OSIRIUM **AUTOMATION**

Automating Network Operations

Simplify complex network operations and improve security.

OSIRIUM

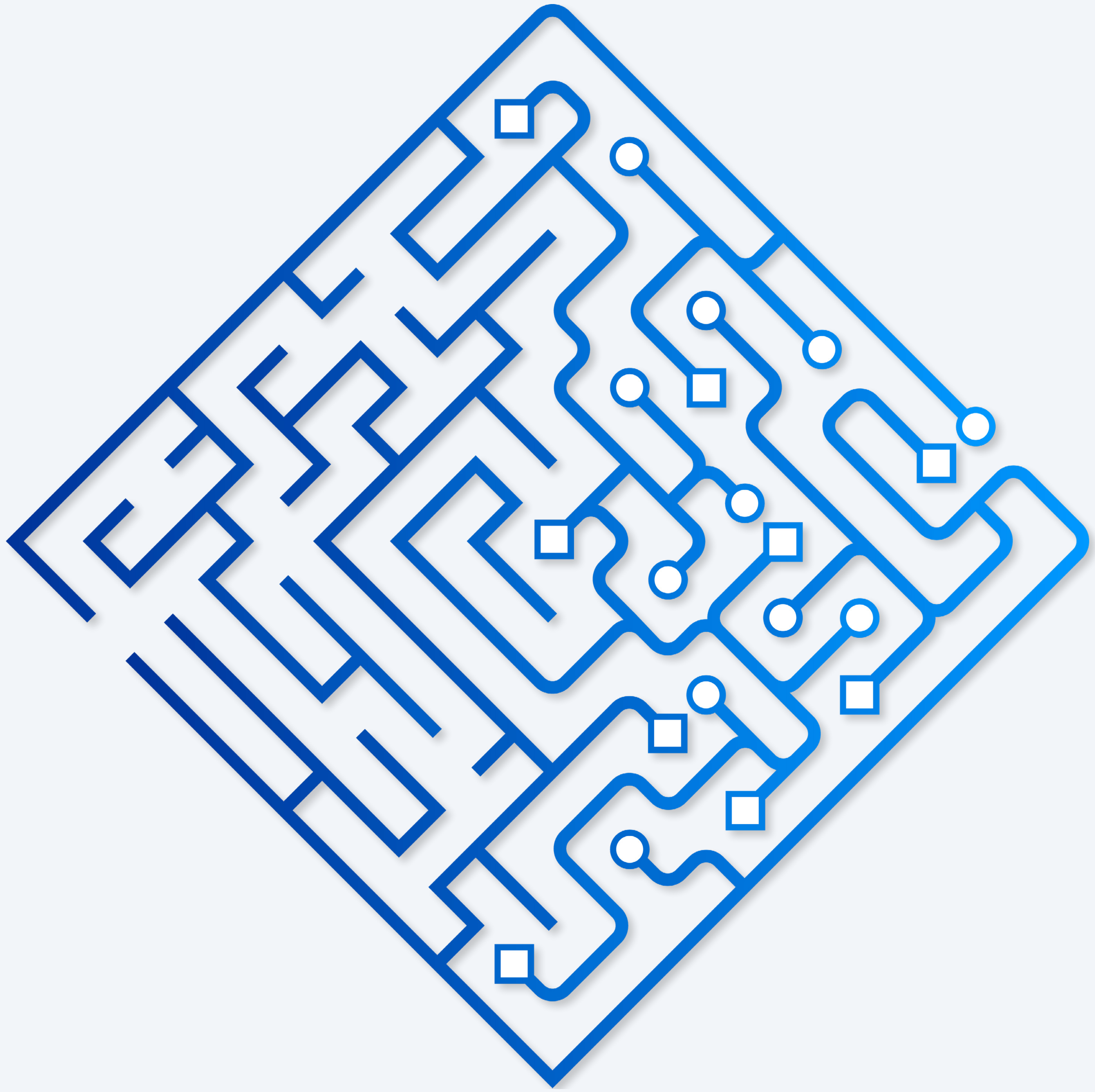
Contents

Introduction

Network Operations (NetOps) is at the heart of every IT organisation. It's a service that covers a wide range of activities: end users' workstations connecting to corporate servers, access to cloud and internet services, remote access for workers at home, third parties and suppliers, and much more. It's hard to think of any business service that doesn't rely on network operations.

It's vitally important that any updates to network systems are performed in timely manner and done right the first time. If not, then the business can be exposed to cyberattacks, business users can't get on with their work or customers can't access the company's services.

In this e-book, we'll look at the common challenges for NetOps teams and how automation can be safely applied to deliver better service and improve security. Osirium Automation, a unique solution for automating IT and business processes that traditionally require expert skills, can be applied in a vast range of NetOps tasks but we'll focus on three to demonstrate the possibilities with automation. If you have other tasks you'd like to automate, please get in touch.



Meet ANA

Introducing the automated assistant for Network Operations

In this book, we'll introduce you to the Osirium Automated Network Assistant, also known as ANA. In reality, ANA will be a set of automated playbooks or tasks for common network operations tasks. These playbooks capture your NetOps' expert experience so that changes are made according to best practice and in compliance with corporate policies.

With that experience, ANA is the specialist assistant for NetOps engineers. It can take care of the routine tasks that need to be performed every day. Whether that's a self-contained task such as checking that a server is contactable or automating complicated multi-step updates to save the expert time and reduce the risk of manual errors.

A rich set of pre-built playbooks are available for free in the Osirium Automation Resource Hub to get you started as quickly as possible. You can extend or build news skills for ANA to match your needs.

ANA is just one example of the assistants that could be built with Osirium Automation. Visit https://www.osirium.com/automation for more examples.

Typical NetOps Operations

Updating Network Switch Configuration

A common task for NetOps is to update the configuration of a network device. For example, changing the speed on a port on a network switch.

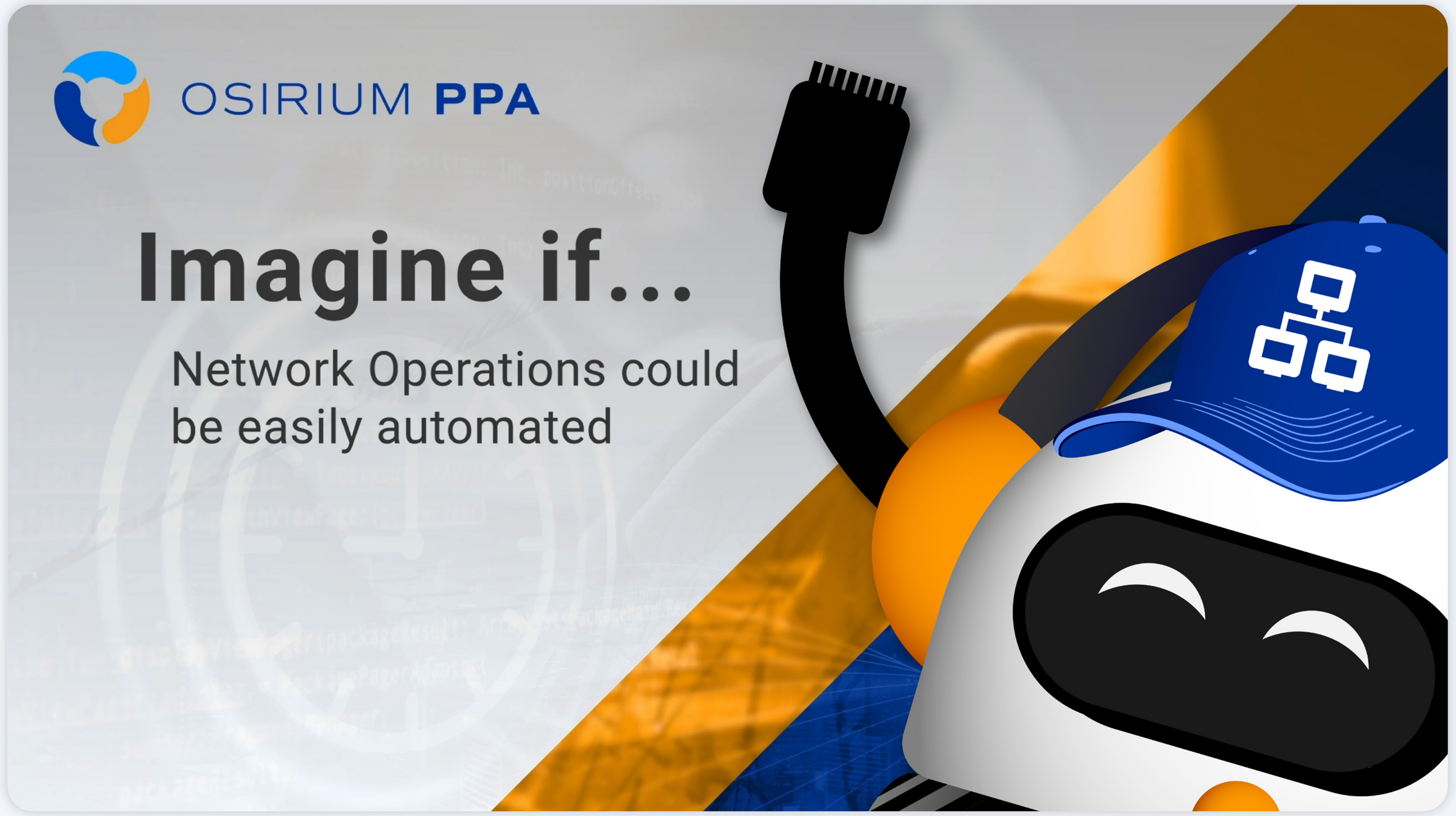
Those changes are often made by logging into a management console or via SSH to the device. Each manufacturer, Cisco, Juniper, etc., will have their own management system, so the change has to be made by the right expert. Even the experts may take time to navigate through the complex management tool to find the function they need which makes a simple task slow, boring and potentially error prone.

Automation to the rescue!

With Osirium Automation, that change becomes easy. As you'll see in this video the automated playbook retrieves the necessary administrator credentials from a secure vault. It then asks the engineer to confirm which device(s) need to be updated and the change to be made.

Automation takes care of making the change and there's a full audit trail to show exactly what happened.

You can see how in this demonstration:



https://www.osirium.com/videos/imagine-if-network-operations-was-easy

Typical NetOps Operations Continued

Run Ansible Playbook

Ansible is commonly used for network device deployment and management. Ansible is a powerful automation tool that can remove some of the complexity of managing many devices, but it's still complicated. Ansible is best at making a single change across an inventory of devices, but find those inventories, confirming the devices and performing more than one set of changes is complicated. And there's the issue of ensuring the admin credentials used by the playbooks are properly protected.

Automating Ansible Automation

ANA can remove complexity. As you'll see in this example, the NetOps engineer starts an Osirium Automation playbook to perform the required task. In this demonstration, it's a very simple operation, but it could be anything that could be included in an Ansible playbook. The engineer chooses which hosts in the inventory should be included and then which operation to perform.

You can see how in this demonstration:

BITESIZED DEMO

Run Ansible playbook

OSIRIUM PPA

https://www.osirium.com/videos/ppa-bitesized-run-ansible-playbook

Typical NetOps Operations Continued

Updating Firewall Configuration

Another common task is updating the configuration of software devices such as firewalls. When the updates are to critical infrastructure such as a web server or security device such as a firewall, it's important that the changes are performed accurately. Of course, it also has to be done securely. If an attacker should acquire the firewall admin account credentials, they could open ports ready to exfiltrate data before activating ransomware to encrypt data on the network.

Configuration Automation

Again, firewalls typically have complex and varied management systems. ANA is the ideal assistant to take care of that complexity and ensure all changes are fully recorded for audits. Take a look at this video to see ANA in action.

You can see how in this demonstration:

https://www.osirium.com/videos/privileged-process-automation-ppa-for-secops-with-check-point

About Osirium Automation

Automate Everyday NetOps Tasks

Osirium Automation is a unique solution for automating IT and business processes that traditionally require expert skills.

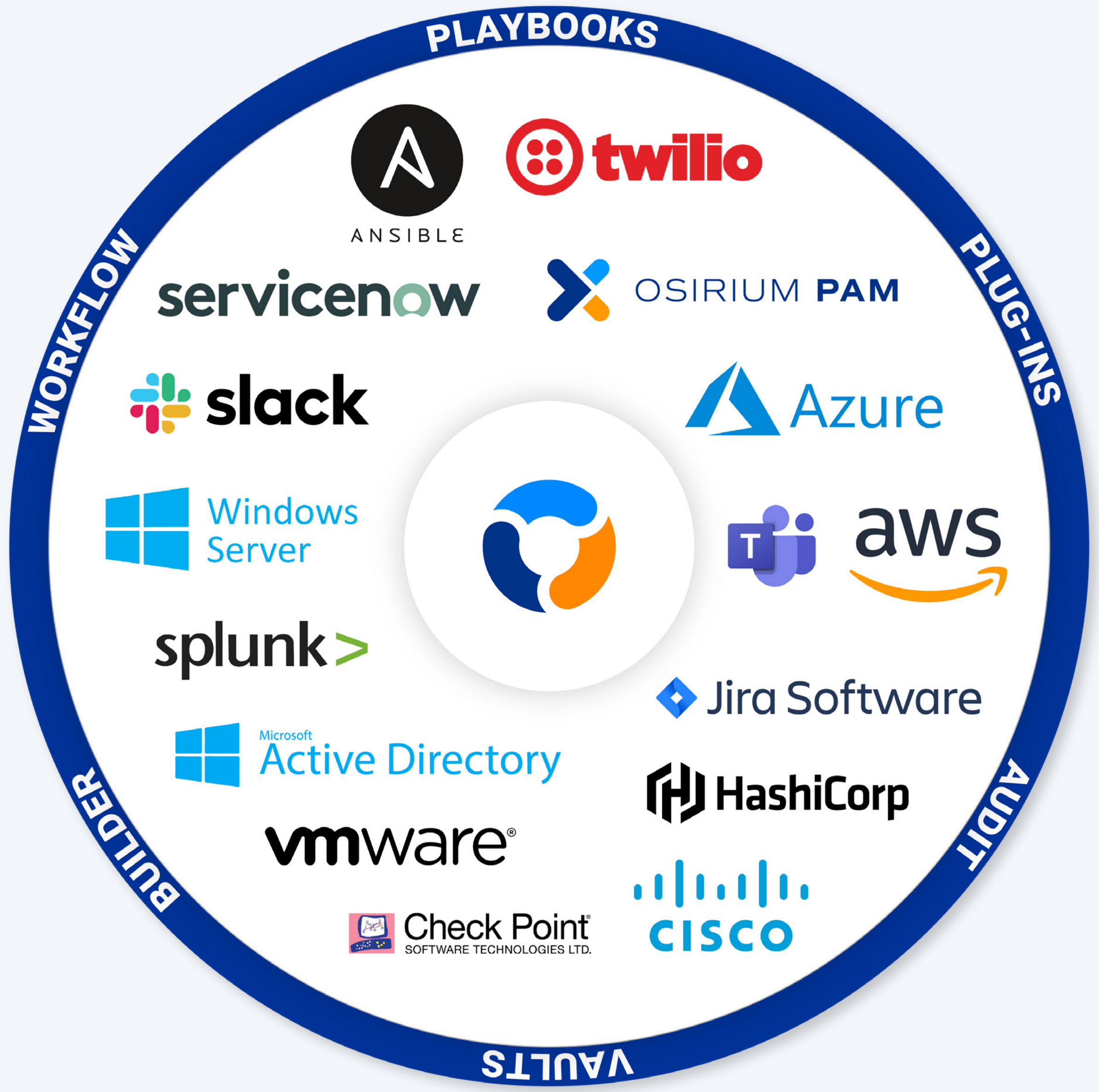
Its flexibility comes from the open, secure Privileged Process Automation (PPA) framework to automate workflows across systems via API, REST, SSH, or command lines.

By hiding the complexity and need for specialist technical knowledge, processes can now be securely delegated and accelerated.

Credentials stored in secure vaults such as Osirium PAM or HashiCorp and are always protected when interacting with the back-end IT systems, such as network devices or Active Directory. Those credentials are never passed back to the user's workstation so can't be intercepted on the network or misused by the user.

NetOps tasks are automated using "playbooks" – simple, low-code automation built using the built-in development and test environment. Those playbooks have a simple, conversational interface so any user can complete tasks with little knowledge of the underlying systems.

The playbooks can include workflow and approval mechanisms via email, Microsoft Teams or Slack to ensure that particularly sensitive changes are reviewed before being completed. A complete audit trail is maintained of all the changes and approvals. A rich set of pre-built playbooks is available from the PPA Resource Hub, including the NetOps tools. Automation integrates with existing service desk management tools such as ServiceNow or corporate intranet portal so that existing processes and tools can be used with the final changes implemented by Osirium Automation.



Regular operations, such as generating lists of group memberships, can be scheduled to run weekly or monthly.

Full audit logs are maintained within PPA and your preferred SIEM logging systems such as Splunk.

If you'd like a demo of Osirium Automation, please get in touch. You can also download Osirium Automation for free and start automating your own NetOps tasks.

About Osirium

Osirium is the leading UK-based vendor of Privileged Access Security (PAS) solutions. Osirium's cloud and on-premises products protect critical shared IT infrastructure and endpoints, and securely streamline IT operations to deliver digital transformation fast.

Besides, Osirium Automation, Osirium's PAS solution includes modern Privileged Access Management (PAM) to protect valuable services and enables managed access by third-party vendors and partners. It includes high-availability clustered servers, session recording, just-in-time approvals, and simple deployment.

It also includes Privileged Endpoint Management (PEM) to remove local administrator accounts and manage applications approved to run with elevated privileges. Removing local admin rights is a critical part of any "least privilege" strategy.

For more information, please visit https://www.osirium.com/automation.

> *"Osirium's automation allows vital processes to be automated and delegated without compromising security."*

SAUNDERSON
HOUSE