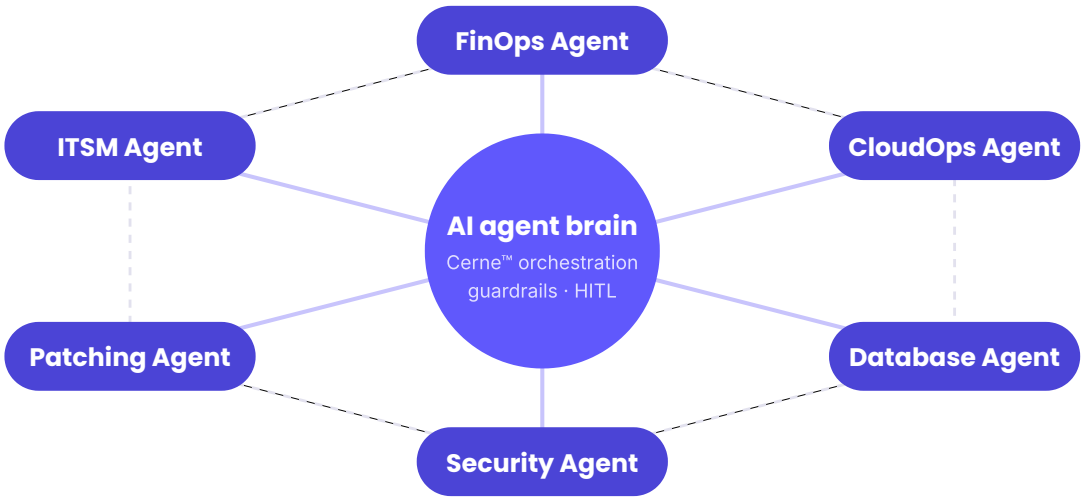
CERNE™
Agentic Cloud Management

TECHNICAL BROCHURE · AGENT ECOSYSTEM

# Stateful, governed AI agents for autonomous cloud operations

FinOps, CloudOps, Database, Security, Patching and ITSM agents, orchestrated by the Cerne™ agent brain and executed through 300+ tools under policy guardrails.




**6**
**Specialized AI agents**

**100+**
**Prebuilt agentic workflows**

**300+**
**Integrations**

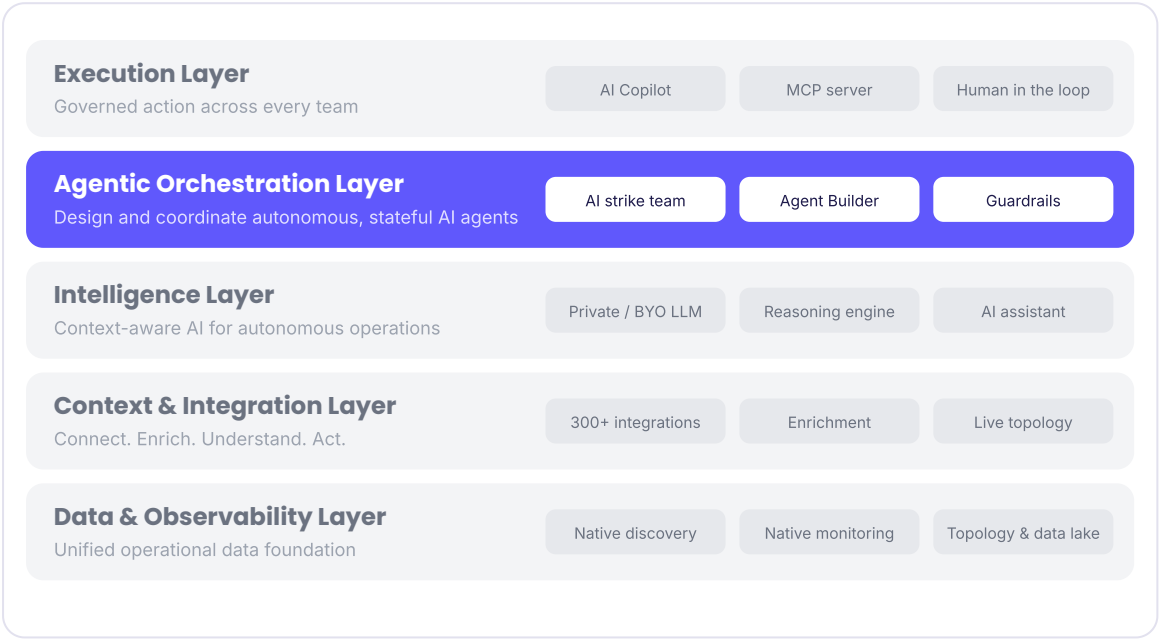
**350+**
**Global customers**

© Copyright 2026 By UnityOne AI 

WHERE AGENTS LIVE

# The Agentic Orchestration Layer of Cerne™

Agents sit on four other platform layers: unified data, enriched context and AI intelligence below, governed execution above.




## AI agent brain

- Stateful and context aware
- Reasoning, decision making and learning
- Creates workflows
- Takes actions via tools
- Cross-agent collaboration

## Agent Builder and control plane

- Low-code Agent Builder
- Policy-driven guardrails
- Observability and monitoring
- Audit and RBAC control
- Private LLM or bring your own LLM

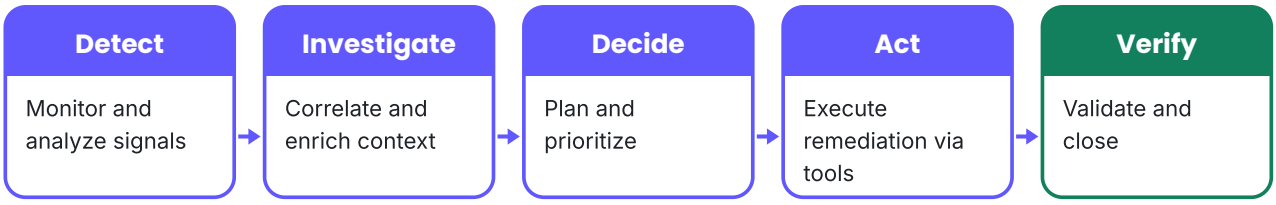
© Copyright 2026 By UnityOne AI 

AGENT ANATOMY

# Six stages in every agent

| | |
|---|---|
| **Trigger** | A UnityOne event, alert, ticket, policy signal, schedule, API call or natural-language prompt starts the agent. |
| **AI service agent** | An LLM-powered agent with memory reasons over the event, correlates context and recommends actions. |
| **Tool integrations** | Agents read from and act through ITSM, SIEM, CMDB, monitoring, cloud APIs, scanners and patch repositories. |
| **Decision engine** | Classifies severity and chooses a path, such as auto, approval or escalate, based on policy and maintenance windows. |
| **Actions** | Executes the change, with rollback, incident creation and ITSM updates where needed. |
| **Output and governance** | Notifies and reports, records an audit trail, and learns from the outcome. |

## Agentic workflow




© Copyright 2026 By UnityOne AI 

AGENT ECOSYSTEM

# FinOps Agent

Finds cloud waste and removes it, continuously.

**Trigger**

- Scheduled cost analysis
- Cloud usage and spend data

**AI service agent**

- Identifies cost anomalies and idle resources
- Recommends optimization actions

**Tool integrations**

- Cloud data: Azure Resource Manager, Cost Management
- Assets: resource groups, disks, NICs, public IPs
- Telemetry: usage and billing metrics
- Actions: cloud APIs to delete or rightsize

**Decision engine**

- Detects unused and underutilized resources
- Prioritizes high-cost optimization opportunities

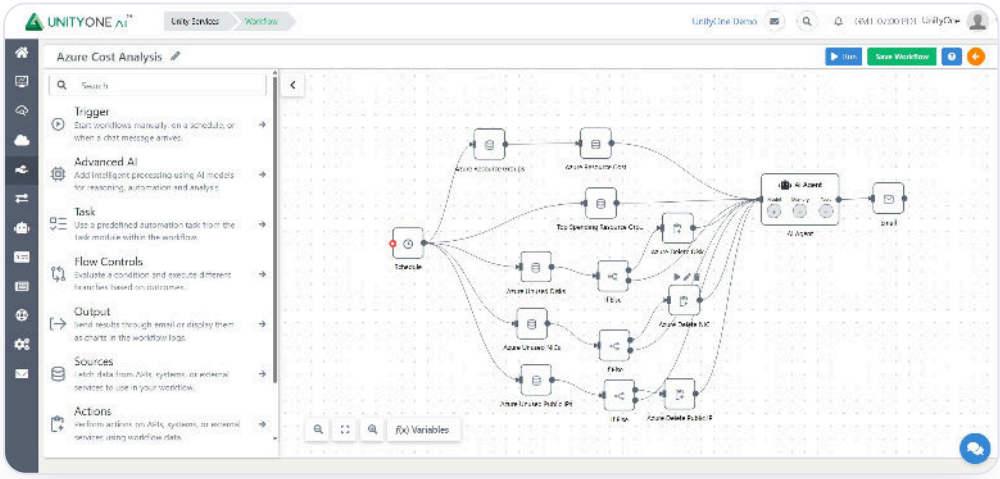
**Actions**

- Delete unused disks, NICs and public IPs
- Optimize high-cost resources
- Email the cost report

**Outcome**

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

**Decision modes:** Auto | Approval | Escalate




*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.*

AGENT ECOSYSTEM

# CloudOps Agent

Keeps hybrid and multicloud environments healthy, compliant and right-sized.

**Trigger**

- Event-driven alerts
- Policy and governance signals

**AI service agent**

- Correlates telemetry, logs and topology
- Identifies incidents and optimization opportunities

**Tool integrations**

- ITSM: Jira and ticketing systems
- Monitoring: telemetry collector, Qualys
- Security: SIEM alerts, user logs
- Context: network topology, maintenance data

**Decision engine**

- Classifies issue severity
- Decides to auto-remediate, seek approval or escalate

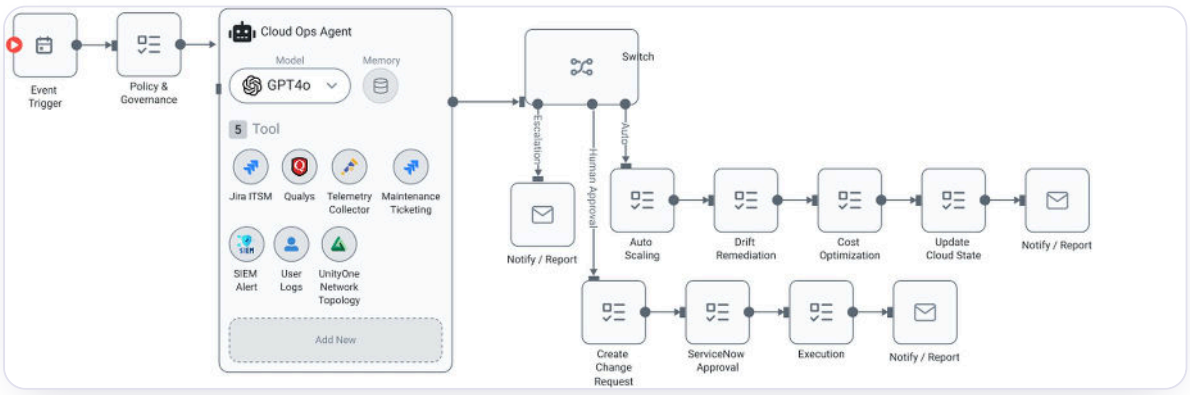
**Actions**

- Auto-healing and drift remediation
- Auto scaling and cost optimization
- Change request, ServiceNow approval and execution

**Outcome**

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

**Decision modes:** Auto | Approval | Escalate




*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

AGENT ECOSYSTEM

# Database Agent

Tunes, protects and changes databases safely.

**Trigger**

- Event or schedule-based trigger
- Policy or maintenance window

**AI service agent**

- Validates backup and database health
- Assesses impact and readiness

**Tool integrations**

- ITSM: Jira and ticketing
- Telemetry: database metrics and monitoring
- Ops: backup and maintenance systems

**Decision engine**

- Auto, approval or escalate
- Policy-driven validation

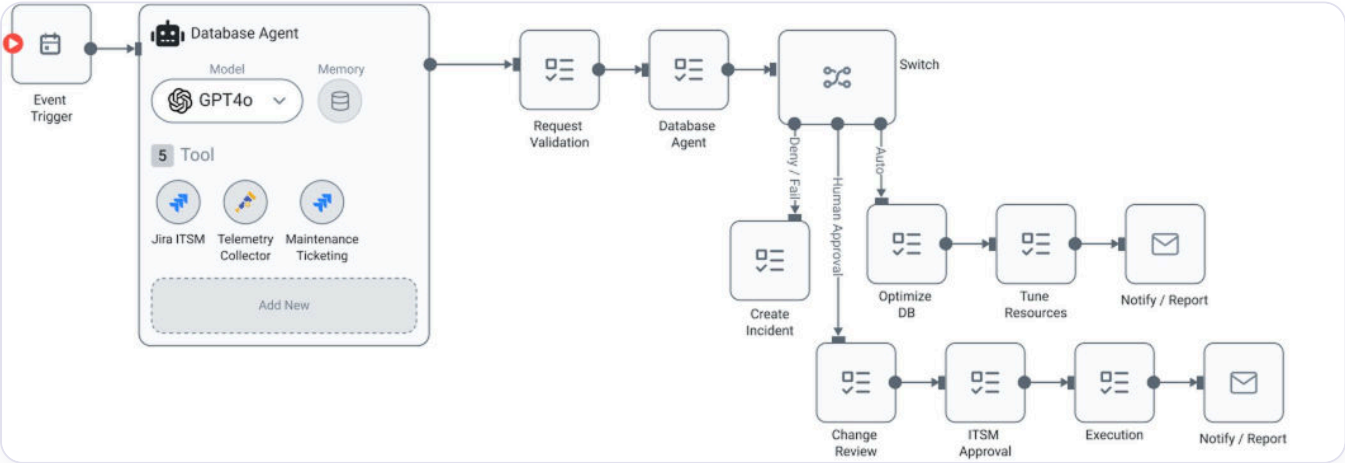
**Actions**

- Optimize databases and tune resources
- Execute changes, or roll back
- Raise an incident or change request

**Outcome**

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

**Decision modes:** Auto | Approval | Escalate




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

AGENT ECOSYSTEM

# Security Agent

Detects threats, contains them and records every step.

**Trigger**

- UnityOne event: security anomaly detected
- Security alerts, anomalies and threat intelligence

**AI service agent**

- Correlates user, asset and network behaviour
- Detects threats and risk patterns

**Tool integrations**

- SIEM and threat intelligence feeds
- CMDB for asset context
- User logs and behaviour analytics
- Network topology and telemetry; ITSM

**Decision engine**

- Classifies threat severity
- Decides to notify, contain or escalate

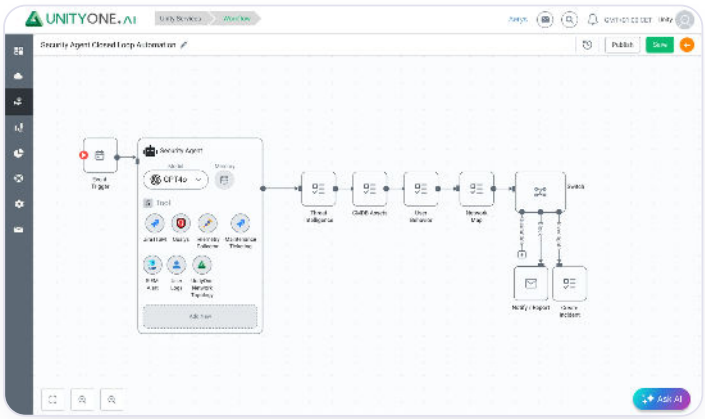
**Actions**

- Block or isolate
- Create an incident
- Notify and report

**Outcome**

- Faster threat detection and response
- Reduced security risk exposure
- Automated incident management
- Continuous learning and audit trail

**Decision modes:** Notify | Contain | Escalate




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

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

AGENT ECOSYSTEM

# Patching Agent

Closes vulnerabilities faster, without breaking production.

**Trigger**

- UnityOne event: patch requirement
- Vulnerability detection, patch availability or schedule

**AI service agent**

- Validates patch impact and readiness
- Learns from past outcomes

**Tool integrations**

- Vulnerability data: scanners such as Qualys
- Asset context: CMDB, such as Jira CMDB
- Patch source: repositories, such as SCCM
- Telemetry and ITSM change management

**Decision engine**

- Auto, defer or approval
- Policy and maintenance-window aware

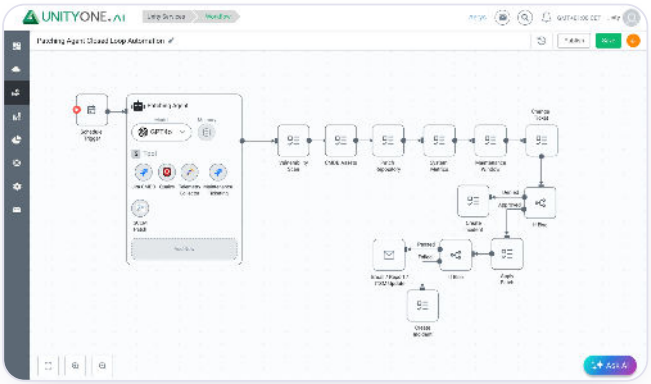
**Actions**

- Apply patch, or roll back
- Create an incident if it fails
- Update ITSM and notify

**Outcome**

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

**Decision modes:** Auto | Defer | Approval



*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.*

© Copyright 2026 By UnityOne AI 

AGENT ECOSYSTEM

# ITSM Agent

Resolves tickets and requests before they queue.

**Trigger**

- Event-driven ticket or alert
- Monitoring or user request

**AI service agent**

- Analyzes ticket context and priority
- Recommends resolution actions

**Tool integrations**

- ITSM: Jira and ticketing systems
- Telemetry: monitoring and alerts
- Ops: maintenance workflows

**Decision engine**

- Auto, approval or escalate
- Priority and policy-based routing

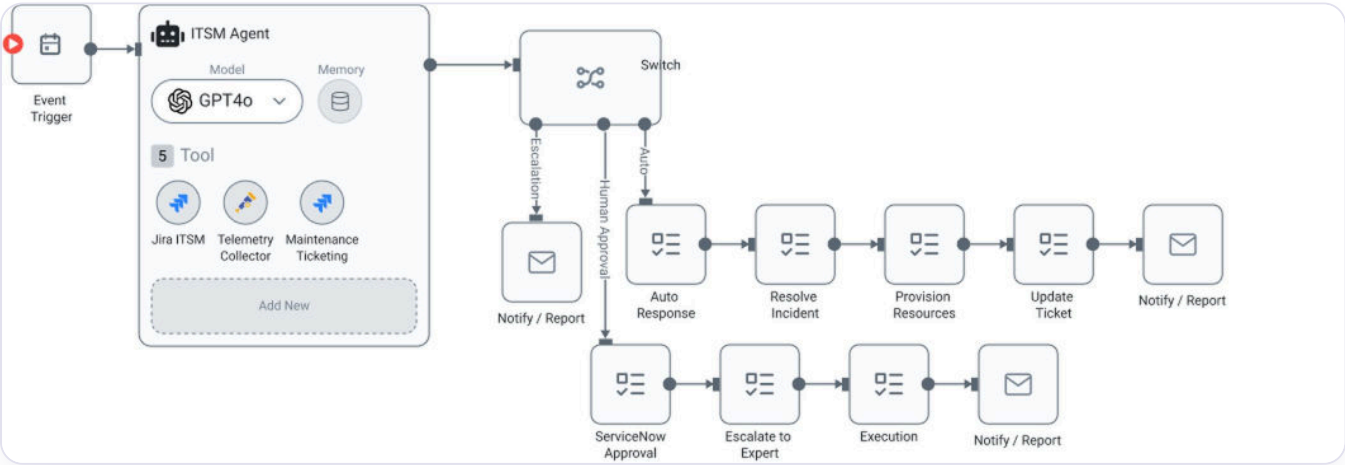
**Actions**

- Auto-resolve incidents
- Provision resources
- Escalate to the right expert

**Outcome**

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

**Decision modes:** Auto | Approval | Escalate



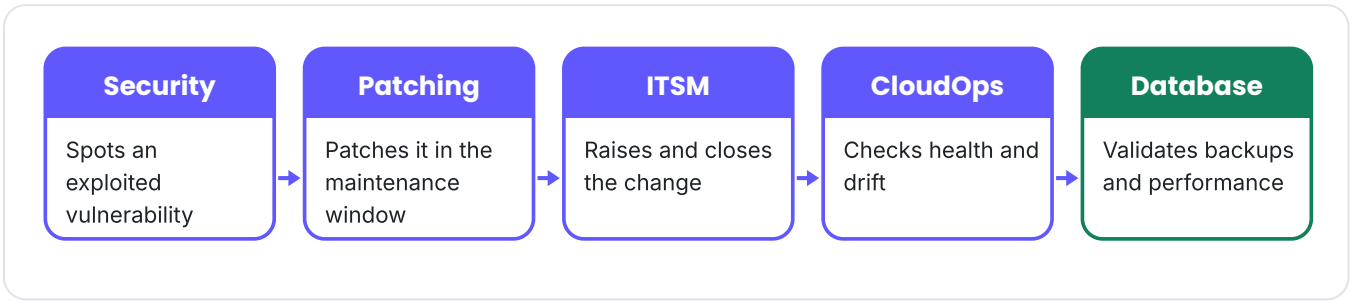

*ITSM Agent workflow: auto response, resolve incident, provision resources and update ticket, or ServiceNow approval and escalation to an expert.*

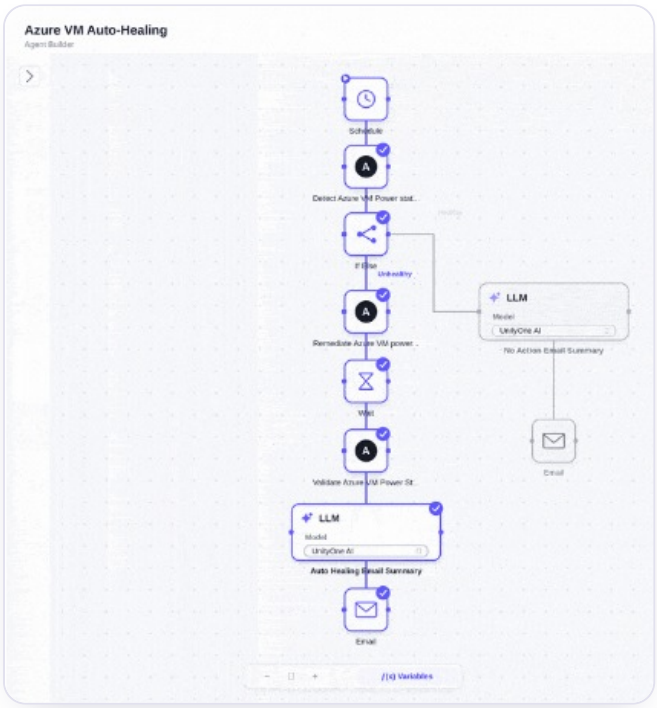
© Copyright 2026 By UnityOne AI | www.unityone.AI

ORCHESTRATION

# Cross-agent collaboration and custom agents

Agents hand context to each other through the agent brain. Example:




*Agent Builder: an Azure VM auto-healing agent with LLM steps and email.*

**Build your own agents**
Low-code skills, agents and workflows.

**Triggers**
Alerts, incidents, policies, schedules, API calls or prompts.

**Tools via MCP**
An MCP server with 300+ tools.

**Monitor every agent**
Steps, results, exceptions and approvals.

© Copyright 2026 By UnityOne AI 

# Technical specifications at a glance

What the Cerne™ agent ecosystem connects, decides and executes.

| Area | Specification |
|---|---|
| **Agents** | FinOps, CloudOps, Database, Security, Patching, ITSM; plus custom agents and 100+ prebuilt workflows |
| **Models** | Private LLM or bring your own LLM; per-agent model and memory |
| **Triggers** | UnityOne events, alerts, tickets, policy and governance signals, schedules, maintenance windows, API calls, prompts |
| **Integrations** | ITSM (Jira, ServiceNow), SIEM and threat intelligence, CMDB, Qualys and vulnerability scanners, SCCM patch repositories, telemetry collectors, cloud APIs such as Azure Resource Manager |
| **Decision modes** | Auto, approval, escalate; notify, contain; defer; policy and maintenance-window aware |
| **Actions** | Delete or rightsize, auto-heal, scale, fix drift, tune databases, block or isolate, patch and roll back, resolve or provision, create incidents and change requests |
| **Governance** | Human in the loop, policy guardrails, audit trail, RBAC, continuous learning |
| **Execution** | MCP server with 300+ tools; UnityOne AI Copilot |

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 