OSIRIUM PAS

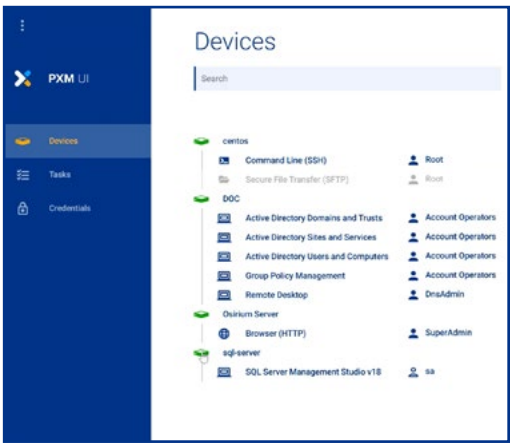
Overview of Privileged Access Security

Privileged Access Security
An Overview

Administrator or “privileged” accounts exist on every device, service, application or IT system. They’re also on staff desktops and laptops and embedded in a multitude of automation tools across the business.

These accounts are highly valuable as they can create or delete users, access private data, or change critical infrastructure configuration. They’re prized targets of attackers as they’re the “keys” to the most valuable corporate assets and data.

Management of these powerful accounts should be a priority for all IT and Security organisations. Privileged Access Security (PAS) is the solution as it focusses on protecting valuable privileged accounts and optimizing IT operations.



The Key to Privileged Access Success - PAM

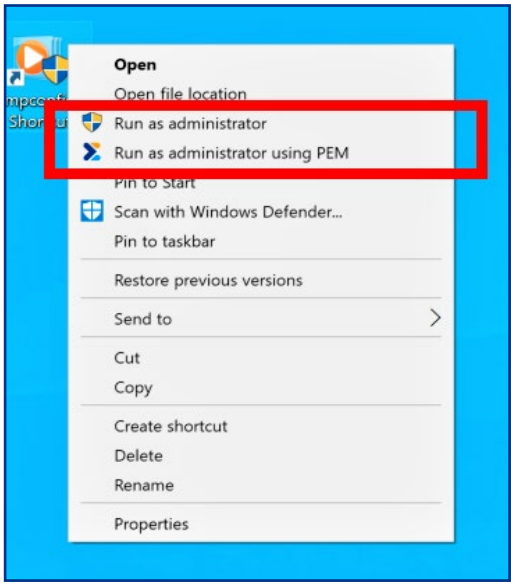
The starting point for most PAS security projects is the implementation of Privileged Access Management (PAM).

PAM brings visibility and control over those valuable administrator accounts. Osirium’s PAM solution, PxM Platform, goes beyond the traditional PAM features of a secure credential vault. It includes advanced capabilities such as session recording, task automation and behavioural analytics.

Managing Endpoint Security - PEM

Organisations often have a huge number of local administrator accounts across the business. In many cases, every desktop or laptop will have a local user with administrator privileges.
They maybe have been created for good reason in the past, such as empowering the user to make changes to their device without calling the IT help desk or the device had been previously allocated to someone that needed administrator rights.

However, those local administrator accounts are a dormant threat: if the account credentials should be acquired (for example, via a spear-phishing attack),

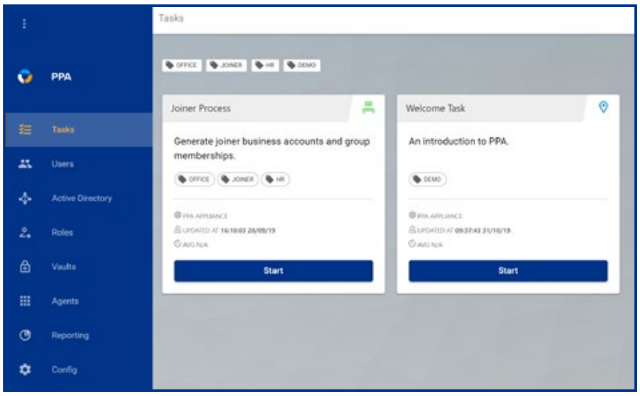


they can be used to install dangerous apps such as keyloggers or have access to the broader network. Osirium's Privileged Endpoint Management (PEM) solves this problem by enabling users to run only approved applications with elevated privileges while using their standard user account.

Users are more productive, help desk load can be reduced, and the corporate security posture improved.

Reduce IT Workload - PPA

IT Infrastructure and Operations (I&O) teams are always under pressure. From end-users requesting new applications through to major corporate strategy initiatives, Operations staff have an ever-growing backlog of work. But, much of that work is repetitive. For example, many organisations cite user account password reset as the most commonly raised issue.



Privileged Process Automation (PPA) enables I&O teams to automate complex and sensitive processes to speed up delivery, release valuable administrator resources and improve service to users. Traditional automation tools and RPA aren't fit for the needs of IT I&O environments that need human oversight and integration with a wide variety of complex systems.

PPA integrates with help desk systems, for example, ServiceNow, to automate the time-consuming, error-prone manual processes normally needed to respond to help desk requests and maintain an end-to-end audit trail.

Osirium Privileged Access Security

Osirium's Privileged Access Security solution includes:

Privileged Access Management – PAM

Modern, easy to deploy management of privileged access to shared devices, services and systems that include session recording, behavioural analytics and rich audit controls.

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.

PAS Benefits

- Protect valuable privileged credentials: never expose them to users or on the network.
- Automate and delegate tasks to users safely and free-up valuable administrator capacity
- Implement "least privilege" policies: users only have the access they need for the time they need it and no more.
- Remove dangerous local admin accounts.
- 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.

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 account management 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 needs.

OSIRIUM LTD.

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