



Connect

NoOps

How the Ansible Automation Platform underpins the shift to zero-touch, self-healing IT operations



Darren Jacques

Automation Sales Specialist (Enterprise Accounts) - UK&I
Red Hat



Chris Renwick

Senior Specialist Solution Architect (Ansible) - UK&I
Red Hat



We aim to answer three questions

?

What does
noOps mean?

?

Why does it
matter right
now?

?

How does
AAP gives us
a path to
noOps?



What is NoOps?

NoOps is an operating model where infrastructure, deployments, and incident response run with **no manual operator intervention** under **normal conditions**, automation handles provisioning, configuration, scaling, patching, and remediation end to end.

It isn't the absence of Ops, it's Ops encoded entirely as automated, auditable, self-executing workflows.



Manual Ops

Humans execute every change



DevOps

Humans + scripts, CI/CD



AIOps

Monitoring + insight, human decides



NoOps

Automation senses, decides, acts



The pressure on IT Ops has changed



10x

faster change velocity expected from
cloud-native, microservice delivery



1000s

of hosts, containers, and network devices
per operator – beyond human scale



24/7

compliance and security posture
required across hybrid and multi-cloud

Traditional Ops teams can't scale headcount fast enough to keep pace – the gap has to close with automation, not people.



The four pillars of a NoOps environment



Self-healing infrastructure

Systems detect drift or failure and automatically remediate without a ticket ever being opened.



Event-driven automation

Alerts, webhooks, and telemetry trigger automation directly – no human in the loop for known conditions.



Self-service enablement

Developers and teams request infrastructure and changes through governed, automated workflows.



Policy & compliance as code

Security baselines, patching, and audit controls are enforced continuously and automatically.



Meet the Ansible Automation Platform

A single, enterprise-grade foundation for building, running, and governing automation at scale.



Automation Controller

Central hub for scheduling, RBAC, and job execution at scale



Execution Environments

Consistent, containerized runtime for every automation job



Event-Driven Ansible

Listens for events and triggers automation with no human step



Private Automation Hub

Curated, versioned content collections and roles



Automation Mesh

Distributed, resilient execution across hybrid networks



Content Collections

Thousands of pre-built modules across the IT estate

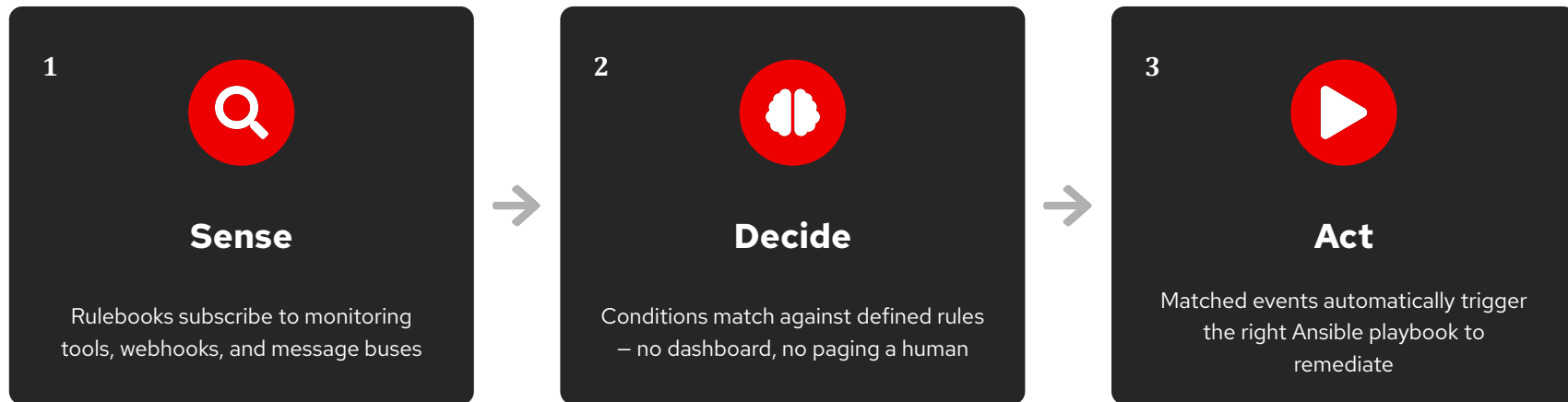


How AAP delivers on each NoOps pillar

NoOps Pillar	How Ansible Automation Platform Delivers It
✓ Self-healing infrastructure	Automation Controller schedules continuous, idempotent remediation playbooks
✓ Event-driven automation	Event-Driven Ansible consumes alerts/webhooks and fires rulebooks instantly
✓ Self-service enablement	Controller's job templates + RBAC expose safe, governed self-service actions
✓ Policy & compliance as code	Automation Hub content + Controller enforce versioned, auditable policy playbooks



Event-Driven Ansible removes the human bottleneck



Mean-time-to-remediate drops from hours to seconds for known failure patterns.



Business impact of a NoOps model

Faster MTTR

reduction in mean-time-to-remediate
for known incident patterns

3-5x

more infrastructure managed per
operator without added headcount

100%

of changes captured in a consistent,
auditable automation trail



Teams shift from firefighting to building – freeing engineers for higher-value platform work rather than repetitive manual tasks.



Done right automation delivers real impact

When companies make automation mission-critical, they win



MAPFRE

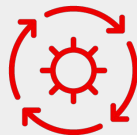
 **55%**

Reduction in lead times

 **85 %**

Reduction in error rates

100,000 events
auto-healed per month



Fortune 50 FSI customer

 **Desjardins**

 **90%**

Improvement in
server patching time



2000

Work days per year
saved by IT team

DAI-ICHI LIFE

Gân bó dài lâu.

 **80%**

Reduction in system
monitoring time

 **80 %**

Reduction application
coding errors



Your path to NoOps

01

Consolidate playbooks and roles
into Automation Hub content
collections

→02

Run all automation through
Automation Controller with RBAC
and audit trails

→03

Layer in Event-Driven Ansible to
react to alerts without manual
triage

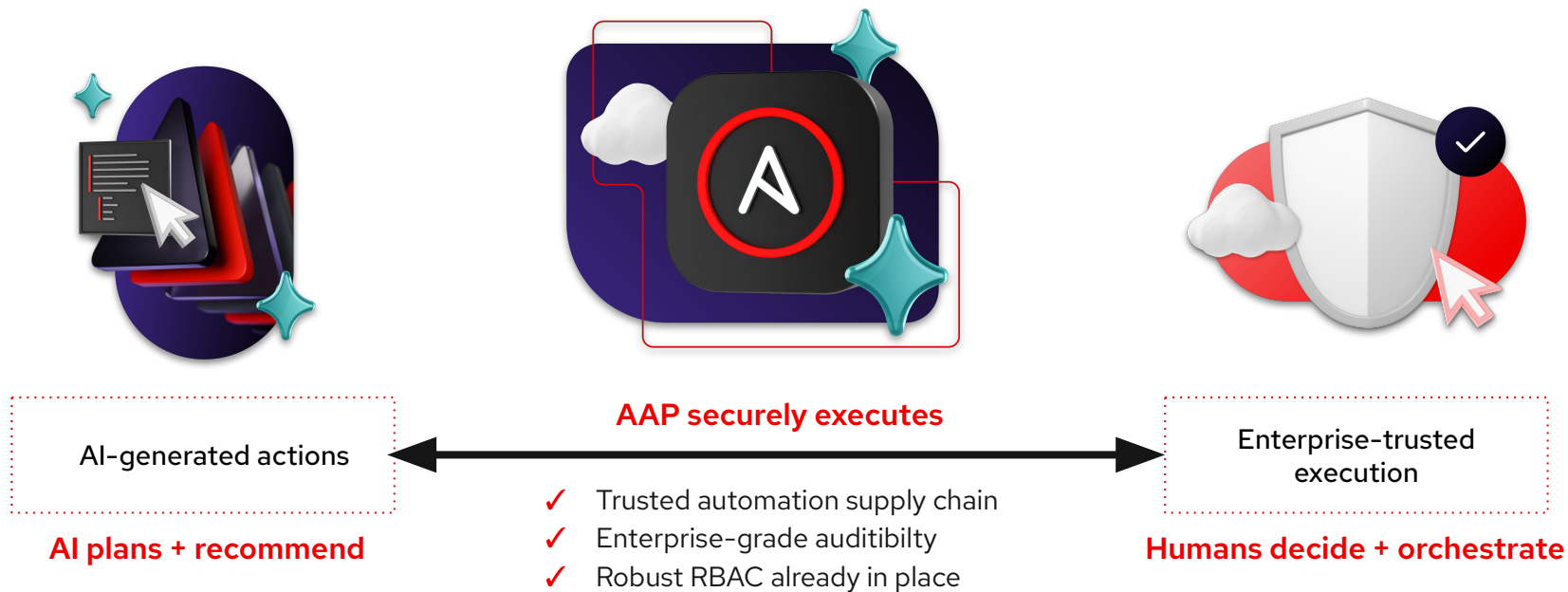
→04

Open governed job templates to
developers and adjacent teams

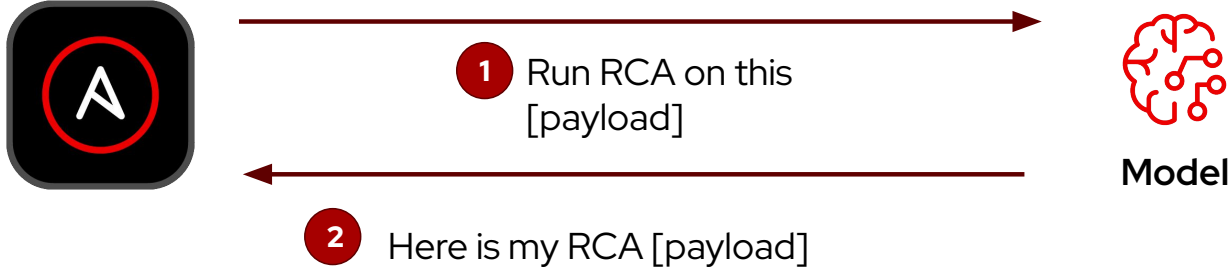
NoOps isn't a product you buy — it's an outcome Ansible Automation Platform makes achievable.



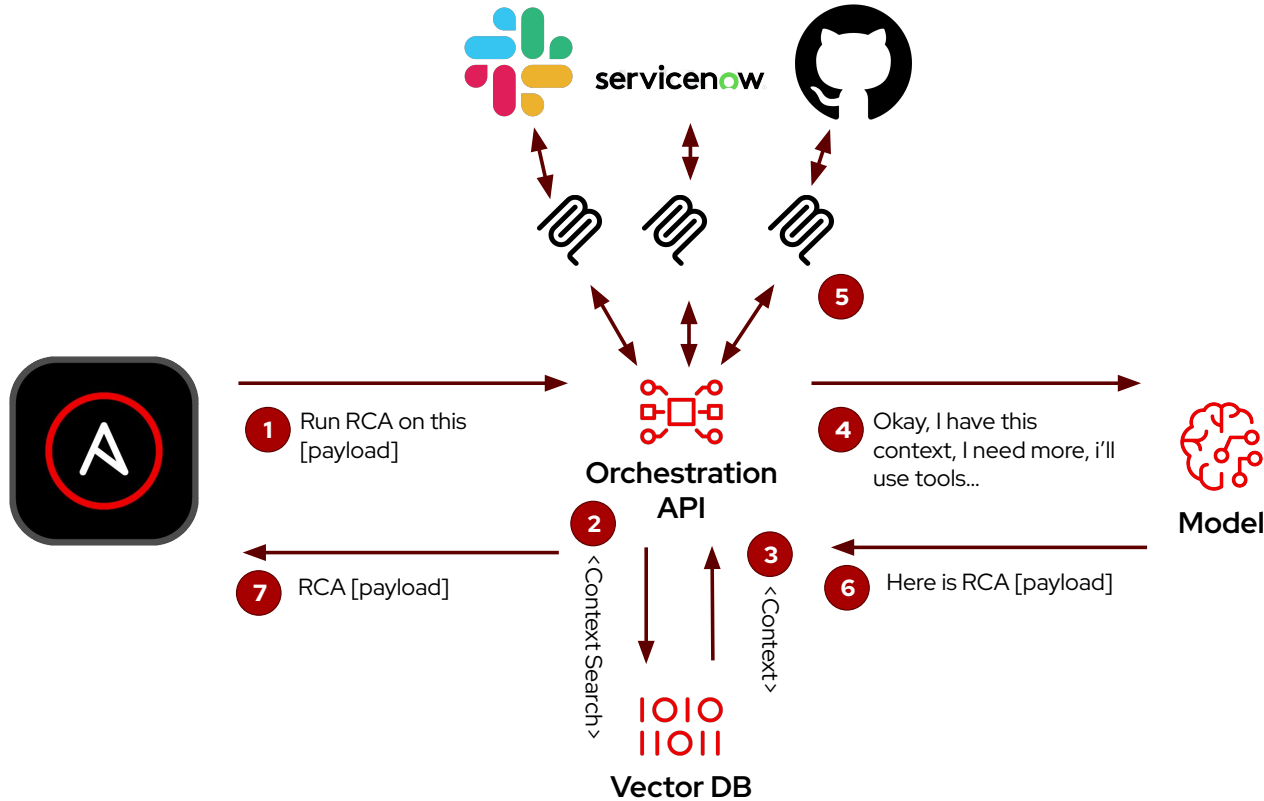
Automation as the foundation for AI in ITOps



Direct LLM communication was the start of AIOps



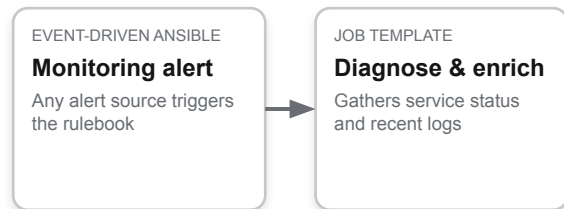
What if you wanted a smarter solution?



We call this agentic AIOps

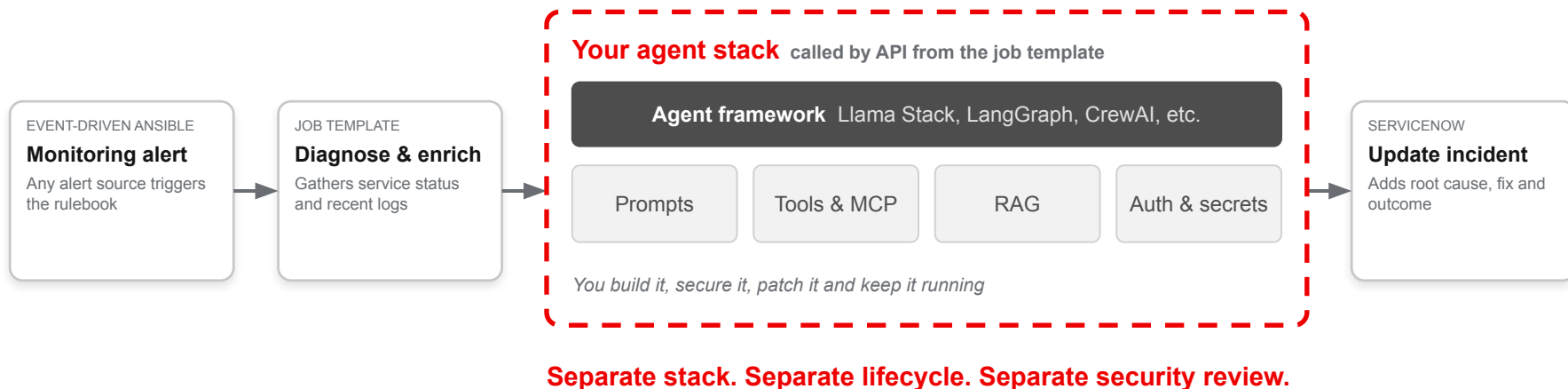
Your easy route into agentic AIOps

Before: AAP calls out to an agent you build and run yourself



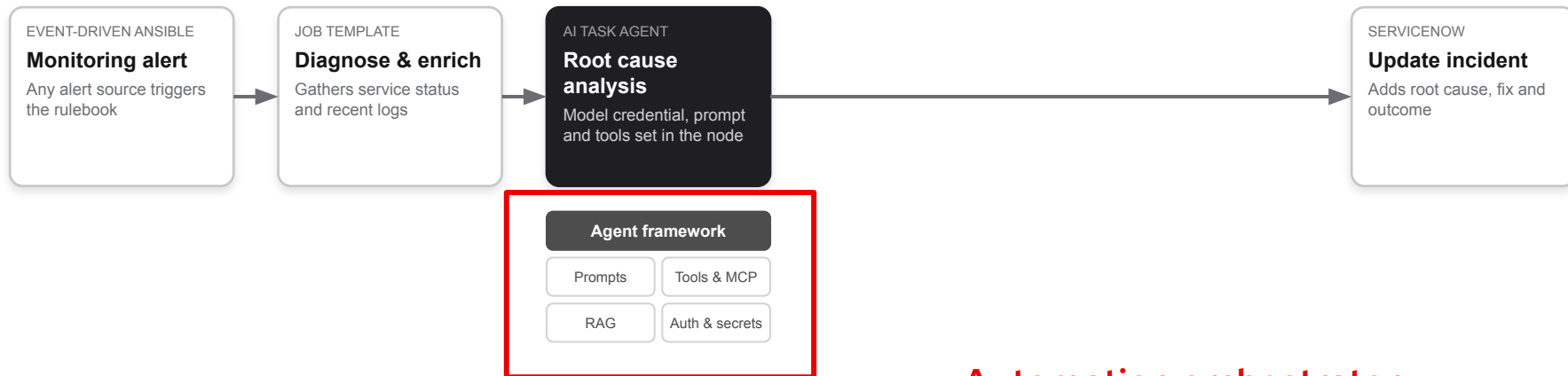
Your easy route into agentic AIOps

Before: AAP calls out to an agent you build and run yourself

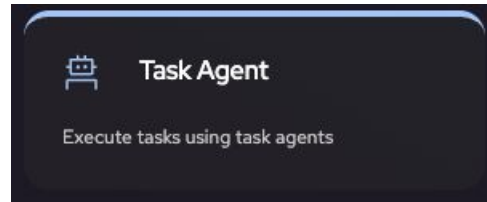


Your easy route into agentic AIOps

Now: the agent is just another step in your AAP workflow



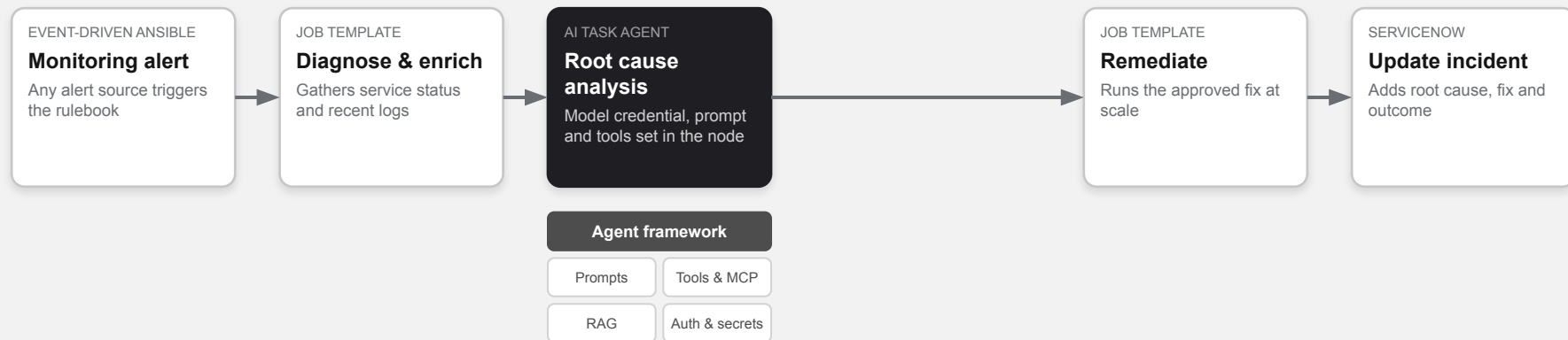
Automation orchestrator



Your easy route into agentic AIOps

Now: the agent is just another step in your AAP workflow

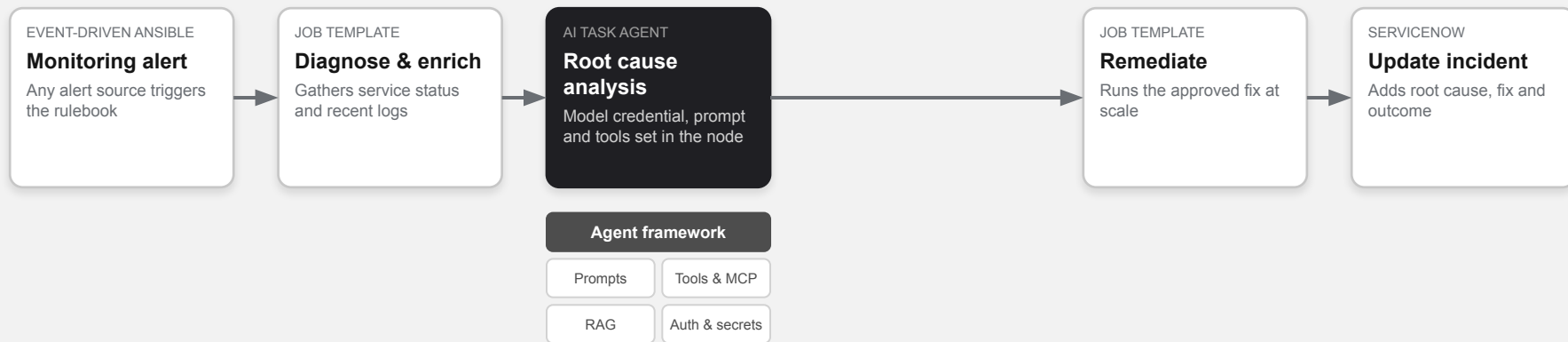
Automation Orchestrator workflow



Your easy route into agentic AIOps

Now: the agent is just another step in your AAP workflow

Automation Orchestrator workflow



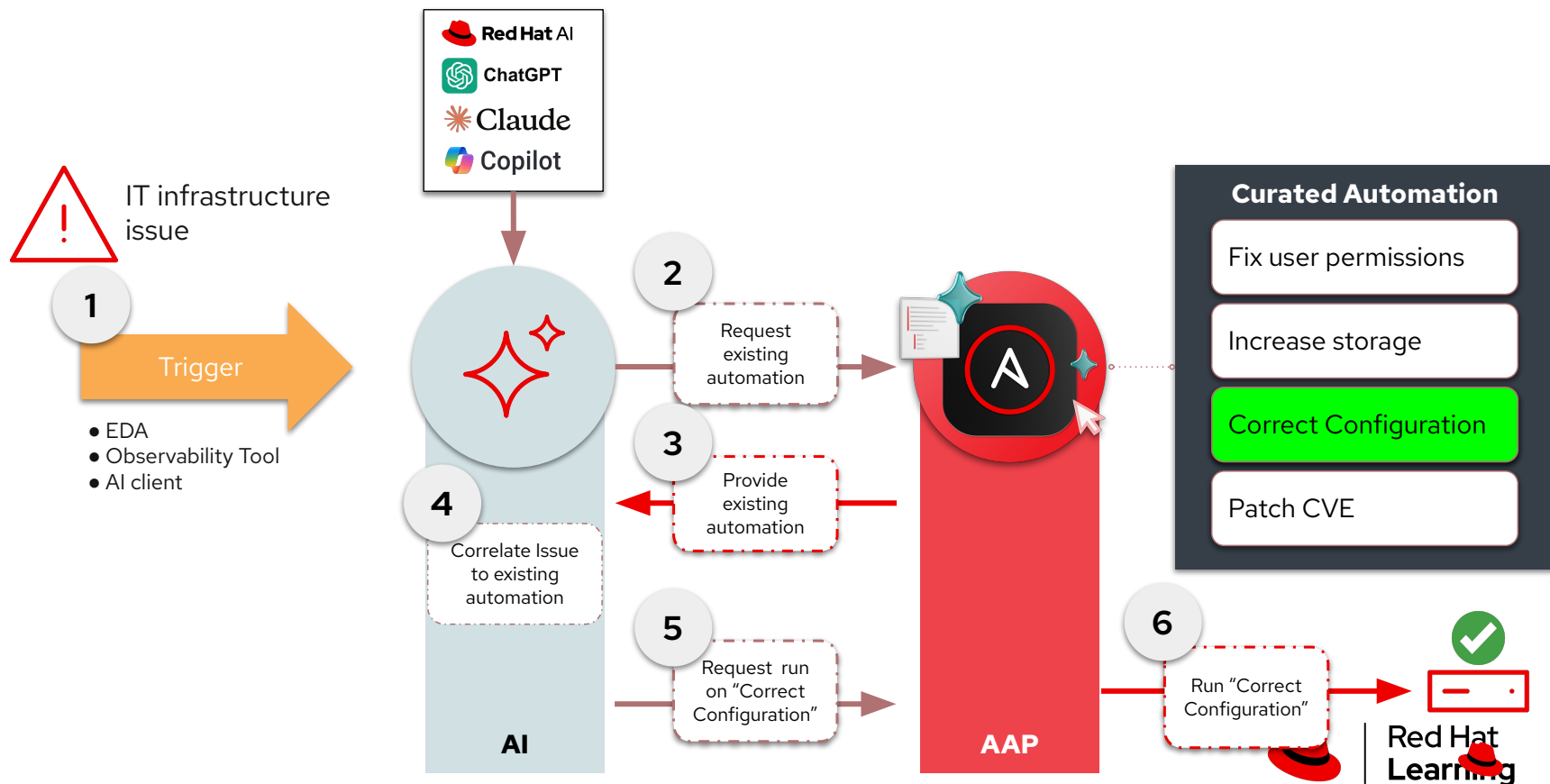
Agents and playbooks on one canvas

Humans approve before anything changes

No separate agent platform to host

Same outcome, none of the plumbing

Curated automation remediation



Live Presentation

Live NoOps Demo

Watch Ansible Automation Platform automatically detect, analyze, and remediate a simulated service outage in real time—completely hands-free.

● READY TO RUN

ansible-rulebook --verbose

```
[ansible] Listening for Prometheus alert...  
[event] Alert received: web_service_5xx_error  
[rulebook] Condition matched: response_code ==  
503  
[action] Triggering service_remediation.yml  
[playbook] Task: Gather system diagnostics [OK]  
[playbook] Task: Restart web application service  
[OK]  
[success] Verification health check passed!  
[status] Service recovered in 42 seconds.
```



Reference architecture

Monitoring

ITSM

Cloud APIs

Network



Event-Driven Ansible – rulebooks match conditions and dispatch jobs



Automation Controller – RBAC, scheduling, job templates, audit trail

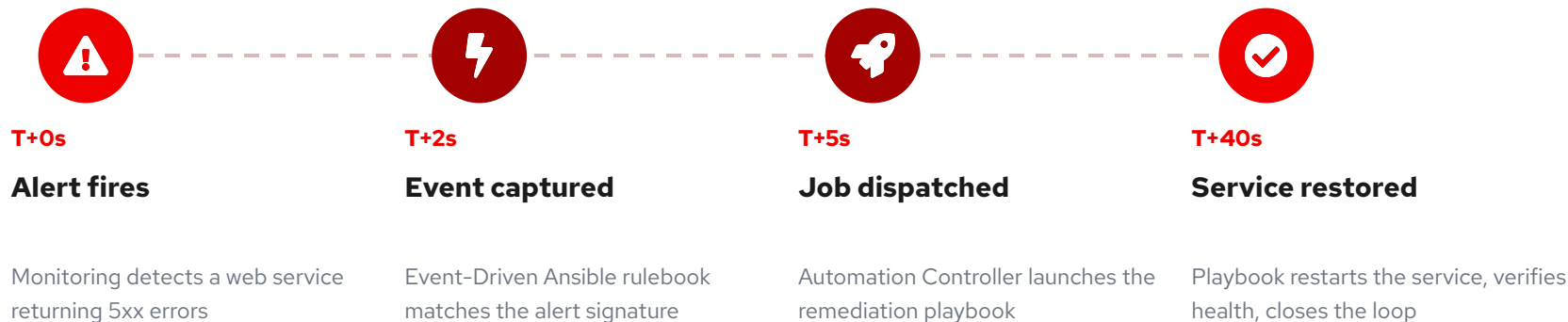
Automation Mesh (distributed execution)

Execution Environments (containerized runtime)

Target infrastructure – cloud, on-prem, network, security, edge



Use case: automatic remediation of a failed service



No ticket. No page. No human touch. Under 60 seconds, fully audited.





Connect

Thank you



[linkedin.com/company/red-hat](https://www.linkedin.com/company/red-hat)



[facebook.com/redhatinc](https://www.facebook.com/redhatinc)



[youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)



x.com/RedHat

