Preventing AI Agent Sprawl: An Executive Guide to AI Management

By Boomi

Agentic artificial intelligence (AI) is the focus for every executive looking to future-proof their organization. With ambitious AI mandates from the CEO and board, the stakes are high. The risks of falling behind include losing a competitive edge, not meeting customer expectations, and missing out on the scalability and efficiency that AI promises.

Business executives know implementing agentic AI is more complex than a simple switch. Still, the momentum is undeniable. Gartner estimates that 33% of enterprise software applications will include agentic AI functionality – an increase from less than 1% in 2024. Deloitte also reports that 26% of organizations are exploring autonomous agent development. AI agents are rapidly reshaping industries and workflows. But as they proliferate with a growing number of AI vendors, causing agent sprawl and multiplying digital complexity, one pressing question remains:

Who governs them?

This is where AI management plays a pivotal role. It creates a responsible path to delivering AI value while maintaining security and compliance.

What Is AI Management?

AI Management is a new, emerging market category driven by the rise of AI agents. The term refers to the strategic oversight and optimization of AI agents throughout their lifecycle, from development and deployment to governance and maintenance, ensuring secure and seamless integration into business and technical workflows. It aligns AI initiatives with business goals while promoting ethical and responsible AI use.

As AI agent adoption grows across industries, so does agent sprawl. This refers to the proliferation of AI agents from different providers operating within your business. It's a looming problem that can lead to increased digital complexity and costly AI security failures. Managing these AI agents effectively is crucial to preventing sprawl and maintaining robust control. Key aspects of AI management include lifecycle management, governance, and risk mitigation. These proactive measures enhance the reliability of AI systems, reducing reputational, security, and compliance risks while building trust and confidence in AI agents.

How Do I Get Started With AI Management?

Here are five practical steps to cultivate an agentic AI mindset and adopt AI management solutions within your business:

Stay Informed

The speed of AI technologies is unprecedented. Seek to understand the evolving developments in agentic AI as well as the compliance and regulatory landscape. Executive leaders don't need to become technical or legal experts. However, having a basic understanding will help inform your thinking and strategy to guide your teams toward the future.

Assess Current State

Evaluate your infrastructure – data, applications, APIs, and AI systems – to determine where you are on your AI readiness journey. Remember, helpful AI agents are grounded in trusted data. In addition, assess your team's AI expertise to determine whether a skills gap exists to find an appropriate tool and level of support for them.

Develop Your Strategy

In partnership with line-of-business leaders, set clear business goals and understand associated risks. Balance stakeholder demands for AI initiatives and prioritize action items based on a risk-benefit analysis. While the title may differ depending on the size and structure of your organization, your chief AI officer, head of AI, CIO, or head of integration can guide the team through strategy formulation and spearhead new AI initiatives.

Select the Right Platform

Explore and evaluate AI management solutions to ensure you know your options. Take a strategic approach to your selection process to avoid additional technical debt when adding an AI stack. Choose a platform that addresses both your current state and long-term vision. Also, look for a provider with a track record of consistent innovations. That kind of provider will be well-positioned to become your innovation partner.

Implement and Iterate

Start small with a pilot project. The solution you choose should automatically help your team quickly develop and deploy AI agents that meet business needs while enabling you to monitor progress and mitigate risk without additional, unnecessary work required by your busy team.

How Do I Evaluate AI Management Solutions?

Choosing the right solution is essential for maximizing the return on your AI investments. Effective AI management should possess these key capabilities:

Trust Boomi to Ensure Data Quality

Lifecycle Management

You'll need a way to efficiently manage the entire AI agent lifecycle, from development to maintenance to retirement. At a minimum, your AI management solution should provide built-in templates, tools, and guardrails so that you can scale responsible AI agent development and worry-free deployment. Integrating AI agents into existing business processes and applications should be as seamless as possible.

Governance

Centrally registering AI agents from different third-party providers to govern the agents and their activities provides full transparency across the entire ecosystem. Your AI management solution should include agent lineage, tracing the origin and ownership of each agent, and visually displaying their relationships.

Risk Mitigation

Monitoring agent activities with an easily understandable metrics dashboard reduces the likelihood of rogue agents that might expose your organization to increased operational risks. A practical solution should identify standard patterns and deviations in AI agent behaviors, preventing potential security and compliance failures.

What Are the Benefits of AI Management?

Investing in effective AI management unlocks a range of key benefits, such as:

Simplicity

Streamlined AI agent development and deployment allow you to support various use cases for every business area without having deep technical AI experience. Also, low-code AI solutions are cost-effective for organizations with limited budgets, lowering learning curves for AI agent creators while providing customization options to meet business demands.

Improved Productivity

Empowering your teams with intuitive templates and tools allows them to create unique AI agents that improve their workflows. Democratizing access to agentic AI capabilities can reduce effort across the business, freeing up valuable time to focus on other strategic priorities.

Increased Trust

It's crucial that AI agents behave reliably, responsibly, and securely while meeting regulatory and compliance requirements. AI management explains agent behaviors to help users understand how they arrive at decisions. It also enforces pre-defined operational guardrails. Grounding AI agents in enterprise data increases their contextual understanding and reduces hallucinations.

Reduced Risk

AI management provides 360-degree visibility into AI agents across your entire ecosystem, helping mitigate problems associated with AI development and deployment. These risks include data breaches, shadow IT (using or creating AI without IT approval), and the loss of money and reputation that can arise from security breaches and an inability to meet regulatory compliance. AI management also proactively detects and addresses potential issues and errors. This minimizes the impact of unintended consequences such as leaked confidential information or compliance violations.

The rise of AI agents unlocks enormous business opportunities but also poses significant risks. AI management is the key to successfully navigating this new landscape, keeping everything under control while providing a sustainable path to deliver long-term business benefits.

Learn more about Boomi's groundbreaking AI management solution at boomi.com/ai