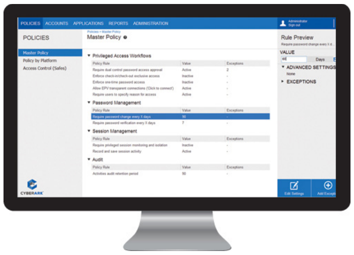
CyberArk Shared Technology Platform

Simplify deployment, unify management, and centralize privileged account security policy management and reporting with the CyberArk Shared Technology Platform.



Privileged Access Workflows

Policy Rule	Value	Exceptions
Require dual control password access approval	Active	2
Enforce check-in/check-out exclusive access	Inactive	-
Enforce one-time password access	Inactive	-
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Active	-

Password Management

Policy Rule	Value	Exceptions
Require password change every X days	90	-
Require password verification every X days	7	-

Session Management

Policy Rule	Value	Exceptions
Require privileged session monitoring and isolation	Inactive	-
Record and save session activity	Active	-

Audit

Policy Rule	Value	Exceptions
Activities audit retention period	90	-

Single pane of glass administrative interface for all privileged account security products delivers streamlined, centralized management and unified reporting.

Why CyberArk?

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

The CyberArk Shared Technology Platform™ serves as the basis for the CyberArk Privileged Account Security Solution and allows customers to deploy a single infrastructure and expand the solution to meet expanding business requirements. Seamless integration of products built on the platform provides organizations with lower cost of ownership, simplified deployment and expansion, unified management, and centralized policy management and reporting.

The Challenge

A complete end-to-end privileged account security solution requires multiple products to manage, control and monitor privileged credentials as well as detect active threats. As a result, organizations are faced with the challenge of integrating and managing multiple solutions in order to achieve maximum protection. Solutions involving multiple products introduce the following challenges in an organization:

Costly Integrations. Integrating multiple products from one vendor or many vendors can be expensive due to professional services and custom engineering costs.

Inefficient Management. The task of managing separate products through individual interfaces is time-consuming and resource intensive for IT and security teams.

Inconsistent Reporting. Compiling reports from several different products leads to inaccuracies and incomplete data. Cumbersome reporting leads to time-consuming and expensive audit processes.

Decentralized Policy. Managing policies in separate systems leads to potential inconsistencies and conflicts.

The CyberArk Privileged Account Security Solution is built on a common platform, The CyberArk Shared Technology Platform. The consolidated platform delivers a single management interface, centralized policy creation and management, a discovery engine for provisioning new accounts, enterprise-class scalability and reliability, and a secure Digital Vault®. The individual products in the CyberArk Privileged Account Security Solution integrate with the consolidated platform, enabling organizations to centralize and streamline management.

Organizations can leverage the CyberArk Shared Technology Platform whether they are deploying multiple products for a comprehensive solution, or a standalone product. The platform is designed to easily integrate into any IT environment, whether on-premises or in the cloud.

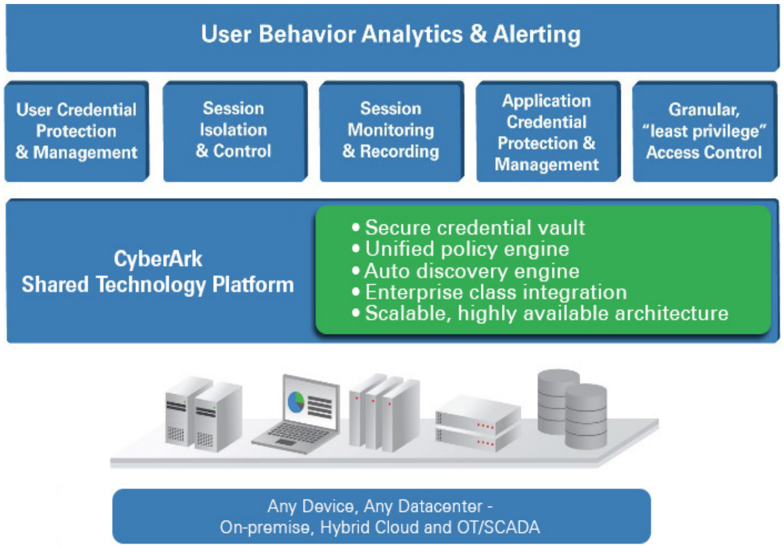
Components of the platform include:

The Digital Vault offers segregation of duties, high availability, disaster recovery and unprecedented protection with nine layers of security in an isolated and bastion hardened server. All CyberArk products interact directly with the vault, allowing products and components to benefit from the secure storage of keys, passwords, policy settings and audit logs.

Master Policy enables customers to set, manage and monitor privileged account security policy in a single, simple, natural language interface.

Discovery Engine facilitates constant up-to-date protection by ensuring that all privileged account activity is accounted for and secure. The engine finds new, unmanaged privileged accounts and automatically provisions them by continuously scanning the IT environment.

CyberArk Shared Technology Platform


User Behavior Analytics & Alerting
User Credential Protection & Management
Session Isolation & Control
Session Monitoring & Recording
Application Credential Protection & Management
Granular, "least privilege" Access Control
CyberArk Shared Technology Platform
• Secure credential vault
• Unified policy engine
• Auto discovery engine
• Enterprise class integration
• Scalable, highly available architecture
Any Device, Any Datacenter - On-premise, Hybrid Cloud and OT/SCADA

Enterprise Class Integration delivers out-of-the-box support for devices, networks, applications and servers, including web sites and social media.

Scalable, Flexible, Low-Impact Architecture ensures that individual products in the Cyberark Privileged Account Security Solution work independently, but integrate seamlessly into the same platform infrastructure. This ability to leverage shared resources allows organizations to scale the solution to and adapt to changing business needs with minimal impact.

Features

Tamper-proof storage for credentials, log files and recordings ensures sensitive information is protected from unauthorized access and misuse

High availability and disaster recovery modules include built-in fail-safe measures, secure backup and simple recovery to meet disaster recovery requirements

Out-of-the-box integrations with hundreds of solutions including SIEM, ticketing systems, and identity management solutions ensure seamless deployment in any environment

Support for strong authentication including multi-factor solutions enables companies to leverage existing authentication solutions for privileged accounts

FIPS 140-2- validated cryptography addresses compliance and security requirements

Benefits

Establish unprecedented security for privileged accounts. A patented, superior vaulting technology with multiple, build-in security layer delivers strong authentication, encryption, tamper-proof audit storage and data protection.

Accurately meet business requirements for global policy controls. The innovative policy engine delivers centralized policy creation and management based on business rules. This allows global policy to be set while providing controlled, granular-level exceptions to meet the unique operational needs of each business.

Centralize management. The platform is managed via a single pane of glass administrative interface for all privileged account security products. This interface improves ease of use for administrators and end users with centralized management and unified reporting.

Save valuable audit preparation time and cost. Streamlined Master Policy enables organizations to meet and more easily demonstrate compliance regulations such as PCI DSS, Sarbanes Oxley, NIST, NERC-CIP and more.

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