Isolate, control and monitor all privileged administrator sessions to protect your databases, virtual environments, network devices and servers from insider threats and external cyber attacks and provide proof to your auditors around privileged session activity.

**The Challenge**

Privileged accounts such as sysadmin, root, Oracle system, Administrator in Hypervisor or Windows and others are prevalent throughout your datacenter. These privileged accounts allow access and manipulation of all your sensitive business information with potentially devastating business impact. Since privileged accounts are so powerful, they are repeatedly the target of both internal and external attacks. How many times have you asked yourself, who is using these privileged accounts and what activities are actually being performed? You may need insight to learn what caused a disruption on one of your production systems or view in real-time what is happening in a privileged session. Perhaps you also want more control over who can connect to these accounts and ensure that third parties who need to connect to your systems can do so without knowing the administrator credentials? Knowing what happened during privileged administrator sessions means you can:

- **Comply with Audit Requirements**
  Audit requirements are going deeper and wider and you need to prove to your auditors that you know what was done in a certain privileged session. Regulations across many industries specify the need to “track and monitor all access to network resources”. Others refer to the ‘Four Eye Principle’ where there is a need for an additional person to approve or overlook a privileged activity.

- **Mitigate Insider Threats & Cyber Attacks That Severely Impact Your Business**
  In the 2011 Insecurity of Privileged Users Survey issued by the Ponemon Institute, more than 60% reported accessing sensitive or confidential data out of curiosity, not job function. Too many people in the organization have uncontrolled privileged access. At the same time, cyber attacks have also become common occurrences and are becoming more sophisticated, better planned and targeted at all sectors. These attacks may include planting viruses on mission-critical servers, tapping into source code, abusing sensitive consumer data and paralyzing critical national infrastructure. Such attacks, for the most part, go after vulnerabilities that result in gaining privileged access or hard-coded application passwords that can do significant damage to an organization’s bottom line and reputation. External threats are increasingly penetrating the organization and abusing privileged accounts to cause detrimental damage. These attacks are becoming more sophisticated and better targeted and therefore a preventative approach is needed from the start.

**The Solution**

CyberArk’s Privileged Session Manager (PSM) is a central point of control for protecting target systems accessed by privileged users and accounts. It’s a single solution that isolates, controls and monitors all privileged activity across the datacenter.
CyberArk’s Privileged Session Manager includes:

**Privileged Session Manager® for Servers**
Isolate, control and monitor privileged access to sensitive servers including Windows, Unix/Linux, Mainframes (zOS), iSeries and network devices. Provide full privileged session recording with DVR playback, real-time viewing as well as secure remote access to these sensitive systems using privileged single sign-on without having to expose credentials to end-users e.g. external vendors. PSM for Servers can also act as a jump server solution with the added benefit of session control and monitoring.

**Privileged Session Manager® for Databases**
Database administrators are highly privileged – they can view or change any piece of data in your organization. A recent Independent Oracle User Group survey reported that 75% of DBAs say their organization cannot monitor them. CyberArk’s Privileged Session Manager for Databases introduces an easy to deploy and novel approach to database security with zero footprint and no impact on performance, while capturing every operation performed by database administrators. Deployment is dramatically faster and without risks to production business applications in comparison to other database activity monitoring solutions.

**Privileged Session Manager® for Virtualization**
Hypervisor privileged accounts allow access to multiple servers and are therefore more vulnerable. Managing and monitoring privileged access to the hypervisor becomes critical since multiple customer organizations or business units could be at risk. CyberArk is pioneering the risk and compliance market with PSM for Virtualization. Every hypervisor connection is managed, access controlled, and a full video session recording is provided without the need to install agents on the hypervisor or guest images and servers.

**Benefits**

**Isolate Privileged Sessions for a Better Security Posture Against Cyber Attacks**
PSM creates a powerful isolation between users’ desktops and target systems separating between potentially harmful code or malware on the desktop and the sensitive target system, thus eliminating the risk of malware spreading to critical systems. By safeguarding and isolating these critical assets, as well as knowing what happened in any privileged session, you can avoid human errors, minimize insider threats and prevent targeted external attacks.

Facts & Figures:

CyberArk secures 8 of the 10 largest banks in the world.
1 in every 3 Fortune 50 companies have selected CyberArk.
“One of great things about CyberArk is that its solutions act as a facilitator for the IT department – removing lengthy and laborious processes and replacing it with a simple, secure and effective system.”

Jethro Cornelissen,
Global Lead & Head of Global Security Operations Center, Rabobank International

Ensure Continuous Monitoring for Protection and Compliance Without Impacting the Business
To meet audit and compliance requirements such as PCI DSS, SOX, HIPAA, Basel III and more, you need to prove to your auditors you are controlling privileged access to sensitive systems and provide proof as to what was done on your target systems, databases, virtual servers and web applications whether in real-time or as forensic evidence.

Increase Efficiency with Central Control and Management
All privileged sessions on any target system are centrally controlled and managed based on pre-defined policies and workflows. Whether you need to define session access controls, view session recordings or monitor sensitive events across your entire datacenter, you can do so via a single web interface.

Shorten Time to Resolution & Minimize Financial Consequences
By easily being able to search, locate and alert on sensitive events, root-cause analysis can quickly be unveiled, minimizing the potential damage to the organization due to the security breach or human error. Moreover, DVR recordings help you see the complete picture of what happened in a session in a user friendly manner rather than filter through an exhaustive list of logs.

Be Reactive to Risky Operations
By monitoring a live privileged session you can intervene or terminate privileged sessions if suspicious activity is happening. You also gain a real-time view to what third party vendors or internal personnel are doing on your network without the need to be physically next to them.

Rapidly Deploy for Quick Time to Value
Most database activity monitoring and Hypervisor security solutions require network topology changes and re-routing all application and business transactions through the monitoring solution. This extends the deployment process as every business application needs testing to ensure no negative impact was caused to production systems. Since the Privileged Session Manager focuses only on privileged users and accounts, and requires no installation on production servers, there is no need for lengthy application performance tests or impact analysis, which in turn results in dramatically faster deployment time.

Features
Become audit-ready and improve your security posture with a rich set of product features, such as:

Security and Audit
- Highly secure repository utilizing FIPS 140-2 validated cryptography for storing all audit logs and recorded sessions
- Proxy architecture creates an isolated and secure environment, as opposed to potentially vulnerable endpoint desktops, where malware can interfere with administrative or privileged sessions
- Centralized audit and compliance management through built-in audit-ready reports and self-serve access for auditors

Privileged Session Access & Workflows
- Enforce enterprise policies and workflows, e.g. dual control for initiating sessions, submit a reason in the pre-integrated ticketing system, control the session duration time, etc.
- Secure HTTPS-based access allows secure local and remote access to enterprise managed devices
Enable session recording and monitoring according to enterprise policy and end-user roles for any type of privileged account. Personal accounts and non-managed privileged accounts can also be monitored by PSM.

Privileged single sign on for initiating sessions without the need to expose privileged credentials to third party vendors.

Supports a wide variety of protocols and clients for initiating privileged sessions including Unix, Linux and network devices (SSH, Telnet), Windows RDP, RAdmin, Remotely Anywhere, AS400, Mainframes, web based applications, databases, hypervisors and virtualization management tools.

**Privileged Session Recordings**

- DVR style playback of recorded privileged sessions for event analysis and forensic review.
- Keystroke logging of SSH sessions and SQL commands audit for Oracle sessions.
- Search for privileged events with ‘point in time’ viewing within a session recording.
- Single server supports over 100 concurrent session recordings stored in highly compressed format. Highly scalable with load balancing/high availability.
- Privacy regulation support allowing on-screen user notification when a session is being recorded.

**Enterprise Readiness**

- Integration with the CyberArk Shared Technology Platform delivers scalability, high availability and centralized management and reporting.
- Out-of-the-box integration with Privileged Account Security products provides complete management, monitoring, recording and secure single-sign-on for privileged accounts.
- Distributed architecture with central management and storage that is ideal for multi-network and multi-site environments and benefits from a single administration, audit and monitoring interface.
- Integration with enterprise infrastructure, including strong authentication (2-factor, SecurID, Radius, PKI, LDAP and more), monitoring and SIEM integration, SNMP, Syslog and SMTP, built-in HA/DR architecture and much more.

Secure your sensitive web applications:

Manage access credentials and monitor session activity.