Singulr AI

Runtime AI Governance for the Modern Enterprise

Control autonomous AI systems across your environment with real-time enforcement and outcome-based accountability.

AI is rapidly becoming embedded in core business operations, decision support, regulatory reporting, and third-party platforms. For most enterprises, AI is no longer a pilot initiative. It is becoming operational infrastructure.

Yet most governance models were built for deterministic systems, not probabilistic agents operating autonomously across cloud, SaaS, and enterprise environments.

Singulr is the **Enterprise AI and Agentic Control Plane** that delivers enforceable governance, measurable control, and independent assurance for AI systems and agentic workflows operating across your organization.

The AI Governance Challenge

AI introduces a structural shift in enterprise risk. Traditional access control and policy documentation do not translate cleanly into agent-driven environments. The result is a widening gap between what governance says should happen and what actually happens. That is the control gap.

Identity Without Accountability

AI agents execute under service accounts and machine identities. When an AI system influences a high-impact business or regulatory outcome, authentication logs do not answer the most important question: who owns the consequence?

Permission Sprawl in Complex Pipelines

AI workflows now span business data, operational systems, and third-party services. To preserve functionality, permissions expand. Least privilege degrades. Control models erode quietly.

Segregation of Duties Breaks Down

AI systems ingest data, generate analysis, trigger actions, and produce reports. There is often no clear separation between decision support and decision execution.

Risk Without Data Movement

AI does not simply move data. It transforms it. Summaries, embeddings, inferences, and aggregations create new forms of sensitive insight. Risk lives in the meaning produced, not just in the dataset accessed.

Governance That Stops at Deployment

Most AI governance is strongest at approval and weakest in production. Visibility tools observe. They do not constrain behavior. Policies on paper do not enforce themselves.

Security Absorbs What Governance Misses

Security teams have become the default owners of every AI problem, including the ones that should have been caught upstream. Without runtime enforcement, security ends up acting as a safety net for governance failures, drowning in preventable escalations instead of focusing on true adversarial risk.

The Singulr Unified Control Plane

Singulr operates through three tightly integrated runtime pillars, each encircled by the Singulr Assurance™ Layer, providing continuous intelligence and independent proof across your entire AI environment.

Powered by the Singulr Assurance™ Layer

Singulr Runtime Governance™
Define enforceable intent and risk thresholds across AI systems, agents, and cross-system interactions.

Singulr Runtime Control™
Translate governance into real-time enforceable boundaries across AI interactions and agentic execution paths.

Singulr Runtime Security™
Focus security on true adversarial behavior across AI systems and agents, reducing preventable escalation.

A Different Governance Model for AI

Singulr introduces a runtime governance layer designed around how AI and agentic systems actually behave in production. Instead of relying on access controls or post-incident analysis, Singulr enforces governance at execution and proves it with independent evidence.

Instead of relying solely on access controls or post-incident analysis, Singulr helps govern AI at execution.

Continuous AI Discovery and System of Record

Singulr creates a living inventory of AI across the enterprise: tools and copilots used by employees, autonomous agents and internal AI pipelines, embedded AI inside third-party platforms, and AI-to-AI interactions across systems.

Result: No shadow AI. No blind execution zones.

Runtime Enforcement, Not Just Observation

Traditional tools observe access. Singulr enforces governance. The platform measures whether controls are actually working at execution time, detecting behavioral drift, anomalous transformations, and execution patterns that exceed defined boundaries.

Result: Governance operates where risk emerges, at execution.

Capability Boundaries Instead of Permission Sprawl

Singulr lets organizations define outcome-based boundaries. Rather than asking only what a system can access, Singulr governs what it is allowed to do. Escalation triggers tie to impact thresholds.

Result: Containment replaces documentation.

Governing Transformation Risk

Derivative insight can be as sensitive as raw data. Singulr treats embeddings, summarizations, aggregations, and predictive outputs as governance events. Classification extends beyond data type to data effect.

Result: Strategic insight remains protected, even when transformed, reducing financial, regulatory, and reputational exposure that lives in the meaning produced, not just the data accessed.

Independent Assurance, Not Just Reporting

The Singulr Assurance™ Layer provides longitudinal, tamper-evident proof that AI controls are operating as intended. This is not reporting. It is verifiable evidence for governance teams, auditors, and regulators.

Result: Governance becomes provable, not assumed.

Outcome-Based Accountability

Singulr aligns AI oversight with enterprise risk categories: operational impact, safety exposure, regulatory non-compliance, financial harm, and reputational risk. Accountability lives at the leadership and operational level, not buried in access logs.

Result: Stewardship, not paperwork.

> *"As an innovation-driven company, we must move fast to harness the power of AI, but we can't do it blindly. Singulr provides the intelligence and guardrails that let us adopt and innovate with AI quickly and confidently, while continuing to protect our customers, employees, and company."*
>
> —Michael Armer,
> **Chief Information Security Officer, RingCentral**

About Singulr AI:

Founded in Palo Alto, California, Singulr is the Enterprise AI and Agentic Control Plane™ for the modern enterprise. The platform transforms AI governance from static documentation into enforceable, measurable runtime control, closing the gap between what governance says should happen and what actually happens across live AI systems and agentic workflows.

Enterprise IT, Security, Governance, and Risk teams can now scale AI adoption with confidence, backed by independent, tamper-evident proof that controls are operating as intended, all powered by Singulr Pulse™, the industry's leading AI risk intelligence system.

For more information, visit https://www.singulr.ai

We Put You In Control Of AI™