OPUS

Privileged IT Operations Automation

For IT operations, Help Desks, Managed Service Providers, Network Operations, Security Operations Centres, Third Party Access

Introduction

Robotic Process Automation (RPA) is transforming traditional business processes by automating repetitive operations. However, those tools are not suitable for IT Operations teams. IT admins need access to many complex tools and privileged user access which traditional RPA can't handle. Until now, they have been forced to continue using slow, insecure, and error-prone manual processes. Opus changes all this as the world's first secure IT Operations process automation tool.

Opus 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 compliancy 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

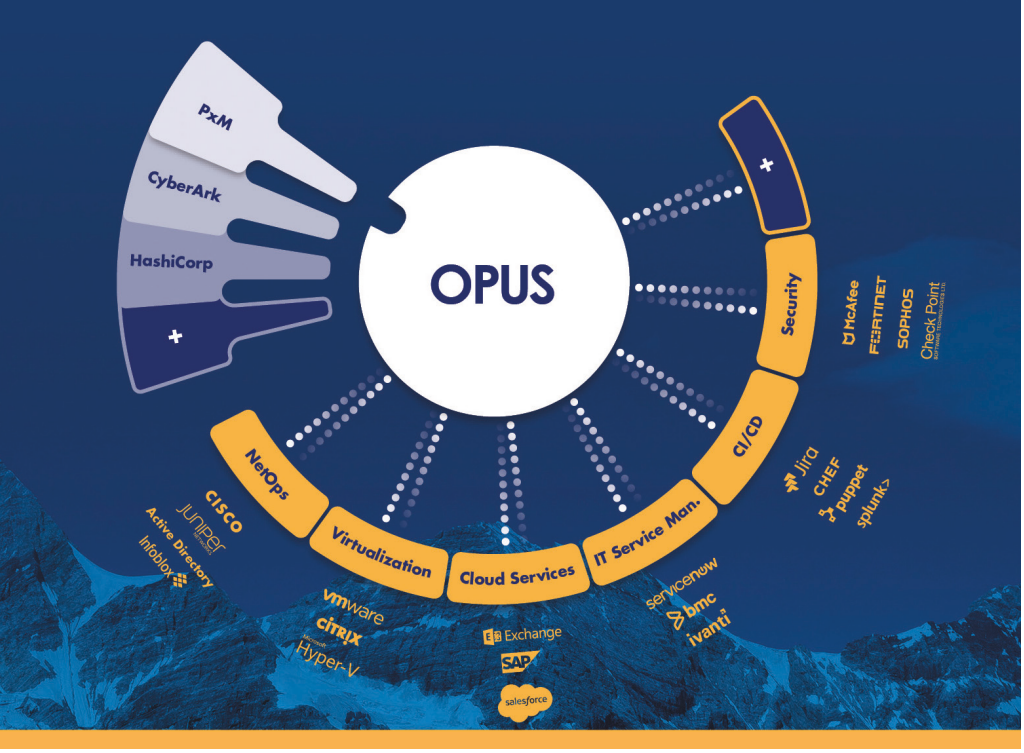
Resuse existing tools to avoid rework.

- 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 Opus uses libraries of pre-configured operations for common IT systems and devices. Additional libraries can be built as needed to enable automation across the IT estate. The highly-scalable, container architecture can support the largest enterprise IT environments.

Typical Opus use cases for Privileged Automation

Opus is an open architecture, highly-extensible environment to securely automate IT operations. Most IT tasks touch multiple IT servers or devices. Opus 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

Availability

Opus is available now from Osirium.
Contact Osirium for more information.

About Osirium

Osirium Technologies plc (AIM: OSI.L) is a leading vendor of Privileged Access Management ("PAM") and Privileged IT Process Automation 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, removing unnecessary access and powers of Privileged Account users.