

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 can be recorded in a DVR playable format.



DVR-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 prove controls are in place and meet the challenges of monitoring “who” is accessing “what” within your organization. Sensitive systems and devices are often accessed by internal IT personnel and, in some cases, also need to be accessed remotely by 3rd party vendors or outsourced administrators. Organizations are looking to demonstrate 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 raise 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’s 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

SPECIFICATIONS

PSM Server Platforms:

- Windows 2003, Windows 2008

Encryption Algorithms:

- AES-256, RSA-2048 (FIPS 140-2 validated cryptography)
- HSM integration

User Management and Workflow:

- 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
- Multiple Disaster Recovery sites
- Integration with enterprise backup system

Monitoring:

- SIEM integration
- SNMP traps
- SMTP Email notifications



need to install any agents, change the network architecture or create “holes” in the firewall.

FEATURES & BENEFITS

PSM leverages Cyber-Ark’s Patented Digital Vault Technology™ built-in and tamper proof storage for session recordings as well as all critical information related to sensitive network resources, such as identity lists, procedures and network diagrams.

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 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.
- Privileged 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.
- Simplify and Secure the Network.** PSM enables the separation of the IT operations network from production servers by acting as a gateway for privileged sessions into the network, enabling enterprises to simplify network topology and limit access from workstations to remote production servers only via the monitored and controlled PSM Server.
- Save of Enterprise Computing Power.** PSM’s proxy architecture eliminates the need to deploy resource consuming audit solutions on all server machines. Ensuring immediate ROI as the customer’s machine computing power will be only utilized for the business applications and not auditing.
- 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, audit statistics and an overview of the activity in the system.
- Enterprise Readiness.** Easily integrates with the enterprise infrastructure. It includes LDAP and IAM integration for user management and automatic account provisioning; use of Windows domain, RADIUS, PKI, SSO or RSA SecurID for authentication; monitoring and SEIM integration using SNMP, Syslog and SMTP; integration with ticketing and workflow systems; robust SDK, built-in HA/DR and much more!

THE POWER OF PIM

PSM solution is part of the market leading PIM Suite, a full life cycle 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. ■