CYBERARK

DATA SHEET

PRIVILEGED ACCESS SECURITY SOLUTION

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

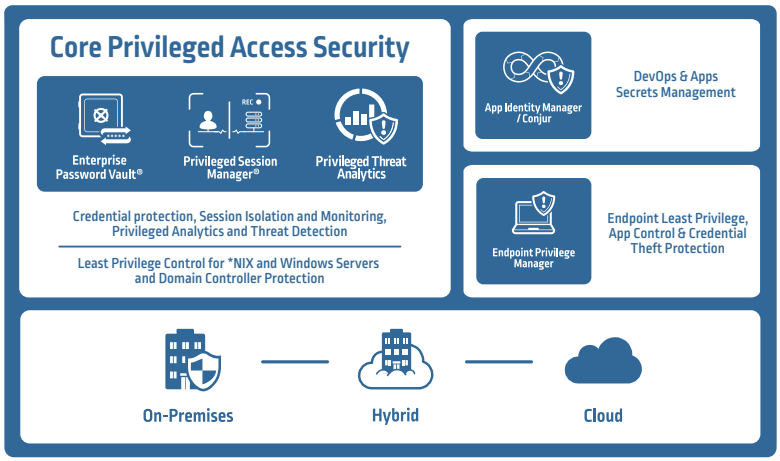
Sample Supported Managed Devices:

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

Continued on the next page...

Privileged access is pervasive and provides the "keys to the IT kingdom." This access can allow complete control of data, infrastructure and assets, across the enterprise, in the cloud and throughout the DevOps pipeline.

CyberArk is the market share leader and trusted expert in privileged access security. Designed from the ground up for security, the CyberArk Privileged Access 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 Access Security Solution is tamper-resistant, scalable and built for complex distributed environments to provide the utmost protection from advanced external and insider threats.



Core Privileged Access Security (PAS)

Credential protection and management

The CyberArk solution centrally secures and controls access to privileged credentials based on privileged access 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.

Isolate, control, monitor, and record privileged sessions

The CyberArk solution isolates and secures privileged user sessions, protects target systems from malware on endpoints, and enables privileged account access without exposing sensitive credentials. Monitoring and recording capabilities enable security teams to view privileged sessions in real-time, automatically suspend and remotely terminate suspicious sessions, and maintain a comprehensive, searchable audit trail of privileged user activity.

Specifications

- 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, 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.

Analytics and alerting on malicious privileged access activity

Threat detection and analytics enable 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 and applies a complex combination of statistical and deterministic algorithms. This allows organizations to detect indications of compromise early in the attack lifecycle by identifying malicious privileged access activity.

The solution uses machine learning algorithms to examine typical patterns of individual privileged users, privileged accounts, and system activities to determine a baseline of "normal behavior." It compares real-time activity to the baseline to identify unusual user behavior and system activity indicative of an attack including suspected credential theft, lateral movement, and privilege escalation.

Least privilege access control for *NIX and Windows

The CyberArk solution 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.

Additionally, organizations have the ability to block and contain attacks on Windows servers to reduce the risk of information being stolen or encrypted and held for ransom. The solution protects against advanced threats that exploit privileged credentials by interlocking privilege management, application control, and targeted credential theft protection to stop and contain damaging attacks on critical servers.

Domain controller protection

Attackers can exploit vulnerabilities in the Kerberos authentication protocol to impersonate authorized users, gaining access to confidential data and critical IT resources. CyberArk offers an ultra-light weight Windows agent that performs network behavior analytics to detect in-progress Kerberos attacks. The solution provides comprehensive domain controller protection, safeguarding against impersonation and unauthorized access. It enforces least privilege and application control on the domain controllers and helps protect against a variety of common Kerberos attack techniques including Golden Ticket, Overpass-the-Hash, and Privilege Attribute Certificate (PAC) manipulation.

DevOps and Apps Secrets Management

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, with zero impact on application performance. The product is designed to meet high-end enterprise requirements for availability and business continuity, even within complex and distributed network environments.

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 machine identities (applications, micro-services, CI/CD tools, APIs, etc.) and by users throughout the DevOps pipeline.

Endpoint Least Privilege, App Control, and Credential Theft Protection

Enforce privilege security on the endpoint

Endpoint Privilege Manager secures privileges on endpoints, 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 combined with credential theft protection helps to prevent malware from gaining a foothold on the endpoint.