# OSIRIUM PPA

## Privileged Process Automation

**Automate business and IT processes to reduce cost and risk while improving customer service and productivity.**

# Introduction

**Automation is the key to streamlining business and IT processes, but traditional approaches and RPA have significant security risks. They often contain embedded credentials and is hard or impossible to maintain end-to-end audit trails.**

**Privileged Process Automation (PPA) is a new class of automation that automates IT operations, service desks and business processes.**

# PPA benefits

### Automate secure IT operations

The only automation system built for privileged access to critical IT systems.

- Securely automate standard operations such as reset password, creation of new test environments
- Co-ordinate privileged activities across multiple systems
- Never reveal privileged credentials.

### Enhance systems security & compliance

Enhancing existing IT systems. Automate privileged operations for IT systems

- Enforce corporate policies such as content of free-form fields, e.g. descriptions or reasons for change
- Implement fine-grained role-based access controls on tools with limited security.

### Simplify complex privileged tasks

Reduce complexity and standardise privileged operations.

- Reduce dependency on highly-skilled staff to perform every day operations
- Use standard processes across different hardware or software systems
- Wizard-style operation for even the most complex processes.

### Full audit trail

Full audit trail of all operations.

- Satisfy compliance requirements transparently
- Track who runs which processes, where and when
- End-to-end record of actions to track changes back to help desk (e.g. ServiceNow) tickets.

### Bring your own code

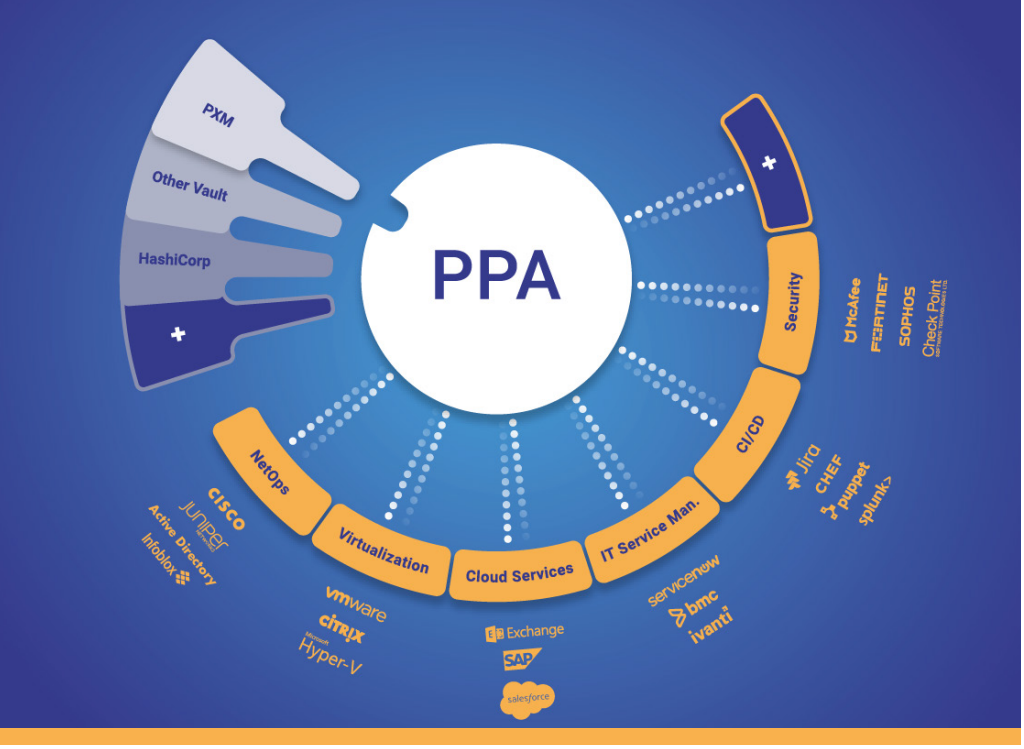
Reuse existing tools to avoid rework.

- Reuse existing tasks and scripts
- Implement fine-grained role-based access controls on tools with limited security
- Isolate scripts from privileged credentials.

### Keep credentials secure

Isolate credentials from devices.

- Users never have access to privileged credentials
- Seamlessly operates with Osirium Privileged Access Management or other PAM tools
- Never embed valuable secrets in scripts or code.




### Securely enhance existing IT infrastructure

Osirium PPA uses standard open interfaces to automate a broad rang of services, devices and applications. Its container-based architecture is highly-scalable and secure to support the largest enterprise environments.

# Typical PPA use cases for Privileged Automation

**PPA is an open architecture, flexible and extensible framework for the automation of IT operations and business tasks. Most IT tasks touch multiple IT servers or devices. PPA automates all the steps removing the opportunities for manual error. Typical scenarios include...**

### New starter - Developer

- Create account in Active Directory
- Create virtual machines for Dev & Test
- Create development databases
- Create accounts in CI/CD tools
- Update HR records

### Network operations

- Update ports
- Create DNS records
- Configure routings, across different hardware vendor platforms

### Reset password

- Verify requesting user ID
- Set temporary password in AD
- Set 'reset next login' flag
- Update ServiceNow ticket

### CMDB Update

- Validate CMDB accuracy and data integrity
- Implement ServiceNow change request
- Round-trip update of ServiceNow ticket

# About Osirium

Osirium Technologies plc (AIM: OSI.L) is a leading vendor of Privileged Access Management ("PAM") and Privileged IT Process Automation ("PPA") software. Osirium's cloud-based products protect critical IT assets, infrastructure, and devices through automation and by preventing targeted cyber-attacks from directly accessing Privileged Accounts, and removing unnecessary access and powers of Privileged Account users.