The CyberArk Privileged Account Security Solution

A complete solution to protect, monitor, detect, alert and respond to privileged account activity

Table of Contents

The Privileged Account—a Real, Pervasive, Threat

Malicious hackers 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. The outsiders are breaking through the perimeter and gaining internal access. Once inside they are seeking 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. In 100 percent1 of these recent breaches a stolen, abused or misused privileged credential is to blame.

Privileged accounts 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, server and social media account on-premises, in the cloud and in ICS systems
- Privileged accounts 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 account activity.

Privileged Account Credentials – The Keys to the IT Kingdom

Privileged account credentials are the keys to the IT kingdom. They are required to unlock all 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 passwords and SSH keys to authenticate users and systems to privileged accounts. When left unsecured, attackers can compromise these valuable 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. In fact, in 2013 over half the enterprises surveyed by the Ponemon Institute admitted to being impacted by an SSH-related compromise.

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

1 2013 CyberSheath Report, APT Privileged Account Exploitation

Learn From the Experts: CyberArk Privileged Account Security

CyberArk is the trusted expert in privileged account security. We have more experience with privileged account 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 accounts.

To mitigate the risk of a serious breach, enterprises need to adopt a security solution that specifically addresses their privileged account exposure. CyberArk's privileged account security solution provides the comprehensive protection, monitoring, detection, alerting, and reporting that is a mandatory requirement to thwart the malicious insider and advanced attacker.

Are You Underestimating Your Level of Risk?

In the recently released CyberArk Privileged Account Security & Compliance Survey Report for 2013, we discovered that eighty-six percent of large enterprises either do not know, or have grossly underestimated, the magnitude of their privileged account security problem. Thirty percent of respondents from these organizations believed they had between 1-250 privileged accounts. However, for an organization with 5,000 employees, the number of privileged accounts is estimated to be at least five to ten times higher. The survey also found that over one third of the respondents did not know where to find privileged accounts in their organizations.

In addition, as the risk of advanced threats increases, compliance regulations like PCI DSS, Sarbanes Oxley, NIST, NERC-CIP, HIPAA and more, have increased their requirements to control, manage and monitor privileged account access. Organizations that do not fully understand their privileged account environment face the prospect of audit failure resulting in steep fines and penalties and leave themselves vulnerable to a serious breach.

Who Are Your Privileged Account 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, 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.

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 themselves 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.

Policy First: Aligning Risk Management with Business Objectives

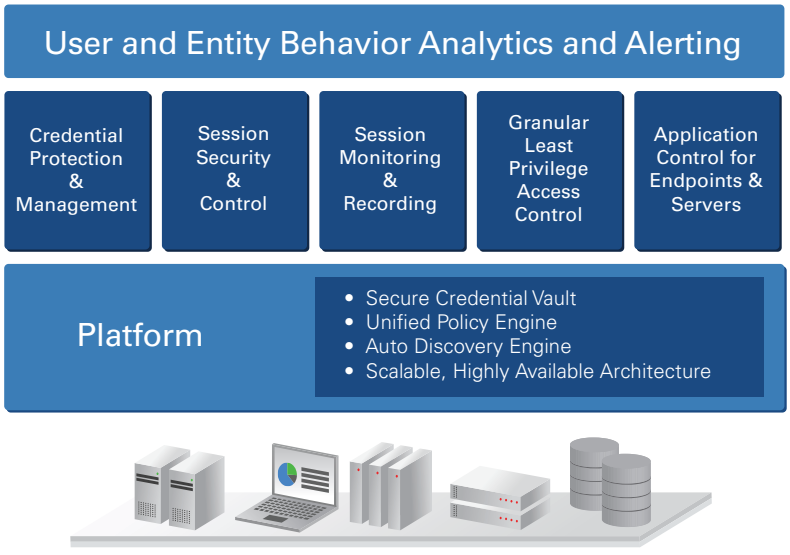
Best practice dictates that organizations create, implement, and enforce privileged account security policy to reduce the risk of a serious breach. Effective enterprise security and compliance begins with well executed business policy. A policy first approach ensures that the exposure to external threats, 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 account security, CyberArk has combined a powerful underlying infrastructure with our core products to provide the most comprehensive solution for on-premises, cloud and ICS environments.

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 accounts.

CyberArk products 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 to protect, monitor, detect and respond is tamper-proof, scalable and built for complex distributed environments to provide the utmost security from insider and advanced threats.



Any Device, Any Datacenter – On Premises, Cloud and ICS

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 account 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 all of CyberArk's privileged account 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 account 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, (making them tamper-proof). 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-proof storage, and data protection with no backdoor or DBA access provides unprecedented security for privileged accounts.
- **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, the discovery engine enables constant up-to-date protection and ensures that all privileged account activity is accounted for and secure. As new servers and workstations are added or removed, changes in privileged accounts are automatically discovered.

Enterprise Class Integration

CyberArk's Privileged Account Security Solution is ready to leverage your existing investment with out of the box support for more devices, networks, applications, and servers, including web sites and social media.

- **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 discovery and protection of hypervisor and guest image accounts for cloud administrators, AWS, SaaS applications, and social media accounts such as Twitter, Facebook, and LinkedIn.
- **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 ticketing systems such as Remedy, HEAT, HP Service Manager, and 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.

Scalable, Flexible, Low-Impact Architecture

CyberArk's Privileged Account 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 Account 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 account security and all 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.

Steps to protecting your privileged accounts:

- 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

Enterprise Password Vault®

Protection, management and audit of privileged passwords

Enterprise Password Vault prevents malicious use of privileged user passwords and brings order and protection to vulnerable accounts. Enterprise Password Vault secures privileged passwords based on your privileged account security policy and controls who can access which passwords and when. This automated process reduces the time-consuming and error-prone task of manually tracking and updating privileged passwords to easily meet audit and compliance standards.

- Discovers privileged accounts and dependent services and provisions these accounts to the Digital Vault for management
- Controls access to privileged account passwords based on policy
- Offers customizable workflows for password requests, including dual controls and integrations with helpdesk ticketing systems
- Ability to 'click to connect' so as not to expose the end user to the password
- Schedules automatic password changes based on your requirements
- Provides controls for one time use passwords
- Integrates with help desk and ticketing systems
- Verifies credentials on an on-going basis and automatically recovers and resets passwords when out of sync
- Receives alerts from Privileged Threat Analytics on potentially compromised privileged accounts and automatically rotates the impacted passwords

SSH Key Manager™

Security, rotation and monitoring of privileged SSH keys

SSH Key Manager helps organizations prevent unauthorized access to private SSH keys, which are frequently used by privileged Unix/Linux users and applications to authenticate to privileged accounts. SSH Key Manager secures and rotates privileged SSH keys based on your privileged account security policy and controls and monitors access to protected SSH keys. This solution enables organizations to gain control of SSH keys, which provide access to privileged accounts but are often left unmanaged.

- Securely stores and controls access to private SSH keys in the Digital Vault
- Automatically rotates SSH key pairs in accordance with organizational policy
- Supports and enforces strong access controls to authenticate and manage elevated-privilege requests
- Adheres to preset policy for check-out and check-in of SSH keys
- Enables administrators to track and report on the use of SSH keys by users and applications

Privileged Session Manager®

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

Privileged Session Manager secures, controls, and monitors privileged user access and activities to critical Unix, Linux, and Windows-based systems, databases, virtual machines, network devices, mainframes, websites, SaaS, and more. It provides a single-access control point, prevents malware from jumping to a target system, and records every keystroke and mouse click through 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 ensures continuous protection for privileged access as well as real-time intervention to terminate sessions if any activity is deemed suspicious. The Privileged Session Manager also provides full integration with third-party SIEM solutions with alerts on unusual activity.

- Establishes a single point of control for privileged sessions
- Protects privileged passwords and SSH keys from advanced attack techniques such as key-stroke logging and pass-the-hash attacks
- Secures and controls privileged sessions to prevent malware or zero-day exploit from bypassing controls
- Extends privileged session monitoring to application clients, web applications, or websites with custom connectors
- Creates an indexed, tamper-proof record of privileged sessions
- Offers command line control and native SSH access while still providing secure access to privileged users using either passwords or SSH keys
- Exports data to SIEM products for forensic analysis on privileged sessions
- Provides AD Bridge capabilities that enable organizations to centrally manage Unix users and accounts that are linked to AD through the CyberArk platform

Privileged Threat Analytics™

Analytics and alerting on malicious privileged account activity

CyberArk Privileged Threat Analytics is 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 network taps/switches. 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 account activity.

- Detects and alerts in real-time
- Enables automatic response to detected incidents

- Establishes profiles of typical privileged user behavior
- Identifies anomalies including malicious privileged account activities and suspicious Kerberos traffic indicating an in-progress attack
- 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

Application Identity Manager™

Protection, management and audit of embedded application credentials

Application Identity Manager eliminates hard-coded passwords and locally stored SSH keys from applications and scripts. CyberArk's Application Identity Manager ensures that your high-end enterprise requirements for availability and business continuity, even within complex and distributed network environments, will be met. The product eliminates embedded application credentials often without requiring code changes and with zero impact on application performance.

- Replaces hard-coded passwords and locally stored SSH keys with a script that enables applications to retrieve these credentials from the Digital Vault on-demand
- Provides a secure, local cache on the server for high availability and to maintain high performance
- Provides on-the-fly application credential replacement without increasing latency
- Authenticates applications requesting credentials based on its physical properties such as path or application signature
- Offers High Availability and Reliability for production systems
- Provides a unique patented solution for managing data-source credentials on Application Servers

Viewfinity

Least privilege and application control for endpoints and servers

Viewfinity enables organizations to enforce least privilege policies for business users and IT administrators while seamlessly elevating privileges when needed to run authorized applications or commands. This helps organizations reduce the attack surface, minimize accidental or intentional damage to endpoints and servers, and segregate administrative duties on Windows Servers. Complementary application controls help prevent malicious applications from infiltrating the environment, while allowing unknown applications to run when in a safe, restricted mode.

- Enables organizations to remove administrator rights from everyday business users without halting productivity
- Automatically creates privilege elevation and application control policies for more than 90 percent of applications in the environment
- Segregates duties on Windows Servers by controlling administrator privileges based on user role
- Seamlessly elevates privileges based on policy when needed to run authorized applications or commands
- Prevents malicious applications from entering and propagating throughout the environment
- Enables users to run unknown applications in a "Restricted Mode," helping users stay productive
- Integrates with Check Point, FireEye and Palo Alto Networks threat detection solutions to enable automated analysis of unknown applications
- Identifies the original source and all locations of malicious applications in the environment to accelerate remediation
- Supports three deployment methods, including Server, SaaS and Microsoft GPO

On-Demand Privileges Manager™

Least privilege access control for Unix and Linux

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 function. Granular access control is given while continuously monitoring all administrative commands super users run based on their role and task.

- 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
- Links a root account and activity with a personal username
- Enables commands to be whitelisted/blacklisted on a per-user and/or per-system basis

Why Choose the CyberArk Privileged Account Security Solution?

Enterprise-Proven, Industry-Leading Experts

With our award winning, patented technology and proven expertise, CyberArk is the only company that can provide full protection from advanced and insider threats to mitigate your risks and meet high stakes compliance requirements.

CyberArk has more deployments in large-scale distributed and virtual environments, solving more privileged account security challenges than any other vendor. We can support the vast majority of devices in on-premises, cloud and ICS environments. CyberArk is the only vendor with a native solution that can provide full credential protection, session security, least privilege and application control, and continuous monitoring to rapidly detect threats and report on privileged account activity.

Start Assessing Your Privileged Account Risk Today

CyberArk DNA™ (Discovery and Audit) is a free assessment tool that will help you discover where your privileged accounts are throughout your enterprise. With a clear accounting of all your user accounts, SSH keys, service accounts, devices, and applications, we can help you achieve an understanding of the size and magnitude of your privileged account security risk. This tool will assist in building your business case or planning for a privileged account security project to help you to decide where you are most vulnerable and how to prioritize your project.

While some organizations choose to deploy the whole strategic solution across the enterprise, the power and flexibility of the CyberArk solution allows you to begin your privileged account security project where you are most vulnerable. Some organizations will begin by securing privileged credentials and then move to monitoring when their priority has shifted. Because the infrastructure is already in place, it is easy to add additional components to increase the protection for your privileged accounts. Ultimately the whole solution will provide your organization peace of mind that you are protected against insider and advanced threats.

About CyberArk

CyberArk is the only security company laser-focused on striking down targeted cyber threats; those that make their way inside to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk is trusted by the world's leading organizations to protect their highest-value information assets, infrastructure, and applications.

For over a decade CyberArk has led the market in securing enterprises against cyber attacks that take cover behind insider privileges and attack critical enterprise assets. Today, only CyberArk is delivering a new category of targeted security solutions that help leaders stop reacting to cyber threats and get ahead of them, preventing attack escalation before irreparable business harm is done. At a time when auditors and regulators are recognizing that privileged accounts are the fast track for cyber attacks and demanding stronger protection, CyberArk's security solutions master high-stakes compliance and audit requirements while arming businesses to protect what matters most.

For additional information, visit www.cyberark.com.