OVERVIEW

Overview of Osirium PAM

Privileged Access Management without the complexity

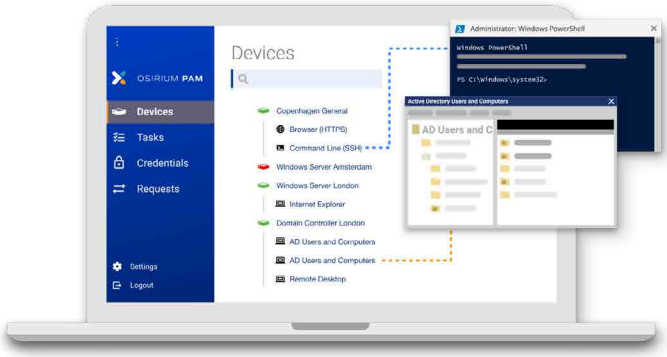
OSIRIUM **PAM**

Privileged Access Management An Overview

What is Privileged Access Management (PAM)?

Every server, device, or service in your IT infrastructure that keeps your business running has multiple administrator accounts. These accounts are so powerful that they are the number 1 target for attackers.

Privileged Access Management (PAM) protects those valuable credentials providing a point of visibility and control over access to your vital shared IT systems.



A complete solution for Privileged Access Management

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.

Automate Privileged Work

Move beyond traditional PAM to further protect privileged accounts. Wrapping tasks with **Osirium Automation** (included with Osirium PAM) prevents users making changes they shouldn't and ensures regulatory compliance meaning IT work can be delegated safely.

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.

Protect Application Access

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 presents just the application they need and no more.

Built-in Reliability

PAM can be set up as a failover pair to ensure high-availability without additional database licenses or complex network dependencies.

Cloud or On-Premises

Osirium PAM can be deployed in the cloud on AWS or Azure, or on your own servers to best support your corporate strategies.

With Osirium PAM you can...

Control third-party and vendor access

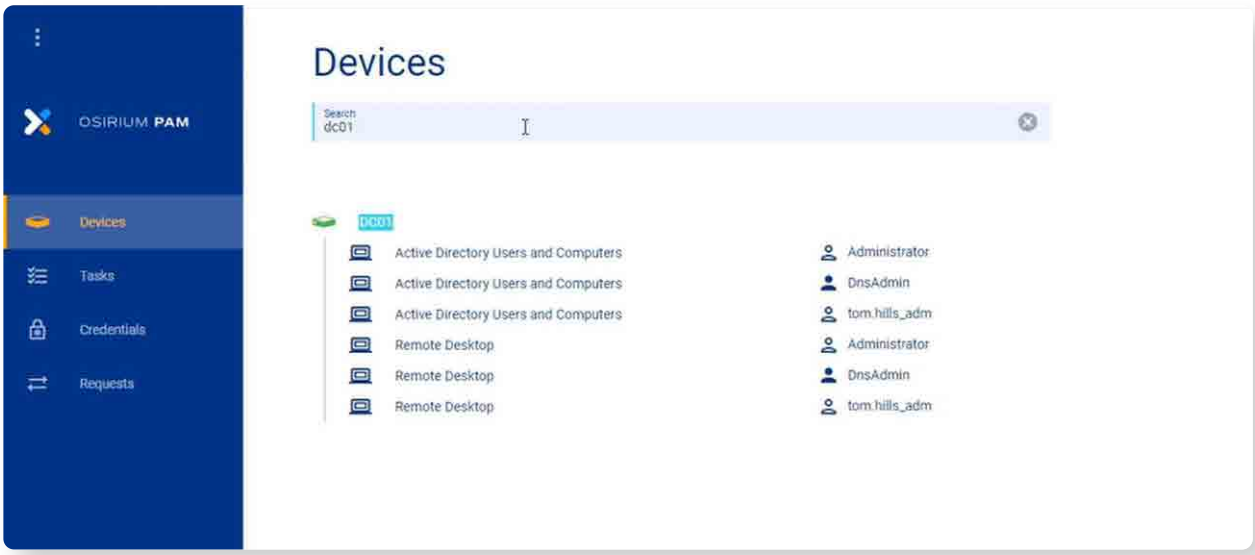
Take full control and visibility of what third parties are doing when they access the network.

Manage and grow privileged access

Administer your growing inventory of devices, accounts and users from a central UI.

Mitigate insider and latent threats

Give users the right access to the right privileged accounts at the right time — No more, no less.



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.

> *We had Osirium up and running in under a day.*
> **Dave Pritt**, IT Infrastructure Manager, Saunderson House

The PAM Solution for IT and Cybersecurity Leaders

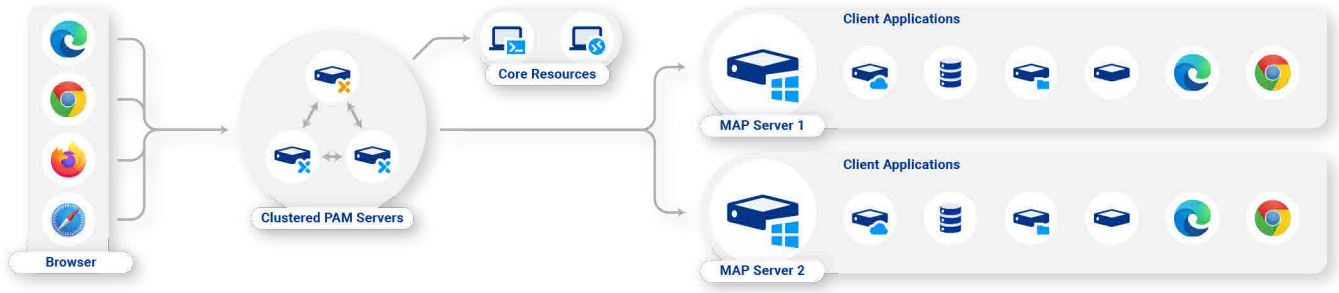
Osirium PAM gives IT Leaders visibility and control of the privileged accounts within the entire IT landscape. Visibility and control allow safe delegation of access to vital IT systems. PAM is a critical capability for compliance corporate policies and standards including Cyber Essentials, ISO27001, PCI DSS and many more.

The PAM Solution for SysAdmins

IT System Administrators have a single interface for all the privileged access they need: no more, no less. They can get fast, secure access to their services, applications, and devices or automate common admin operations. With no agents needed on the target systems, a browser-based client, and no need for a VPN, admins, including third-parties, can get their work done when and where they need.

Osirium PAM Capabilities

A complete solution for Privileged Access Management that's easy to deploy and manage.



Above: Diagram showing how Osirium PAM works

Enterprise Credential Management

- Credentials such as usernames, passwords and secrets protected in an enterprise-class credential vault
- Secure, encrypted credential vault
- Automated password lifecycle management to create, rotate, and retire credentials
- Enforce corporate password policies for length and complexity
- Audit devices to ensure accounts are managed correctly
- Synchronize user accounts with Active Directory (AD)
- Access multiple AD domains

Simple deployment

- Deploy on-premises or in the cloud
- Osirium PAM is supplied as pre-built virtual appliances ready to be deployed in existing virtualisation environment such as Hyper-V, VMware, Azure or AWS
- No agent installation required on target systems and devices
- Device Group Separation (DGS) for easier management by MSPs or segregation of systems for PCI DSS

Extensible Integration System

- Secure integration with target systems via SSH or APIs
- Integration library with more than 200 templates including Microsoft, Cisco, Dell, and many more. Full list here at https://osirium.com/plays-well-with/
- Generic web client interface extends PAM to almost all online services
- Service desk integration to ensure valid change ticket before granting access
- Audit trails published in CEF format for existing SIEM tools

Flexible, Secure Authentication

- Built-in Multi-Factor Authentication (MFA) with Time-based One-Time Passwords (TOTP)
- Integrate with common strong authentication tools for multi-factor authentication (MFA) and Single Sign On (SSO)
- SAML2 integration for Single Sign-On with Identity Providers

Privileged Session Management

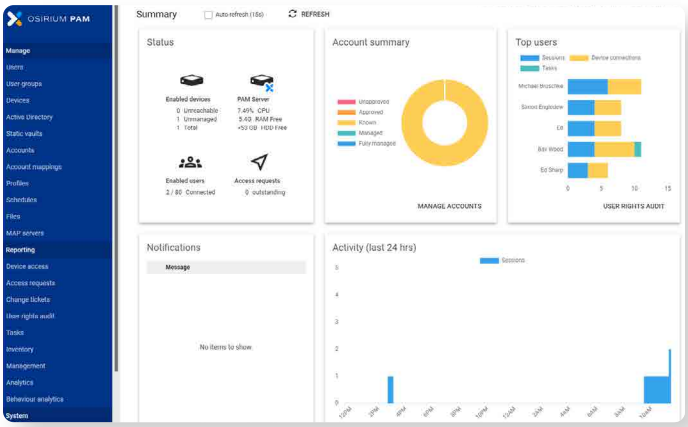
- Granular control of RDP access for users and applications
- Multiple "break glass" emergency access options

Rich Client for SysAdmins

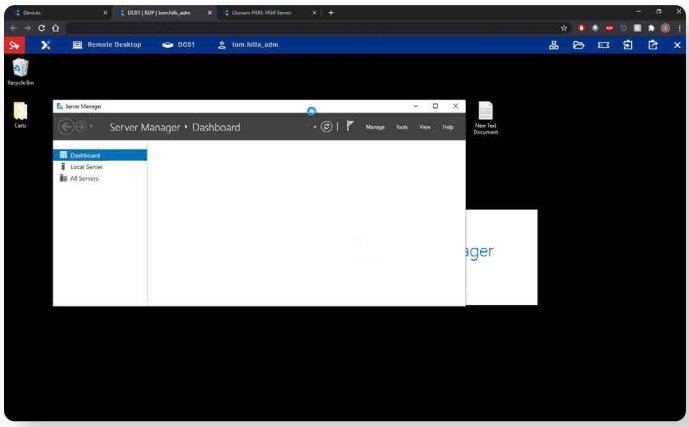
- Zero-footprint browser-based interface
- Optional desktop client
- Credentials automatically injected into target system, service or device
- Credentials never passed across the network to the user's workstation
- User roles determine which devices can be accessed and the type of access permitted
- Grant access for specific time windows at specific times (Just in Time access)
- Assign flexible metadata to devices for easy filtering, searching and access in the PAM client
- Admin of the PAM environment via browser
- Management dashboard with detailed analytics for device and user activity

High Availability Built-in

- High-availability server architecture to ensure SysAdmins can work even if their primary PAM server goes offline.
- Automatic failover active "follower" PAM instance
- No dependencies on database add-ons or network configuration for high availability



Above: Admin interface



Above: PAM Session recording desktop

MAP Server

- Remote access to permitted applications
- No need to install applications on the Admin's workstation
- Safely access "legacy" applications that aren't supported on the Admin's workstation
- Access multiple, conflicting versions of admin apps
- Seamless working with remote applications
- Credentials automatically injected into target system, service or device
- Prevent users doing anything on servers other than using the permitted applications

Task and Process Automation

- Ultimate protection of privileged actions by automating the entire process
- PAM includes three free Osirium Automation licenses
- Admin credentials always protected by Automation and never exposed to users
- Automated playbooks work across multiple back-end systems via REST, SSH, APIs or command lines
- Full audit trail across systems
- Role-based access to automated playbooks
- Build new automated playbooks with the built-in YAML development tool

Session Monitoring and Recording

- Record privileged sessions with target systems via SSH, HTTP(S), RDP, and application clients
- Monitor sessions in real-time
- Record all screen and keyboard actions for selected users
- Only record the application of interest
- Search recordings for events of interest such as when a user ran a specific command
- Configurable notification to users that sessions are being recorded
- Find out what happened on a device at a time for forensic investigation of incidents
- Flexible management of recordings – how long kept, where they're stored, option to export as standard video files

Osirium PAM Availability

Osirium PAM is available as a pre-configured virtual application for use with Microsoft Hyper-V or VMware vCenter. It is also available as an Amazon Web Services Community AMI and in the Azure Marketplace. Details of pre-requisites are available online in the **Osirium PAM documentation**.

For small teams, Osirium PAM Express is available free of charge. **Find out more on osirium.com**.

Further information is available **on request from Osirium**.

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

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