PsM

Privileged Session Management

Privileged Session Management not only ensures full user access accountability and visibility for meeting compliance mandates, but also acts as a unique deterrent against SysAdmin malpractice by providing irrefutable evidence of their privileged activities.

RECORD EVERY SESSION ON EVERY DEVICE

All SysAdmin sessions on the PxM Platform can be recorded.

- Visual capture allows video playback of each and every session.
- Thumbnail views allow searching at a glance.
- We use native management tools so that no plug-ins or agents are necessary.

SHADOW ANY SESSION AS IT HAPPENS, IN REAL TIME

All SysAdmin sessions on the PxM Platform can also be shadowed.

- See what your users are doing, as they are doing it.
- Even 3rd party service provider sessions can be monitored as they happen.
- Terminate sessions manually whilst shadowing.

FULLY CAPTURE ALL KEYSTROKES MADE

Optionally enable comprehensive keytroke capturing on all sessions.

- Enable SuperAdmins to search and identify particular keystrokes during each session.
- Capture what video can't - keylogging works in tandem with video capture to register what cannot be captured visually.

IMPLEMENT THE RED BOX TO DETER WRONGDOING

Whilst a session is being recorded, a red box appears around the session window.

- Clear indication to the user that they are being either recorded or monitored in situ.
- This feature can be disabled so that the user is unaware that sessions are being monitored.

SEARCH SESSIONS BY META-INFORMATION

Device Access Reports can search by a wide range of useful and tailored criteria.

- Including date/time, user, device, access level, protocol.
- Even search through recorded sessions by window titles.

CHANGE MANAGEMENT/ HISTORY LOG

Provide full accountability with a comprehensive audit of all sessions and their activity.

- Privileged Session Management can act as an irrefutable change control record within an IT infrastructure, removing any doubt or ambiguity.

+44 (0)118 324 2444

osirium.com

OSIRIUM

WHAT IS PRIVILEGED SESSION MANAGEMENT?

Oftentimes it is vital to know exactly what has been done to a system. For example it may be useful to see how a vendor has solved an issue. When mistakes have been made PSM can show the series of events that lead up to the problem - if you know what has been done, you know what to undo. With PSM, you can get an overview of a session through thumbnails, and then zoom into the details through video and keystroke analysis.

PSM makes it very clear what is being recorded: there's a red box around the recorded session. This acts as a constant reminder that activity is being monitored. To malicious insiders it's a real deterent, even if they are using a generic account such as 'root' or 'administrator'. Osirium ties the recording to both the identity and the account used.

In the case of security-sensitive third party access, Osirium's PxM Platform has the facility to shadow the session, you can see in realtime what the remote admin has done whilst the session is simultaneously recorded.

Admins can also terminate active sessions and disable the user at the same time. Should malicious activity be spotted, you can react instantly and stop the threat. This can also be used for every-day housekeeping tasks, such as cleaning up RDP sessions being left open on a server.

TAKE THE AMBIGUITY OUT OF ACCOUNTABILITY

PSM provides the ability to track and monitor what has been done to a system, from where, and by whom. This could be to investigate suspicious behaviour or for audit purposes. The PxM Platform's Privileged Session Management enables security and compliance managers to record, store and playback any privileged activities that take place across their entire hybrid-cloud infrastructures.

Privileged Session Management not only ensures full user access accountability and visibility for meeting compliance mandates but also acts as a unique deterrent against SysAdmin malpractice by providing irrefutable evidence of their privileged activities.

INFRASTRUCTURE & SYSTEM REQUIREMENTS (PXM PLATFORM)

Virtualisation:	VMware 5 through 6, Xen, Hyper-V, Azure, AWS.
Osirium appliance allocations:	IP Address, 40GB storage, 2 x CPU cores, 8GB RAM.
Desktop Client Requirements:	Microsoft Windows & Microsoft .NET Framework v4.5.2 / macOS 10.9 or later
Minimum Browser & Plugins:	Internet Explorer 10 / Chrome 50