CYBERARK

DATA SHEET

CORE PRIVILEGED ACCESS SECURITY

Efficiently secure 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

The Challenge

Privileged accounts and the access they provide represent the largest security vulnerability an organization faces today. These powerful accounts exist throughout the 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.

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

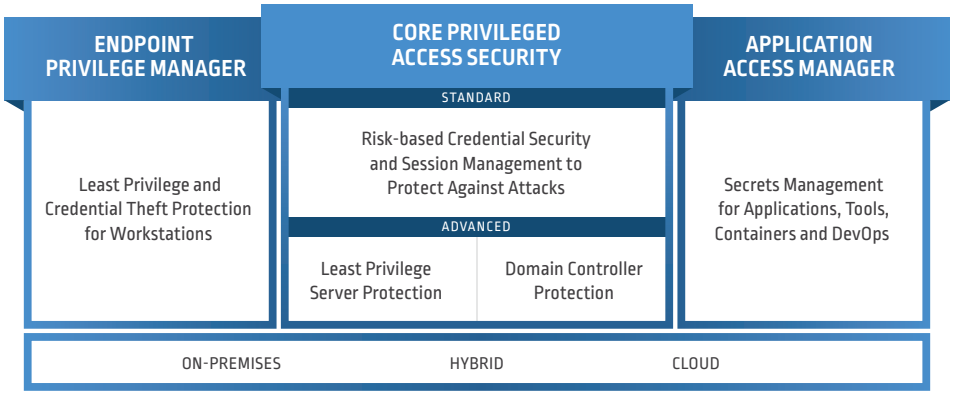
Organizations face a number of challenges protecting, controlling, and monitoring privileged access including:

- **Discovering privileged access.** Most organizations do not have a way to continually discover privileged access. Digital transformations facilitate constant creation and provisioning of new accounts and access.
- **Managing account credentials.** Relying on repetitive, manually intensive processes to manage privileged credentials is inefficient, risky and costly.
- **Isolating privileged sessions.** When privileged credentials are required for access to critical systems, hashes left on workstations can dramatically increase the attack surface.
- **Monitoring privileged activity.** Many enterprises cannot centrally monitor and control privileged sessions, exposing the business to security threats and compliance violations.
- **Alerting and responding to 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 control privileged access to cloud and web-based applications creating compliance risks and complexity.
- **Enforcing least privilege rights on servers.** It can be difficult to ensure that administrators and developers do not have standing superuser access to Windows and *NIX servers.
- **Protecting Windows domain controllers.** Attackers can exploit vulnerabilities in the Kerberos authentication protocol to impersonate authorized users and gain access to domain controllers.

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. The solution delivers risk-based credential protection and session management to detect and prevent attacks involving privileged access. It is the foundational layer upon which every privileged access program should be established, with multi-layered security built-in to mitigate the risk of advanced attacks.

CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION



Standard

- **Continually discover and onboard privileged accounts and credentials.** Run continuous discovery for privileged accounts and credentials that are created across on-premises, cloud or hybrid environments. On-board and rotate credentials automatically for unmanaged privileged accounts to minimize time attackers have to misuse privileged access.
- **Centrally manage and secure access to privileged credentials based on administratively-defined security policies.** Automated credential (password and SSH key) rotation eliminates manually intensive, time consuming and error-prone administrative tasks.
- **Isolate and record privileged sessions.** All privileged sessions are automatically recorded and stored in the encrypted CyberArk vault. Enable secure connections to critical systems by never exposing credentials directly to end users or their client. Provide 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 access activity. Remediate suspicious behavior by initiating automatic credential rotation, and privileged session suspension or termination based on pre-defined high risky activity or commands.

Advanced

- **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. Enable 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 and potential attack detection. Defend against impersonation and unauthorized access and 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.** Protect the access to privileged credentials. Defend systems against malware and attacks. Efficiently detect and respond to suspicious activity and malicious actions.
- **Reduce operations expense and complexity.** Simplify operations and improve the efficiency of IT security teams by introducing a variety of native workflows, just-in-time privileged access controls, and automated risk reducing policies. Enable security team to focus on riskiest activities occurring in the environment via automation, and risk-based approach.
- **Improve regulatory compliance.** Institute policy-based privileged access controls to ensure compliance with government and industry regulations. Easily demonstrate policies and processes to auditors by allowing them to jump to the riskiest activities, commands.
- **Accelerate time-to-value.** 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 robotic process automation, and SIEM solutions.