PAM

Privileged Access Management

Every IT estate is managed by privileged users – users granted elevated control through accessing privileged accounts to ensure that the uptime, performance, resources and security of the computers meet the needs of the business. The PxM Platform's Privileged Access Management addresses both security and compliance requirements by defining who gets access to what and when.

GRANULAR ACCOUNT CONTROL FEATURES

Give every account on your IT estate a particular, defined state.

- Start using the PxM Platform without making any changes
- Define who has access to what, where and when through PxM profile configuration
- Use role based or mapped accounts to meet and exceed compliance mandates.*

SECRET LIFECYCLE MANAGEMENT

Auto-generate secrets meeting maximum allowable complexities.

- Mitigate the effectiveness of brute-force attacks
- Secret cycling can be either scheduled or event-based
- Rules are defined per-device
- Individual secrets are used for every managed account.

COMPLETE END-TO-END ACCOUNTABILITY

Give every audit trail created by every device personalised details.

- Audit trail for every connection including details of the identity to role mapping used
- Personalisation renders information immeasurably more useful to existing SIEM systems
- Eliminate the need for any manual cross-referencing.

STRONG AUTHENTICATION PROTOCOL SUPPORT

Login to the PxM Platform using your standard username and password.

- 2-factor authentication available using your existing solutions
- Token-based authentication using RADIUS also fully supported for stronger authentication options.

COMPLETE MULTI-ACTIVE DIRECTORY SUPPORT

Handle access to Windows Workstations and Servers within multiple domains.

- Automatically provision accounts into the correct Active Directory domain(s)
- Automatically trigger Single Sign-on using the correct domain account.

TEMPLATE-BASED DEVICE SUPPORT

Most devices are supported out of the box, but we can provide templates for those that aren't.

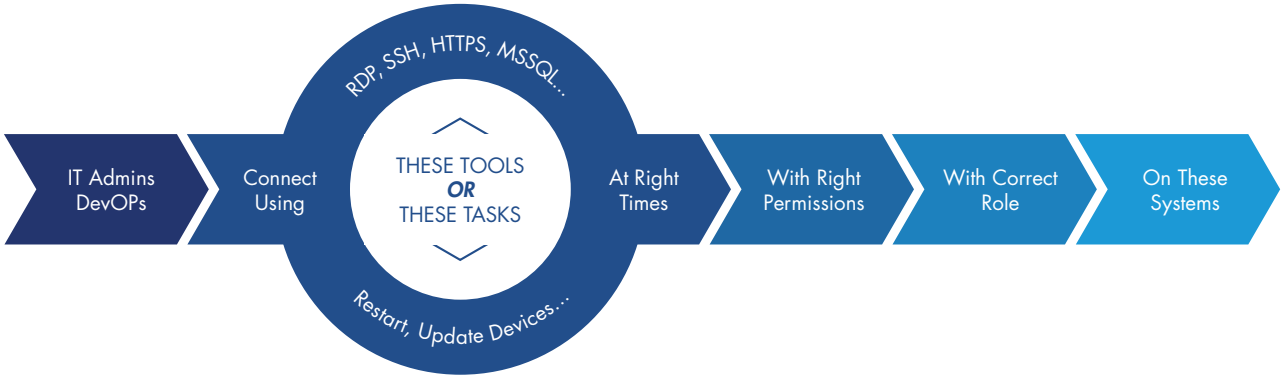
- Easily implement support using the template guide available to customers at osirium.com
- Build templates directly within the PxM Platform, allowing for immediate implementation.

+44 (0)118 324 2444

osirium.com

OSIRIUM

WHAT IS PRIVILEGED ACCESS MANAGEMENT?



PERMANENTLY SEPARATE PEOPLE FROM PASSWORDS

Every IT estate is managed by privileged users – users granted elevated control through accessing privileged accounts to ensure that the uptime, performance, resources and security of the computers meet the needs of the business. Our Privileged Access Management solution addresses both security and compliance requirements by defining who gets access to what and when.

Privileged account abuse presents one of today's most critical security challenges. Uncontrolled access by insiders or even contractors to these accounts leaves an organisation vulnerable to data leaks and cyber-attacks – ultimately causing irreparable damage to both the business and its' reputation.

The PxM Platform's Password Lifecycle Management ensures that all managed passwords are as strong as possible. Additionally, full break glass and rollback features allow the platform to cope seamlessly with devices that leave the network or are restored from backups.

*Use Active Directory security group integration to automatically onboard PxM users.

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