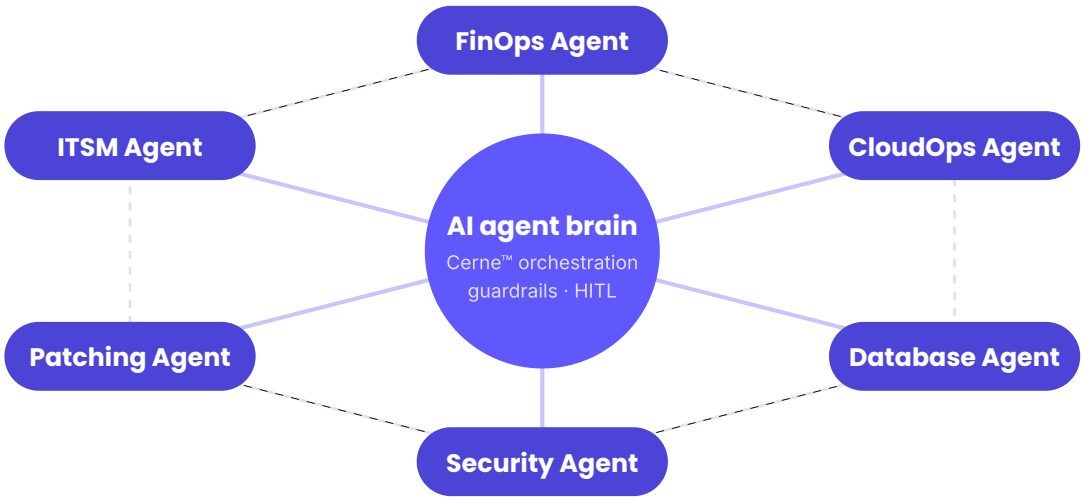
CERNE™
Agentic Cloud Management

CERNE™ AGENT ECOSYSTEM

Your AI operations team, always on

Six specialized AI agents for cloud cost, cloud operations, databases, security, patching and service management. They spot problems, decide what to do and fix them, within the limits you set.



6
Specialized AI agents

100+
Prebuilt agentic workflows

Up to 85%
L1/L2 incidents resolved autonomously

3x
Engineering productivity

© Copyright 2026 By UnityOne AI | www.unityone.AI

WHY IT MATTERS

Operations teams can't keep up by hand

Cloud waste grows, vulnerabilities stay open, tickets pile up and alerts never stop. Adding people doesn't scale, and skilled engineers are hard to hire.

29%

of cloud spend is wasted

Flexera 2026 State of the Cloud Report.

20%

of breaches start with vulnerability exploitation

Verizon 2025 DBIR.

241 days

average breach lifecycle

IBM Cost of a Data Breach Report 2025.

Without agents

- Waste found months after it was billed
- Patches waiting on manual checks
- Threats buried in alerts
- Tickets queuing for routine fixes
- Database changes squeezed into late nights

With Cerne™ agents

- Idle resources found and removed on schedule
- Patches validated, applied and rolled back if needed
- Threats correlated, contained and logged
- Routine tickets resolved automatically
- Databases tuned and changed safely

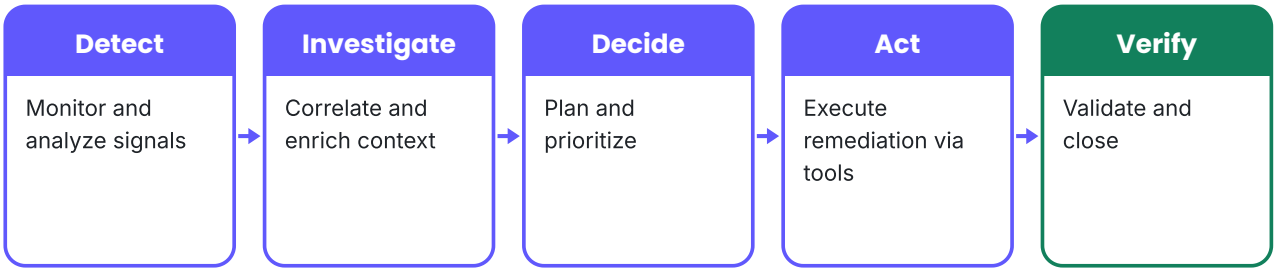
Six agents, six problems solved

Agent	Problem it solves
FinOps Agent	Finds cloud waste and removes it, continuously.
CloudOps Agent	Keeps hybrid and multicloud environments healthy, compliant and right-sized.
Database Agent	Tunes, protects and changes databases safely.
Security Agent	Detects threats, contains them and records every step.
Patching Agent	Closes vulnerabilities faster, without breaking production.
ITSM Agent	Resolves tickets and requests before they queue.

© Copyright 2026 By UnityOne AI | www.unityone.AI

HOW AGENTS WORK

Every agent follows the same five steps



You decide how much they do alone

For every type of action you choose one of three paths.

AUTO

Routine, low-risk work is done straight away and logged.

APPROVAL

The agent prepares the change; a person approves it, for example in ServiceNow.

ESCALATE

Anything unusual goes to the right expert with the context attached.

Built to be trusted

Private or BYO LLM
Data stays in your environment.

Human in the loop
Approval for sensitive actions.

Policy guardrails
Autonomy levels set per workflow.

Audit and RBAC
Every step logged and controlled.

© Copyright 2026 By UnityOne AI | www.unityone.AI

MEET THE AGENTS

FinOps Agent

Finds cloud waste and removes it, continuously. Cloud bills keep growing because idle disks, unattached network interfaces, unused public IPs and oversized resources keep billing long after anyone needs them. The FinOps Agent runs scheduled cost analysis, finds that waste, prioritizes the biggest savings and cleans it up within your policies.

The problem

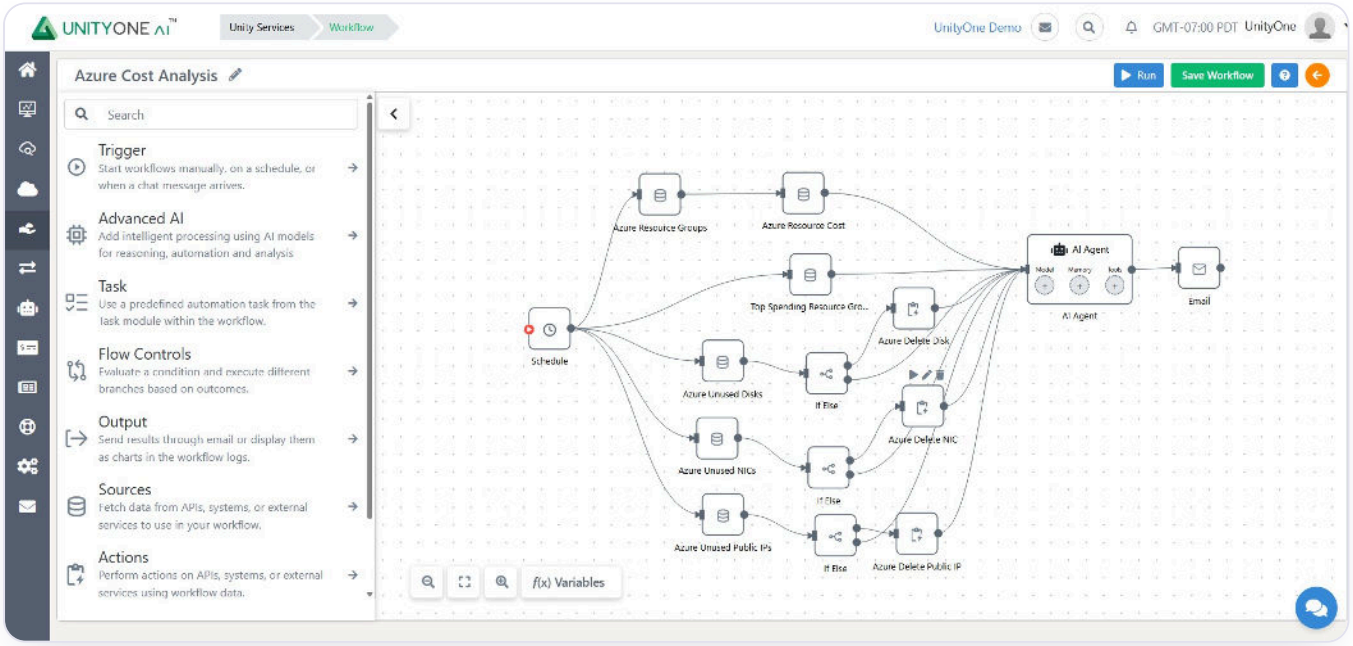
- Idle and orphaned resources billing every month
- High-cost resources nobody reviews
- Manual, occasional cost clean-ups

What it does

- Identifies cost anomalies and idle resources
- Recommends optimization actions
- Delete unused disks, NICs and public IPs
- Optimize high-cost resources

What you get

- Reduced cloud spend
- Improved resource utilization
- Continuous cost governance



Azure cost analysis workflow: scheduled scan of resource groups, top-spending resources, unused disks, NICs and public IPs, with an AI agent summary by email.

MEET THE AGENTS

CloudOps Agent

Keeps hybrid and multicloud environments healthy, compliant and right-sized. Cloud environments drift from their intended state, scale at the wrong time and generate alerts faster than teams can act. The CloudOps Agent correlates telemetry, logs and topology, then auto-heals, fixes drift, scales and raises change requests, asking for approval when the policy says so.

The problem

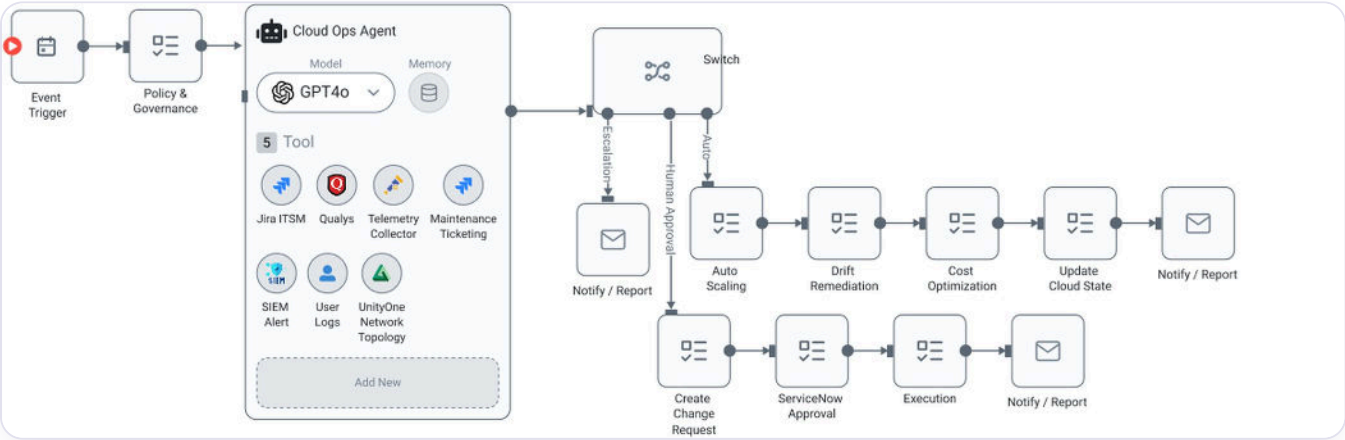
- Configuration drift nobody notices until it breaks
- Manual healing and scaling at 3 a.m.
- Changes raised and tracked by hand

What it does

- Correlates telemetry, logs and topology
- Identifies incidents and optimization opportunities
- Auto-healing and drift remediation
- Auto scaling and cost optimization

What you get

- Reduced MTTR and operational effort
- Improved system reliability
- Continuous governance and reporting



CloudOps Agent workflow: event trigger, policy check, agent with Jira, Qualys, SIEM and topology tools, then auto scaling, drift remediation, or change request with ServiceNow approval.

© Copyright 2026 By UnityOne AI | www.unityone.AI

MEET THE AGENTS

Database Agent

Tunes, protects and changes databases safely. Database teams spend hours validating backups, tuning performance and pushing changes through maintenance windows. The Database Agent checks backup and database health, assesses impact and readiness, then optimizes, tunes or executes changes with rollback, inside the policy and window you define.

The problem

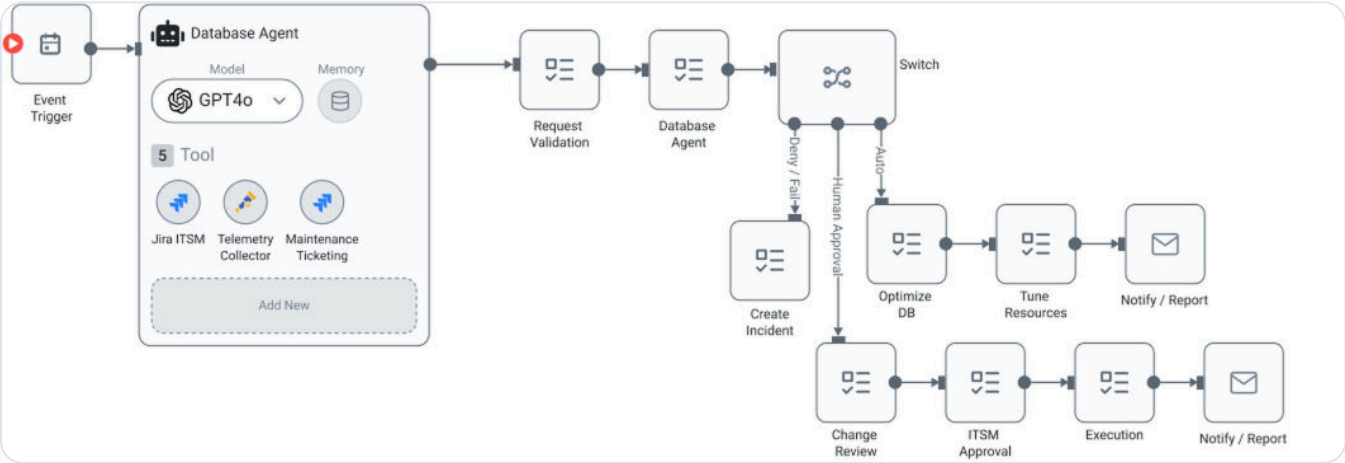
- Backups assumed good until a restore fails
- Performance tuning done by hand
- Risky changes squeezed into maintenance windows

What it does

- Validates backup and database health
- Assesses impact and readiness
- Optimize databases and tune resources
- Execute changes, or roll back

What you get

- Improved database performance and reliability
- Reduced manual effort
- Audit-ready operations



Database Agent workflow: request validation, then optimize and tune automatically, or route through change review and ITSM approval before execution.

MEET THE AGENTS

Security Agent

Detects threats, contains them and records every step. Threats hide in a flood of security alerts, user logs and network signals that no team can read in full. The Security Agent correlates user, asset and network behaviour with threat intelligence, classifies severity, and notifies, contains or escalates, with an incident opened automatically.

The problem

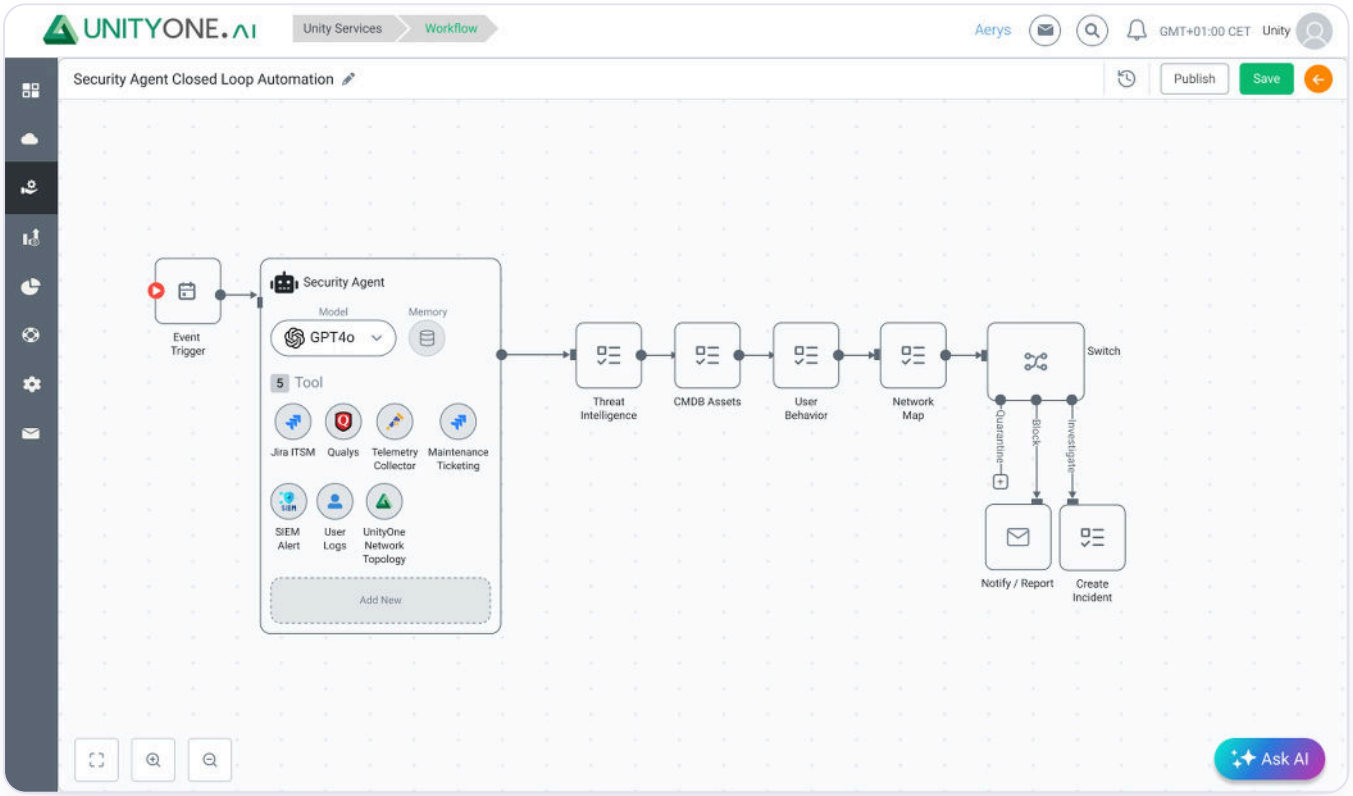
- Threats buried in SIEM alerts
- Slow correlation of users, assets and network
- Manual containment and incident creation

What it does

- Correlates user, asset and network behaviour
- Detects threats and risk patterns
- Block or isolate
- Create an incident

What you get

- Faster threat detection and response
- Reduced security risk exposure
- Automated incident management



Security Agent closed-loop automation: threat intelligence, CMDB assets, user behaviour and network map, then quarantine, block or investigate.

MEET THE AGENTS

Patching Agent

Closes vulnerabilities faster, without breaking production. Unpatched vulnerabilities are one of the most common ways attackers get in, yet patching stalls on impact checks, change approvals and maintenance windows. The Patching Agent validates patch impact and readiness, learns from past outcomes, and applies, defers or routes patches for approval, with rollback and incident creation if a patch fails.

The problem

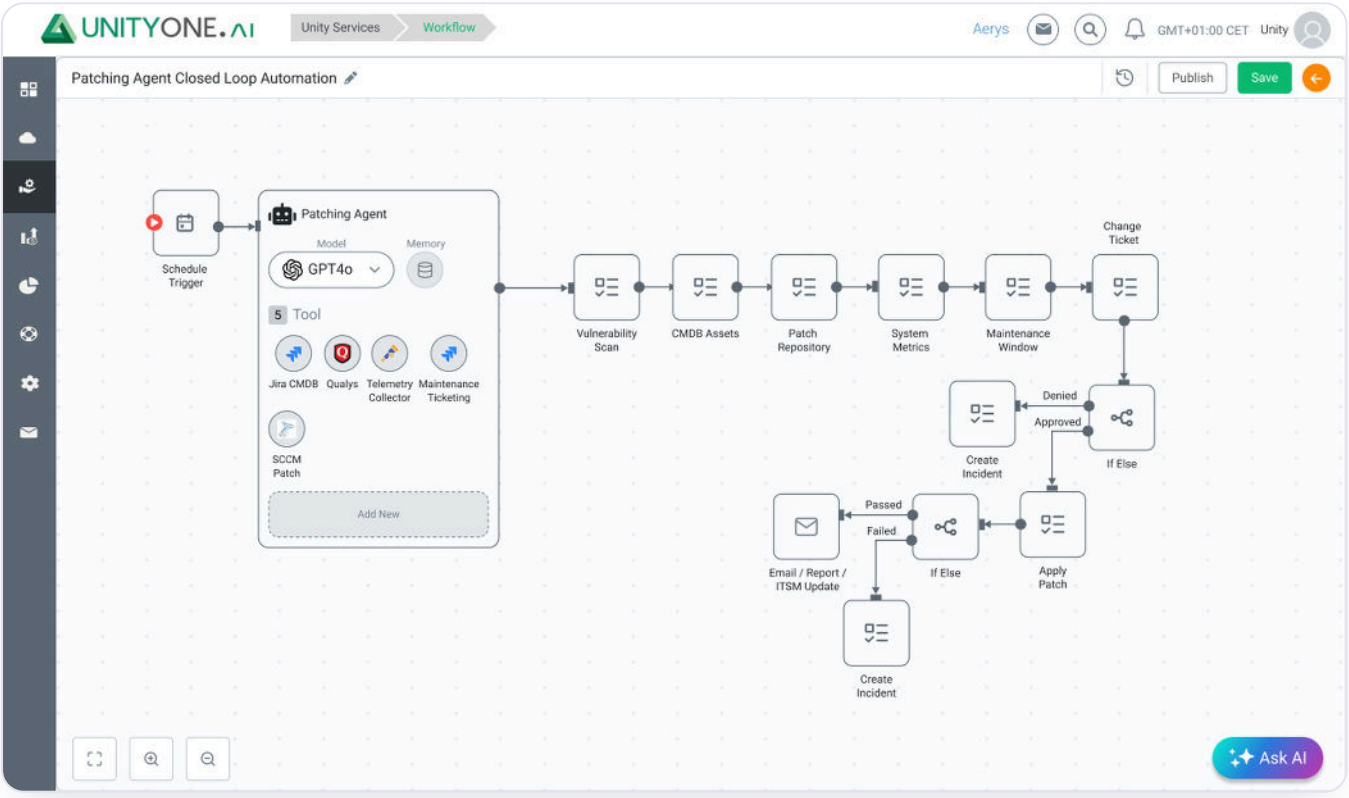
- Vulnerabilities open for weeks or months
- Patches delayed by manual impact checks
- Change tickets and approvals handled by hand

What it does

- Validates patch impact and readiness
- Learns from past outcomes
- Apply patch, or roll back
- Create an incident if it fails

What you get

- Reduced vulnerability exposure and risk
- Automated patch compliance
- Change and incident tracking in ITSM



Patching Agent closed-loop automation: vulnerability scan, CMDB, patch repository, system metrics and maintenance window, then change ticket, apply patch, and incident if it fails.

MEET THE AGENTS

ITSM Agent

Resolves tickets and requests before they queue. Service desks drown in tickets that follow the same patterns: alerts to triage, requests to fulfil, incidents to route. The ITSM Agent analyzes ticket context and priority, recommends or applies the fix, provisions resources and escalates to the right expert when needed.

The problem

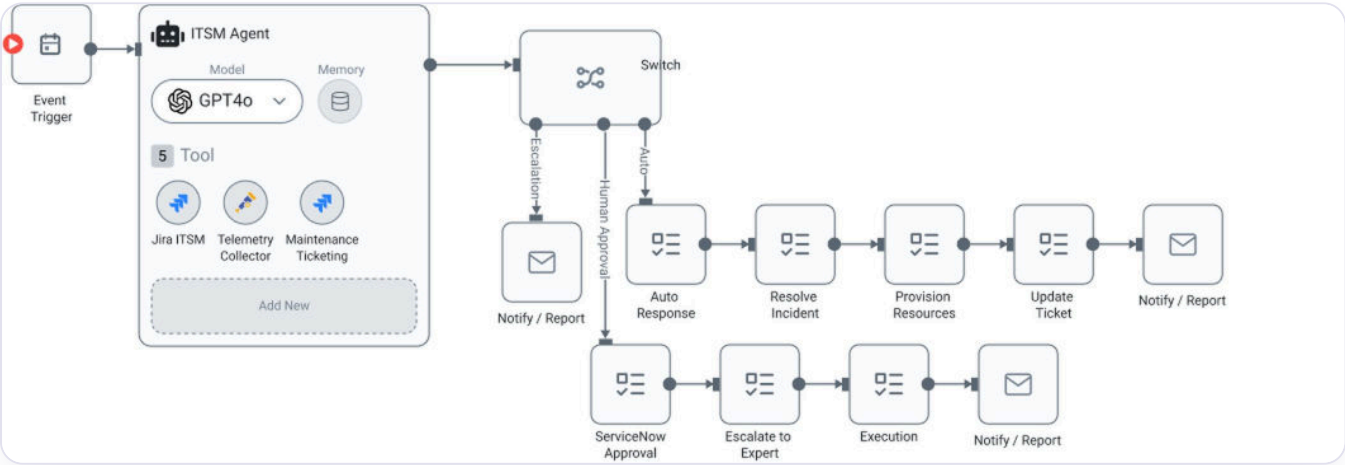
- Growing ticket backlogs
- Manual triage and routing
- Slow resolution of repeat incidents

What it does

- Analyzes ticket context and priority
- Recommends resolution actions
- Auto-resolve incidents
- Provision resources

What you get

- Faster incident resolution (MTTR)
- Reduced manual effort
- Improved service efficiency



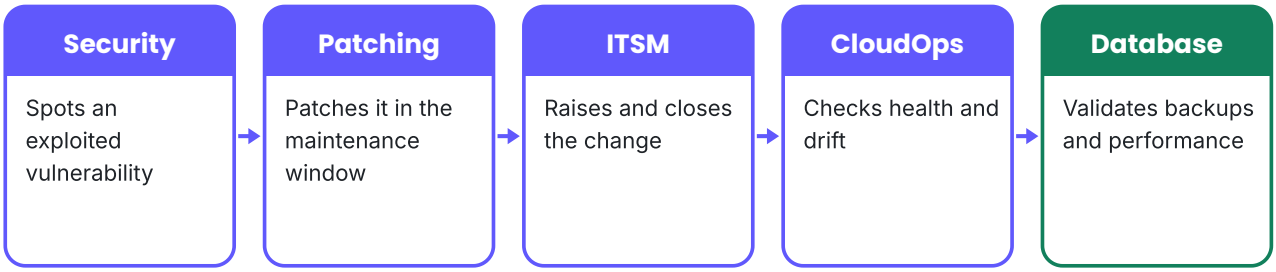
ITSM Agent workflow: auto response, resolve incident, provision resources and update ticket, or ServiceNow approval and escalation to an expert.

© Copyright 2026 By UnityOne AI | www.unityone.AI

BETTER TOGETHER

Agents that work as a team

The agent brain in Cerne™ passes context from one agent to the next, so a single problem is handled end to end.



Who benefits

IT AND CLOUD OPERATIONS

Fewer late-night fixes and a shorter queue.

SECURITY TEAMS

Faster containment and patching with audit trails.

FINOPS AND FINANCE

Waste removed continuously, not quarterly.

DATABASE TEAMS

Healthy, tuned databases and safe changes.

SERVICE DESK

Routine tickets resolved before they queue.

IT LEADERS

More done by the same team, with full control.

© Copyright 2026 By UnityOne AI

GETTING STARTED

Start with one agent, grow to a team

STEP 1

Pick an agent

Start where the pain is greatest, often FinOps or ITSM.

STEP 2

Set guardrails

Choose auto, approval or escalate for each action.

STEP 3

Expand

Add agents and let them work together.

> **Leader and Outperformer, GigaOm Radar for Cloud Management Platforms 2025.** *"UNITYONE.AI stands out as a comprehensive cloud management platform by bridging on-premises automation with multicloud orchestration."*

6	**100+**	**300+**	**350+**
Specialized AI agents	**Prebuilt agentic workflows**	**Integrations**	**Global customers**

GET STARTED

Put Cerne™ agents to work

See the agent ecosystem hands-on in the UnityOne AI Playground, or talk to our team about which agents to deploy first in your hybrid and multicloud estate.

Enter Playground **Contact Us**

Email: contact@unityone.ai · Playground: cerne.unityone.ai · Sales: unityone.ai/contact-us

© Copyright 2026 By UnityOne AI | www.unityone.AI