

CISCO Live !

Ansible Meets AI:

Driving Automation Operations Through Natural Language

Sean Cavanaugh

Senior Principal Technical Marketing

Red Hat Ansible

@IPvSean



Agenda

- The Operational Problem
- What MCP Actually Is
- Where AAP Fits
- Demo Architecture / Flow
- Why This Matters Operationally
- Real Use Cases



The Operational Problem

Modern operations teams already have:

- Automation & Management platforms
- Monitoring and telemetry
- Large amounts of operational data

But interacting with these systems requires:

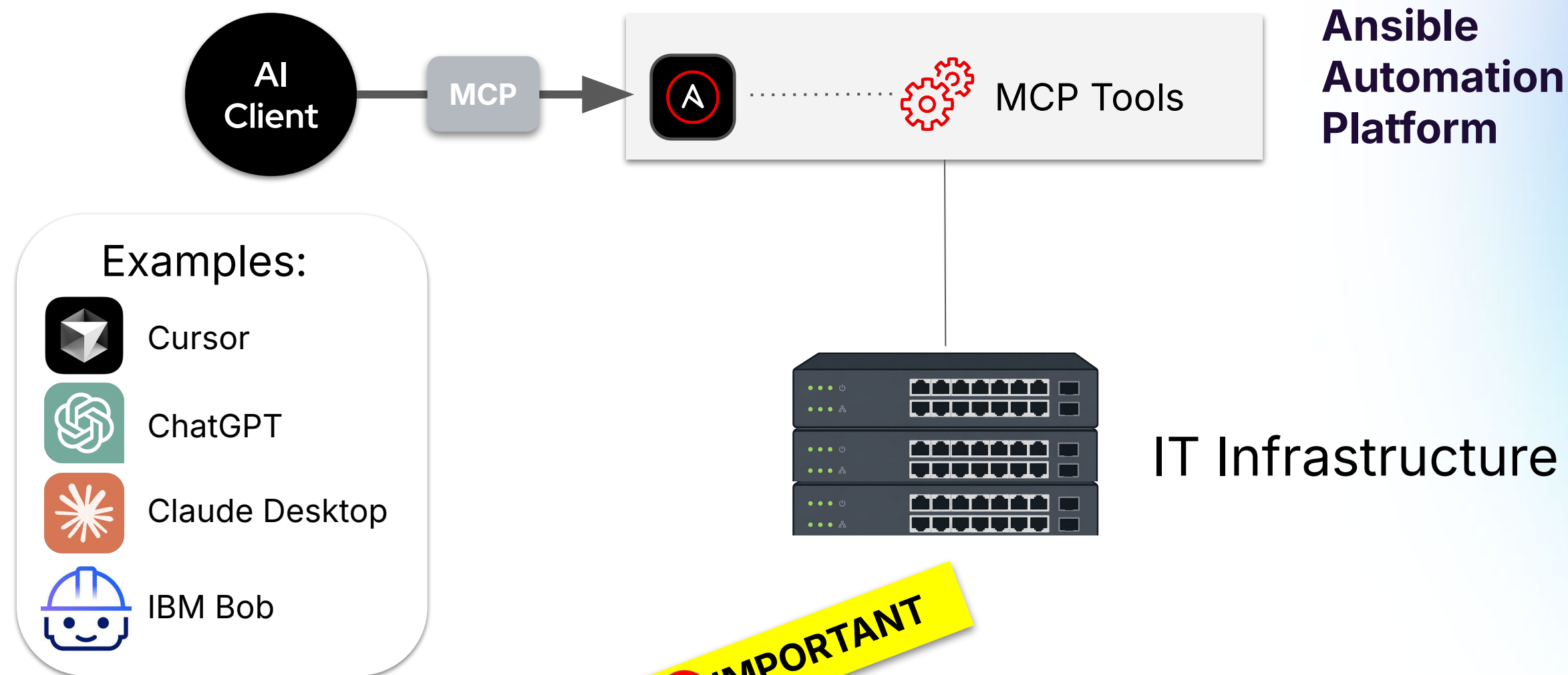
- Complex interfaces
- Specialized expertise
- Context switching between tools

What if engineers could interact with automation systems using intent instead of interfaces?



What MCP Actually Is

MCP: Model Context Protocol- standardized way for AI systems to securely interact with external tools and platforms



i IMPORTANT

The AI is not replacing the automation platform.
AAP remains the execution and governance layer.

Where Ansible Fits

Human interface

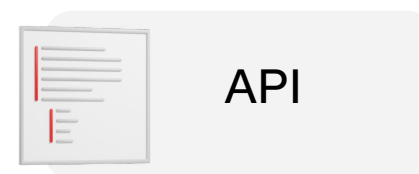
The WebUI enables operators to configure, launch, and monitor automation through a role-based interface.



Web UI

Application interface

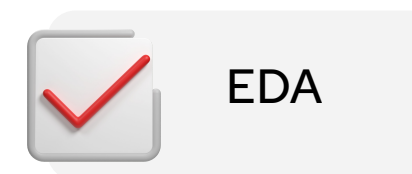
Token-based authentication enables third-party tools and services to securely integrate with the platform using OAuth 2.



API

Event interface

An EDA plugin connects Ansible to external event sources and triggers automation when defined conditions are met.



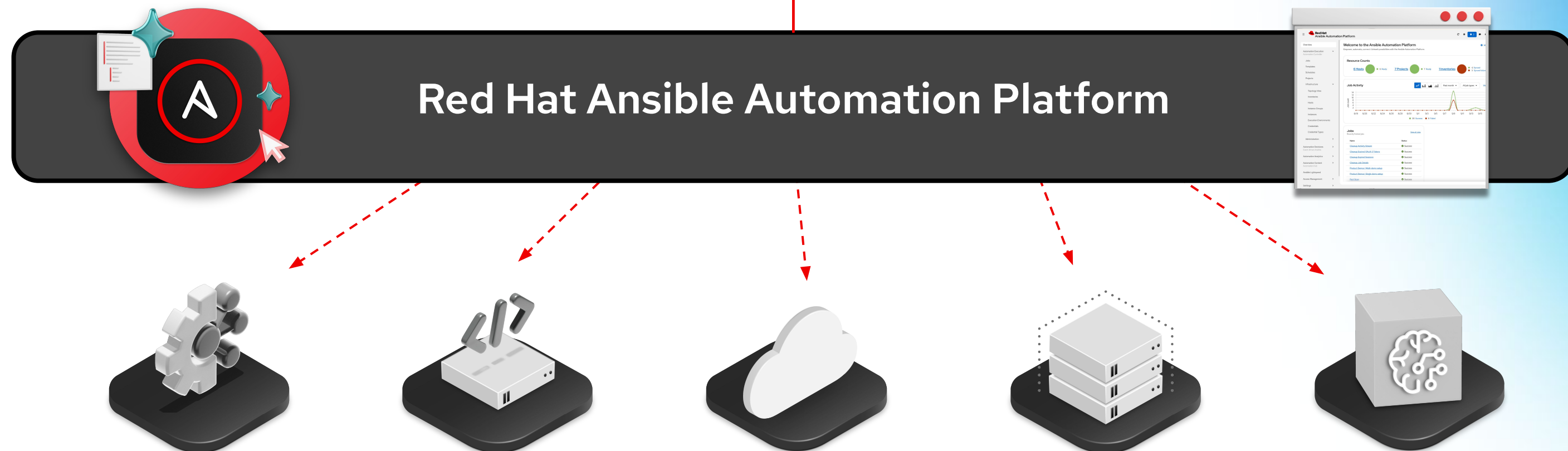
EDA

AI interface

An MCP server enables AI models to query Ansible Automation Platform and launch automation within defined boundaries.



MCP



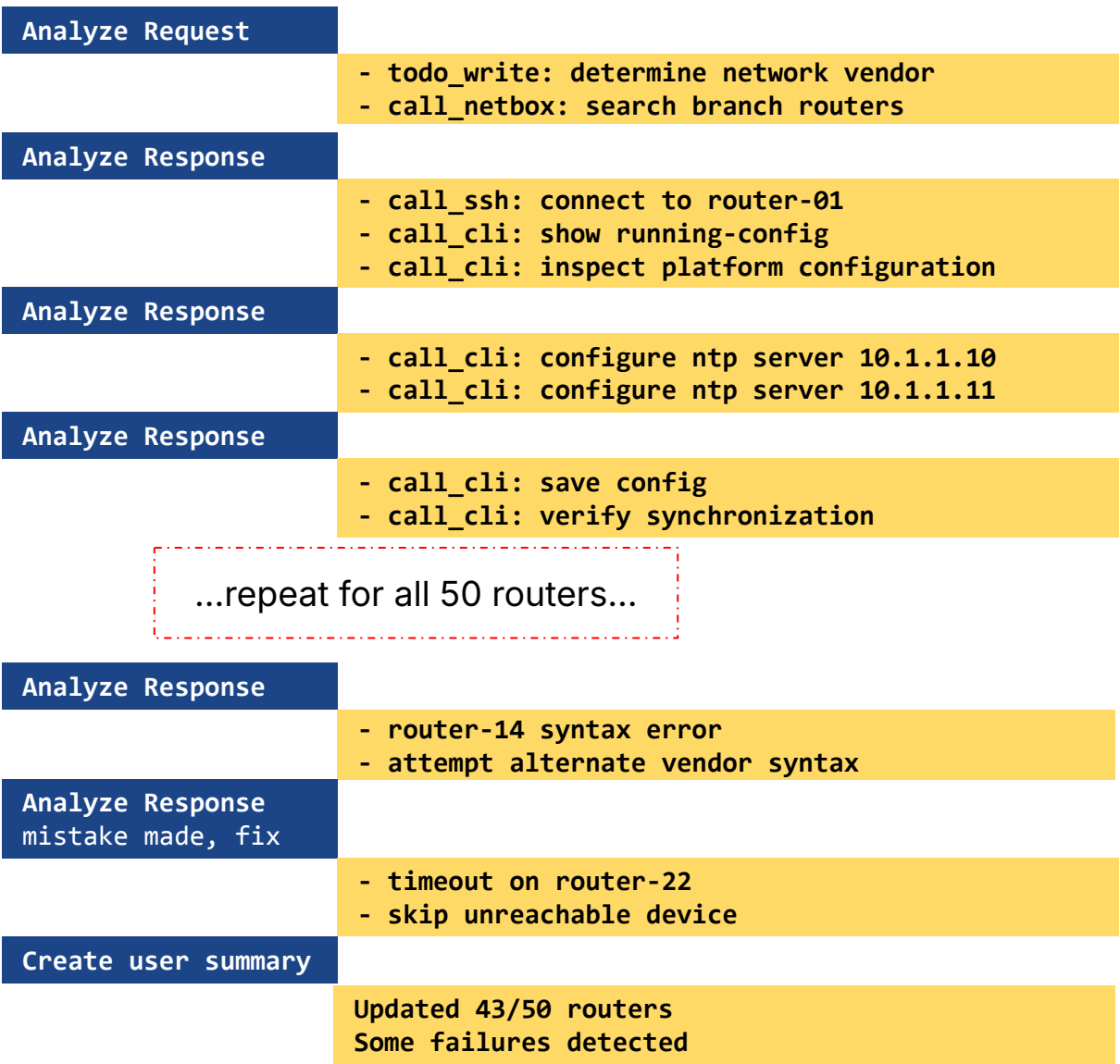
Where Ansible Fits

Prompt:

“Update all branch edge routers to use the new NTP servers and verify compliance”

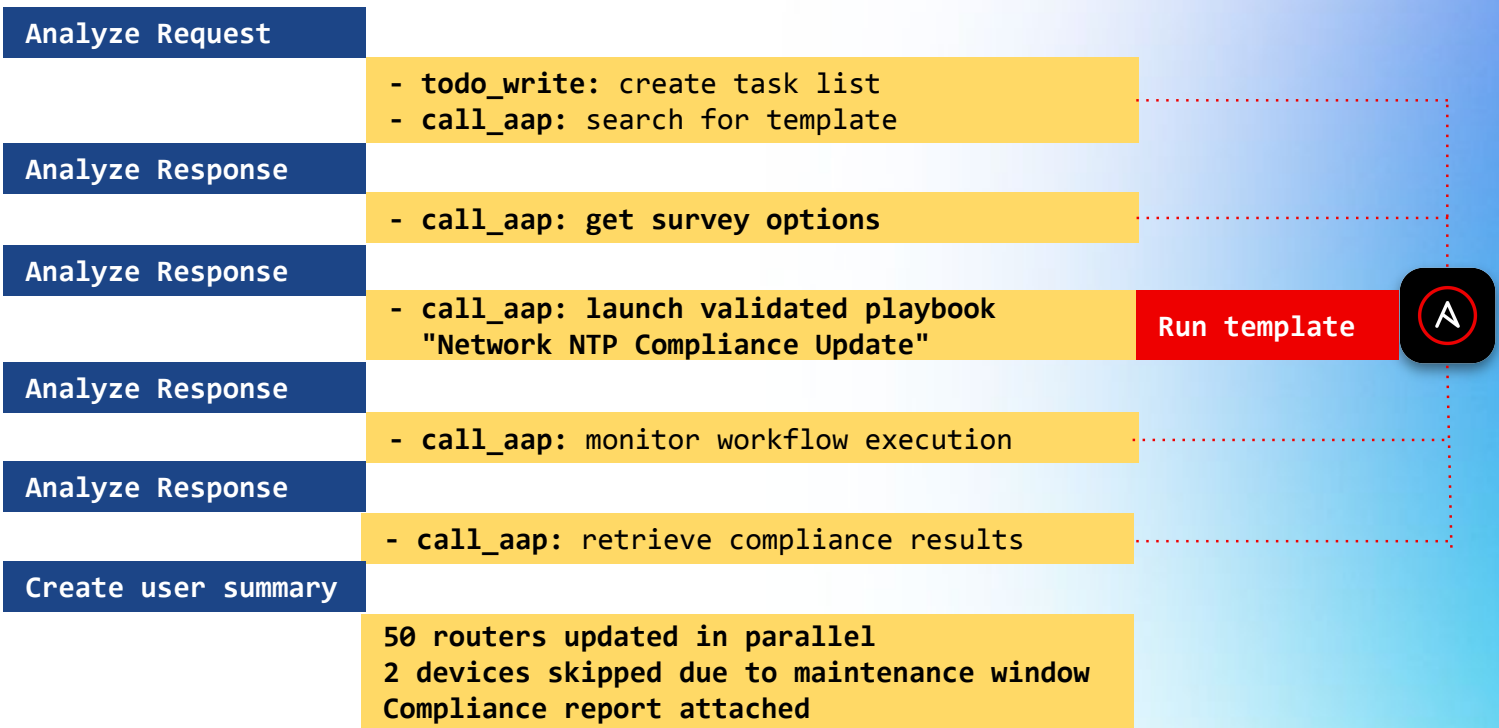
Direct agentic execution

Agentic example: Cursor with Claude 4.5 Sonnet



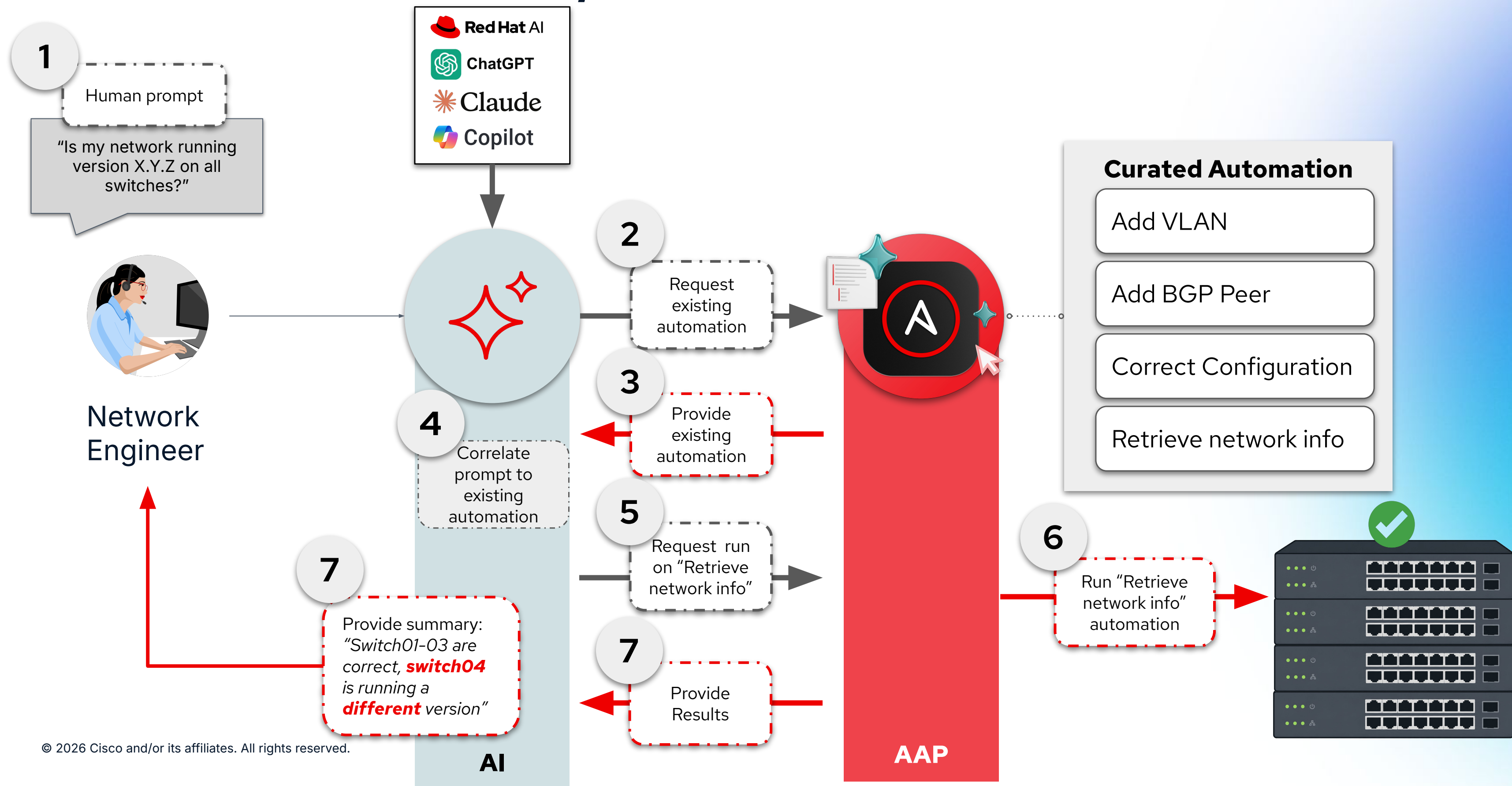
Deterministic execution

Using the AAP MCP Server

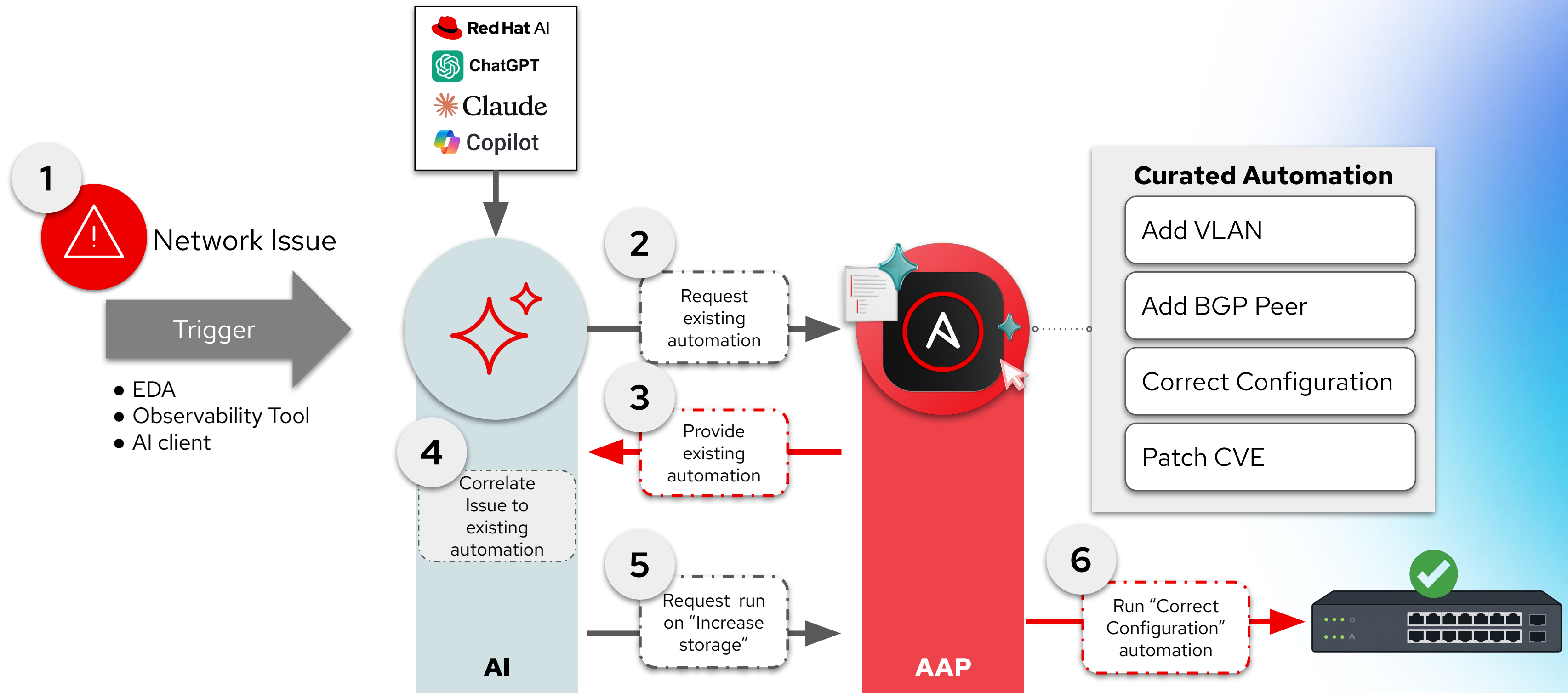


- ✓ Audit trails and compliance
- ✓ Standardized, repeatable workflows
- ✓ RBAC policies and approval workflows

Demo Architecture / Flow



Demo Architecture / Flow



Why This Matters Operationally

Benefits:

- Lower operational friction
- Faster access to automation
- Reduced knowledge silos



This is **NOT**:

- fully autonomous infrastructure
- unsupervised AI making production changes

This **IS**:

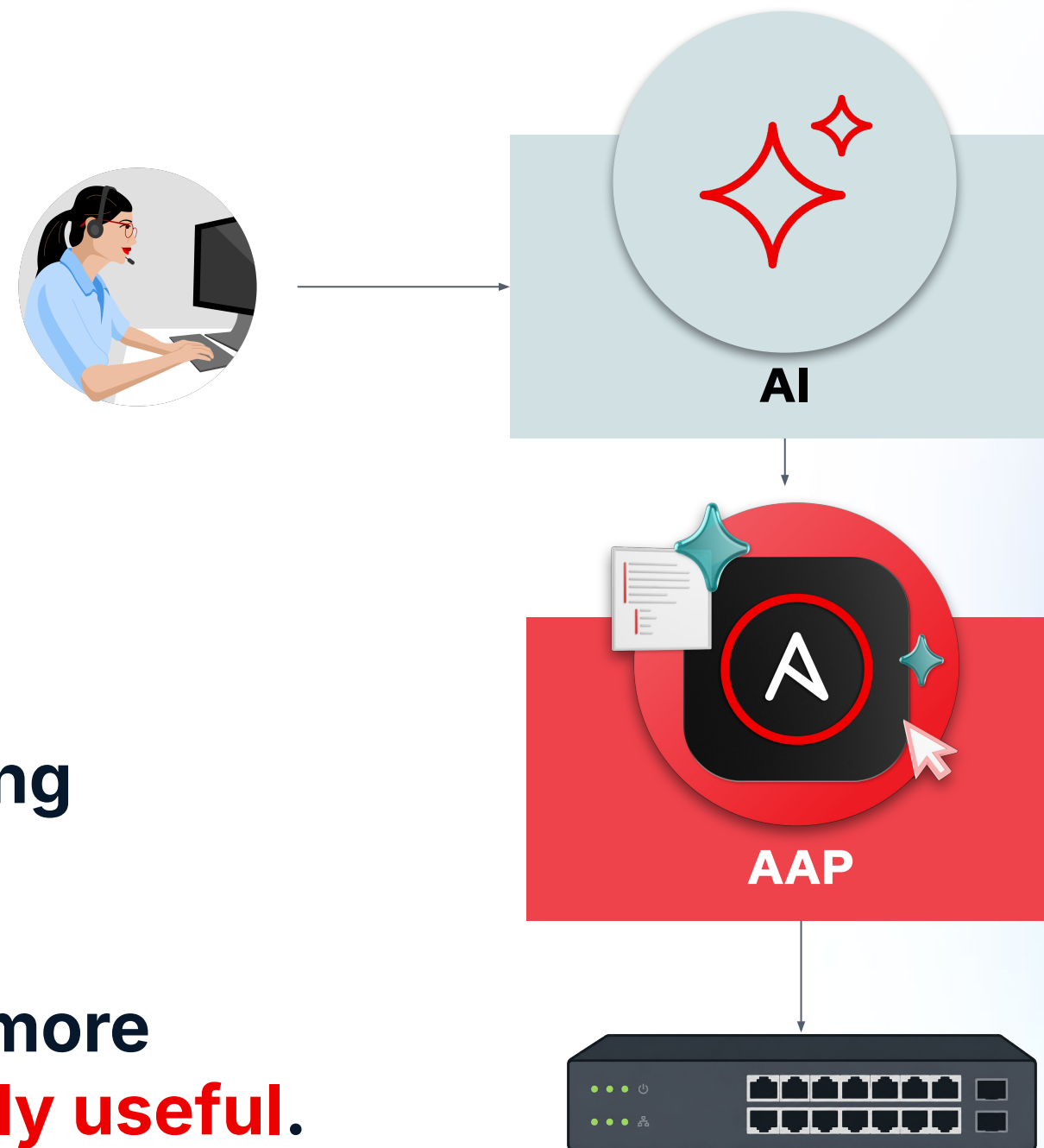
- guided operations
- human-approved workflows
- conversational interfaces to existing automation

Real Use Cases

- Launch compliance checks
- Gather switch facts
- Troubleshoot failed jobs
- Patch systems
- Query inventory state
- Trigger remediation from incidents

The future of operations isn't AI replacing automation.

It's AI making automation dramatically more **accessible, contextual, and operationally useful.**



AAP becomes the trusted execution layer underneath intelligent interfaces.



Q & A



Thank you!

- Solution guides: red.ht/aiops-solution-guides



- Interactive demos: [Ansible Automation Platform + AI](#)



Thank you!



linkedin.com/company/red-hat



youtube.com/AnsibleAutomation



facebook.com/redhatinc



x.com/Ansible