OSIRIUM PAM

Overview of Privileged Access Management

OSIRIUM

Privileged Access Management
An Overview

Administrator or “privileged” accounts exist on every device, service, application or IT system. These accounts are highly valuable as they can create or delete users, access private data, or change critical infrastructure configuration. These accounts are the prized targets of attackers as they are the “keys” to the most valuable corporate assets and data.

With growing complexity and more demands on admin resources, it’s no wonder dangerous shortcuts are taken such as sharing login credentials, using weak access controls or not removing unneeded accounts. Risks also arise where third-party, external partners (for example, an outsourced help desk) need access to internal systems but there will be less control over those people.

It doesn’t matter how many cybersecurity tools and policies are in place if there is no control over access to those tools.

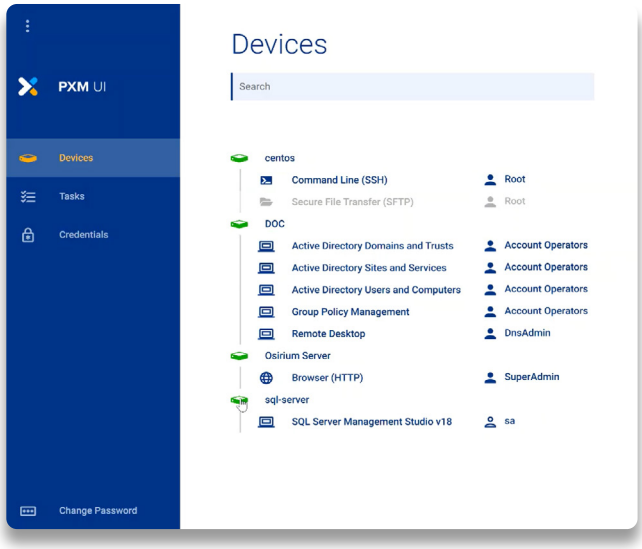
Management of these powerful accounts should be a priority for all IT and Security organisations. Privileged Access Management (PAM) is the solution. Osirium is a leader in this field with its PxM platform.

The Key to PAM Success – Separating Users from Credentials

The starting point for a PAM strategy is to identify the privileged accounts and bring them under control within a secure, scalable credential vault.Once under control, PxM provides all the tools necessary to manage the lifecycle of those credentials ensuring compliance with corporate policy.Once under control, it’s possible to map users to the systems they use and define the level of access to be granted.

Once the user identifies themselves to the PxM Platform (using corporate standard MFA tools), PXM presents the list of devices or systems they can access and provides simple access and login to the device without the user ever knowing the actual connection credentials.

With PxM Platform at the centre, users are separated from privileged credentials and the organisation has a single point of control, visibility and audit to manage access and investigate potential violations.



Right : PAM Administration console screen

Advanced PAM Capabilities

PxM Platform is the key to advanced productivity and security. It includes:

Privileged Session Management

Recording all screen and keyboard interactions during privileged sessions are an ideal audit log. The recordings can be used in an audit trail, for training purposes or forensic investigation following a suspected breach.

Privileged Task Management

Wrap frequently performed tasks to expose just the functionality needed to perform the task, not the entire application. For example, a less experienced help desk agent may have a simple task to reset a locked account without needing full access to the Active Directory Console.

Privileged Behaviour Management

Visualise potential threats in your organisation and anomalous behaviour, which can prevent privileged account misuse.

Osirium Privileged Access Security

Privileged Access Management is a component of Osirium's Privileged Access Security solution that also includes:

Privileged Process Automation – PPA

IT Operations teams are overloaded with user requests, but traditional automation and RPA tools aren't appropriate. PPA securely automates IT processes to enable "shift-left" delegation of tasks.

Privileged Endpoint Management – PEM

Many organisations have deployed local administrator accounts to users' desktops or laptops to avoid frequent calls to the help desk to install applications or make configuration changes. Those are valuable accounts and could compromise cybersecurity. PEM enables removal or those accounts without increasing the load on the help desk.

Osirium PAM Benefits

Delegate tasks to users safely: limiting their access and maintain full audit logs and session recordings.

Implement "least privilege" policies: users only have the access they need for the time they need it and no more.

Manage third-party access to internal systems with time-limited access and session recordings.

Easily comply with corporate security policies and provide auditors with the data they need.

Flexible deployment: PxM Platform can be installed on-premise or in AWS or Azure cloud environments.

About Osirium

Osirium is the UK's innovator in Privileged Access Management. Founded in 2008 and with its HQ in the UK, near Reading, Osirium's management team has been helping thousands of organisations over the past 25 years protect and transform their IT security services.

The Osirium team have intelligently combined the latest generation of Cyber-Security and Automation technology to create the world's first, built-for-purpose, Privileged Protection and Task Automation solution.

Tried and tested by some of the world's biggest brands and public-sector bodies, Osirium helps organisations drive down Business Risks, Operational Costs and meet IT Compliance.

OSIRIUM LTD.

Theale Court, 11-13 High Street, Theale, Reading, Berkshire, RG7 5AH
+44 (0) 118 324 2444, info@osirium.com, osirium.com