OSIRIUM

Privileged Access Security

Privileged Access Management and Automation to protect vital IT assets and securely automate business and IT processes

OSIRIUM PXM

Privileged Access Management

Modern privileged access management (PAM) needs to be secure, fast and flexible. PXM offers complete end-to-end accountability and an audit trail of who did what, where and when.

- Separate users from valuable privileged credentials
- Gain visibility into the most complex IT organisations of who has access to which devices
- Secure task automation
- Safely manage and enable third-party access and collaboration

OSIRIUM PEM

Privileged Endpoint Management

Implement "least privilege" policies by removing administrator accounts from endpoints while still enabling applications to be run with elevated permissions as needed.

- Learn which applications need to be run with admin privileges to avoid impacting users
- Allow mobile workers to request permission to run admin apps even when not connected to the corporate network

OSIRIUM PPA

Privileged Process Automation

IT and Business Process Automation framework with a focus on security and a deployment that is easy to implement and manage.

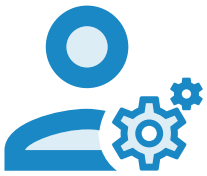
- Automate privileged operations for IT and business systems
- "Shift-left" IT Help Desk operations
- Empower business users while keeping secure control over access to vital systems and devices

Typical Usage Scenarios

FOR IDENTITY AND ACCESS MANAGERS

Moving beyond identity management to protect and manage administrator accounts

Identity and access management is only the start of protecting powerful system or administrator accounts. Identity proves the "who" but Osirium's PXM solution determines the "what" - what systems, what permissions, and what access the user has. These permissions may be for short periods of time for third parties and temporary staff or they may be an application to application integration.



FOR IT OPERATIONS LEADERS

Deploying and managing security systems must be easy to be effective

Traditional PAM tools have had significant infrastructure dependencies and consumed operations staff time to keep up to date and running efficiently. As a result, the tools aren't being deployed across the whole organisation, updates are delayed, and the enterprise is vulnerable to attack. Osirium's PXM Platform is designed to be easy to deploy and manage. IT Operations teams can focus on their business, not keeping the tools running.

FOR SECURITY PROFESSIONALS

Protecting privileged accounts is the foundation for all security strategies

Protecting valuable system and administrator accounts must be job #1 in every security strategy. That needs much more than having a simple shared password vault. A rounded solution for privileged accounts includes task automation, session management and even behavioural analytics.

FOR ENDPOINT MANAGERS

Removing local administrator rights made secure and simple

Most organisations are moving to a "least privilege" model - remove as many elevated permissions from users as possible to reduce the potential attack surface and the chance of lateral movement of an attack. The risk is that removing permissions impacts end-user productivity. With endpoint privilege management end-users can run applications with elevated permissions where needed without having more permissions than they need.

About Osirium

Osirium Technologies plc (AIM: OSI.L) is a leading vendor of Privileged Access Management ("PAM") and Privileged IT Process Automation ("PPA") software. Osirium's cloud-based products protect critical IT assets, infrastructure, and devices through automation and by preventing targeted cyber-attacks from directly accessing Privileged Accounts, and removing unnecessary access and powers of Privileged Account users.