CYBERARK®

WHITE PAPER

THE CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION

The industry's most complete solution to reduce risk created by privileged credentials and secrets

Table of Contents

The Privileged Access — a Real, Pervasive, Threat

Attackers are wreaking havoc across the globe with advanced cyber attacks that are well planned, sophisticated, and directly targeted at the most valuable core assets of an enterprise. More and more organizations are adopting cloud first strategies and implementing DevOps methodologies, widening the attack surface and providing attackers with new pathways to exploit unprotected businesses. Once the attackers get in, they seek access to the heart of the enterprise with the intent to cause costly harm that can include damaged reputations, financial losses, and stolen intellectual property. Coming to light as well are those already inside the organization who have divulged sensitive information to the public or planted seeds to cause internal damage. Forrester estimates that 80 percent of security breaches involve privileged credentials.[1]

Privileged accounts, and the access they provide, represent the largest security vulnerabilities an organization faces today. Why are attackers inside and outside the enterprise zeroing in on privileged accounts?

- Privileged accounts are everywhere, in every networked device, database, application, and server on-premises, in cloud and ICS environments, and through the DevOps pipeline
- Privileged accounts used by both human and non-human/machine users have all-powerful access to confidential data and systems
- Privileged accounts have shared administrative access making their users anonymous
- Privileged accounts grant too broad access rights, far beyond what is needed for the user to perform their job function
- Privileged accounts go unmonitored and unreported and therefore unsecured

Simply put, privileged accounts allow anyone who gains possession of them to control organization resources, disable security systems, and access vast amounts of sensitive data. All predictions point to privileged account abuse worsening in the future unless organizations take action now. 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, alert and respond to all privileged activity.

Privileged Credentials – The Keys to the IT Kingdom

Privileged credentials are the keys to the IT kingdom. They are required to unlock privileged accounts, and they are sought out by external attackers and malicious insiders as a way to gain direct access to the heart of the enterprise. As a result, an organization's critical systems and sensitive data are only as secure as the privileged credentials required to access these assets.

Most organizations today rely on a combination of privileged credentials such as passwords, API keys, certificates, tokens, and SSH keys to authenticate users and systems to privileged accounts. When left unsecured, attackers can compromise these valuable secrets and credentials to gain possession of privileged accounts and use them to advance attacks against organizations. In fact, cyber security research shows that the one thing every attacker needs to be successful is access to a privileged account. Notably, as some organizations have started protecting privileged passwords, attackers have shifted their attack methods to SSH keys, which are often overlooked when organizations secure privileged accounts.

To prevent targeted attacks, protect the keys to the IT kingdom and keep sensitive data away from attackers, organizations must adopt a privileged access security strategy that includes proactive protection and monitoring of all privileged secrets and credentials.

Learn From the Experts: CyberArk Privileged Access Security

CyberArk is the market share leader and trusted expert in privileged access security. We have more experience with privileged access security than any other vendor and we put that expertise to work for our customers in a clear and effective approach to managing the risks associated with privileged access.

To mitigate the risk of a serious breach, enterprises need to adopt a security solution that specifically addresses their privileged access exposure. CyberArk's Privileged Access Security Solution provides the comprehensive protection, monitoring, detection, alerting, and reporting required to stay one step ahead of the attackers and safeguard an organizations most critical assets.

[1] The Forrester Wave™: Privileged Identity Management, Q3 2016 by Andras Cser, July 8, 2016

Are You Underestimating Your Level of Risk?

In our recent CyberArk Threat Landscape 2018 Report,[2] we discovered that 89% of IT security professionals recognized that infrastructure and critical data are not fully protected unless privileged accounts, credentials and secrets are secured and protected. Yet, a good proportion of them indicate that their organization has still not implemented a privileged access security solution to store and manage privileged and/or administrative passwords. Furthermore, the 2018 report indicated that enterprises are not doing enough to protect against malware and advanced attacks but yet 87% of respondents indicated that they still allow users to run with local administrative privileges which as we all know most malware requires admin to gain persistence. Combining user accounts that are equipped with local administrative capabilities with actual administrative users creates an ever growing attack surface around privilege accounts.

Additionally, DevOps security has not yet reached the maturity levels of traditional enterprise IT. Half of respondents do not have a privileged security strategy for cloud or DevOps and that nearly 40% store privileged account passwords and secrets in simple text files representing unmanaged, unsecured high value accounts which create a highly risky environment. When you factor in all of this risk associated with the typical enterprise around the [lack of] privilege access security and then face the reality that over 80% of security breeches that have taken place in the last 8 years have involved privileged accounts as part of their success, it becomes very clear where IT security professionals need to have a focused plan of attack.

Compliance, to be or not to be

As the risk of advanced threats increases, compliance regulations like PCI DSS, Sarbanes Oxley, NIST, NERC-CIP, HIPAA, GDPR, and frameworks such as the SWIFT CSCF, have increased their requirements to control, manage and monitor privileged access.

Organizations that do not fully understand their privileged environment face the prospect of audit failure resulting in steep fines and penalties and more importantly, still leave themselves vulnerable to a serious breach without a privilege access security strategy.

Who Are Your Privileged Users?

Enterprises tend to overlook the vast array of privileged account access. Few, if any, security or audit policies have been set to control the risks associated with them. Anonymous, unchecked access to these accounts leaves the enterprise open to abuse that could cripple an organization if compromised.

Third-party providers. Privileged access is granted to perform a job function allowing contractors to work under a cloak of anonymity. Once inside, third-party contractors have unrestricted access to elevate privileges to access sensitive data throughout the organization.

Hypervisor or cloud server managers. Business processes, such as finance, HR, and procurement, are moving to cloud applications, exposing enterprise assets to a high risk from the broad access granted to cloud administrators.

Systems administrators. For almost every device in an IT environment (every endpoint and server), there is a shared privileged account with elevated privileges and unfettered access to its operating systems, networks, servers, and databases.

Application or database administrators. Application and database administrators are granted broad access to administer the systems to which they are assigned. This access allows them to also connect with virtually any other database or application found in the enterprise.

Select business users. Senior-level executives and IT personnel often have privileged access into business applications that hold sensitive data. In the hands of the wrong person, these credentials provide access to corporate financial data, intellectual property, and other sensitive data.

Endusers. Far too many company's *still* allow their endusers to run with local admin access to do things like install software and setup a printer. In the hands of the wrong person, these privileged credentials provide the first place for incoming attackers to persist as they begin their journey toward corporate financial data, intellectual property, and other sensitive data.

[2] CyberArk, "CyberArk Global Advanced Threat Landscape Report 2018," 2018

Social media. Privileged access is granted to administer the corporate internal and external social networks. Employees and contractors are granted privileged access to write to those social media accounts. Misuse of these credentials can lead to a public takeover causing harm for an organization's brand or an executive's reputation.

Applications. Applications use privileged accounts to communicate with other applications, scripts, databases, web services and more. These accounts are often overlooked and pose significant risk, as their credentials are often hard-coded and static. A hacker can use these attack points to escalate privileged access throughout the organization.

DevOps. DevOps pipelines enable organizations to achieve high levels of agility by automatically building and deploying services and applications. To access data and other applications and services, these services require secrets and other credentials which must be secured. Additionally, a typical DevOps pipeline is supported by several powerful tools, each of which is managed by an admin console which is accessed using privileged credentials which must also be protected.

Policy First: Aligning Risk Management with Business Objectives

Best practice dictates that organizations create, implement, and enforce privileged access security policy to reduce the risk of a serious breach. Effective enterprise security and compliance begins with well executed business policy. A policy first approach ensures that the exposure to external threats, insider threats and misuse is reduced and strict government and industry compliance regulations are met.

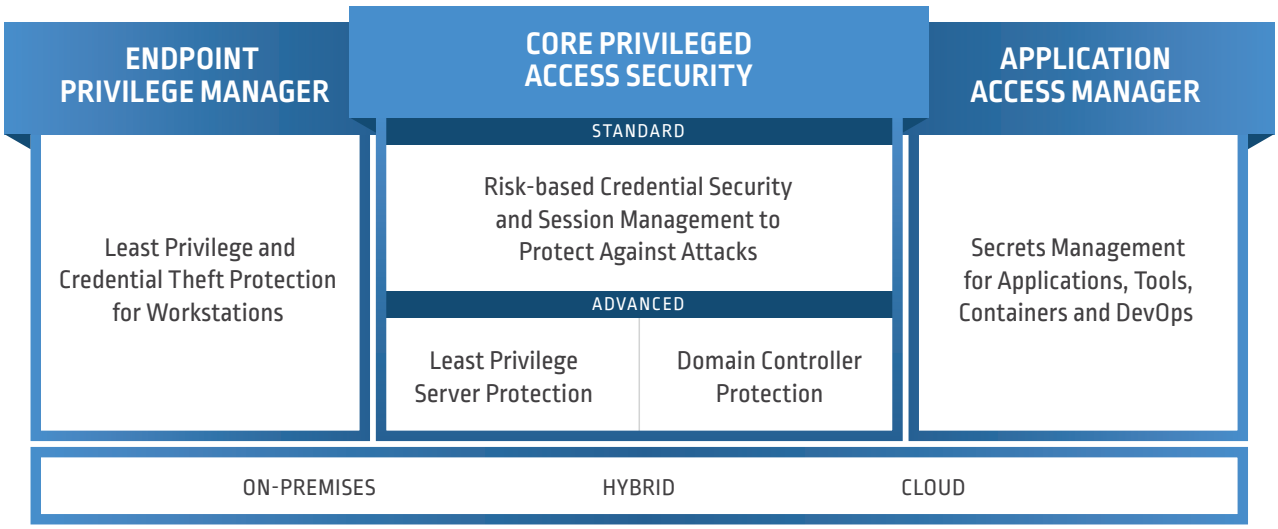
The CyberArk Shared Technology Platform

Designed from the ground up for privileged access security, CyberArk has combined a powerful underlying infrastructure with our core products to provide the most comprehensive solution for any sized organization.

At the core of the infrastructure are an isolated vault server, a unified policy engine, a discovery engine and layers of security that provide scalability, reliability and unmatched security for privileged access. A flexible architecture can start small and expand to the largest and most demanding enterprise deployments.

Only CyberArk provides solutions that help protect, manage and audit user and application credentials, provide least privilege access, control applications on endpoints and servers, and secure, monitor, and analyze all privileged activity – actively alerting on anomalous behavior. This complete enterprise-ready solution is designed to protect, monitor, detect and respond is tamper-resistant, scalable and built for complex distributed environments to provide the utmost security from insider and advanced threats.

CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION



Master Policy™—Simplified, Unified, and Unequaled to set Policy First

Master Policy is an innovative policy engine that enables customers to set, manage and monitor privileged access security policy in a single, simple, natural language interface. The once complex process of transforming business policy and procedures into technical settings is now easily manageable and understandable to an organization's stakeholders including security, risk and audit teams. Master Policy is embedded at the core and its capabilities span across CyberArk's Privileged Access Security products, providing simplified, unified and unequaled policy management.

Master Policy maps written security policy to technical settings and manages this policy in natural language. Privileged access security controls can now be implemented in a matter of minutes, raising the bar on a process that without Master Policy may take days or even weeks. Master Policy enables fast implementation and flexibility to set an enterprise global policy while providing controlled, granular level exceptions to meet the unique operational needs of operating systems, regions, departments or lines of business.

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. To ensure integrity, all CyberArk products interact directly with the vault and share data to allow all product modules and components to communicate securely and benefit from the secure storage of passwords, SSH keys, policy settings and audit logs–that exist within on-premises, hybrid and cloud environments. There is no single point of failure.

- **Segregation of Duties and Strong Access Control.** The vault administrator does not have access to the credentials stored in the vault, which ensure proper segregation of duties. The solution supports multiple authentication methods to ensure security and control over all privileged credential access and activity.
- **Layers of Security.** The seven layers of built-in security for authentication, access control, encryption, tamper-resistant storage, and data protection with no backdoor or DBA access provides exceptional security.
- **High Availability and Disaster Recovery.** The infrastructure is architected for high-availability and has built-in fail-safe measures to meet and exceed disaster recovery requirements, including secure backup and simple recovery.

Discovery Engine

Designed to continually discover changes to your IT environment be it in the cloud or on-premises, the discovery engine enables constant up-to-date protection and helps ensure that all privileged activity is accounted for and secure. As new servers and workstations are added or removed, changes in privileged accounts are automatically discovered.

Secure Audit

CyberArk's Privileged Access Security Solution provides automated enforcement of privileged account policies enabling continuous monitoring to deliver adherence to audit requirements. IT Audit teams have complete visibility into the "who, when and why", but also exactly "what" took place during all privileged sessions. The solution provides simplified, cost-effective audit reporting through a single, centralized repository of all audit data.

Enterprise Class Integration

Privileged Access Security Solution integrates easily with your existing security, operations and DevOp tools with extensive support for automation via REST APIs.

- **SIEM.** Full two way integration with SIEM vendors improves threat detection and alerting capabilities. CyberArk feeds events to SIEM solutions on privileged credential access and operations, as well as command level activity captured through privileged session monitoring.
- **Hybrid Cloud.** Support for hybrid cloud environments enables protection of hypervisor and guest image accounts for cloud administrators, protection of privileged accounts in Amazon Web Services, Microsoft Azure, and Google Cloud Platform.
- **Vulnerability Managers.** Full integration with the leading Vulnerability Management vendors allows them to simplify "authenticated scans" (also known as "deep scans") and fetch privileged accounts from the vault whenever they need to login to a target server to perform a scan.
- **Identity Management.** Integrates with leading Identity & Access Management (IAM) solutions to provision accounts into the solution based on directory details, group memberships or Identity Governance policies. Integrations also enable our customers to leverage previous investments in strong authentication, such as PKI, Radius, Web-SSO, LDAP and more.

- **Help Desk.** Integrates with most enterprise ticketing systems as well as in-house solutions. Capabilities include service request validation, new service request creation, and integration with approvals workflows such as manager approval (dual control) and timed availability.
- **DevOps.** Integrates with the DevOps toolchain secures and manages secrets used by CI/CD tools such as Ansible, Chef, Jenkins and Puppet and container orchestration software such as Docker.

Scalable, Flexible, Low-Impact Architecture

CyberArk's Privileged Access Security Solution was architected for minimal impact and protects your existing investment in your current IT environment. All the components work independently but take advantage of shared resources and data. This flexible approach allows an organization to begin a project at the departmental level and scale to a complex, distributed, enterprise solution over time.

CyberArk Products

Every product in the CyberArk Privileged Access Security Solution is stand-alone and can be managed independently while still sharing resources and data from the common infrastructure.

Each product solves a different requirement for privileged access security and all are designed to work together to provide a complete, secure solution for operating systems, endpoints, servers, databases, applications, hypervisors, network devices, security appliances, and more, for on-premises, cloud and ICS environments, and through the DevOps pipeline.

Recommended steps in protecting your privileged access:

- Set policy first.
- Discover all of your privileged accounts and credentials.
- Protect and manage privileged account credentials used by users and applications.
- Control, secure and monitor privileged access to servers and databases, websites, SaaS and any target application.
- Provide least privilege access for business users and IT administrators.
- Control applications on endpoints and servers.
- Use real-time privileged account intelligence to detect and respond to in-progress attacks.

Core Privileged Access Security

Credential Protection and Management

Discover, manage and protect privileged credentials

The CyberArk solution prevents the malicious use of privileged user passwords and SSH keys, and brings order and protection to vulnerable accounts. It secures privileged credentials based on your privileged access security policy and controls who can access which credentials and when. This automated process reduces the time-consuming and error-prone task of manually tracking and updating privileged credentials to easily meet audit and compliance standards.

- Guard against unauthorized users accessing privileged account credentials and ensure authorized users have the necessary access for legitimate business purposes.
- Update and synchronize privileged passwords and SSH keys at regular intervals or on-demand, based on policy.
- Discover and protect privileged credentials used in on-premises, hybrid, and cloud environments, as well as throughout the DevOps pipeline and on loosely connected endpoints off-network.
- Enable users to automate and simplify privileged account management tasks via REST APIs such as account workflow, onboarding rules, permissions granting, and more.
- Provide security and audit teams with a clear view of which individual users accessed which privileged or shared accounts, when and why.

Session Isolation and Monitoring

Isolate, control, and real-time session monitoring and recording

The CyberArk solution secures, isolates, controls, and monitors privileged user access and activities to critical *NIX, and Windows-based systems, databases, virtual machines, network devices, mainframes, websites, cloud platforms (IaaS and PaaS), SaaS applications, social media, and more. It provides a single-access control point, helps prevent malware from jumping to a target system through the isolation of end users, and records every keystroke and mouse click for continuous monitoring.

DVR-like recordings provide a complete picture of a session with search, locate, and alert capabilities on sensitive events without having to filter through logs. Real-time monitoring helps provide continuous protection for privileged access as well as automatic suspension and termination of privileged sessions if any activity is deemed suspicious. Integration with CyberArk's privileged analytics and threat detection solution provides the ability to assign risk scoring to privileged sessions. The scoring can be pre-defined and customized for each organization to help streamline and prioritize the review and audit of all privileged activity.

- Isolates and controls privileged sessions to prevent the spread of malware from a user's endpoint to critical systems.
- Creates an indexed, tamper-resistant record of privileged sessions and provides searchable metadata.
- Helps protect privileged credentials from advanced attack techniques such as key-stroke logging and pass-the-hash attacks.
- Offers native access for cloud administrators and privileged business users, Windows clients (e.g. RDP, SSMS, etc.) and native command line SSH device connectivity; providing secure access to privileged users using either passwords or SSH keys.
- Provides AD Bridge capabilities that enable organizations to centrally manage Unix users and accounts that are linked to AD through the CyberArk platform.

Privileged Analytics and Threat Detection

Analytics and alerting on malicious privileged activity

CyberArk provides 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 activity.

- Detects and alerts in real-time with automatic response to detected incidents.
- Identifies privileged access related anomalies and malicious activities with the ability to detect in-progress attacks.
- Adapts threat detection to a changing risk environment with self-learning algorithms.
- Correlates incidents and assigns threat levels.
- Enhances the value of existing SIEM solutions with out-of-the-box integrations.
- Improves auditing processes with informative data on user patterns and activities.

Least Privilege Management

Granular level controls for *NIX and Windows servers

On-Demand Privileges Manager allows privileged users to use administrative commands from their native Unix/Linux session while eliminating unneeded root access or admin rights. 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 job functions. Granular access control is given while continuously monitoring all administrative commands super users run based on their role and task. The solution 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.

- Replaces commonly used sudo solutions with a centralized alternative that provides granular privilege controls and secure storage of audit logs.
- Provides proof to auditors of secured, managed, and controlled super-user privileges.

- Provides a detailed audit trail of which individual elevated privileges to root, when and for what reason.
- Limits super-user privileges to only those that are necessary to reduce the risk of exposure to abuse or error.
- Authorizes access to fully delegated root shells for users to work intuitively according to their workflow.
- Out-of-the-box policy templates enable segregation of duties on Windows Servers by controlling administrator privileges based on user role.
- Enables commands to be whitelisted/blacklisted on a per-user and/or per-system basis.

Domain Controller Protection

Safeguard Windows Domain Controllers against Kerberos attacks

CyberArk offers an ultra-light weight Windows agent that performs network behavior analytics to detect in-progress Kerberos attacks. The solution both monitors and protects domain controllers, safeguarding against impersonation and unauthorized access. It helps protect against a variety of common Kerberos attack techniques.

- Detects a range of potential threats including suspected credential theft, lateral movement, and privilege escalation.
- Provides real-time alerts via CyberArk dashboard, email or SIEM dashboard.
- Provides the ability to enforce granular controls for least privilege and application control on the domain controllers.
- Detects a variety of in-progress Kerberos attacks including Golden Ticket, Overpass-the-Hash, and Privilege Attribute Certificate (PAC) manipulation.

Application, Container and DevOps Secrets Management

Application Access Manager™

Protection, management, and audit of application credentials across on-premises, hybrid, containerized, and multi-cloud environments

CyberArk Application Access Manager is designed to provide comprehensive privileged access, credential, and secrets management for widely used application types and non-human identities. For example, Application Access Manager secures credentials for commercial off-the-shelf applications, traditional internally developed applications, and scripts, as well as containerized applications built using DevOps methodologies.

Application Access Manager is designed to provide a strong security solution that enables organizations to control, manage, and audit all non-human privileged access for various application types, across on-premises, hybrid, containerized and multi cloud environments.

- Establishes strong authentication by leveraging the native attributes of applications, containers, and other non-human identities to eliminate the “secret zero bootstrapping” challenge and potential vulnerability.
- Simplifies integrations by supporting validated integrations with a wide range of commercial software platforms, applications and tools, such as business applications, security tools, RPA platforms, CI/CD toolsets, and container platforms.
- Accelerates deployment and usage by providing developers with an easy-to-use solution to secure secrets in application and DevOps environments – allowing them to focus on developing software. Additionally, the open source solutions make it easy for developers and DevOps admins to evaluate, deploy, and secure their DevOps environments.
- Ensures a comprehensive audit on any access by tracking all access and providing tamper-resistant audit.
- Consistently applies access policies by applying role-based access controls on non-human identities, leveraging integrations with other CyberArk and partner solutions to centralize policy management across the enterprise, and other policy-based controls.
- Ensures business continuity and other enterprise requirements including scalability, availability, redundancy and resiliency, alerting, policy-based rotation, and other enterprise requirements.

Endpoint Privilege Management and Credential Theft Protection

Endpoint Privilege Manager

Enforce least privilege on the endpoint

Endpoint Privilege Manager secures privileges on the endpoint (Windows and Mac desktops/laptops) 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 from gaining a foothold, and contains attacks on the endpoint.

- Enables organizations to remove administrator rights from everyday business users without halting productivity, and seamlessly elevates privileges based on policy when needed to run authorized applications or commands.
- Guards against malicious applications including ransomware from entering and propagating throughout the environment, and enables users to run unknown applications in a "Restricted Mode," helping users stay productive and safe.
- Helps an organization detect and block attempted theft of Windows credentials and those stored by popular web browsers thus preventing propagation through the environment.
- Completely integrated to CyberArk Application Risk Analysis service to enable automated analysis and timely policy decisions for unknown applications.
- Seamless integration with Check Point, FireEye and Palo Alto Networks threat detection solutions.
- Support for on premise server and SaaS deployment options.

About CyberArk

CyberArk is the global leader in privileged access 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, please visit www.cyberark.com.