Singulr AI

Discover Every AI Interaction In Your Enterprise

Eliminate blind spots. Close the control gap. Build the foundation for enforceable AI and agentic governance at scale.

Why AI Discovery Is Critical

AI adoption is accelerating across teams, tools, and agentic workflows. Most organizations underestimate usage by 3-5x, creating blind spots that widen the gap between governance policy and what's actually happening across live AI systems and autonomous agents.

- AI assets span diverse platforms, services, agent frameworks, multi-cloud deployments, and LLMs.
- Agents now run on endpoints and inside cloud platforms, often outside traditional asset inventories.
- Signals originate from multiple sources, including AI assets, network activity, identity logs, agent traces, code scans, and container registries.
- Agentic systems act autonomously across systems, invoking tools and triggering downstream actions in ways governance frameworks were never built to anticipate.
- Vendors embed AI into traditional software, often enabled by default and outside formal review.

Key Capabilities

Singulr contextual discovery delivers actionable insights by pairing AI activity with the context that matters for governance, enforcement, and assurance, enabling continuous, correlated, and context-aware AI discovery at enterprise scale.

- **Agentic Discovery Across Platforms and Endpoints:** Surface agents running on centralized and cloud platforms, plus endpoint-installed agents like Claude Desktop, Clawdbot, and IDE assistants, including their tool invocations and downstream system impact.
- **User & Usage Context:** Understand who is using each AI tool or agent, from which accounts, and for what purpose, across internal models, public AI, embedded SaaS features, and autonomous workflows.
- **Sensitive Data Exposure:** Detect how PII, PHI, or proprietary data is exposed through prompts, file uploads, or agent tool invocations.
- **Vendor & Agent Intelligence:** Rich context on third-party services and agent providers, including origin, hosting, regulatory posture, training practices, and subprocessors.
- **MCP Server & Connector Discovery:** Surface MCP servers, AI plugins, connectors, and integrations running in your environment, including the cross-system actions they enable and the data they touch.

Singulr Discovery delivers full-spectrum AI visibility

Homegrown AI

Detect internal LLM apps, agents, MCP servers, and their data flows across environments.

Public AI & Agentic Tools

Identify copilots, browser extensions, chat interfaces, and endpoint agents across both personal and corporate accounts.

Embedded AI in SaaS

Surface native AI features inside trusted tools like Microsoft 365, Slack, Notion, and Zoom. Detect AI subprocessors, default-on settings, and usage behaviors.

Enterprise Impact

Singulr Discovery delivers immediate visibility and governance alignment across your AI footprint, feeding the entire control plane:

- Maintain a complete, real-time inventory of AI models, tools, agents, embedded modules, and endpoint-installed agentic tools.
- Eliminate shadow AI and personal account usage of enterprise data.
- Identify high-risk AI applications, agents, and users before they create exposure.
- Faster vetting and onboarding of AI vendors, agents, datasets, and features.
- Audit-ready evidence to support governance and compliance frameworks.
- Comply with standards like ISO 42001, EU AI Act, and NIST AI RMF, which require real-time AI inventory.

About Singulr AI:

Founded in Palo Alto, California, Singulr AI is the Unified AI Control Plane™ for the agentic enterprise, turning AI governance into enforceable, measurable runtime control. Powered by Singulr Pulse™, Singulr helps IT, Security, Privacy, and Risk teams accelerate AI innovation across the full adoption lifecycle.

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