



Most enterprises can prototype AI agents in days. The gap is production: **agents that work in demos fail at scale due to missing governance, unreliable quality, and zero operational visibility.** Traditional DevOps and CloudOps platforms were built for deterministic code — not for agents that reason, use tools, spawn sub-agents, and call external models across trust boundaries. The result: fragmented tooling, compliance exposure, runaway inference costs, and no repeatable path from 60% demo to enterprise-grade service.

SOLUTION OVERVIEW

MajorDomo AgenticOps is the unified operational control plane purpose-built for enterprise AI. It covers the full spectrum — agent lifecycle, model routing & governance, LLM operations, and cloud infrastructure in a single federated platform. Security, observability, policy enforcement, and evals are built-in from day one: no stitched-together point solutions. Deploy on SaaS or fully air-gapped for data sovereignty requirements.

UNIFIED ENTERPRISE AI OPERATIONS PLATFORM

One platform, four disciplines — Agent Ops, AI Gateway, LLM Ops, and Cloud Ops unified under a single control plane, replacing fragmented point solutions across the AI operations stack with security and governance built in at every layer.

- >

Federated Director/Worker architecture — The Director enforces enterprise policy, budgets, and governance centrally; Worker nodes execute locally per team, region, or isolated environment
- >

Agent-level identity & access control — Every agent runs under workspace-scoped keys with RBAC and SSO enforcement; no shared credentials across workloads, no over-privileged execution
- >

Runtime security built in — Prompt injection detection, jailbreak protection, and PII/PHI redaction screen every request before it reaches a model, with tool-access controls and kill-switches for real-time intervention
- >

Full-stack observability — Session-level traces, agent reasoning visibility, cost attribution by team and workload, and real-time telemetry across every model call, tool invocation, and MCP interaction
- >

Immutable audit trail — Every action logged for compliance, forensics, and regulatory reporting across SOC 2, ISO 27001, and industry-specific frameworks
- >

Air-gapped & data-sovereign deployment — Full platform capability in fully isolated networks; no inference traffic, telemetry, or model weights touch the public internet



MAJORDOMO VALUE PROPOSITION

Product & Engineering Teams › Accelerated AI experimentation and delivery › Reduced operational complexity and cognitive overload › Focus on outcomes, not infrastructure plumbing	Platform & Security Teams › Centralized governance and operational control › Policy-driven security and guardrails by default › Standardized operations across all teams and envs	Leadership & Business › Faster and safer enterprise AI adoption › Predictable cost governance and visibility › Reduced enterprise and compliance risk		
4-in-1 AGENT, GATEWAY, LLM & CLOUD OPS UNIFIED	100% AGENT LIFECYCLE COVERAGE	Zero NO BESPOKE TOOLING REQUIRED	Air-Gap DATA-SOVEREIGN DEPLOYMENT READY	Evals OFFLINE & ONLINE EVALS INTEGRATED WITH CI/CD