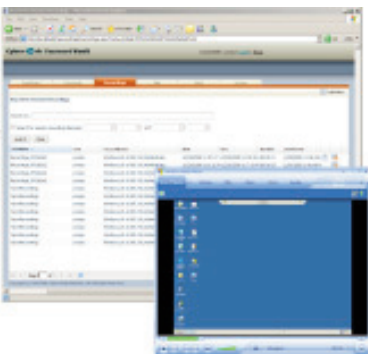


Privileged Session Manager™



PSM enables organizations to secure, control and monitor privileged access to sensitive systems and devices while leveraging privileged single sign-on capabilities. All session operations are recorded in a DVR playable format

VCR-like playback



The Challenge

Privileged access to sensitive resources (e.g. production servers, billing databases, domain servers and key network devices) need to be carefully secured, monitored and controlled from both compliance and security perspectives. There is a growing demand to be more compliant given the challenges of security controls around “who” is accessing “what” within your organization. These devices are usually accessed by internal IT personnel and, in some cases, they also need to be accessed remotely by 3rd party vendors or outsourced administrators. As audits become more granular, organizations must ensure control over not only the “who” that is accessing sensitive systems, networks and information, but “what” they are doing with this privileged access.

Secured privileged access to enterprise resources raises many challenges, including the control behind who is entitled to access the sensitive devices and initiate privileged sessions. Moreover, organizations must have capabilities to audit all activities performed during these privileged sessions as well as protecting and managing the gathered audit information.

Additional challenges and difficulties include securing and managing the credentials required to initiate privileged sessions and offering opportunities to enable secure remote access to an organization’s most sensitive devices.

Finally, providing a transparent solution that does not require changes in the network architecture and user experience as well as finding a solution that is easy to integrate with enterprise infrastructure are all critical factors to consider when addressing controlled, monitored and secured privileged access to sensitive resources.

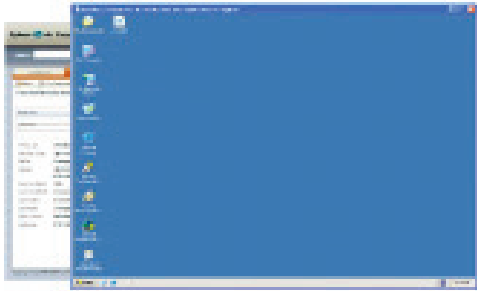
The Solution

Privileged Session Manager™ (PSM), part of Cyber-Ark Privileged Identity Management (PIM) Suite enables organizations to secure, control and monitor privileged access to network devices by:

- **Protecting Privileged Accounts.** PIM suite utilizes the patented Cyber-Ark Vaulting Technology® to store, protect and manage access to privileged accounts at a centralized point and facilitates a control point to any privileged session initiation. The solution offers a simple access control interface that easily pinpoints, who is entitled to use privileged accounts and initiate a privileged session, when, and why.
- **Recording and Monitoring Privileged Session Activities.** PSM can record any activities that occur in the privileged session in a compact format and provide DVR-like playback. Recordings are stored and protected in the Digital Vault Server® and are accessible to entitled auditors.
- **Secure Gateway Architecture.** PSM’s gateway-like architecture separates the end-user from the target machine, and initiates privileged sessions without divulging the password to the end user.
- **Transparent and easy to integrate.** PSM solution can be transparently deployed without the need to install any agents, change the network architecture or create “holes” in the firewall.



Leader in Privileged Identity Management



Specifications

Encryption algorithms:

- AES-256, RSA-2048
- HSM integration

User Management and workflows:

- LDAP directories
- Identity and Access Management integration
- Ticketing and workflow systems integration

Authentication Methods:

- Username and Password
- RADIUS
- PKI and smartcards
- LDAP
- Windows-based Authentication
- RSA SecurID
- Web SSO

High Availability:

- Clustering support
- Disaster recovery solution
- Integration with enterprise backup system

Monitoring:

- SIEM integration
- SNMP traps
- SMTP email notifications

Features & Benefits

PSM includes Cyber-Ark's Patented Digital Vault Technology® built-in and tamper proof storage for session recordings as well as other critical information related to sensitive network resources, such as identity lists, procedures and network diagrams. The solution is ICSA certified.

Additionally, PSM offers a robust set of capabilities such as:

- **Privileged Single Sign-On.** With PSM's Privileged Single Sign-On capability, a single login to the PIM portal optionally using 2-factor authentication allows connections to the managed devices without knowing the connection passwords. This allows customers to enforce 2-factor authentication for sensitive device accesses (including legacy devices that support only password authentication) without the need to deploy a complex SSO solution.
- **Secure Remote Access.** PSM allows browser based access to managed devices. The network traffic is sent over the HTTPS protocol which enables remote and cross-network access without the need to open the corporate firewall to native protocols such as SSH and RDP.
- **Distributed Architecture.** Cyber-Ark's distributed architecture can locate multiple PSM servers on different network segments in a single product instance with centralized audit, access control and user management.
- **Highly scalable architecture.** PSM server can be installed on standard enterprise servers and can easily scale on commercially available hardware for 75-100 concurrent connections. The solution offers adding as many PSM servers as required in LB/HA architecture.
- **Web Interface for Users and Auditors.** PSM offers a flexible access control mechanism to create personalized views of managed devices. Auditors have comprehensive recordings retrieval and a reporting web application. A unique Dashboard presents important usage and audit statistics and an overview of the activity in the system.
- **Enterprise readiness.** Easily integrates to enterprise infrastructure. This includes LDAP and IAM integration for user management, SRP, RADIUS, PKI, SSO RSA SecurID and Windows authentication, Monitoring and SIEM integration using SNMP, Syslog and SMTP, integration with ticketing and workflow systems, automatic provisioning of accounts based on enterprise directory, robust SDK, built-in HA/DR architecture and much more!

The power of PIM

PSM solution is part of the market leading PIM Suite, a full lifecycle solution for centrally managing privileged and shared identities. Policy based definitions allow easily enforced access control and auditing to sensitive network resources as well as ensuring compliance with regulatory requirements for both human and application (unattended) access. The PIM suite provides out of the box support for over 50 types of managed devices, including all common enterprise databases, network devices, operating systems, applications and more, allowing full scale implementation across the IT infrastructure.



Leader in Privileged Identity Management