FOR CTOS · VPS OF ENGINEERING · PLATFORM ENGINEERING

Codify Identity, Policy, and Governance Into One Control Plane

Your engineering org is already shipping agentic features faster than your governance model can keep up with. RuntimeAI's Control Plane codifies agent identity, MCP tool access, policy, and audit into one system — so security has a control plane and your teams still ship at speed.

500+ Governed Tool Integrations

Every agent tool call — database, API, SaaS, communication, code repo — passes through 6 layers of security enforcement.

THE PROBLEM

Governance Retrofitted After Launch Doesn't Scale

🧩

Fleet Visibility Gaps

Agent fleet health, shadow AI sightings, and MCP server status usually live in separate dashboards nobody checks together.

🔁

Retrofit Tax

Bolting policy, identity, and audit logging onto an agent after it's already shipped costs far more than building on governed scaffolding.

🦕

Security as a Bottleneck

Without a pre-approved policy path, every new agent becomes a manual security review that slows the whole team down.

WHAT RUNTIMEAI DOES

Ship Fast, Governed by Default

CAPABILITY	WHAT IT DOES
MCP Gateway	500+ tool integrations, 6-layer security (auth → policy → rate limit → DLP → audit → execution), per-tool per-agent access control
Pilot CLI	One command registers an agent, assigns a pre-approved policy Blueprint, activates governance — security approval is instant
Agent Builder Factory	Pre-governed agent scaffolding — policy inheritance, identity issuance, audit logging, and behavioral monitoring built in from the start
Agent Orchestration Factory	Real parallel/loop workflow execution for multi-agent pipelines — dependency-graph scheduling, cycle detection, concurrent execution
Policy Simulation	Test any policy change against 90 days of real historical traffic before it goes live — see exactly what would have been blocked
BYOM	Register your own proprietary MCP servers and apply the same 6-layer governance as the 500+ pre-built integrations

ONE VIEW, NOT FIVE DASHBOARDS

The CTO Executive Dashboard surfaces agent fleet inventory, shadow AI sightings, platform reliability (p95 latency, error rate, uptime), agent type distribution, and MCP server health — **one view**, not five separate tools.

Real orchestration, not a diagram: the Agent Orchestration Factory runs actual parallel and looped multi-agent workflows, with real dependency resolution and cycle detection — not a marketing description of what a workflow engine should do.

WHO THIS IS FOR

CTOs
Fleet-level reliability and architecture visibility, not per-agent firefighting

VP Engineering
Org-level velocity — security has a control plane, teams still ship at speed

Platform Engineering
One CLI to onboard an agent with governance already attached, not five manual steps

Integration Owners
Bring your own MCP server and inherit the same 6-layer governance as the 500+ built-in ones

WHY THIS MATTERS TO AN ENGINEERING LEADER

5-Minute Onboarding

One CLI command registers an agent, assigns a pre-approved Blueprint, and activates full governance coverage. No manual security review per agent.

Test Before You Ship

Simulate any policy change against real historical traffic before enforcement — eliminate the fear of a policy change breaking production.

Real Multi-Agent Orchestration

Parallel and looped execution across agent pipelines, dependency-resolved and cycle-detected — a real engine, live-verified, not a roadmap slide.

Try Pilot CLI

Onboard your first governed agent in about 5 minutes.

Roshan Shaik
Founder & CEO · RuntimeAI
roshan@runtimeai.io
www.runtimeai.io
calendly.com/roshan-runtimeai/30min