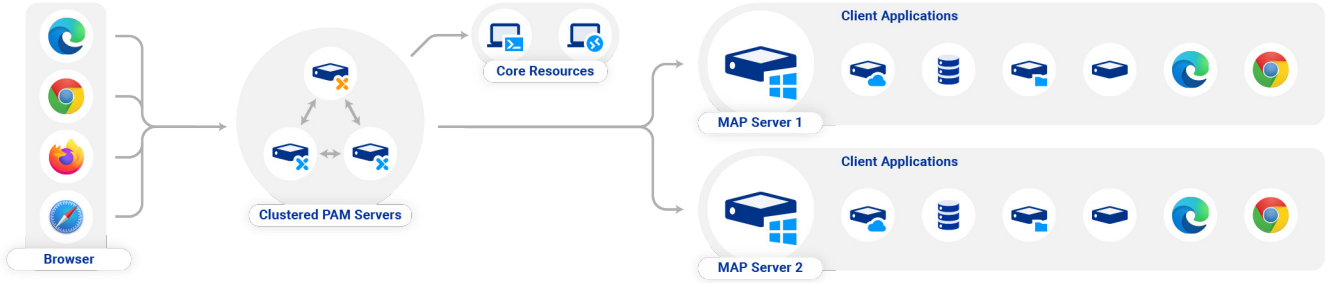
OSIRIUM PAM

Privileged Access Management without the complexity

Osirium PAM Capabilities

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



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

Privileged Session Management

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

Rich Client for SysAdmins

- Browser-based interface for SysAdmins
- No client installation needed, ideal for remote or third-party access
- 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
- Request & Approval workflow before granting access (just-in-time access)
- Assign flexible metadata to devices for easy filtering, searching and access in the PAM client
- Deploy PAM UI outside firewall to remove the need for VPN while protecting PAM
- Admin of the PAM environment via browser
- Management dashboard with detailed analytics for device and user activity

Extensible Integration System

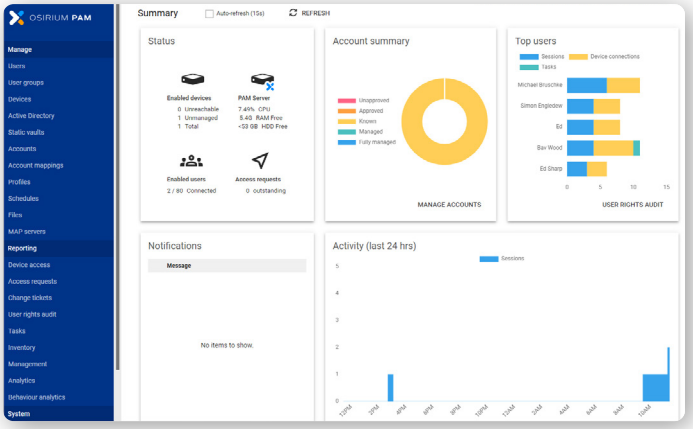
- Integrate with common IAM tools for multi-factor authentication (MFA) and Single Sign On (SSO)
- SAML2 integration for Single Sign On with Okta, Azure AD or other Identity Providers
- Secure integration with target systems via SSH or APIs
- "Plays well with" integration library with more than 200 templates for devices from leading vendors 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

High Availability Built-in

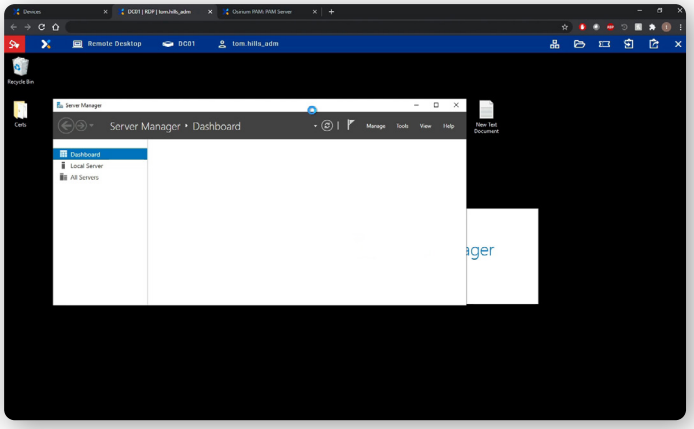
- High-availability clustering server architecture to ensure SysAdmins can work even if their primary PAM server goes offline.
- Automatic failover active "follower" PAM instance
- No dependencies on database add-ons or network configuration for high availability

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



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
- 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
- Recordings can be played fast-forward to quickly locate point of interest
- Configurable notification to users that sessions are being recorded
- Report on device access
- 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
- Export recordings as videos
- Share files and clipboard content between user workstation and remote session

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.

Osirium PAM users access their devices and tools via a browser-based client. No software is required on the target devices or client systems. An optional, cross-platform desktop client is also provided.

PAM licensing is subscription-based, per device. No additional licenses are needed for clustered deployments. Osirium Automation is subscription-based, per-user. Three Automation user licenses are included with Osirium PAM.

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.