

Privileged Session Management Module

e-DMZ Security's Privileged Session Management (PSM),

part of the TPAM Suite of privileged user and access control solutions, provides session control, proxy, audit, recording and replay of 'high risk' users including administrators, remote vendors and others. From a single control point you are able to authorize connections, limit access to specific resources, view active connections, record all activity, alert if connections extend beyond allowed time, and terminate connections as required. PSM comes standard with eGuardPost™ appliance or as an optional add-on for Password Auto Repository™ (PAR) appliance.

Control Access: Through a secure web-browser connection, authorized users are able to request sessions to the specific resources/account(s). The users view of the enterprise is limited to the specific resource(s) they have authorization to request access to. Configuration options support connection authorization workflow to further enhance control and compliance.

Proxy Access: PSM proxies all sessions to target resources. With no direct resource access, the enterprise is protected against any viruses, malware or other items that may exist on the user's system. Unlike other solutions that only proxy and record Unix (SSH) or Windows (RDP) sessions, PSM is able to proxy and record access to Linux/Unix, Windows, AS/400, Web applications, Network Devices, Firewalls, Routers, and more.

Record Access: All access through PSM is recorded and archived to support post session review and forensic review requirements. Recordings are in a compressed proxy format and like a motion sensitive camera, PSM only records activity to minimize online or offline storage requirements. Other solutions record in AVI or other media formats that can easily produce GB single session recordings where a typical PSM recorded session is measured in KB.

Auto-Login: PSM sessions can be configured for either interactive or automatic login. Auto-login enhances security and compliance by never exposing the account credential to the user. Optional full password management including change controls can be added via the Privileged Password Management (PPM) module.
See PPM brochure for more details.

Command Delegation: With the addition of the Privileged Command Management (PCM) module – user sessions can be restricted to a specific command – providing command level access control.
See PCM brochure for more details.

Privileged
Password
Management

Privileged
Session
Management

Application
Password
Management

Privileged
Command
Management

PSM Highlights:

- Delegated Privileged Access
- Limit Unix and Windows tasks/commands
- Limit Script/program access
- Session Proxy
- Auto-login
- Session recording, archive and replay
- Optional Full password management and control
- Optional Command Delegation

PSM Use Cases:

- Remote Vendors
- Remote Consultants
- Remote Developers
- Internal Privileged Access
- Developer Access to Production
- Fire-call Access

PSM Workflow Overview

Simple Workflow: Through the Privileged Session Management interface, authorized users simply select the resource/account they need to connect to from a filtered list of resources they have been granted “requestor” access to.

Session Request Management

Select accounts then click Details tab.

Selected	System Name	Account Name	Details	Description
<input type="checkbox"/>	UnixD1	unixD1user1	Available	
<input type="checkbox"/>	UnixD1	unixD1user2	Approval Required	
<input checked="" type="checkbox"/>	WindowsD1	user1	Available	
<input type="checkbox"/>	WindowsD1	user2	Approval Required	

The requestor enters the expected duration they require, reason for access, and if required, a ticket number (which can be optionally verified as part of the request process) and hits CONNECT.

Session Request Management

RequestID: 2289 Account: user1 System: WindowsD1

Filter	Listing	Accounts	Details	Responses	Approvers
Requested Date:	Aug 27 2009 10:56AM	Release Duration:	0 Days 2 Hours 0 Minutes		
Date Submitted:	Aug 27 2009 10:56AM	Approved Date:	Aug 27 2009 10:56AM		
Expires Date:	Aug 27 2009 12:56PM	Close Date:	Aug 27 2009 12:56PM		
Approvals Required:	0	Canceled Date:			
Ticket System:	ChangeControl	Ticket Number:	A12345		
Request Reason:	Checking System Services.				
Cancel/Expire Reason:					
Characters remaining: 255					
Save Changes	New Request	Export to Excel	Export to CSV	New Accounts	Connect
					Terminate

Full Session Audit, Recording and Replay: All session activity is recorded – every keystroke, application access and mouse click is recorded, archived and available for post review compliance or forensic review. Stored recordings are easily retrieved based on date(s), system, account, ticket number and/or user. Once the recording of interest is selected, REPLAY will automatically load the recorded session and replay the session – with DVR like controls.

Session Logs Listing

RequestID: 2288 Start Date: 8/26/2009 5:20:02 PM

Filter	Layout	Listing	Comments	File Transfers					
UserName	User Full Name	Start Date	RequestID	File Size	Duration	System	Account	Ticket Number	
reqD1	Req_Test	8/26/2009 5:20:02 PM	2288	5496	0:13:37	WindowsD1	user1		
reqD1	Req_Test	8/26/2009 4:38:04 PM	2286	63	0:15:13	WindowsD1	user1		
Export to Excel Export to CSV Replay Session Archive Now									

Additional Add-ons: As part of the TPAM Suite, enhanced functions such as command limited sessions (see Privileged Command Management) and full password management (see Privileged Password Management) can easily be added to further extend capabilities.