enterprise. With a clear accounting of all service accounts, devices, and applications, DNA can help organizations achieve an understanding of the size and magnitude of privileged account security risks. This tool helps organizations prioritize projects based on where they are most vulnerable, and it can be used to assist in building a business case or planning for a privileged account security project.

## Specifications

**Encryption Algorithms:**

- AES-256, RSA-2048
- HSM integration
- FIPS 140-2 validated cryptography

**High Availability:**

- Clustering support
- Multiple Disaster Recovery sites
- Integration with enterprise backup system

**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), Brazilian Portuguese, Korean

**Authentication Methods:**

- Username and Password, LDAP, Windows authentication, RSA SecurID, Web SSO, RADIUS, PKI and smart cards

**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, Twitter, LinkedIn
- WMI remote command execution
- ODBC - passwords stored in database tables
- Configuration files (flat, INI, XML)* - e.g. application server configuration files or any application/script configuration file