The CyberArk Privileged Account Security Solution

A complete solution to protect, monitor, detect and respond to privileged accounts

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 endpoint defenses 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 percent[1] of these recent breaches a stolen, abused or misused privileged credential is to blame.

Privileged accounts represent the largest security threat 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-premise, in the hybrid cloud and in OT/SCADA 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 a company's core security strategy. Privileged accounts are a security problem and need singular controls put in place to protect, monitor, detect and respond to all privileged account activity.

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 risks 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, 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.

1 2013 CyberSheath Report, APT Privileged Account Exploitation

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 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 an often overlooked and significant risk as they are often hard-coded and static. A hacker will use these attack points to escalate privileged access throughout the organization.

Policy First: Aligning Risk Management with Business Objectives

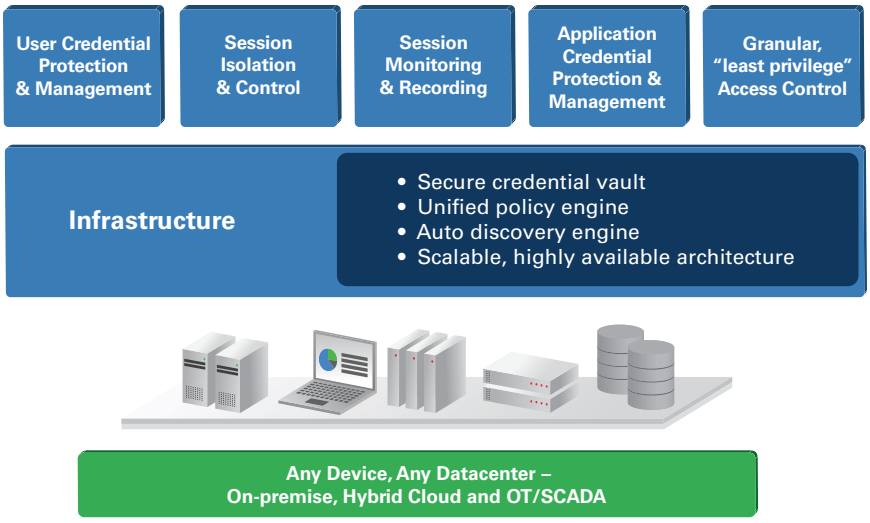
Best practice dictates that organizations create, implement, and enforce privileged account security policy to reduce the risk of a serious breach. Effective enterprise security and compliance begins with well executed business policy. A policy first approach ensures that the exposure to external threats,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

The Unified CyberArk Solution

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-premise, hybrid cloud and OT/SCADA 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 credentials and application credentials, provide least privilege access and isolate, monitor and respond to all privileged activity. 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.



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 that only responds to the vault protocols you set. 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 keys, passwords, 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 provides multiple authentication methods to ensure security and control over all privileged credential access and activity.
- **Layers of Security**
  The 9 layers of security built-in for authentication, encryption, tamper-proof audits, and data protection with no backdoor or DBA access provides unprecedented security for your 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 for syslog and alerting capabilities, including CyberArk feeding events of privileged credential access and operations, and command level activity captured through privileged session monitoring.
- **Hybrid Cloud.** Support for hybrid cloud environments enabling 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 to allow 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 for scanning it.
- **Identity Management.** Integrates with leading Identity & Access Management (IAM) solutions to provision accounts into the solution enabling our customers to leverage previous investment in strong authentication (PKI, Radius, web-sso, LDAP and more), directory details and group memberships, Identity Governance and AD Bridging.
- **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 working together to provide a complete, secure solution for operating systems, databases, applications, hypervisors, network devices, security appliances and more, for on-premise, hybrid cloud and OT/SCADA environments.

Steps to protecting your privileged accounts:

- Set policy first
- Discover all of your privileged accounts
- Protect and manage privileged account credentials and application credentials
- Provide least privilege access
- Control, isolate and monitor privileged access to servers and databases, websites, SaaS and any target application
- Use real-time privileged account intelligence to detect and respond to in-progress attacks

Enterprise Password Vault™
Protection, management and audit of privileged credentials

Enterprise Password Vault prevents malicious use of privileged user credentials, and brings order and protection to vulnerable accounts. Enterprise Password Vault secures privileged credentials 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 credentials to easily meet audit and compliance standards.

- Fully encrypts credentials
- Discovers additions or changes to your systems automatically, including servers, workstations, hypervisors and more
- Schedules automatic password changes based on your requirements
- Provides controls for one time use passwords
- Ability to 'click to connect' so as not to expose the end user to the password
- Adheres to preset policy for check-out and check-in of passwords
- Integrates with help desk and ticketing systems
- Ongoing verification of credentials as well as automatic recovery and reset of passwords when out of sync
- Discovery and management of service accounts such as Windows Services, Scheduled Tasks, and more

Privileged Session Manager™

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

Privileged Session Manager is a zero-footprint solution that isolates, 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.

Real-time monitoring ensures continuous protection for privileged access. 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. The Privileged Session Manager also provides full integration with third-party SIEM solutions with alerts on unusual activity as well as real-time intervention to terminate sessions if any activity is deemed suspicious.

- Isolates and controls privileged sessions to prevent the chance of malware or zero-day exploit to bypass controls.
- Establishes a single point of control for privileged sessions
- Provides single sign-on
- Protects from advanced attack techniques such as key-stroke logging and hash attacks
- Extends privileged session monitoring to any application client, web application, or web site with custom connectors
- Enables real-time “over the shoulder” monitoring
- Provides immediate “kill switch” to terminate suspicious sessions
- Creates indexed, tamper-proof record of privileged sessions
- Offers command line control and native SSH access while still providing secure access
- Exports data to SIEM products for forensic analysis on privileged sessions

Application Identity Manager™

Protection, management and audit of embedded application credentials

A patented solution that eliminates hard-coded application credentials including passwords and encryption 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 accounts often without requiring code changes and with zero impact on application performance.

- Eradicates hard-coded passwords
- Provides secure, local cache on the server for high availability and to maintain high performance
- Ensures that applications encounter zero downtime and zero latency
- Provides on-the-fly application credential replacement
- 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

On-Demand Privileges Manager™

Least privilege access control for UNIX, Linux and Windows

On-Demand Privileges Manager allows for control and continuous monitoring of the commands super users run based on their role and task. The product provides unified and correlated logging of all super-user activity linking it to a personal username. It also integrates with other privileged account activity while still allowing privileged users to use native commands for secure access to the systems they need to perform their job function.

- Minimizes data breaches and outages associated with uncontrolled access and effectively complies with industry regulation
- Provides proof to auditors of secured, managed, and controlled super-user privileges
- Reduces 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
- Allows for the replacement of commonly used SUDO solutions
- 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 any device, any data center, for on-premise, hybrid cloud or OT/SCADA environments. CyberArk is the only vendor with a native solution that can provide full protection, monitoring, detection and reporting of privileged accounts.

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 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 companies – including 40 of the Fortune 100 – 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.

With offices and authorized partners worldwide, CyberArk is a vital security partner to more than 1,300 global businesses, including:

- 40 of the Fortune 100
- 17 of the world's top 20 banks
- 8 of the world's top 12 pharmaceutical companies
- 75 of the leading energy companies
- Global brands in retail, manufacturing and telecommunications/cloud

For additional information, visit www.cyberark.com.