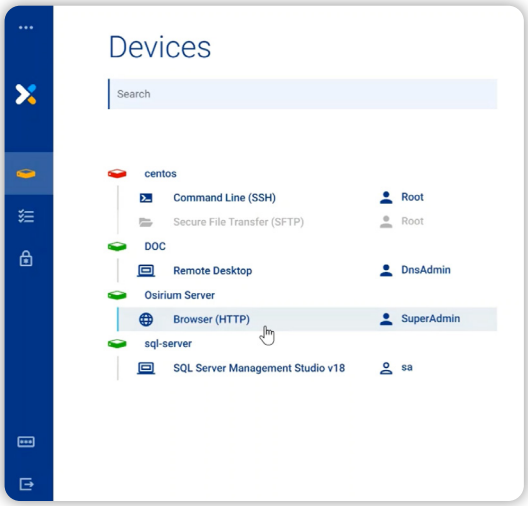
OSIRIUM **PAM**

Protect your critical IT assets with Privileged Access Management

What is Privileged Access Management (PAM)?

Privileged Accounts – the servers, devices, infrastructure housing your vital assets, and managed by your system and network administrators – are increasingly the no.1 source of security breaches. Internal and external. Intentional and unintentional.

Privileged Access gives you control: the right access to the right accounts by the right people at the right times.



Osirium PAM Benefits

Reduce Risk

- Keep administrator credentials off the network
- Prevent credential sharing
- Control and monitor third-party access

Simplified IT Operations

- Fast access to required devices and services
- Visibility of target system availability
- Browser-based interface to work anywhere, anytime

Enforce Governance

- Audit every administrator session
- Record sessions for investigation or audit
- Prevent uncontrolled access to shared assets

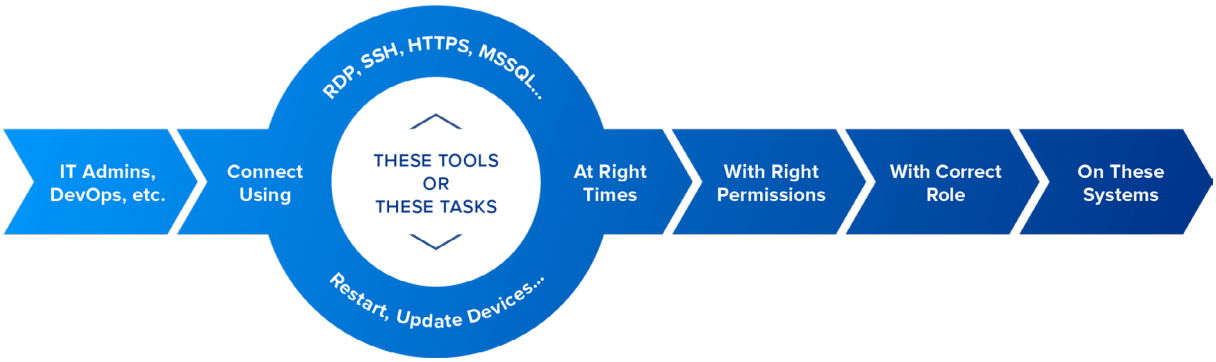
Osirium Privileged Access Security

Osirium PAM is a part of Osirium Privileged Access Security – the comprehensive solution for secure privilege management and process automation.

Privileged Access Management (PAM)
Isolate users from privileged account credentials and securely manage privileged sessions.

Privileged Process Automation (PPA)
Automate cross-system processes to delegate administrator task to help desks and users.

Privileged Endpoint Management (PEM)
Remove administrator rights from endpoints for least privilege compliance without impacting productivity.



Separate People from Passwords and Improve Productivity

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

The solution is to isolate users from the credentials for those powerful privileged accounts. But that must not get in the way of getting work done. Osirium PAM is fast to deploy, easy to manage and integrates with your existing infrastructure and services. It makes access to privileged accounts on share devices, services and data faster and most secure. The best of both worlds.

Credential and Access Management

The heart of any PAM solution is a secure vault to protect valuable administrator credentials. It goes beyond password or credential vaults and identity management to control which users have access to which privileged accounts on which systems.

Task Automation

Moving beyond protecting privileged accounts is to protect privileged activities - what users are doing with those accounts. Wrapping tasks with automation prevents users performing changes they shouldn't and ensures policy or regulatory compliance.

Session Recording and Auditing

The ultimate audit trail is a session recording that captures screen and keyboard actions in real-time. This can be used for auditing, monitoring third-party access or investigation after a security breach

Behavioural Analytics

Having PAM as the centralised access point for all privileged access and accounts provides rich data that is used to spot unusual and potentially risky access. Behavioural analytics maybe your first indicator of compromise.

MAP Server

In most cases, admins only need access to a specific tool to perform their work. Rather than granting access to the whole system, MAP Server present just the application they need and no more.

Cloud or On-Premises

Increasingly, organisations are moving IT systems to the cloud. Osirium PAM is available on both the Azure and Amazon Web Services (AWS) marketplaces.

For more information, visit osirium.com/pam