OSIRIUM PXM PLATFORM OVERVIEW

PxM

PxM PLATFORM

Osirium's PxM suite is the world's first, built-for-purpose Privileged Protection & Task Automation solution for today's complex hybrid-cloud world. It sits at the heart of your business to protect your infrastructure and critical assets, ensuring every action is accountable, visible and auditable.

SEPARATE PEOPLE FROM PASSWORDS

Privileged credentials never enter the user's workstation.

- Solve the shared account problem
- Securely implement the dual account model
- Control & accountability of third-party access
- MSP/MSSP ready
- Built for scalability, cooperation & ease.

PART OF AN ECOSYSTEM

PxM Platform seamlessly integrates with Sailpoint®, Tenable® Nessus, Microsoft® Active Directory and a host of other platforms.

- Safely deploy privileged credentials to vulnerability scanners without risk
- On-board privileged users and enforce policies defined by IAMs.
- Seamlessly on-board Active Directory users by identifying and synchronising with security groups.

DELEGATE THE TASK, NOT THE PRIVILEGE

Run automated tasks without granting insecure direct access to privileged accounts.

- Eliminate human error
- Reduce the number of Privileged Accounts
- Dispose of run books
- Increase security & efficiency.

IMPLEMENT THE LEAST PRIVILEGED MODEL

Eliminate the risk caused by overprivileged accounts.

- Reduce the risk of exposure to abuse or error by limiting administrator permissions with complete granular access control
- Delegate access to systems without having to worry about the risks associated with overprivilege.

IDENTITY IN, ROLE OUT

Prevent attacks on Privileged Accounts by arriving as an identity and leaving as a role.

- Use profiles to map a user's identity to their correct role on any system, device or application
- PxM Platform proxies the connection - credentials never enter the user's workstation.

EFFORTLESSLY MEET COMPLIANCE NEEDS

Because our PxM Platform can record all privileged activity, we close the loop between audit and action.

- See who did what, where, when, and how, with session recording and full audit trail
- ISO-27001, PCI, MAS/ TRM, NIST-800-53 compliant.

PLATFORM COMPONENTS

PAM

Privileged Access Management

- Lock-down vulnerable entry points.
- Separate people from passwords.
- Protect and delegate Privileged Accounts with single sign-on.
- Privileged credentials can't be intercepted.
- Up and running in just 8 minutes.

PTM

Privileged Task Management

- Delegate the Task, not the Privilege.
- Automate routine network administration.
- Trained IT personnel free to manage other higher priority tasks.
- Eradicate human error.
- Efficiently manage employee time and effort.

PSM

Privileged Session Management

- Fully and effortlessly meet compliance mandates.
- Record, monitor, playback and store all Privileged Sessions.
- Terminat a session if suspicious activity is spotted.
- Track third-party network activity that occurs across hybrid-cloud infrastructures.
- Deter malicious insider attacks.

PBM

Privileged Behaviour Management

- Statistical analyses create a series of behavioural baselines for users.
- Montior user activities as they happen, whenever they happen.
- Correlate privileged user data - preemptively display clear cases of exposed risks to infrastructure.

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