CYBERARK

DATA SHEET

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 all business hardware, software, and cloud environments. 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 business damage.

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

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

- **Discovering and managing account credentials.** Many IT organizations rely on manually intensive, error-prone administrative processes to identify, rotate and update privileged credentials. This approach is inefficient, risky and costly.
- **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 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 and PaaS), SaaS applications, databases 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 cloud and hybrid environments. Designed from the ground up for security, the CyberArk solution helps organizations efficiently manage privileged account credentials and access rights, proactively monitor 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 rotation of privileged credentials (passwords and SSH keys) and/or just-in-time privileged access eliminates time-consuming and error-prone administrative tasks, safeguarding credentials used in on-premises, hybrid, and cloud environments.
- **Isolate and monitor privileged user sessions.** Session isolation prevents credentials from crossing end user workstations, while monitoring and recording capabilities enable security teams to view privileged sessions in real-time, automatically suspend and remotely terminate suspicious sessions, and maintain

Efficiently protect, monitor and control privileged access across cloud and hybrid environments

SPECIFICATIONS

Encryption Algorithms:

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

High Availability:

- Active-Active availability services
- 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:

- Session Monitoring, Threat Analytics and risk scoring, SIEM integration, SNMP traps, Email notifications

Continued on the next page...

SPECIFICATIONS

Sample Supported Managed Devices:

- Operating Systems, Cloud Consoles, Virtualization, and Containers: Windows, *NIX, IBM iSeries, Z/OS, OVMS, ESX/ ESXi, XenServers, HP Tandem*, MAC OSX*, Docker
- Public Cloud Environments: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)
- 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, FireEye, Juniper, Blue Coat*, TippingPoint*, SourceFire*, Fortinet*, WatchGuard*, Industrial Defender*, Acme Packet*, Critical Path*, Symantec*, Palo Alto*
- Network Devices: Cisco, Juniper*, Nortel*, HPE*, 3com*, Dell EMC, 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)

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

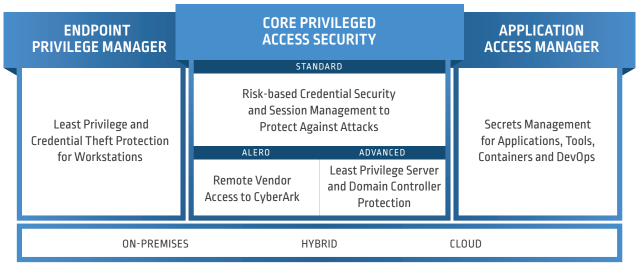
a comprehensive, searchable audit trail of privileged activity. Native and transparent access to multiple cloud platforms and web applications provides a unified security approach with increased operational efficiency.

- **Detect, alert, and respond to anomalous privileged activity.** The solution collects data from multiple sources and applies a combination of statistical and deterministic algorithms to identify and suspend risky privileged activity.
- **Enforce least privilege for *NIX and Windows.** The solution allows privileged users to run authorized administrative commands from their native 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 domain controllers while detecting in-progress attacks. 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.

BENEFITS

- **Mitigate security risks.** Strengthen privileged access management. Protect access to all privileged credentials and SSH keys. Eliminate standing privileges with just-in-time privileged access. Defend systems against malware and attacks. Efficiently detect and respond to suspicious activity and malicious actions. Protect against unauthorized privileged access, impersonation, fraud and theft.

CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION


ENDPOINT PRIVILEGE MANAGER
Least Privilege and Credential Theft Protection for Workstations
CORE PRIVILEGED ACCESS SECURITY
STANDARD
Risk-based Credential Security and Session Management to Protect Against Attacks
ALERO
Remote Vendor Access to CyberArk
ADVANCED
Least Privilege Server and Domain Controller Protection
APPLICATION ACCESS MANAGER
Secrets Management for Applications, Tools, Containers and DevOps
ON-PREMISES
HYBRID
CLOUD

- **Reduce operations expense and complexity.** Automate and eliminate manual, time consuming and error prone administrative processes. Streamline user management with just-in-time privileged access. Simplify operations and improve the efficiency of IT security teams. Free up valuable IT staff to focus on strategic 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 and search detailed audit trails and to streamline compliance.
- **Accelerate time-to-value.** Protect and extend previous investments. Leverage out-of-the box integrations with over 200 IT operations and security systems including authentication systems, ticketing solutions, identity access and management platforms, and SIEM solutions.
- **Improve visibility.** Automatically detect and onboard privileged accounts. Institute well-informed privileged access management policies. Monitor real-time and historical privileged account activity.

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.