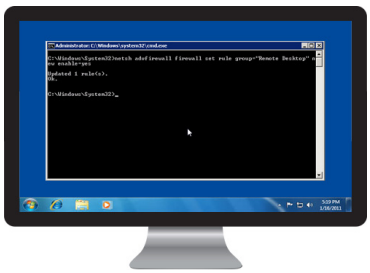
Privileged Session Manager

Isolate, monitor and control privileged sessions to reduce the threat surface, rapidly detect and respond to suspicious activity, and demonstrate compliance.



CyberArk Privileged Session Manager directly connects users to target systems, enabling session monitoring and recording without ever exposing privileged credentials to users or their endpoints.

Why CyberArk?

CyberArk is the trusted expert in helping organizations stop the most critical cyber-attacks before they stop the business.

The Challenge

Privileged accounts provide access to critical systems and sensitive business information, and if misused, these accounts can be used to cause potentially devastating damage to the business. To protect the heart of the enterprise, organizations should take a "zero trust" approach to privileged account activity.

A zero trust approach involves organizations proactively monitoring and recording all privileged session activity to ensure that malicious insiders, inexperienced third-party users or external attackers are unable to damage critical systems or gain unauthorized access to sensitive information. Organizations should also isolate privileged sessions to ensure that malware cannot spread from a user's vulnerable endpoint to a critical system. Without a way to proactively manage privileged sessions – including those initiated by passwords and SSH keys – organizations will face a number of risks, including:

- **Intentional and accidental damage to critical systems.** Organizations grant privileged access to a number of inside and third-party users to allow users to do their jobs, maintaining and managing IT infrastructure. To prevent these users from accidentally or intentionally misusing privileged accounts, security teams should monitor all privileged session activity to ensure that authorized users are only conducting authorized activity. Organizations should also consider enabling privileged single sign-on to ensure that privileged credentials never reach end users or their devices, thus preventing credential hijacking and unauthorized, unmonitored access to the critical target systems.

- **The spread of malware to critical systems.** End user devices are vulnerable to malware, which can easily spread to connected machines. To prevent malware from infiltrating critical systems, organizations should isolate privileged sessions to separate vulnerable end user devices from high-value critical target systems.

- **High administrative costs and increased risk of data breach.** Forensic analysis can be extremely difficult and time-consuming without the ability to easily search, locate and review suspicious privileged activities. While the security team is busy sorting through logs, attackers are busy advancing their attack on the network. Not only do manual, slow processes result in high administrative costs, but they also increase the likelihood of a true data breach.

- **Failed regulatory audits and hefty fines.** Several compliance regulations specify that organizations must track and monitor access to all systems that contain sensitive and regulated data. Failure to monitor this access can result in failed audits, penalties and hefty fines.

By proactively monitoring and controlling privileged sessions, organizations can detect and disrupt suspicious activity, prevent malware from reaching critical systems, and gain a complete audit trail of all privileged session activity.

The Solution

CyberArk Privileged Session Manager is designed to be a central access control point into critical systems, from which organizations can isolate, monitor and control all privileged session activity. Built from the ground-up with a focus on security, the solution scales to meet the needs of large enterprises while maintaining end user convenience.

Features and Benefits

CyberArk Privileged Session Manager enables organizations to:

Isolate critical systems. CyberArk Privileged Session Manager acts as a secure proxy server, separating endpoints from target systems and isolating privileged sessions to prevent the spread of malware from vulnerable end user devices to critical target systems.

Monitor and record privileged sessions. CyberArk Privileged Session Manager enables organizations to monitor all privileged session activity in real-time so that security teams have the opportunity to rapidly detect the misuse of privilege accounts. The solution records all keystrokes and commands for continuous monitoring and generates detailed audit logs and video recordings that can be later reviewed by security and audit teams. CyberArk Privileged Session Manager integrates with many platforms including Windows systems, Unix/Linux systems, databases, Mainframes, network devices, virtual infrastructures and more so that organizations can monitor and record privileged sessions on target systems across the network.

Rapidly respond to threats. Session audit logs and video recordings are securely stored in a tamper-proof digital vault to prevent malicious users from altering their activity trail. During an investigation or audit, these logs and recordings can be easily searched to determine when a suspicious event began, what account was used and what happened next. When suspicious session activity is detected in real-time, security teams can remotely locate and terminate the session to disrupt the potential attack.

Control third-party use of privileged accounts. Third-party users, such as vendors, consultants and auditors, often have no directly-established trust relationship with the organization and typically access critical systems from unmanaged endpoints, posing increased security risks. To mitigate these risks, CyberArk Privileged Session Manager enables organizations to isolate third-party sessions, enable privileged single sign-on, and monitor and record all third-party session activity to quickly identify unapproved and potentially damaging activity.

Prevent direct access to critical systems. CyberArk Privileged Session Manager can be configured as the only access point into critical systems, requiring users to authenticate to CyberArk before being able to reach target systems. Since monitoring and recording occur on the proxy, instead of via agents on target systems, skilled users are unable to disable controls from their end points. Further, by integrating the solution with CyberArk Enterprise Password Vault and/or CyberArk SSH Key Manager, organizations can provide privileged access without exposing target system credentials to users or their devices.

Provide secure privileged access without impacting user experience. Once authenticated to the CyberArk Solution, users can directly access target systems with just one click. CyberArk also preserves the Unix/Linux user experience by enabling users to access target systems via CyberArk directly from the native command line. Optional Active Directory (AD) Bridge capabilities can enable AD authentication and provisioning of Unix accounts through the CyberArk platform.

Demonstrate compliance. CyberArk Privileged Session Manager helps organizations address regulatory requirements that mandate the proactive monitoring and recording of privileged sessions. Access to read-only session audit logs and video recordings can be granted to auditors to demonstrate compliance with relevant regulations.

A Comprehensive Privileged Account Security Solution

By isolating, monitoring and controlling privileged session activity, organizations can reduce the attack surface, rapidly detect and respond to compromised privileged accounts, and prove compliance with industry regulations. CyberArk Privileged Session Manager seamlessly integrates with CyberArk's Privileged Account Security solution, enabling organizations to secure, protect, and detect suspicious usage of privileged account credentials, including passwords and SSH keys, from one common infrastructure that is managed behind a single pane of glass.

Specifications

Support Available for:

Unix, Linux, and Network devices:
- SSH (including file-transfer)
- Telnet

Windows:
- Windows RDP (including file-transfer)
- Windows Remotely Anywhere
- Windows RAdmin sessions

IBM:
- OS/390 (Z/OS)
- AS400 (iSeries)

Web & Applications:
- Web-based tools and applications*
- SAP*

Databases:
- Oracle
- Microsoft SQL Server

Virtualization:
- vSphere / vCenter / ESX Hosts
- HyperV console

Cloud, SaaS & Social Media:
- Amazon (AWS)
- Azure*
- Office365*
- Salesforce*
- Facebook*
- Twitter*
- And others...

Remote Access:
- Citrix*
- VNC

Storage:
- NetApp*

Universal Connector:
- Any additional platform monitoring can be easily added through Universal Connector

Privileged Account Security Platform Features:

Encryption and Security:
- AES-256, RSA-2048
- HSM integration
- FIPS 140-2 validated cryptography
- Common Criteria Certified

High Availability:
- Clustering and load balancing support
- Disaster recovery
- Integration with enterprise backup system

Monitoring:
- SIEM integration
- SNMP traps
- SMTP email notifications

** This plug-in may require customizations or on-site acceptance testing. Please consult CyberArk Sales Engineering for more details.*