Privileged Session Management Suite:
Solution Overview

June 2012
# Table of Contents

1. **The Challenges of Isolating, Controlling and Monitoring Privileged Sessions** .................................................................3  

2. **Cyber-Ark’s Privileged Session Management Suite** ...............4  
   2.1 PSM Architecture ................................................................................................................................. 4  
   2.2 Prevent cyber attacks by isolating sensitive target machines .......... 6  
   2.3 More Control over Privileged Sessions .......................................................... 7  
   2.4 More Visibility into Privileged Activities .............................................. 8  

3. **Privileged Session Manager® for Servers ...........................................10**  

4. **Privileged Session Manager® for Databases ..................................11**  

5. **Privileged Session Manager® for Virtualization ..............................13**  

6. **PSM for Personal and Non-Managed Accounts ............................15**

---

All rights reserved. This document contains information and ideas, which are proprietary to Cyber-Ark Software. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, without the prior written permission of Cyber-Ark Software.

PSMSO007-1-0-1

Copyright © 2000-2012 by Cyber-Ark® Software Ltd. All rights reserved.
1 The Challenges of Isolating, Controlling and Monitoring Privileged Sessions

Privileged accounts such as root on UNIX, sys on Oracle, Administrator in Hypervisor and Windows and many more 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 actually using these privileged accounts and are they being misused? Perhaps you also want more control over who can connect to these accounts, especially external third party vendors or want to investigate the root cause for the disruption to one of your Production systems this morning by reviewing all administrative activity done prior to the disruption?

Without answers to these critical questions, you risk:

- **Failure to 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 e.g. PCI DSS section 10 specifies the ability to "track and monitor all access to network resources and cardholder data". Lack of compliance could result in penalties and cost the organization much more than it would have cost to secure the privileged accounts and sessions in the first place.

- **Internal & external threats that severely impact the business** – in the 2010 Cybercrime Survey issued by the Ponemon Institute, 62% of respondents reported malicious insider breaches. Cyber crimes have also become common occurrences and are becoming more sophisticated, better planned and targeted. These attacks may include planting viruses on mission-critical servers, stealing and publishing confidential business data, tapping into source code, abusing sensitive consumer data such as bank accounts, credit card details etc and paralyzing critical national infrastructure. Such attacks, on 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

- ** Longer recovery time and extended damage impact** - Without being able to track what sensitive information was stolen or what was done on critical systems to bring them down, minimizing the damage becomes impossible and the time to resolving the problem is prolonged.
Cyber-Ark’s Privileged Session Management Suite

Cyber-Ark’s Privileged Session Management (PSM) Suite is a central control point for protecting target systems accessed by privileged users and accounts across your datacenter. It complements Cyber-Ark’s market-leading Privileged Identity Management Suite, an enterprise-class, unified policy-based solution that secures, manages and enforces policies and workflows for all privileged and shared accounts in datacenters.

![Figure 1 Protect Critical Assets from Internal and External Threats](image)

### 2.1 PSM Architecture

PSM Suite architecture is proxy based on which the PSM Server proxies the connection to target systems and by that isolates them from the end user desktops. The solution requires no agents on the target systems, and therefore has zero footprint on the organization’s IT infrastructure.

From the end-user's point of view, accessing a target system is simply logging on to the Password Vault Web Access (PVWA) portal, locating the target system you wish to connect to and clicking on the “Connect” button. Alternatively, the session can be opened directly from a desktop shortcut. Under the hood, the following steps are performed in order to initiate a privileged session:

1. User logs into the web portal (PVWA) with the option of utilizing 2-factor authentication
2. User searches for target system. The Digital Vault access control allows the user to see and access only the systems he is entitled to. The solution allows giving on-demand temporary access to a machine e.g. for 3rd party vendor access, without divulging the privileged credentials. In addition, the solution can initiate approval workflow or validation against ticketing and change control systems to validate the request.
3. In order to connect to the target system, the user clicks the connect button within the PVWA.
   a. The PSM server proxies the connection to the target system and injects the privileged credentials that are required to initiate a session to the target device. It is important to state that the privilege credentials never reach the end-user’s browser and thus remain secure.

4. At this point, a session to the target system is opened without the need to specify a connection password. The user can now continue to work normally on the target system.

5. All the activities of the session are recorded by the PSM Server and, at the end of the session, are securely stored in the secure, tamper-proof Digital Vault repository in highly compressed format (approx. 200kb/min for GUI sessions and 70kb/min for console sessions).

6. Session events (SQL commands, SSH keystrokes) are written to the Vault audit and can also be sent in real-time to any SIEM solution for further analysis and automated responses.

The unique PSM architecture helps the enterprise to isolate, control and monitor privileged accesses to the data center sensitive systems as is described in the next sections.
2.2 Prevent cyber attacks by isolating sensitive target machines

The PSM proxy based architecture allows the users to isolate the desktop machines, which are potentially vulnerable to malware and targeted attacks such as advanced persistent threats (APT) from the data-center sensitive servers.

As shown in the diagram, even if the desktop user is infected by malware, the proxy architecture, which enforces protocol termination, blocks the malware access to the target servers.

PSM also helps simplifying the IT network topology and avoids complex firewall deployments, which are typically required to separate between the IT desktops and the production systems. This means that deployment is faster and expansion of the solution does not require ongoing network topology changes.
2.3 More Control over Privileged Sessions

PSM is the gateway to privileged access and allows customers to add multiple controls over the privileged sessions.

Ironically, strong authentication is usually deployed for non-privileged personal accounts while for privileged accounts, legacy user/password authentication is used. More-ever, privileged accounts are often shared among the IT and their accessed is not personalized which leads to lack of accountability and compliance issues.

![Figure 4 - Controlling Access to Privileged Sessions](image)

PSM allows the security officer to view in real-time the list of live sessions, and also to dive into a session and monitor it in real-time. This is extremely beneficial when wanting to monitor 3rd party vendors in real-time who are working on your critical systems. In case of suspicious activities, PSM also allows you to take control of the session or terminate it.

With PSM, you can:

- Connect to target systems using Privileged Single Sign On (P-SSO) - connections to the target systems are performed without divulging the connection password
- Leverage the P-SSO capabilities for third party IT contractors to enable ad-hoc and temporary access for your non-internal personnel who may not have the same level of trust as your internal personnel
- Enforce strong authentication to the PSM portal before accessing critical servers.
- Control access to these servers using policy based access control
- Monitor privileged sessions in real-time with the ability to interact with the session or terminate suspicious ones.
- Deploy access workflows such as dual control approval
- Integrate with change control and ticketing systems
- Apply restrictions on the privileged session duration.

### 2.4 More Visibility into Privileged Activities

PSM monitors the privileged sessions. All connections to systems are logged in a personalized audit trail and the sessions themselves are recorded in highly compressed DVR format.

The PSM embedded video player allows you to:

- ‘Click to play’ PSM Video streaming directly from PVWA – no need to download the full video file to end-user’s computer.
- Jump to point-in-time - Seen an interesting event in the search results? Press “play” and you will be taken to the point in time of the event within the video to see exactly what happened.
The recording is valuable both from an audit and a compliance perspective (e.g. the need to monitor administrative activities) as well as for forensic purposes.

The recording can also be leveraged for quicker root cause analysis, and by that shorten the recovery time from outages and server failures.

In addition to video monitoring, PSM adds textual logging for Oracle SQL commands and SSH keystrokes. Each command in the privileged session is audited in real time, and can be forwarded to a SIEM console as well as be presented in the Activities Report.

Moreover, session recordings are searchable according to specific audit information (e.g. find the sessions where the Salaries table was updated).

Session events are stored in minimal size text format, alongside (or instead of) the video recording, giving the auditor a complete picture across all activities, correlating logs and recordings that were conducted during a privileged session.

Figure 6 - Search for events in session

Figure 6 above shows a search for all the session recordings to Oracle servers that include the word “salary”. In the search result, the user can see all relevant commands in the session, and can click-to-play and view the relevant part of the video rather than searching through an exhaustive list of logs.
3 Privileged Session Manager® for Servers

Control and monitor privileged access to sensitive servers e.g. Windows, Unix/Linux, Mainframes (zOS), iSeries and network devices etc. PSM for Servers provides full privileged session recording with DVR playback, as well as secure remote access to sensitive systems using privileged single sign-on without having to expose credentials to end-users e.g. external vendors.

PSM for Servers also allows you to isolate, control and monitor web-based application access. With PSM you know who is doing what on your sensitive web applications such as SalesForce, the Corporate Facebook account or your router appliance web configuration to name but a few.

![Figure 7 – Privileged Single Sign On to Web Applications](image)

Today, in order to achieve isolation and controlled access to backend servers, many organizations are using Jump Servers. PSM for Servers can be the ultimate Jump Server solution for your organization while improving the security posture and streamline access of existing legacy solutions. PSM adds to the traditional Jump Server privileged SSO, session monitoring and extended control over the sessions to your critical servers.

PSM for Servers supports the following Protocols:

- Windows Servers – RDP, RAdmin, RemotelyAnywhere
- Unix, Linux Servers and Network Devices – SSH, Telnet
  - Including supporting indirect root logon
- Web Applications – HTTP and HTTPS protocols
- Mainframe / AS400 – 3270
- File transfer for Windows & Unix
4 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. Cyber-Ark’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. As a result, deployment is dramatically faster and without risks to production business applications in comparison to other database activity monitoring solutions.

Monitoring and controlling DBAs is a difficult task, and there is always a tradeoff between the level of security and the performance and stability of the sensitive databases. In many cases, customers will prefer to avoid monitoring and take the security and compliance implications rather than risking the availability of its critical databases.

Native database auditing is usually not an option for performance reasons and for that reason SIEM tools cannot really capture the read operations (“SELECT’s”).

The conventional way to monitor and control database is by Database Activity Monitoring (DAM) tools, however, as we will see below, these tools are very complex to deploy, expensive and do not hermetically close the databases from internal and external threats targeted at privileged users.

![Figure 8 - PSM for Databases Architecture](image-url)
While DAM tools can be a good choice when the need is to monitor web-facing databases and protect it against SQL injections and frauds, PSM for Databases has many benefits when the requirement is to protect and monitor the database from privileged access. Moreover, the traditional DAM solution does not protect the database host server which might be a serious loophole.

PSM allows you to isolate control and monitor only the DBA sessions where most of the risk lies while keeping the business applications untouched and unaffected. PSM for Databases takes advantage of the inherent control point that holds the privileged credentials required to connect to a database, and by that provides a zero footprint solution that focuses only on monitoring and controlling the DBA sessions.

In addition, PSM for Servers and the On-Demand Privileges Manager complement the solution by also protecting accesses to the database host OS.

DBA are highly privileged users and are potential targets for advanced attacks. PSM for Databases can also isolate the potentially vulnerable desktops from the target databases and by that reduce the risk of attacked launched by malware or Advanced Persistent Threats that infect personnel desktops.

With PSM for Databases the customer can now:

- Isolate database sessions from targeted attacks
- Avoid exposing privileged credentials with privileged single sign on
- Control privileged session access
- Monitor & record DBA activities with a zero footprint solution
- Searchable SQL level audit for Oracle privileged sessions
- Personalize DBA access

With the complementary Privileged Identity Management (PIM) Suite, the customer can further improve the security around privileged accounts.

- Manage database system accounts and DBA shared account with Enterprise Password Vault
- Manage access to the Unix/Linux database host users & data files with On-Demand Privileges Manager
- Remove hard-coded DBA credentials in applications/scripts with Application Identity Management
5 Privileged Session Manager® for Virtualization

In a virtual environment, hypervisor privileged accounts allow access to multiple servers and as a result, malicious attacks on the hypervisor, whether from the inside or externally, have exponential risk on a much greater magnitude in the organization. In a multi-tenant, cloud environment managing and monitoring privileged access to the hypervisor becomes critical since multiple customer organizations could be at risk. Cyber-Ark is pioneering the risk and compliance market in virtualization security with PSM for Virtualization. Not only is every hypervisor connection managed and access controlled but a full video recording of what was done in these privileged sessions is provided. Furthermore, due to the sensitivity and closed nature of hypervisor systems, PSM for Virtualization secures without requiring installing any agent on the hypervisor or the guest images.

Figure 9 - PSM for Virtualization Architecture

PSM for Virtualization controls and monitors the privileged sessions to the VMWare hypervisor. This is performed by proxying all the sessions to the hypervisor and its management tools, including privileged access to vCenter and ESX hosts servers using the vSphere Client machine as well as emergency access to ESX host machines over SSH protocol.

PSM protects VMWare infrastructure, and controls and monitors privileged sessions on the Guest virtual machines.

In addition, PSM addresses one of the challenges in the virtual environment, which is to keep track of the frequent changes in this type of environment. In the Private Cloud datacenter,
systems are dynamically added or removed on a daily basis and adapting these changes to your security solution is not easy.

Cyber-Ark’s Privileged Identity Management automatically detects privileged accounts in virtual environments and provisions these accounts in the Vmware environment. Enterprises no longer need to manually manage changes in the virtual environment and by streamlining the process of system provisioning can ensure all privileged accounts in the virtual environment are secured and managed in accordance with policy.

The automatic detection for private clouds includes:

- Automatic provisioning of ESX and ESXi hosts
- Automatic provisioning of all guest machines

With zero footprint on the hypervisor, PSM for Virtualization complements PIM providing:

- An innovative solution to monitor and control access to VMWare Administrator tools including vCenter, ESX/ESXi hosts and Guest systems
- Privileged Single Sign On across the virtual environment
- Access workflows enforcement for privileged sessions e.g. session initiation approval, change management, ticket validation, restrictions on session connection time etc
- Strong authentication for Hypervisor access and management

Complementing the PSM Suite with Cyber-Ark’s Privileged Identity Management Suite will allow you to:

- Automatically detect and provision privileged accounts across your virtual environment including ESX/ESXi servers and guest machines.
- Secure the privileged credentials in a highly secure, tamper-proof Digital Vault
- Personalize audit trail and accountability around the usage of ESX/ESXi and vCenter privileged and shared accounts
- Monitor privileged account usage via a managerial dashboard and built-in audit and operational reports for tracking who used the privileged account, when and for what reason
- Enforce security policies such as periodic and automatic replacement of all privileged credentials of the hypervisor and guest images
- Enforce change-management approval procedures as part of emergency access and system maintenance workflows
6 PSM for Personal and Non-Managed Accounts

There are use cases in which there is a need to monitor the privileged sessions, but there is no need to manage the privileged account credentials. For example, when using personal users to access sensitive systems, or when privileged account management is out of the project scope. For such scenarios and others, PSM Secure Connect functionality provides organizations the ability to monitor, control and isolate privileged sessions when the accounts are not managed in Cyber-Ark's Vault.

When using PSM Secure Connect, the end-user simply needs to type the connection details of the target account and click on the “Connect” button. The PSM will proxy the privileged session to the target system. All the activities of the session are recorded, similar to a regular PSM session.
Summary

Cyber-Ark’s Privileged Session Management Suite is a comprehensive solution for continuous monitoring and compliance of your datacenter. Using a common infrastructure, organizations can isolate, control and monitor all privileged sessions whether on servers, databases or virtual machines, providing both ease of management and unified reports for times of audit. This allows you to control and secure all privileged datacenter activity in a single solution.

With Cyber-Ark’s complementary Privileged Identity Management Suite you can secure, manage and track all privileged and shared account usage found across your datacenter and hard-coded in applications.