CYBERARK®

DATA SHEET

PRIVILEGED ACCOUNT SECURITY SOLUTION

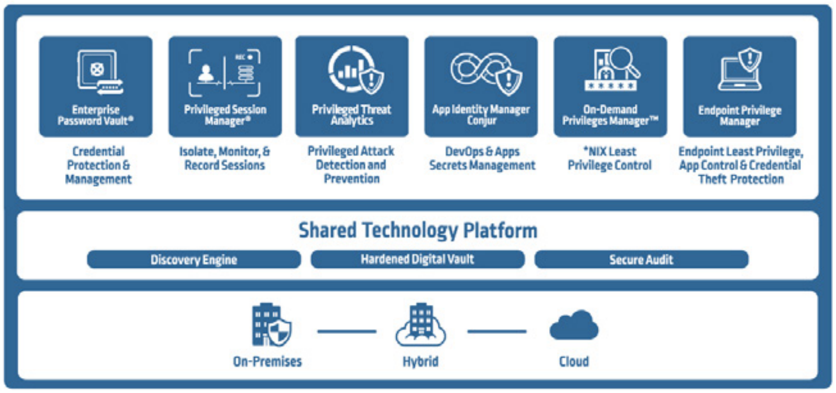
Best practices dictate that privileged accounts should be incorporated into an organization's core security strategy. Privileged accounts are a security problem and need singular controls put in place to protect, monitor, detect and respond to all privileged account activity.

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 market share leader and 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 all systems on-premises and in the cloud, from every endpoint, through the DevOps pipeline. This complete enterprise-ready Privileged Account Security Solution is tamper-resistant, scalable and built for complex distributed environments to provide the utmost protection from advanced external and insider threats.

CyberArk Privileged Account Security Solution


Enterprise Password Vault®
Credential Protection & Management
Privileged Session Manager®
Isolate, Monitor, & Record Sessions
Privileged Threat Analytics
Privileged Attack Detection and Prevention
App Identity Manager Conjur
DevOps & Apps Secrets Management
On-Demand Privileges Manager™
*NIX Least Privilege Control
Endpoint Privilege Manager
Endpoint Least Privilege, App Control & Credential Theft Protection
Shared Technology Platform
Discovery Engine
Hardened Digital Vault
Secure Audit
On-Premises
Hybrid
Cloud

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.

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, SAML, smart cards

Monitoring:

- SIEM integration, SNMP traps, Email notifications

Sample Supported Managed Devices:

- Operating Systems, Virtualization, and Containers: Windows, *NIX, IBM iSeries, Z/OS, OVMS, ESX/ESXi, XenServers, HP Tandem*, MAC OSX*, Docker
- 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

Continued on the next page...

Scalable, Flexible, Low-Impact Architecture. CyberArk's component-based architecture is simple to deploy and maintain and can easily scale to the most complex enterprise deployments with full support for high availability and disaster recovery.

Secure Audit. CyberArk's Privileged Account Security Solution provides automated enforcement of privileged account policies for continuous monitoring, complete visibility into all privileged account related activity, and delivers cost-effective audit reporting through a centralized repository for all data.

Enterprise-Class Integration. CyberArk's Privileged Account Security Solution integrates easily with your existing security, operations and DevOp tools with extensive support for automation via REST APIs.

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 these solutions provide the industry's most complete, secure solution.

Enterprise Password Vault™

Credential protection and management

Enterprise Password Vault centrally secures and controls access to privileged credentials based on privileged account security policies. Automated password and SSH key rotation reduces the time-consuming and error-prone task of manually tracking and updating privileged credentials to easily meet audit and compliance standards.

Privileged Session Manager

Isolate, control, monitor and record privileged sessions

Privileged Session Manager acts as a secure jump server to isolate and secure privileged user sessions, protect target systems from malware on endpoints and enable privileged account access without exposing sensitive credentials. Monitoring and recording capabilities enable security teams to view privileged sessions in real-time, remotely terminate suspicious sessions and maintain a comprehensive, searchable audit trail of privileged user activity.

Privileged Threat Analytics™

Analytics and alerting on malicious privileged account activity

CyberArk Privileged Threat Analytics is a security intelligence solution that allows organizations to detect, alert, and respond to anomalous privileged activity indicating an in-progress attack. The solution collects a targeted set of data from multiple sources, including the CyberArk Digital Vault, SIEM, and the network. Then, the solution applies a complex combination of statistical and deterministic algorithms, enabling organizations to detect indications of compromise early in the attack lifecycle by identifying malicious privileged account activity.

Application Identity Manager™

Protection, management and audit of embedded application credentials

Application Identity Manager eliminates hardcoded passwords and SSH keys from applications and scripts and replaces them with secure, dynamic credentials. The product is designed to meet high-end enterprise requirements for availability and business continuity, even within complex and distributed network environments. The product replaces static, embedded application account credentials often without requiring code changes and with zero impact on application performance.

Specifications

- Security Appliances: CheckPoint, Cisco, IBM, RSA Authentication Manager, Juniper, Blue Coat*, TippingPoint*, SourceFire*, Fortinet*, WatchGuard*, Industrial Defender*, Acme Packet*, Critical Path*, Symantec*, Palo Alto*
- Network Devices: Cisco, Juniper*, Nortel*, HP*, 3com*, F5*, Nokia*, Alcatel*, Quintum*, Brocade*, Voltaire*, RuggedCom*, Avaya*, BlueCoat*, Radware*, Yamaha* McAfee NSM*
- Applications: CyberArk, SAP, WebSphere, WebLogic, JBOSS, Tomcat, Cisco, Oracle ERP*, Peoplesoft*, TIBCO*
- Directories: Microsoft, Oracle Sun, Novell, UNIX vendors, CA
- Remote Control and Monitoring: IBM, HP iLO, Sun, Dell DRAC, Digi*, Cyclades*, Fijitsu* and ESX
- Configuration files (flat, INI, XML)
- Public Cloud Environments: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)

*This plug-in may require customizations or on-site acceptance testing. Please consult CyberArk Sales Engineering for more details.

Conjur

Secure secrets used by machines and users throughout the DevOps pipeline

CyberArk Conjur is a secrets management solution tailored specifically to meet the unique infrastructure requirements of native cloud and DevOps environments. The solution helps IT and information security organizations secure and manage secrets used by machines identities (applications, micro-services, CI/CD tools, APIs, etc.) and by users throughout the DevOps pipeline. Conjur is designed for cloud-scale, and is based on a distributed, high availability architecture for optimal performance and availability. Conjur is available in open source and enterprise versions.

On-Demand Privileges Manager™

Least privilege access control for Unix and Linux

On-Demand Privileges Manager allows privileged users to run authorized administrative commands from their native Unix or Linux sessions while eliminating unneeded root privileges. 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 various job functions.

Endpoint Privilege Manager

Enforce privilege security on the endpoint

Endpoint Privilege Manager secures privileges on endpoints, both desktops and servers, and contains attacks early in their lifecycle. It enables revocation of local administrator rights, while minimizing impact on user productivity, by seamlessly elevating privileges for authorized applications or tasks. Application control, with automatic policy creation, allows organizations to prevent malicious applications from executing and runs unknown applications in a restricted mode. This, combined with credential theft protection, helps to prevent malware gaining a foothold on the endpoint.

Start Assessing Your Privileged Account Risk Today With CyberArk DNA™

CyberArk DNA™ (Discovery and Audit) is a powerful assessment tool (available at no charge) that can help organizations understand the scope of privileged account security risks in on-premises and cloud environments, as well as within DevOps tools. DNA discovers the location and status of privileged accounts, SSH keys, service accounts, devices, and applications throughout the enterprise. This tool can help organizations prioritize projects, build a business case and plan for a privileged account security project.

About CyberArk

CyberArk is the global leader in privileged account security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders. A global company, CyberArk is headquartered in Petach Tikva, Israel, with U.S. headquarters located in Newton, Mass. The company also has offices throughout the Americas, EMEA, Asia Pacific and Japan.

To learn more about CyberArk, www.cyberark.com.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.