

The AAP roadmap

Massimo Ferrari

Senior Manager, Product Management

Red Hat Ansible Business Unit



The principles of IT automation remain the same. But the stakes have changed.

Agents and AI-driven workflows are fundamentally altering the ITOps landscape



The threat environment is more challenging than it has ever been, and AI tools in the wrong hands are a big reason why.

Security



Pressure is on to unlock value from AI + AIOps investments - and close the insight to action gap

AIOps



Global compliance regulations continue to tighten at the same time AI adoption is expanding, requiring more oversight and auditability.

Regulatory



Automation is key to staying ahead in a post-Mythos threat environment

45%

of vulnerabilities remain
unpatched after 12 months

Source: CETAS / Alan
Turing Institute, 2025

Frontier AI models can now find and exploit vulnerabilities in **hours, not weeks**. The bottleneck isn't finding the exposure anymore – it's **controlling it before a fix exists**.

How IT automation can help teams respond, from discovery to remediation

1

MITIGATE

Isolate & contain
affected systems before
a patch exists

2

PATCH

Orchestrated, validated
patching across hybrid
infrastructure

3

VALIDATE

Confirm the fix works,
with automated rollback
if it doesn't

4

VERIFY

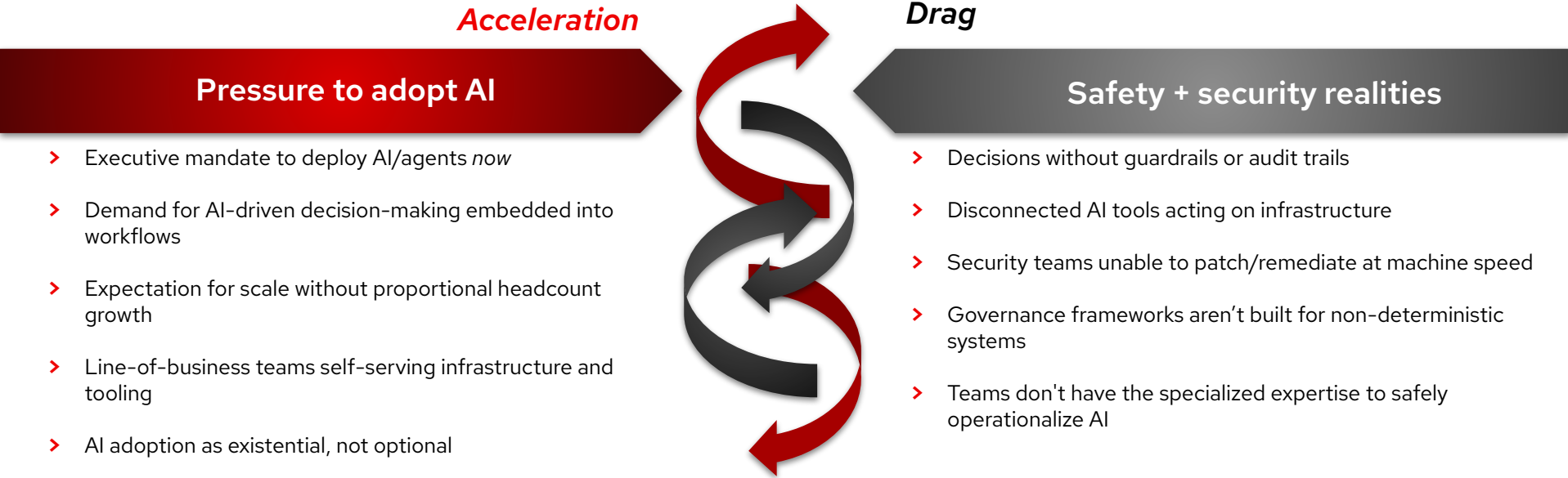
Continuous compliance,
drift detection, full
audit trail

When a vulnerability drops, the window between discovery and remediation is where the risk lives.

Ansible Automation Platform closes that gap.



Two competing forces are at the root of AI disruption



Automation can help bridge the AI governance gap

Pressure to adopt AI

29%

Shadow AI Epidemic

29% of employees use unsanctioned AI agents outside IT visibility.

1.5 million corporate agents are currently unmonitored.

– Microsoft Cyber Pulse, 2026

Governance gap

The most effective way to close this gap is with a unified governance model.

Operational boundaries defined by automation playbook libraries.

Oversight managed through strict division of labor. AI proposes, but automation is the execution layer.

Full audit trail of all execution that captures AI reasoning, human approvals, and specific steps taken.

Safety + security realities

21%

Governance Immaturity

Only 21% have mature agent governance models.

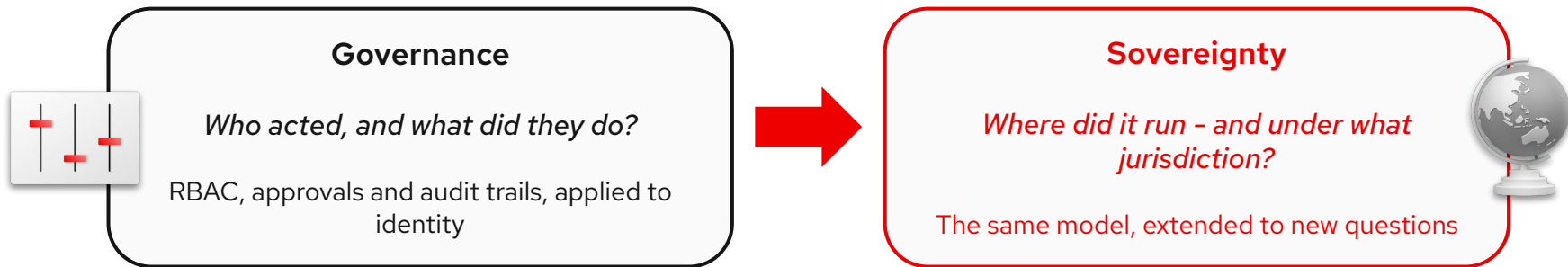
Only 14.4% have full security approval for agent fleets.

– Deloitte & Gravitee, 2026



You will need a governance infrastructure that is built to adapt

Organizations can easily extend their existing governance model to meet new demands



With Red Hat Ansible, “we have oversight” isn’t just an assertion. It’s immediately provable.

Region-pinned execution | Actions only run within approved geographic boundaries

Jurisdiction-aware logging | Audit trails record where a workflow ran, and under which jurisdiction

Enforced regardless of source | A person, a script, or an AI agent all pass through the same boundary



Technology teams don't need binary choices. They need options.

Deterministic automation has limits...but so does AI.



Deterministic automation

Task-driven, event-driven

Proven, consistent, reliable,
cost-effective, and easily governable at scale

It can only do what it was told to.
It can't adapt, reason on the fly, or handle issues that
weren't anticipated.

Orchestration gap
*Automation works well, but still requires a high degree of
manual coordination*

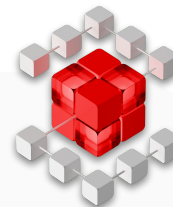
Modes

Strengths

Limitations

Implications

AI



AI-driven, agentic

Adaptable, intelligent, proactive, and can quickly solve
for new problems no playbook could predict

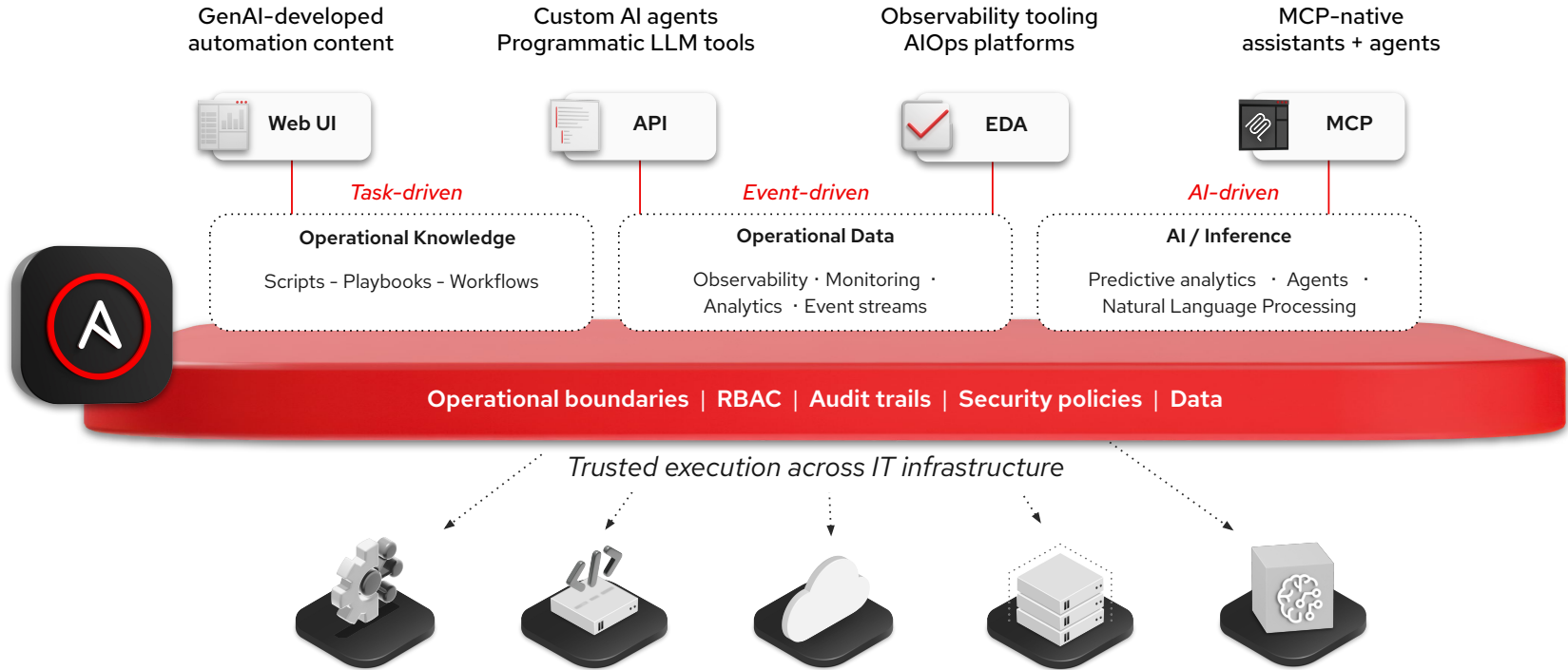
It's expensive, probabilistic, and can't be trusted to
execute against production infrastructure without
strong guardrails in place.

Trust gap
*The reasoning is powerful. Knowing what it will actually
do next time is a wild card.*



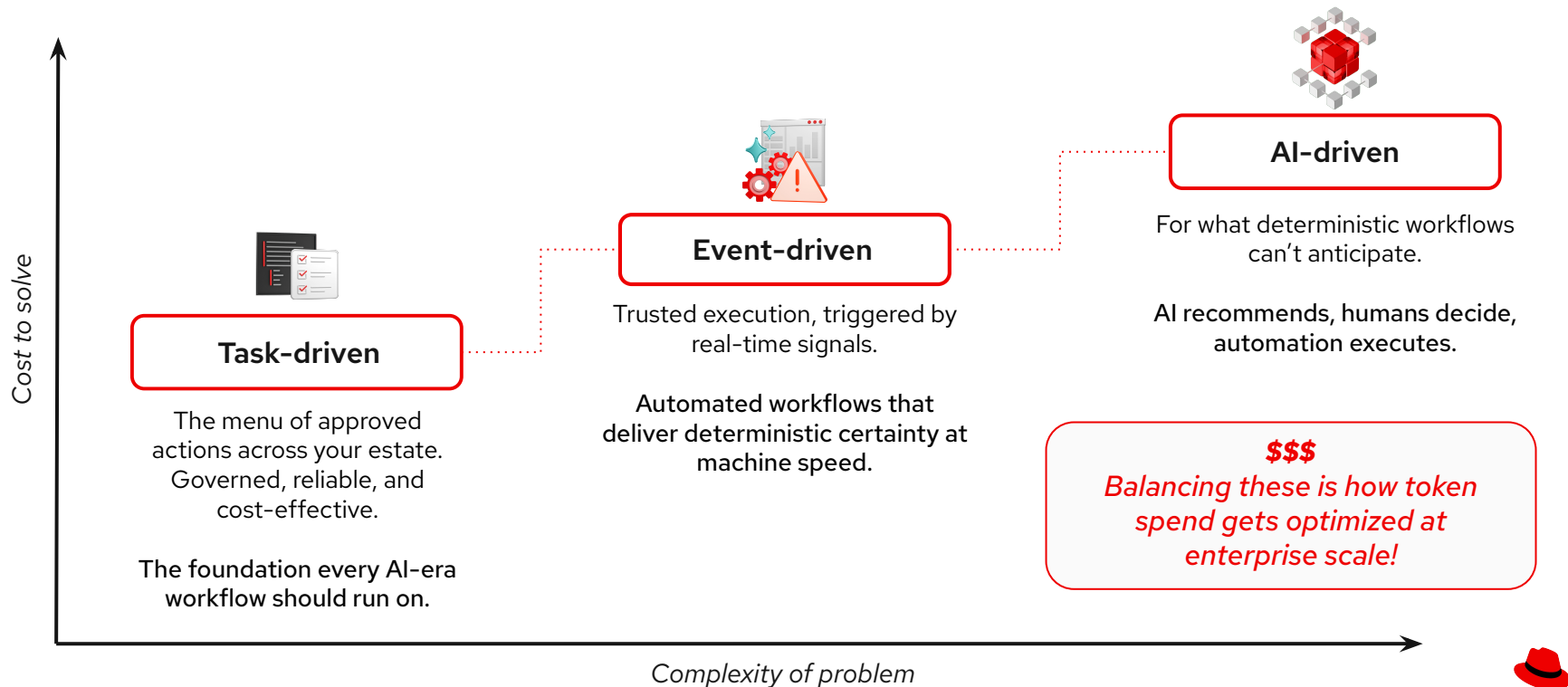
The ITOps landscape is growingly increasingly complex

AI + agents are changing the way ITOps teams interact with infrastructure. Automation must evolve too.



The future of IT automation is multimode

Effective orchestration across modes is the key to good governance and cost optimization



And governance isn't an afterthought. It's the glue for IT operations.

The nature of enterprise workflows is evolving, but core governance principles don't change



Task-driven automation



Event-Driven automation



AI-driven automation

Operational boundaries

Playbook-defined. Explicit scope.
No deviation.

Rulebook-defined.
Set in advance. Auto-enforced.

Certified playbook library.
AI operates within approved actions only.

Oversight

Human initiates.
Human owns the outcome

Human authors the rulebook.
Platform enforces it.

AI proposes.
Human approves at explicit decision gate

Audit trail

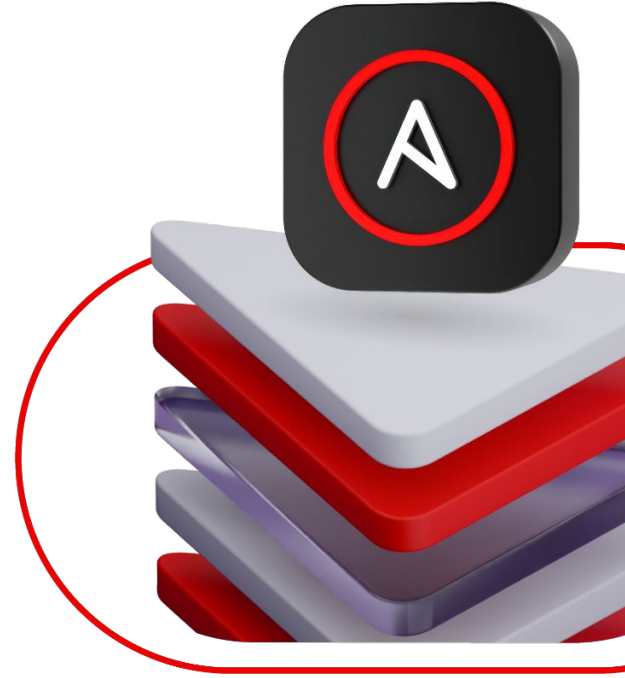
What ran, in what order, against which systems.

What triggered it, which rule matched, what executed.

AI reasoning, human approval, trusted platform execution – full chain.



Red Hat Ansible Automation Platform



Red Hat Ansible Automation Platform 2.7

Join our Red Hat® Ansible® Automation Platform product managers for in-depth overviews of product releases.

What's new in Red Hat Ansible Automation Platform

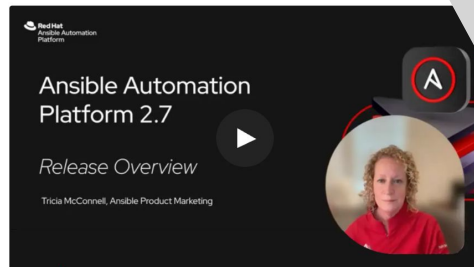


Introducing Red Hat Ansible Automation Platform 2.7

The latest updates to Ansible Automation Platform build upon previous releases to help you adopt enterprise-wide automation—with the governance needed to ensure resilient IT operations in an AI-centric world.

With Ansible Automation Platform 2.7, IT teams can:

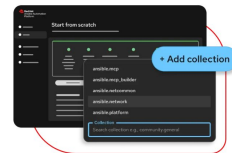
- **Empower platform engineering** and boost developer productivity
- **Drive automation adoption at scale** and eliminate friction
- **Unlock AI-driven automation**, turning intelligence into trusted action



Empower platform engineering

The [self-service automation portal](#)—now available for deployments of Red Hat Enterprise Linux 9 and 10—introduces a visual **execution environment builder** that eliminates manual configuration and enforces consistency. A new centralized content catalog now enables administrators to aggregate trusted content, so developers can quickly find what they need.

[Learn more](#) →



Drive automation adoption at scale

Ansible Automation Platform is now an **OIDC provider for HashiCorp Vault** (Technology Preview), offering modernized identity management to support automation in zero trust environments. Automation jobs authenticate with short-lived, job-specific tokens instead of static service accounts, eliminating credential sprawl and minimizing attack surfaces.

[Learn more](#) →



Unlock AI-driven automation

MCP server for Ansible Automation Platform (now in Technology Preview), helps you bring an agentic, AI-driven approach to your operations. You can manage jobs, troubleshoot issues, and even launch workflows using natural language prompts. It's a faster, more intuitive way to automate at scale.

[Learn more](#) →

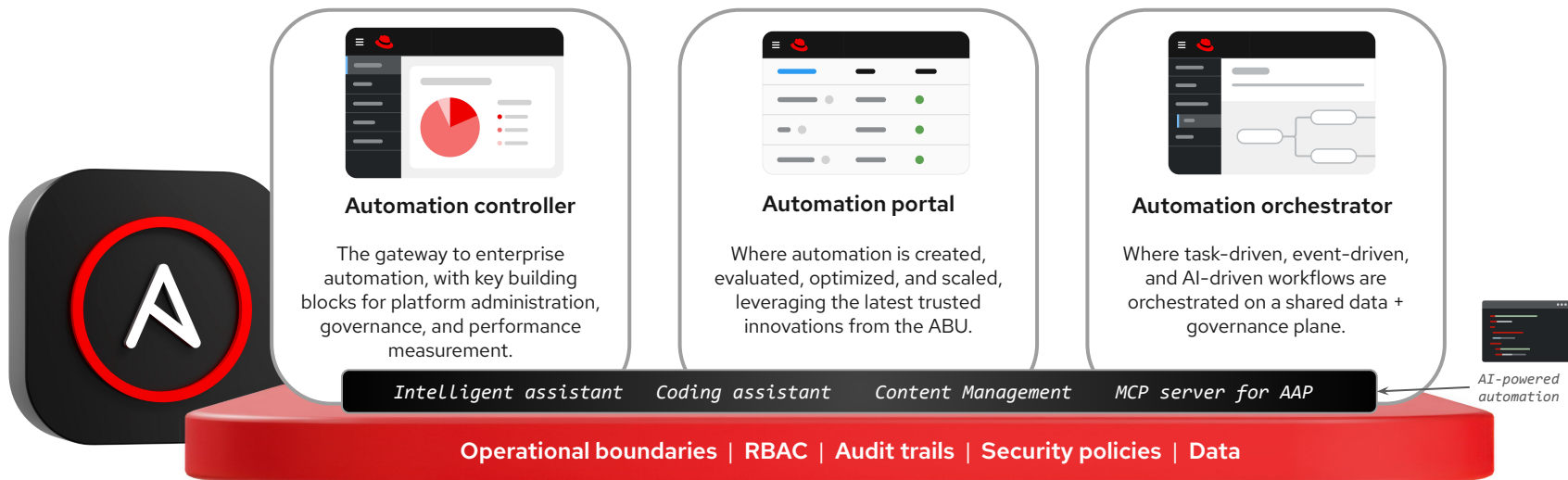


<https://www.redhat.com/en/technologies/management/ansible/whats-new>



Red Hat Ansible Automation Platform

The trusted orchestration and execution layer for IT ops in the agentic era

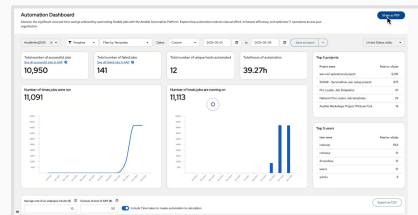




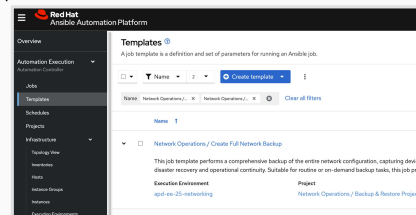
Ansible Automation Platform 2.7

- ✓ Efficiency
- ✓ Resilience
- ✓ Governance
- ✓ Scale

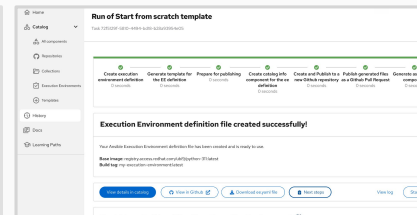
Adoption acceleration



Automation dashboard

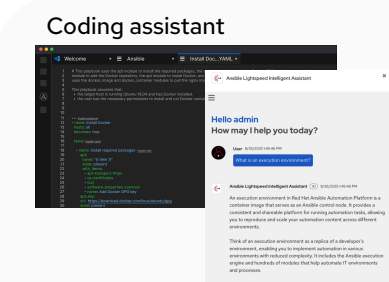


Self-service automation

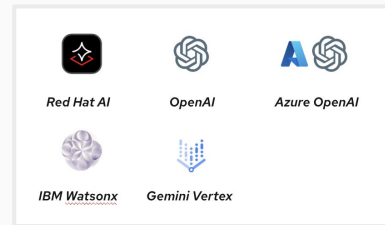


Execution environment builder

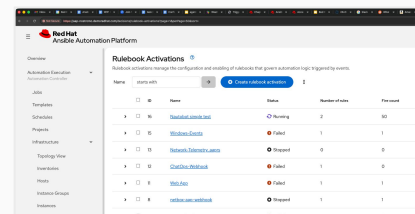
AI-driven automation



Intelligent assistant

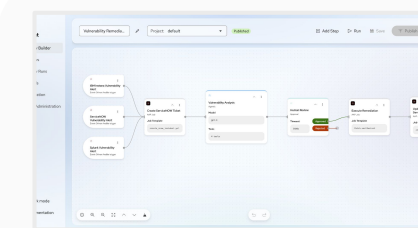


BYOM (Bring your own model)

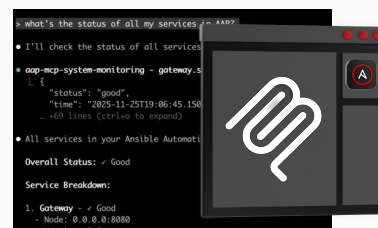


Automated, event-driven AIOps

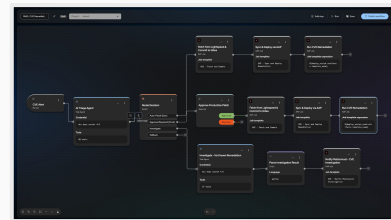
Workflow evolution



Reimagined workflow experience



Ansible MCP servers + plug-in framework



Multimode orchestration

Automation portal



The Ansible Automation Platform Roadmap for 2027 + beyond

Our goal: Continue to **lead enterprise automation today**, while **supporting the future of agentic ITOps**

Resilient, trusted platform foundation

Cement AAP as the trusted operational foundation for multi-cloud, sovereign, and AI-driven enterprise automation, through:

- ✓ Simplified deployment topologies
- ✓ Supported HA/DR architectures
- > Streamlined upgrades across future platform releases
- > Database neutrality
- > Sovereign deployment models for regulated environments

AI-powered automation acceleration

Multimode automation + orchestration



Roadmap: Resilient, trusted platform foundation

Migration + configuration as code

Supported migration tooling that automates the path from RPM-based AAP to containerized and operator-managed deployments (2.4→2.7+), paired with a declarative *Configuration-as-Code* model so platform configuration is version-controlled, reproducible, and promotable across lifecycle stages.

Platform resilience + HA / DR

Customers no longer need to design and maintain their own HA/DR configurations.

Red Hat delivers a prescriptive, fully supported reference architecture covering OpenShift deployment, storage, networking, and infrastructure, with EDB and similar DB vendors providing the redundant database layer.

Red Hat also provides the tooling to manage failover processes, so customers get production-grade resilience without custom engineering.

Platform modernization

Make AAP easier to operate and adopt at scale, with database neutrality (MS SQL Server) so customers aren't locked to a single Postgres-only database, and Microsoft-aligned buyers get a native procurement path, with MS SQL Server's built-in high availability as a secondary benefit for customers who choose it.

Other benefits:

- > Improved observability
- > Simplified deployment topology
- > API/backward-compatibility that keeps upgrades from breaking existing integrations.

Context for deterministic execution

Provide a structured view of the AAP platform estate (*installed content, topology, execution patterns, credentials, RBAC, automation orchestrator workflows*) so that AI agents (via skills or MCP) are enabled to make platform aware automation recommendations without requiring customers having to take novel steps to reimplement discovery.





The Ansible Automation Platform Roadmap

Our goal: Continue to lead enterprise automation today, while shaping the future of agentic ITOps

Resilient, trusted platform foundation



AI-powered automation acceleration

- > **Accelerate enterprise-wide adoption** and deliver a user experience optimized for the creation, modernization, and scaling of automation content.
- > **Expand governance controls and policy validation** to be end-to-end across IT automation workflows, including boundaries and audit trails for AI recommendations and IT ops agents.
- > **Enable customers to leverage AI-assisted workflows** to modernize existing Ansible assets - and seamlessly migrate non-Ansible automations into AAP.

Multimode automation + orchestration

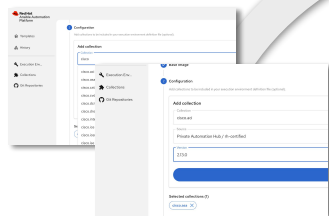
Ansible Automation Platform | Automation portal

Integrated tools for applying DevOps + Platform Engineering principles to IT automation

Discover

Unified search | Find verified content

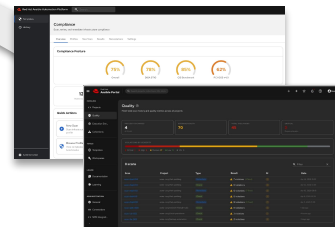
Content discovery



Monitor and optimize

Track production performance
Feedback for improvement

*Content modernization
Compliance experience*

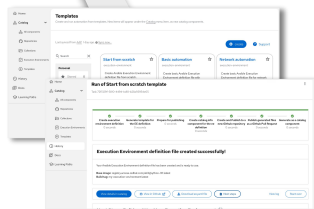


Automation portal

Create and edit

Build new playbooks | Golden Paths + AI

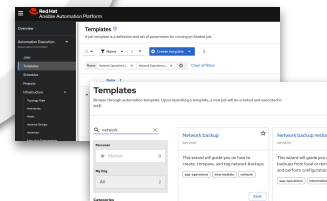
Execution Environment Builder



Deploy and manage

Deploy into production with AAP

Self-service automation

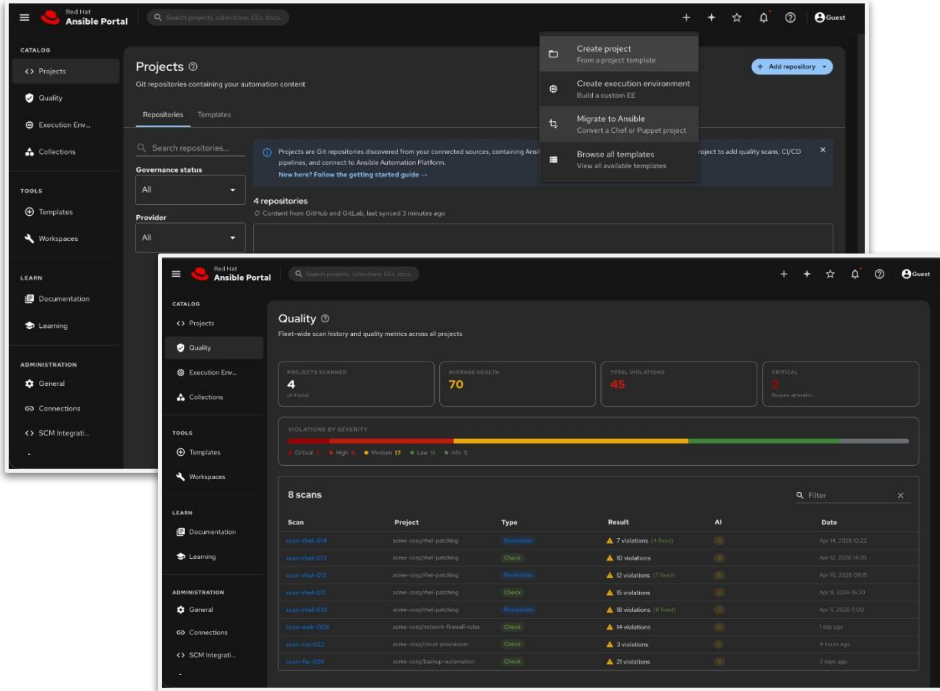


A continuous feedback and accountability loop for scaling governance, standards, and best practices



Ansible Content Migration and Validation

AI powered Ansible playbook scanning, migration and remediation

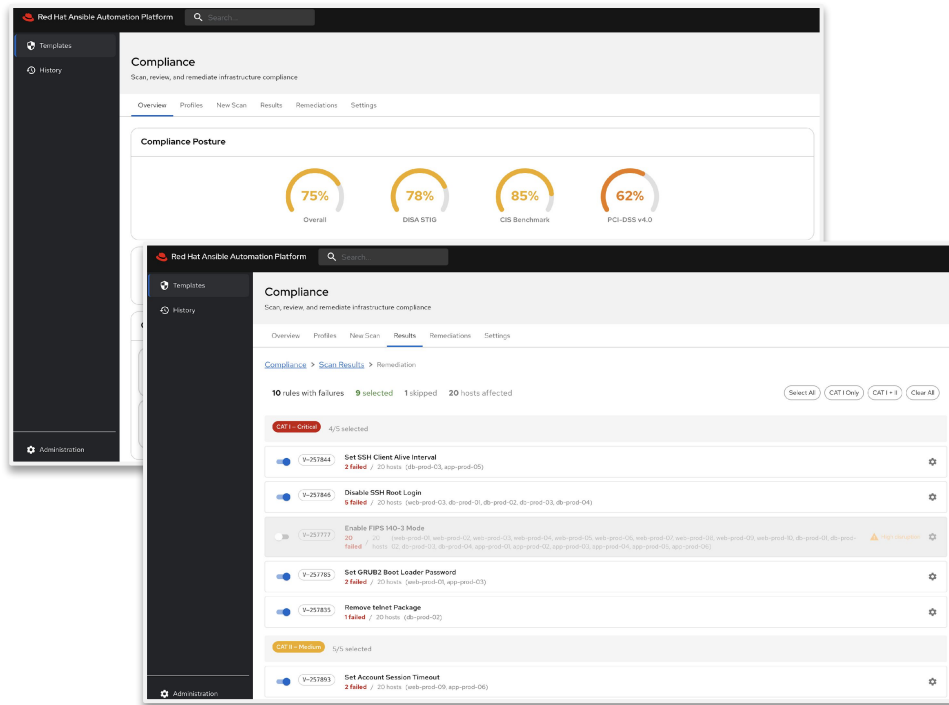


Analyzes automation content for known syntax, standards and security focused considerations

- > Project based workflow to **allow granular control** across teams and areas of responsibility
- > **Rules based, AI powered or human alerted** output to identify resolutions to known playbook or automation standards/versions
- > **Ongoing compliance and upgrade scanning** as part of regular CI/CD or GitOps workflows, or via self service initiation

In-Platform Compliance Experience

Scan, review, and remediate infrastructure compliance from the Automation Portal



End-to-end compliance experience built into the Ansible Portal – from scanning infrastructure against DISA STIG, CIS, and other compliance standard profiles to reviewing per-host findings and executing targeted remediation

- Scanner orchestration across a three-tier model – ship OpenSCAP and PowerSTIG out of the box, integrate Tenable, Qualys, or Insights via bring-your-own-scanner adapters
- Granular remediation builder with per-rule toggles, parameter customization, and host-level targeting – powered by Compliance-As-Code content from the trusted RHEL supply chain
- Agentless and scalable pre-assessment for continuous monitoring, alongside audit-grade scanner results for compliance certification

AI skills for platform operations

Ready-to-use AI skills and agents that assess, audit, and report on your automation platform



Platform Health & Readiness

Validates your configuration against Red Hat's tested reference architectures and lifecycle data. Pre-upgrade readiness, topology verification, and supportability assessment.

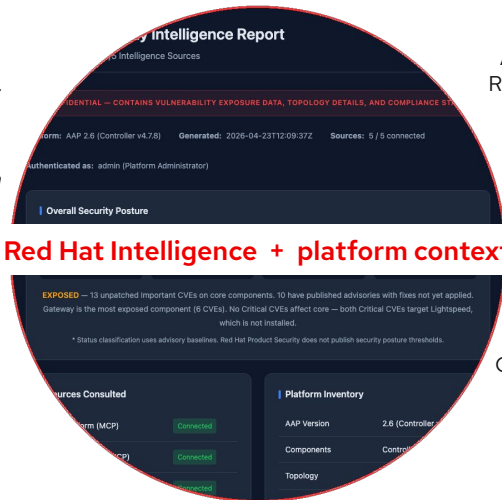
Health check · Upgrade readiness · Topology validation



Operations Intelligence

Combines Red Hat operational guidance with your usage analytics, capacity data, and configuration state. Drift detection across the automation mesh.

Analytics · Drift detection · Capacity monitoring



Red Hat Intelligence + platform context

Security & Access Governance

Applies Red Hat security best practices to your RBAC, authentication posture, and activity data. Role sprawl detection, permission gap analysis, and audit compliance review.

RBAC audit · Auth posture · Activity analysis



Security Intelligence

Correlates Red Hat CVE databases, errata, and advisories with your installed components. Prioritized by actual deployment exposure – not generic severity scores.

CVE correlation · Vulnerability assessment



Subscription value in the age of AI – Red Hat expertise, your platform context, governed agents



The Ansible Automation Platform Roadmap

Our goal: Continue to lead enterprise automation today, while shaping the future of agentic ITOps

Resilient, trusted platform foundation



AI-powered automation acceleration



Multimode automation + orchestration

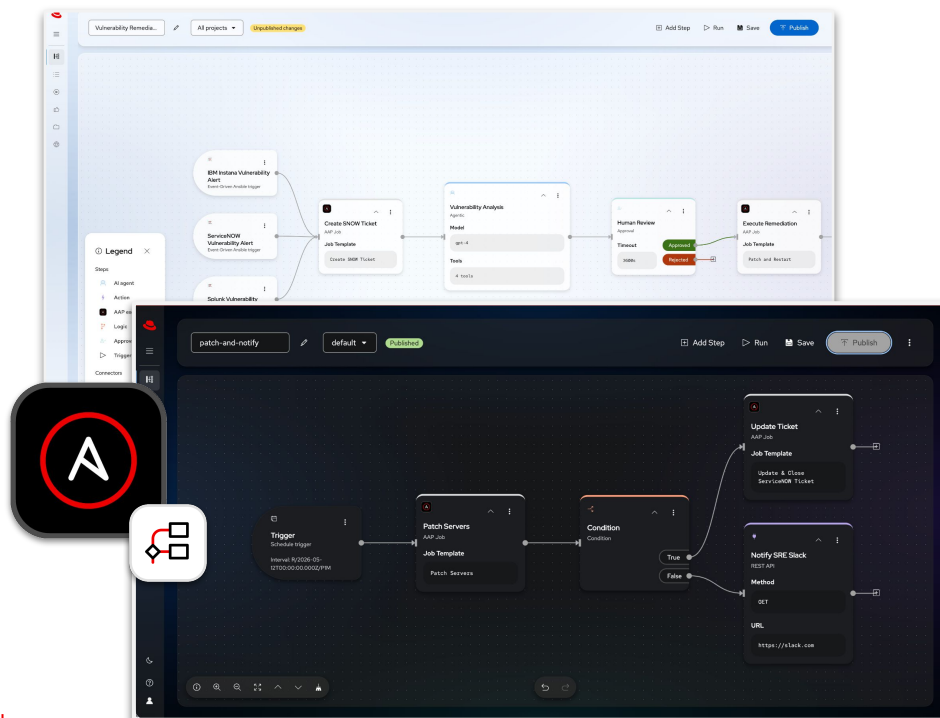
Establish AAP as the trusted coordination and execution layer for agentic IT operations:

- > Continue to mature Event-Driven Automation with AAP as the default mechanism for AIOps teams looking to turn intelligence into trusted action
- > Build on the GA of the *automation orchestrator*, as customers leverage multimode automation at scale to connect AI systems, workflows, and deterministic automations to completely redefine how they orchestrate and operate infrastructure at enterprise scale.



Introducing: Automation orchestrator

The composable workflow canvas for Ansible Automation Platform



The automation orchestrator* is designed to help automation teams design and deploy workflows that extend far beyond linear playbook execution.

- **Composable workflows that expand on what you've built**
Existing job templates and collections become workflow steps immediately, with no migration or rebuilds required, while providing a single control plane across the stack.
- **Proven governance that extends automatically**
The same RBAC, audit trails, and credential management that you already trust to govern your environment automatically extends to automation orchestrator, avoiding costly rebuilds and disruptive migrations.
- **An experience enhanced for multimode automation**
Seamlessly connect automated tasks, event-driven triggers, logic steps, AI reasoning, and approval gates to create flexible, resilient IT ops workflows.

*Automation orchestrator requires an additional purchase



Automation orchestrator | Governance-first automation in action

Your established + proven governance automatically extends to new workflows

Access Management

Users Groups Projects **Policies** Roles Assignments Can I?

Y Name Filter by name

Name	Description	Type
admin:full:any	Full administrative access to all resources	Built-in
workflow:create:any	Create workflows in any project	Built-in
workflow:read:any	View workflows in any project	Built-in
workflow:update:any	Edit workflows in any project	Built-in

Most recent run details

Search

Human Approval
10:00:00 AM - 10:00:01 AM, 26 Jan 2026 Successful

Remediation
10:00:01 AM - 10:00:13 AM, 26 Jan 2026 Successful

RCA Report Agent
10:00:13 AM - 10:02:25 AM, 26 Jan 2026 Running

Substeps

Governance Route Decision

Switch

- Auto Patch Approved (Policy Approved)
- Manual Patching required (Policy Enforced)
- Application Patched/Deployed
- Fallback

Human Review

Approval

Timeout 3600s

Approved Rejected

RCA Report Agent

Input Search

```
{
  "event_id": "evt_987654321",
  "timestamp": "2026-01-26T08:38:00Z",
  "source": "Prometheus-Alertmanager",
  "payload": {
    "alert_name": "High CPU Utilization",
    "severity": "critical",
    "tags": {
      "env": "prod",
      "region": "us-east-1",
      "ip_address": "10.0.4.52",
      "remediation_type": "config_change"
    }
  },
  "details": {}
}
```

Role and Policy Based Access Control

Fine-grained permissions on who can design, execute, and view workflows. Deny-by-default across every mode.

Approval gates

No production change, AI-recommended or otherwise, runs without explicit human approval (at runtime or via predefined policy)

Credential & Secrets Management

Scoped per workflow step, injected at runtime. Never logged, displayed, or exposed.

SSO & Identity integration

Connect to existing identity providers via OIDC. No separate user database required.

One audit trail across every mode

Every step logged in a single, unified trail. Stronger governance that doesn't require extra work.

Automation orchestrator | Trusted AI for IT Operations

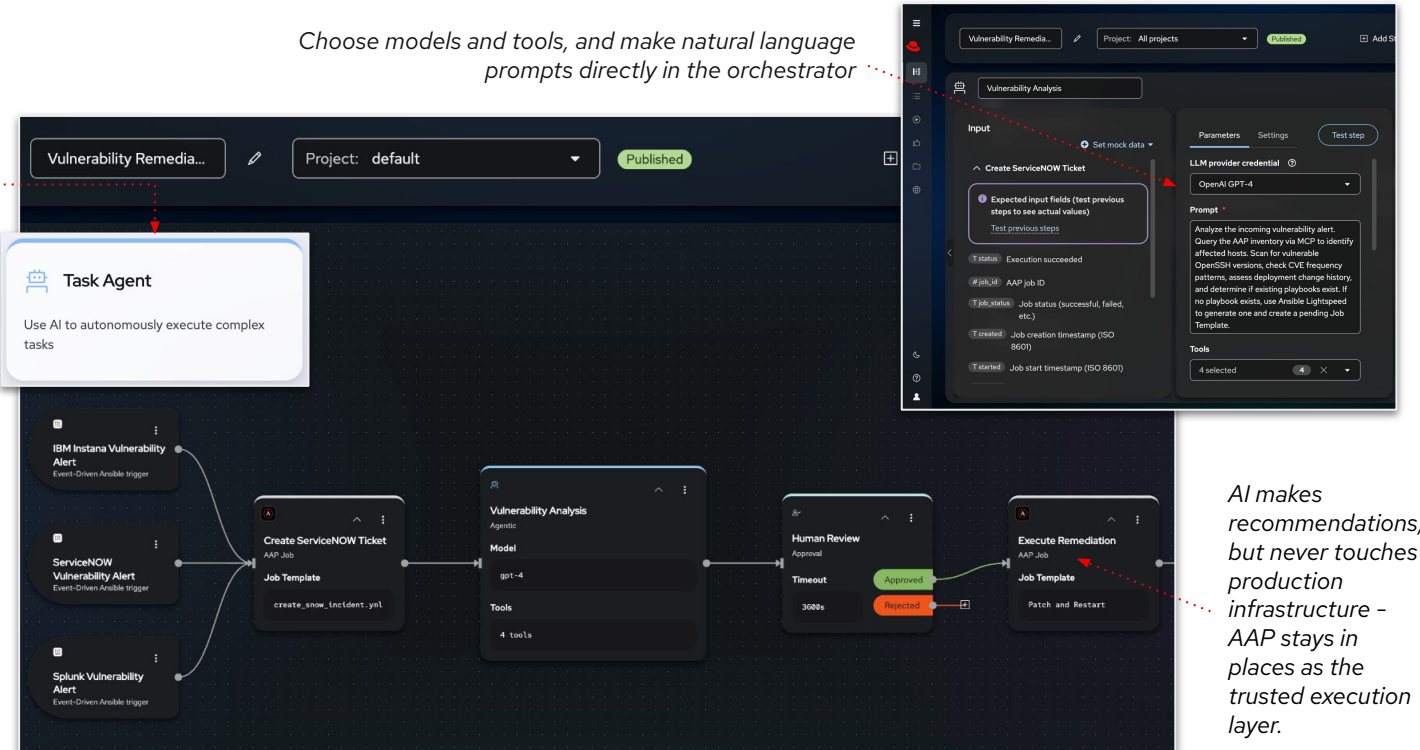
AI recommends, humans decide, AAP executes

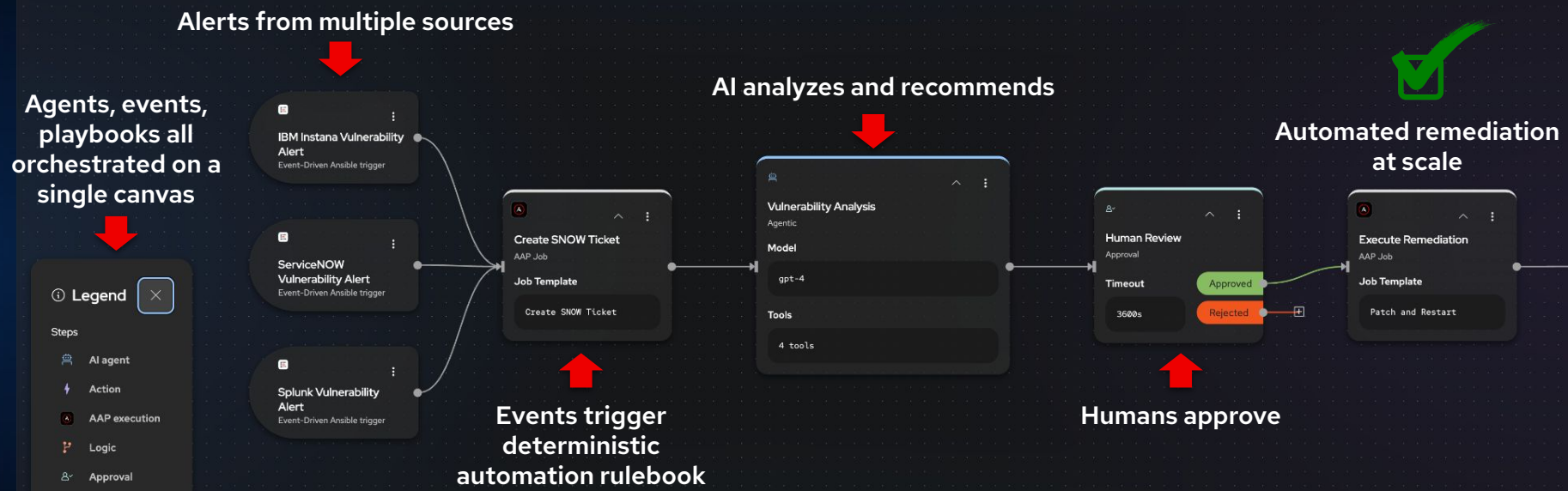
Leverage AI in your operations, trust AAP to execute.

Infusing ITOps workflows with more intelligence no longer requires building new playbooks to call agents or LLMs via API call.

With new task agents, AI recommendations for IT operations are woven directly into workflows as steps, with governance automatically extended.

Choose models and tools, and make natural language prompts directly in the orchestrator





Legend

Steps

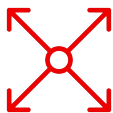
- AI agent
- Action
- AAP execution
- Logic
- Approval
- Trigger

Connectors

- Approved
- Rejected

Automation orchestrator: **near-term roadmap + strategy**

Continuous innovation around this feature will continue to drive critical differentiation for AAP



Redefining how workflows can be executed at scale

- Workflow steps will execute directly via automation orchestrator, at global scale.
- The AO execution plane will sustain hundreds of thousands of concurrent tasks



Extending the depth and breadth of the Ansible ecosystem

- The Ansible ecosystem will continue to deepen around the orchestrator
- Ecosystem partners will be able to create extensions for the workflow canvas, following same certification process for content today



Expanding the aperture of event-driven automation

- Event-Driven Ansible has the webhook side of events covered, and it is fully integrated into AO.
- Automation orchestrator will unlock the other half of the equation - providing full event bus connectivity.

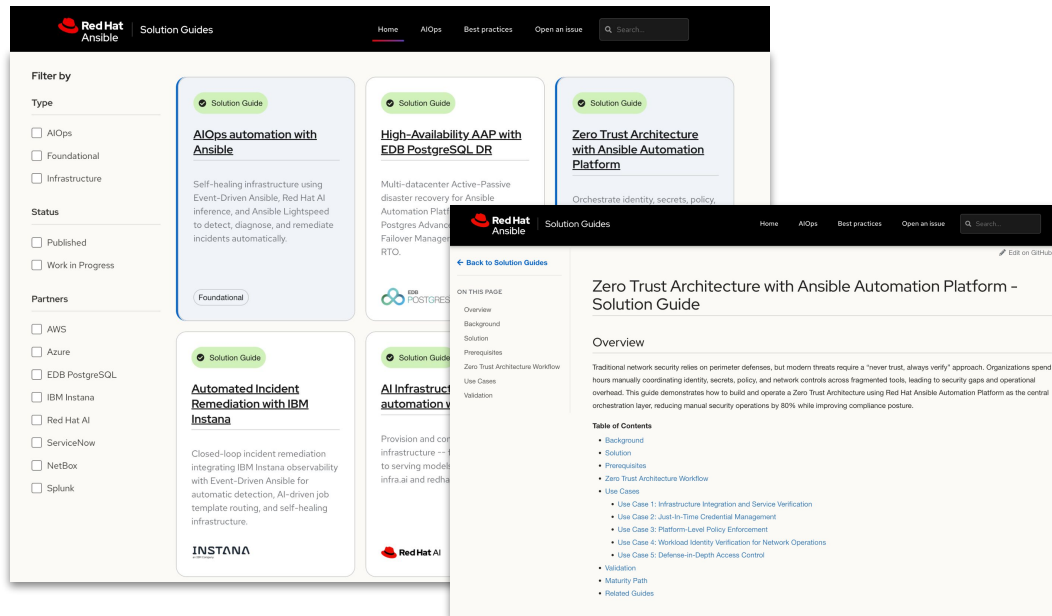


Introducing Ansible Solution Guides

An Ansible Automation Platform (AAP) *solution guide* is a prescriptive document that demonstrates how to solve a specific operational challenge using the platform.

Solution guides provide a streamlined, step-by-step path that enables even non-technical stakeholders to understand high impact automation features.

- ✓ Detailed walkthroughs
- ✓ Partner-focused
- ✓ RAG-enabled (coming soon)



Learn more!



red.ht/aap-whats-new



red.ht/automation-orchestrator



red.ht/AAP-tech-preview



Thank you!



linkedin.com/company/red-hat



facebook.com/redhatinc



youtube.com/user/RedHatVideos



twitter.com/RedHat



Automated governance and security improve risk posture and resilience

AAP provides a foundation that enables customers to evolve and scale with confidence

