

CORE PRIVILEGED ACCESS SECURITY

THE CHALLENGE

Privileged accounts and the access they provide represent the largest security vulnerability an organization faces today. These powerful accounts exist in every piece of hardware and software on a network. When employed properly, privileged accounts are used to maintain systems, facilitate automated processes, safeguard sensitive information, and ensure business continuity. But in the wrong hands these accounts can be used to steal sensitive data and cause irreparable damage to the business.

Privileged accounts are exploited in nearly every cyber-attack. Bad actors can use privileged accounts to disable security systems, to take control of critical IT infrastructure, and to gain access to confidential business data and personal information.

Organizations face a number of challenges protecting, controlling, and monitoring privileged access including:

- **Managing account credentials.** Many IT organizations rely on manually intensive, error-prone administrative processes to rotate and update privileged credentials—an inefficient, risky and costly approach.
- **Tracking privileged activity.** Many enterprises cannot centrally monitor and control privileged sessions, exposing the business to security threats and compliance violations.
- **Monitoring and analyzing threats.** Many organizations lack comprehensive threat analysis tools and are unable to proactively identify suspicious activities and remediate security incidents.
- **Controlling Privileged User Access.** Organizations often struggle to effectively control privileged user access to cloud platforms (IaaS a PaaS), SaaS applications, social media and more; creating compliance risks and operational complexity.
- **Protecting Windows domain controllers.** Attackers can exploit vulnerabilities in the Kerberos authentication protocol to impersonate authorized users and gain access to critical IT resources and confidential data.

THE SOLUTION

The CyberArk Core Privileged Access Security Solution is the industry's most complete solution for protecting, controlling, and monitoring privileged access across on-premises, cloud, and hybrid infrastructure. Designed from the ground up for security, the CyberArk solution helps organizations efficiently manage privileged account credentials and access rights, proactively monitor and control privileged account activity, intelligently identify suspicious activity, and quickly respond to threats.

- **Centrally secure and control access to privileged credentials based on administratively defined security policies.** Automated privileged account credential (password and SSH key) rotation eliminates manually intensive, time consuming and error-prone administrative tasks, safeguarding credentials used in on-premises, hybrid, and cloud environments.

Efficiently protect, monitor and control privileged access across on-premises, cloud, and hybrid infrastructure

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

Continued on the next page...

SPECIFICATIONS

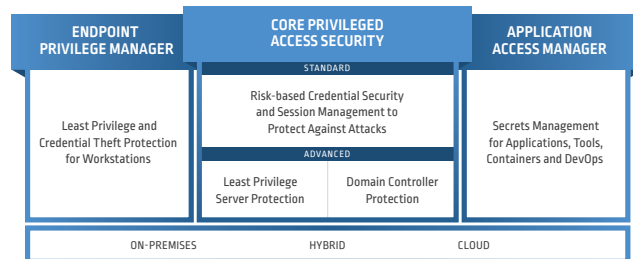
Sample Supported Managed Devices:

- 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
- 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.

- Isolate and secure privileged user sessions.** 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. Native and transparent access to multiple cloud platforms and web applications provides a unified security approach with increased operational efficiency.
- Detect, alert, and respond to anomalous privileged activity.** The solution collects data from multiple sources and applies a complex combination of statistical and deterministic algorithms to identify malicious privileged account activity.
- Control least privilege access for *NIX and Windows.** The solution allows privileged users to run authorized administrative commands from their native Unix or Linux sessions while eliminating unneeded root privileges. It also enables organizations to block and contain attacks on Windows servers to reduce the risk of information being stolen or encrypted and held for ransom.
- Protect Windows Domain Controllers.** The solution enforces least privilege and application control on the domain controllers as well as provides in-progress attack detection. It defends against impersonation and unauthorized access and helps protect against a variety of common Kerberos attack techniques including Golden Ticket, Overpass-the-Hash, and Privilege Attribute Certificate (PAC) manipulation.

CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION



BENEFITS

- Mitigate security risks.** Strengthen privileged access security. Protect the access to privileged account passwords and SSH keys. Defend systems against malware and attacks. Efficiently detect and respond to suspicious activity and malicious actions. Protect against unauthorized privileged account access, impersonation, fraud, and theft.
- Reduce operations expense and complexity.** Eliminate manually intensive, time consuming and error prone administrative processes. Simplify operations and improve the efficiency of IT security teams. Free up valuable IT staff to focus on strategic tasks to support core business activities.
- Improve regulatory compliance.** Institute policy-based privileged access controls to ensure compliance with government and industry regulations. Easily demonstrate policies and processes to auditors. Produce detailed audit trails and access histories to exhibit compliance.
- Accelerate time-to-value.** Protect and extend previous investments. Leverage out-of-the box integrations with a wide variety IT operations and security systems including authentication systems, ticketing solutions, identity access and management platforms, and SIEM solutions.
- Improve visibility.** Understand what privileged accounts exist and who has access to them. Institute well-informed privileged account security policies. Monitor real-time and historical privileged account activity.

©CyberArk Software Ltd. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 08.19. Doc. 380705392

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.