Discover, Govern, and Accelerate Enterprise AI

Protect Data, Ensure Compliance, and Manage Risk in Every AI Interaction

Your organization is already using AI across three fast-growing areas: in-house models and agents, public tools like ChatGPT and Cursor, and embedded features within SaaS platforms such as Grammarly, Notion, and Slack.

Many of these services operate without formal oversight, making it hard to balance rapid AI adoption with the security, compliance, and cost controls your business needs.

Singulr delivers complete visibility and control across the enterprise AI landscape, connecting written policy to live, contextual enforcement for safe, governed innovation at scale. It helps enterprises discover all AI activity, govern it intelligently, and accelerate adoption without compromising security or compliance.

Every AI interaction must be:

Transparent

Maintain full visibility into what AI service is in use, who is using it, and for what purpose across employees, partners, and AI agents.

Secure

Protect against data leakage, model training on sensitive information, prompt injection, and adversarial misuse.

Compliant

Align with evolving regulations (EU AI Act, NIST, ISO) and enforce security policies in real time.

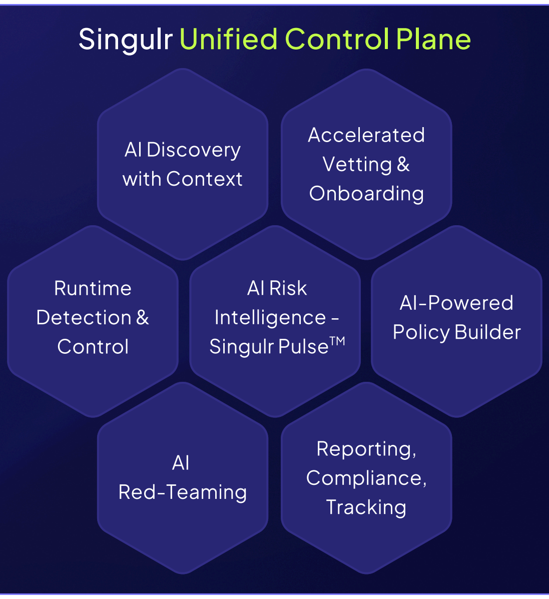
Auditable

Context-rich audit records to ensure compliance with internal governance teams, regulators, and auditors.

AI initiatives are raising urgent questions for enterprise leaders:

- How efficiently are new AI tools and projects vetted and onboarded?
- Where is sensitive data being accessed or processed by AI?
- Are employees exposing confidential data?
- What unsanctioned interactions are expanding our attack surface?
- Are AI agents or plugins triggering actions without oversight?
- How do embedded AI features affect compliance with GDPR, HIPAA, and the EU AI Act?

Singulr Unified Control Plane


AI Discovery with Context
Accelerated Vetting & Onboarding
Runtime Detection & Control
AI Risk Intelligence - Singulr Pulse™
AI-Powered Policy Builder
AI Red-Teaming
Reporting, Compliance, Tracking

Contextual AI Discovery

Singulr uncovers all AI models, agents, and services, including default-on AI features hidden inside SaaS tools, and maps their usage by department, user, and data flow. This includes third-party AI apps, in-house applications, MCP servers running in your environment, and even fourth-party processors used by your vendors.

Global AI Intelligence with Singulr Pulse™

Singulr Pulse maintains a continuously updated global directory of AI services, agents, and datasets, featuring in-depth metadata on domains, capabilities, compliance certifications, headquarters details, and other relevant risk factors.

Accelerated Vetting & Onboarding

Singulr combines intelligence (Singulr Pulse™) with automated research, continuous vetting, and context-rich reviews to speed up decision-making.

AI-Powered Policy Controls

Singulr turns policies into live, context-aware controls that can allow, guide, restrict, educate, redact sensitive prompts, or block interactions based on risk level and user role. Policies can also be translated and pushed to your existing enforcement systems, such as SASE, cloud security platforms, API gateways, and MDM, working seamlessly alongside Singulr's native controls.

Pre-Deployment AI Red-Teaming

Simulate targeted attacks on in-house applications, models, and agents using customizable scenarios that address responsible AI risks, adversarial threats, NIST guidelines, OWASP Top 10 vulnerabilities, and other regulatory standards.

Fine-Grained Runtime Detection & Control

Gain visibility into all AI usage, including user and department activity, PII/PHI exposure, file uploads, prompt content, copy-paste actions, account types, and MCP-based services.

Reporting, Compliance, & Tracking

Singulr centralizes AI usage, risk, and compliance reporting with complete change history. This enables faster audit preparation, supports defensible compliance reporting, and gives stakeholders clear visibility into AI adoption trends, policy enforcement outcomes, and risk reduction over time.

Singulr is Integration First by Design:

- **Extensible**: works across diverse environments, no vendor lock-in
- **Accelerates time-to-value**: cuts onboarding from weeks to hours
- **Maximizes ROI**: connects with your existing identity, security, compliance, and DevSecOps tools

Integrated with tools you may already use:

- **Identity & Access**: Okta, Azure AD
- **Cloud & Infra**: AWS, Azure, GCP
- **Security Stack**: SIEMs, DLPs, endpoint security
- **AI Platforms**

List above is not exhaustive

> *"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**

To learn more about how Singulr helps you drive AI innovation with control, book a demo at: singulr.ai/request-a-demo