Transforming Business Operations with Privileged Process Automation

Five common scenarios that should be automated

OSIRIUM

Transforming Business Operations with Automation
Five common scenarios that should be automated

Introduction

Every business wants to do more, move faster, reduce costs, minimise security risks. But how can that be done without reducing quality of service? Surely, that's asking too much?

Too many priorities. Not enough resources. Not enough time.

Imagine if there were a way?

Automation is frequently spoken of as the answer, and traditional automation tools are good for automation in limited situations. But too often they quickly become expensive. Or they lack security. Or they're not flexible enough for many services delivered by IT.

Time for a new approach then. It's called **Privileged Process Automation**, or **PPA** for short, from cybersecurity and process software specialist Osirium. In this e-book join us on a short journey not just to imagine, but to see in reality how PPA lets you meet and solve five thorny, complex and painful IT and business challenges.

What is Privileged Process Automation?

Imagine if…

- your business could complete common tasks in minutes rather than hours or days?
- complex tasks didn't rely on IT specialists and could be safely handed to service desk or business managers?
- you could improve efficiency, reduce human error and ensure consistency every time?

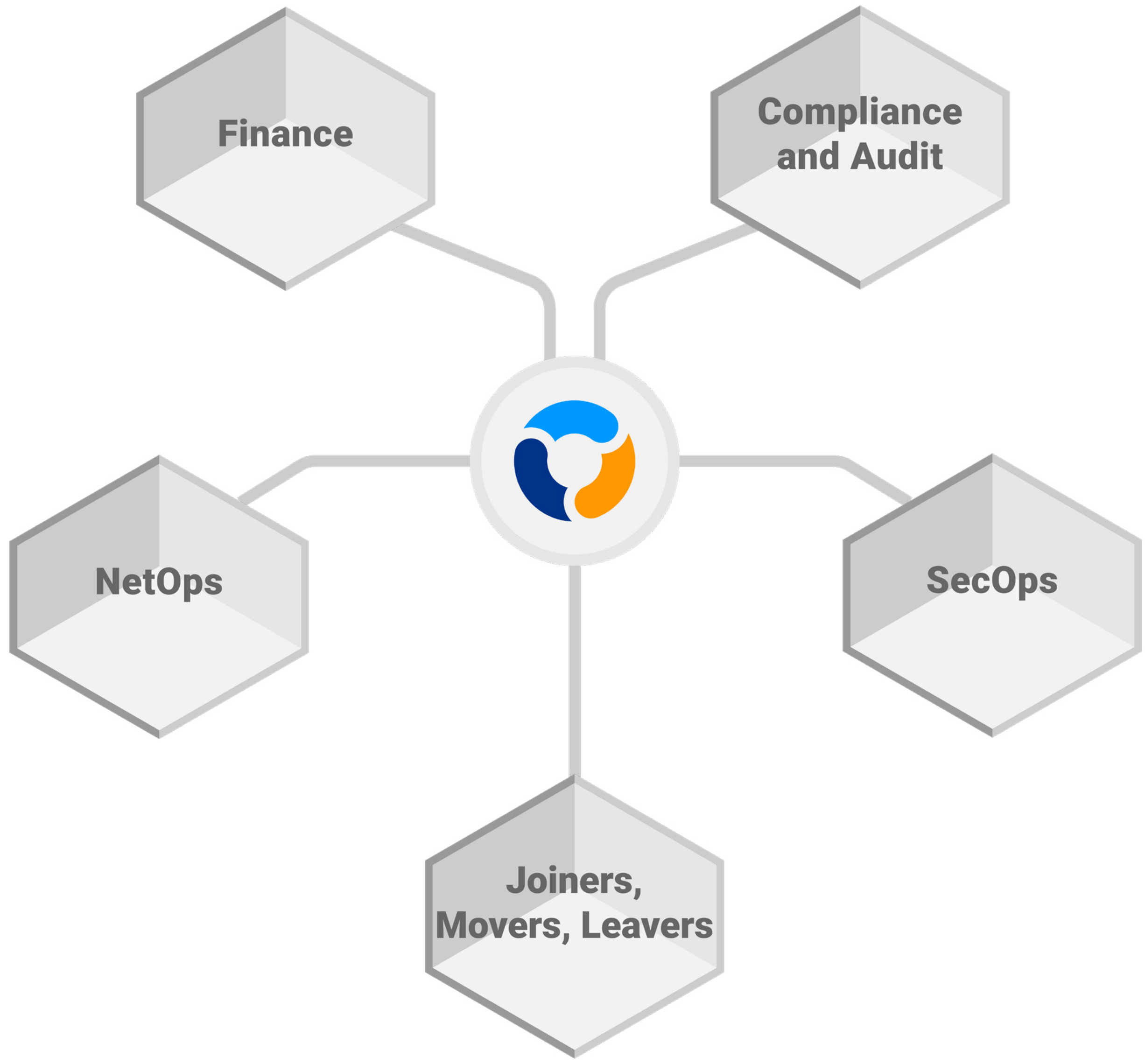
That's why we created PPA, a platform that allows your organisation to transform complex manual processes into simple automated actions. Tasks that used to require expert IT skills or special security levels can now be safely delegated and automated.

PPA is a low-code and API-driven platform so it can deliver joined-up intelligent processes with any of your systems. Created for both IT and non-technical users, PPA processes can be scheduled, or intelligently interact with users for input and follow approval workflows.

Designed by Privileged Access Management experts, Osirium, credentials are picked up from credential stores and are NEVER exposed within the process code or to the user. This means that your automated tasks are 100% secure and fully audited.

What benefits can you imagine?!

Let's look at five scenarios that show how customers are using PPA to solve and take the pain out of complex process challenges. Faster. Simpler. Cheaper.



Scenario #1

Imagine if… Account Recertification wasn't a time-consuming chore

The Challenge

Just about every organization has to do regular privileged account recertification. It might be called something else, but the need is to check that only the right people have privileged access to shared devices, applications or services.

In many cases, it's a legal requirement defined in standards such as NIST-800, CAF, PCI-DSS and many others: run regular reviews and audits of privileged accounts.

Too often it leaves teams overwhelmed by manual, time-consuming and error-prone processes:

- create lists of privileged accounts
- send them to departmental leads
- have departmental managers review and update changes e.g. marking which people should no longer have access
- then… return all the marked-up lists to IT who manually make changes in Active Directory

It's slow, tedious work. Very easy to make mistakes.

Scenario #1

Imagine if… Account Recertification wasn't a time-consuming chore

The Osirium Solution

Take a look at this video to see how PPA walks the user through the process to gather the required details, verify the choices and perform the necessary updates.

If above link is broken please follow https://youtu.be/cjfnzQWT5rQ

It's a classic illustration of how PPA:

- simplifies and delegates previously laborious, labour-intensive tasks
- wraps the entire process so the manager can't do anything they shouldn't
- securely connects to Active Directory without the risk of exposing the credentials used for the connection
- for compliance, maintains a full audit trail to show what changes were made

Scenario #2

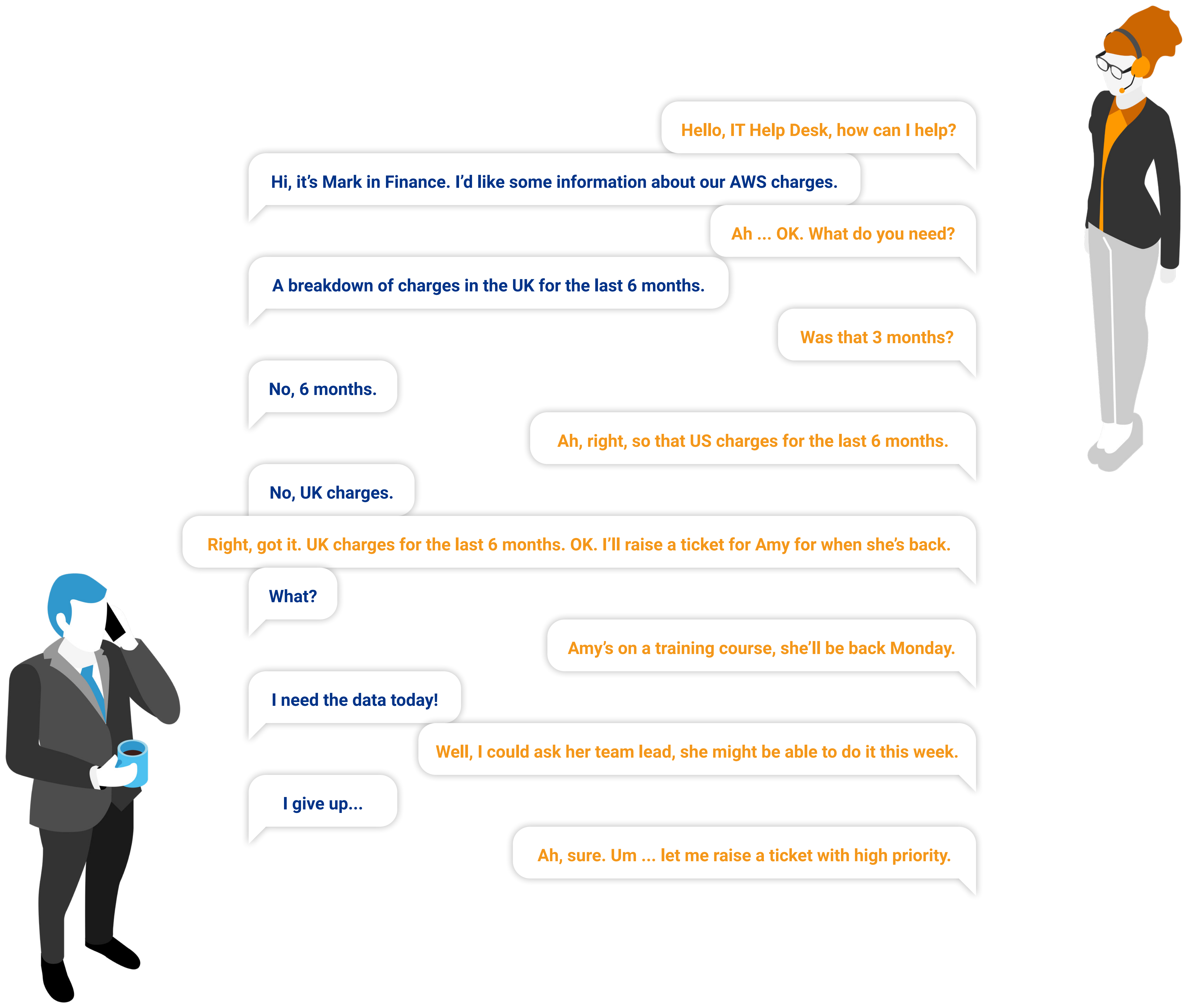
Imagine if… getting system billing data didn’t rely on IT specialists

The Challenge

No-one is happy with the kind of conversation on the right.

- the Help Desk agent didn’t give great service (and ends up with an open ticket against her metrics)
- the user didn’t get what he needed, so may not be able to do his job, and may well try to bypass IT next time
- IT management won’t be happy because their customer satisfaction stats will take a hit and, besides, they really don’t like not being able to help

IT would love to enable business users to get the data they need for themselves, but that means exposing credentials to access the AWS management console.
Business users would like to do it, but they don’t know how and don’t have time to learn.



Hello, IT Help Desk, how can I help?

Hi, it’s Mark in Finance. I’d like some information about our AWS charges.

Ah ... OK. What do you need?

A breakdown of charges in the UK for the last 6 months.

Was that 3 months?

No, 6 months.

Ah, right, so that US charges for the last 6 months.

No, UK charges.

Right, got it. UK charges for the last 6 months. OK. I’ll raise a ticket for Amy for when she’s back.

What?

Amy’s on a training course, she’ll be back Monday.

I need the data today!

Well, I could ask her team lead, she might be able to do it this week.

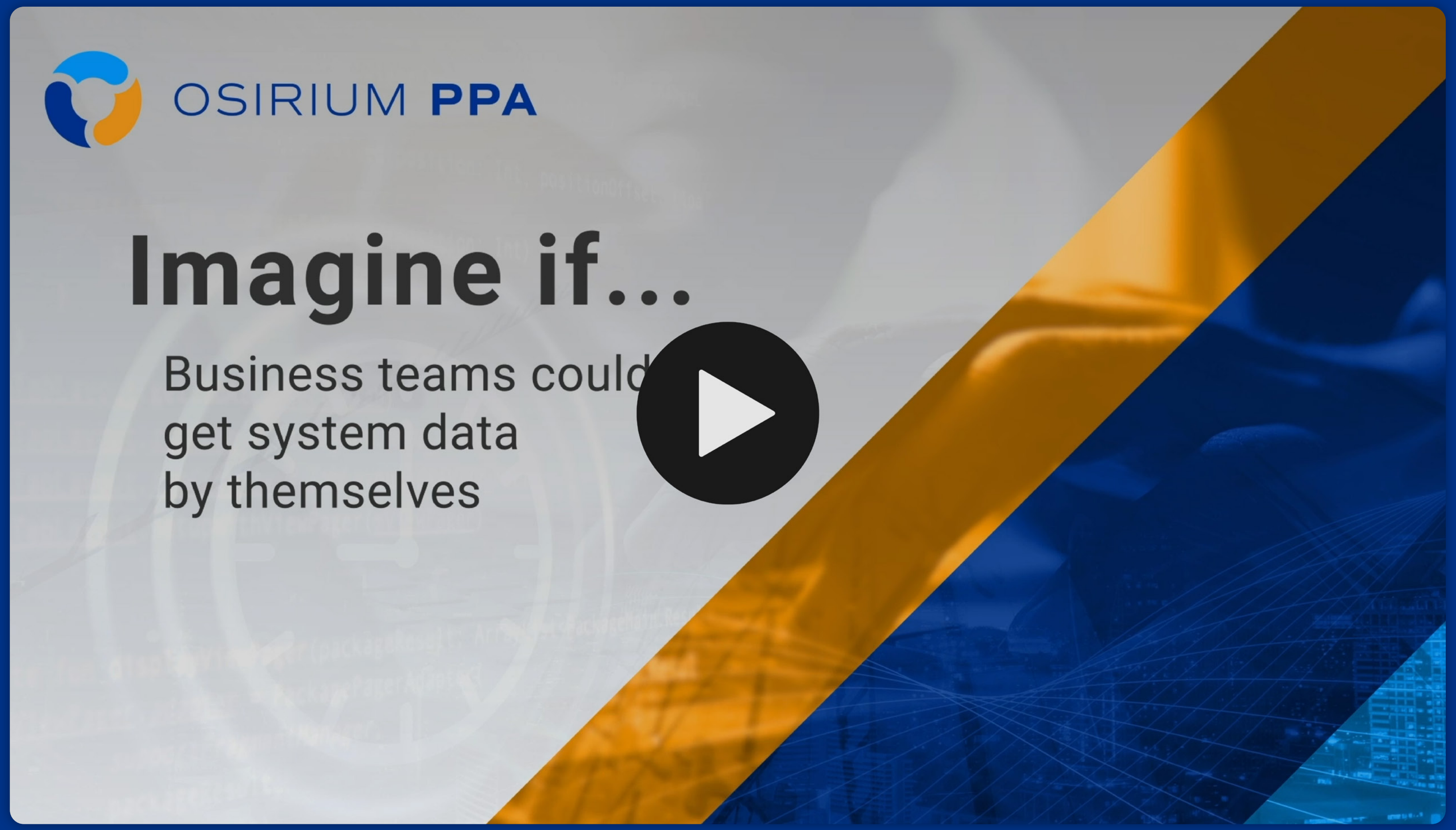
I give up...

Ah, sure. Um ... let me raise a ticket with high priority.

Scenario #2
Imagine if… getting system billing data didn’t rely on IT specialists

The Osirium Solution

Take a look to see how PPA guides the user through the process.



If above link is broken please follow https://youtu.be/maBStcOIbdY

There are multiple benefits for both users and IT:

- the user doesn’t need to know anything about how the AWS management portal works
- they can’t do anything they shouldn’t
- they’re not reliant on skilled IT admins, who are now free to concentrate on more complex tasks
- administrator credentials are never exposed to the user, so there’s no risk of a security breach

AWS billing data is just one example. Finance or HR teams may want to get data from other cloud providers (such as Azure or Google Cloud Platform), or web services such as Salesforce.com, SAP and many others. PPA’s flexible framework is ready to wrap cloud services or in-house systems to make that happen.

Scenario #3

Imagine if… a Joiner-Mover-Leaver process was smooth and simple

The Challenge

It's exciting when someone new joins your company or team. But how often do they come to the office, buzzing with enthusiasm only to find they can't log in to their computer, or their email account hasn't been set up, or they can't access the HR system to set up where their pay should be sent, or…

For IT teams, it can be an almost full-time job creating accounts for new joiners, removing accounts when they leave or updating accounts when people move between teams.

And every system (Active Directory, Office 365, Jira, Workday, and many more) will have its own administrators. Each of those admins will have their list of tasks to do and may be busy with other projects. Or unavailable.

So… there's no guarantee when all the accounts will be ready.

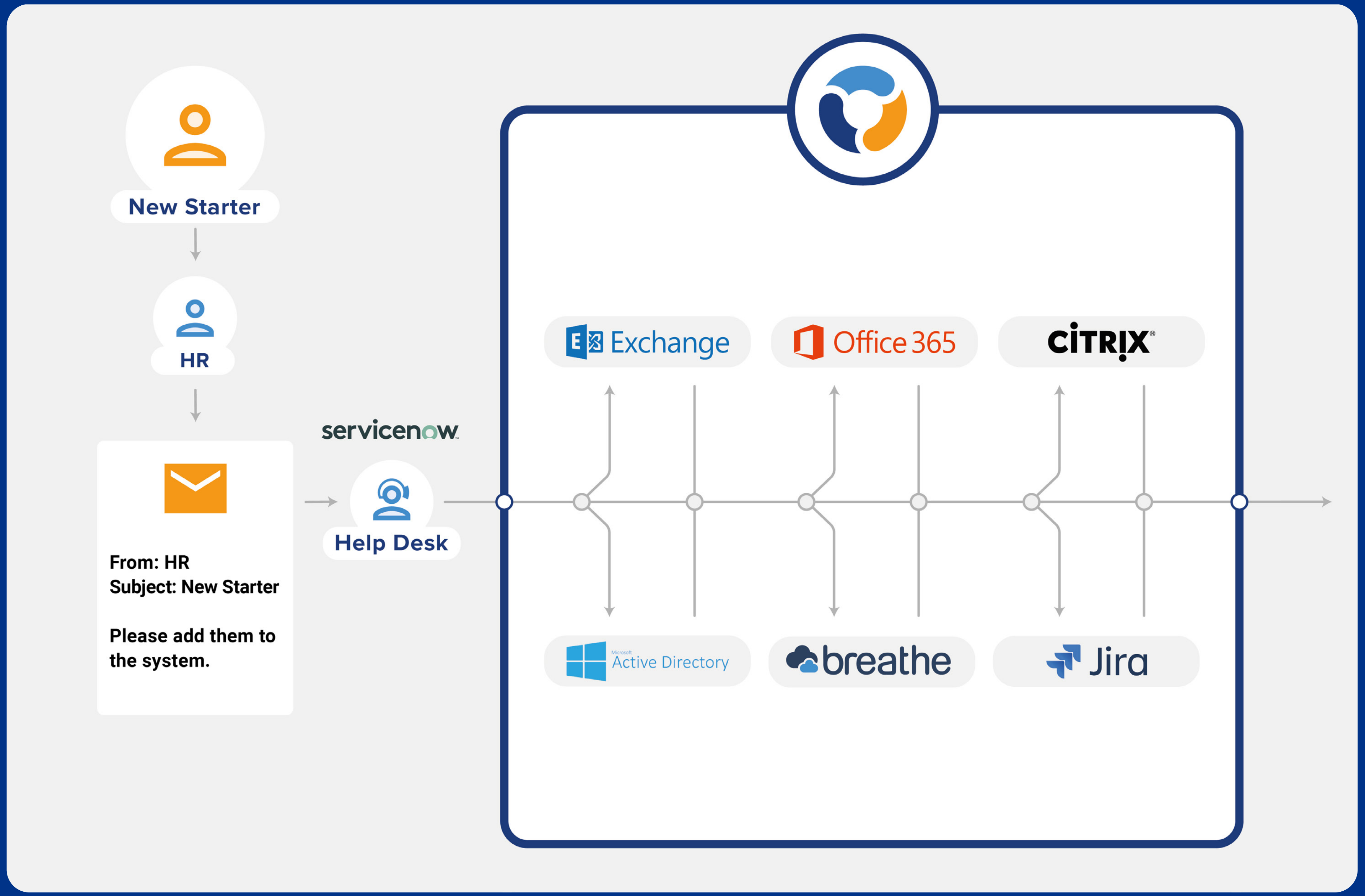
Scenario #3

Imagine if… a Joiner-Mover-Leaver process was smooth and simple

The Osirium Solution

A simple, step-by-step, guided experience.

If above link is broken please follow https://youtu.be/l_zLY2pOQ20



From: HR
Subject: New Starter

Please add them to the system.

In the background, PPA is connecting to and coordinating complex, multi-system processes, but hiring managers or HR staff don't need to know the detail.

Just as this process automates the account creation tasks, processes can be built to handle account removal and updates for when people move between teams.

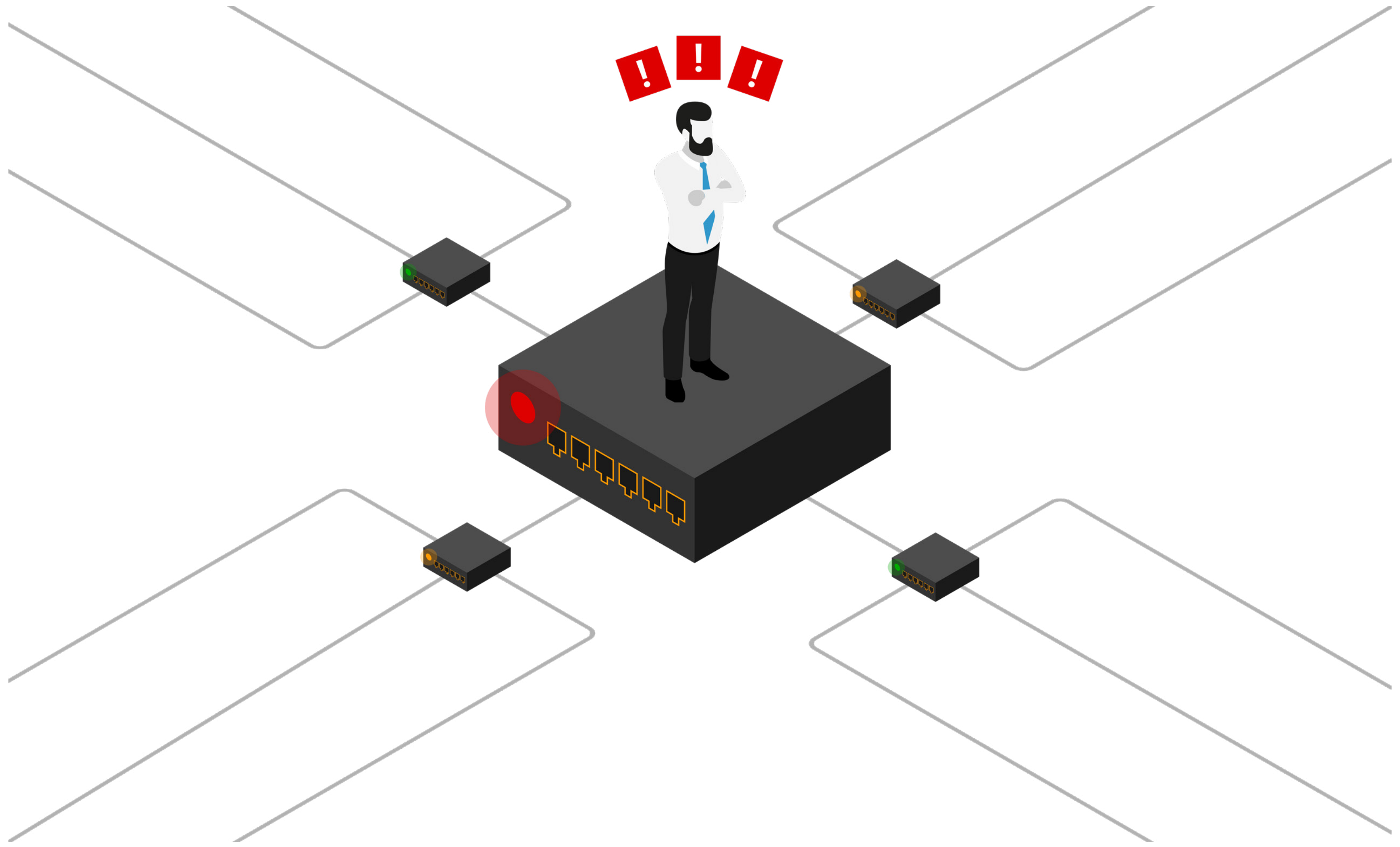
Scenario #4
Imagine if… you could take the complexity out of network changes

The Challenge

Changes to network devices are complicated and important. A misconfiguration of a router, access point or internet connection could prevent staff from working, or customers from buying your products and services. It could also leave gaps in security defences waiting to be discovered by an attacker.

So even the simplest change needs to be handled by a specialist. Someone that knows the different tools used by each network device vendor. Indeed, specialists are generally needed for each vendor so they can't cover each other's work.

So these experts are in high demand. And, because of complexity and reliance on specialists, seemingly small changes can be delayed by days or weeks.

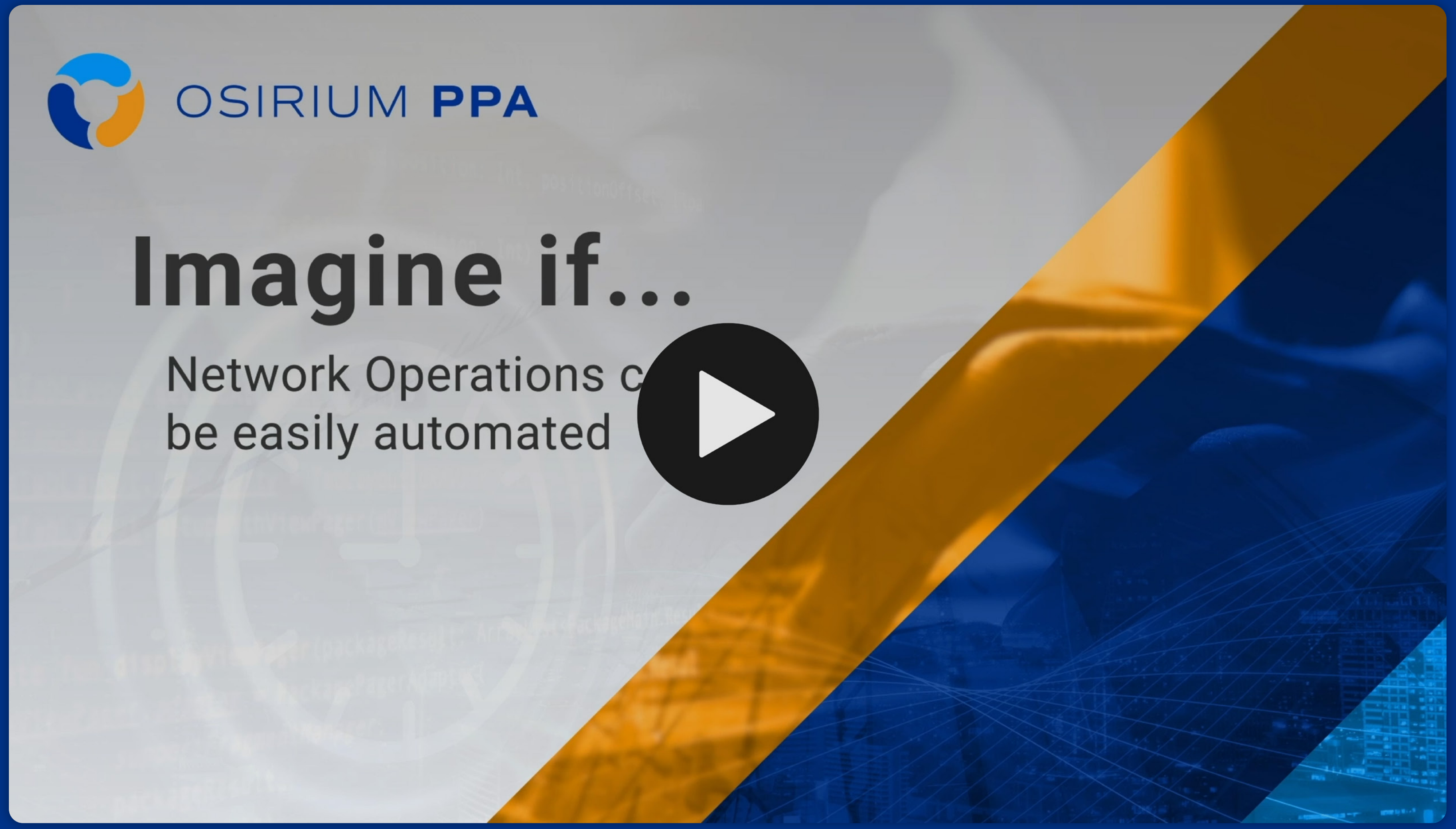


Scenario #4

Imagine if… you could take the complexity out of network changes

The Osirium Solution

The process may appear to need specialist skills, but PPA simplifies the entire workflow.



If above link is broken please follow https://youtu.be/pFLJMWTu5UQ

Network Operations tasks can be made quickly and securely

- Complex operations are wrapped eliminating manual errors and ensuring consistency across different platforms
- Admin credentials are protected so updates can be delegated to the help desk
- A full audit trail and automated workflow ensures policies are enforced.

Once NetOps can be easily automated, changes become easier to plan and execute. For example, re-configuring the network to increase security or remove bottlenecks is achievable in the short term, not a project for next year.

Scenario #5

Imagine if… security updates were fast and easy?

The Challenge

Or imagine if security updates were so easy, they were never missed and never delayed?

The challenge here is that the security elements within the corporate infrastructure are mostly complex and need advanced or specialist skills to manage and update. Getting the update wrong can rapidly lead to a major security breach.

A typical example is updating firewall rules when a new application server is being provisioned. Any delays in the update results in lost sales opportunities. Any errors could expose the company to attack. It's no wonder traditional approaches are long and complex to try to reduce risk. There has to be a better way.

Scenario #5

Imagine if… security updates were fast and easy?

The Osirium Solution

Managing security updates can be both fast and safe. Check it out.

If above link is broken please follow https://youtu.be/e1ULsiGDH3U

Security was actually the original driver for creating PPA. Privileged Access Management (PAM) is where the Osirium business started. The processes and measures taken in the video show how we've carried that understanding of privileged access and privileged accounts into PPA.

This example of carrying out updates to complex security systems shows the essence of Privileged Process Automation. It's about the power of delegation without having to worry about privilege. It's about extending privilege without extending risk.

PPA Overview

A flexible framework for automation

Human-Guided or Fully Automated

There are three styles of process automation available with PPA to suit different scenarios where some need interactive guidance from a human, such as the account re-certification process, others that need limited interaction like provisioning new accounts or fully automated such as performing regular scheduled server health checks.

Human Guided

Staff access their PPA Dashboard via a web-browser. They see only those tasks they have permissions to access as defined by their Active Directory group or permissions granted in PPA. Processes can request additional information or decision making/approval from a manager as part of the process.

API Integration

Many organizations already have automation systems like RPA or IT Service Management tools such as ServiceNow. ServiceNow may be used to automate change request review and approval. Ultimately, that request may be delegated to an engineer to implement. PPA can automate that final link in the chain with a full audit trail maintained in the ServiceNow change request. These automated tasks can still request human review and approval if needed.

Scheduled

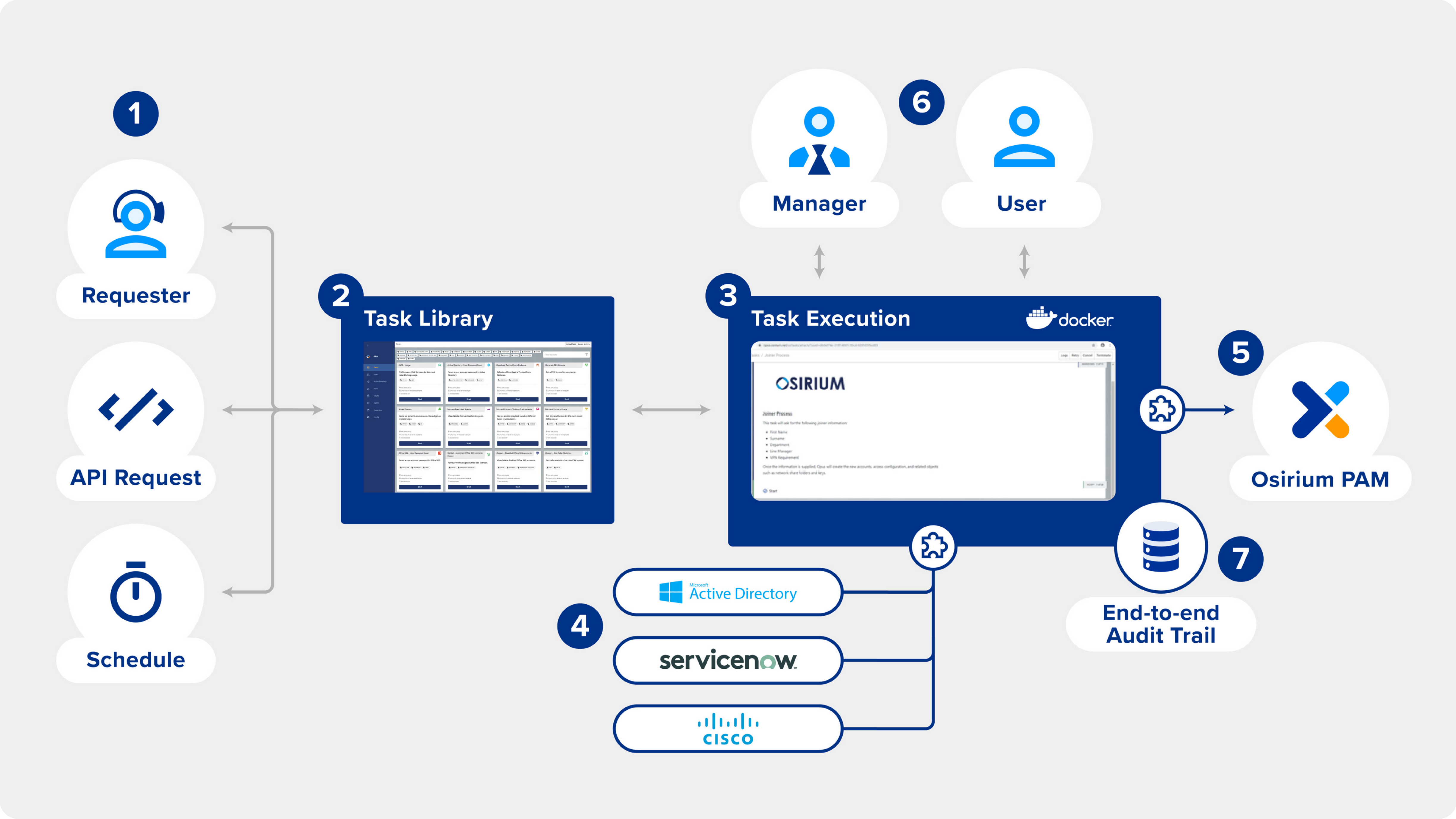
Many tasks need to be run on a frequent cycle. For example, checking on server health or running a backup. PPA can automate tasks to run on such a regular schedule. All credentials are always protected and status can be reported through email or messaging.

PPA Overview

A flexible framework for automation

Let’s look a typical flow of actions.

1. a Task is triggered by one of the available methods
2. from the Task Library PPA presents a pre-defined Tasks pecifying the exact process to be followed and preventing non-approved processes from beingattempted. Only tasks that have been approved for that user are shown.
3. the task is executed, integrating
4. with the relevant systems in the sequence required
5. behind the scenes, PPA retrieves account credentials from a secure vault such as Osirium PAM, HashiCorp or other vault. The credentials are always protected by PPA and never exposed to the user.
6. if required, in line with the defined process, managers and users approve workflows and make permitted choices
7. PPA maintains an end to end audit trail



Additional Resources

Summary

Once you start using PPA, you start to see opportunities to automate everywhere.

Old style automation with scripts or RPA were too expensive to build or too risky to contemplate using for tasks that were only run occasionally or needed privileged access to hardware and software.

If you've got an idea for automating a process in your business, get in touch and discuss the options.

Find out more at https://osirium.com/ppa-express

OSIRIUM **PPA**

Privileged Process Automation is available free for a single-user. It has the full functionality including access to the PPA Playbook and Plug-In repository and Task Builder to create new playbooks.

GET PPA FOR FREE

About Osirium
Cybersecurity and IT Operations Innovators

Who we are

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 cybersecurity and automation technology to create the world's first, built-for-purpose, privileged account management and process 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 needs.