IBM

The Case for an Enterprise Agentic AI Platform: Orchestrating the Future of Work with Agentic Applications
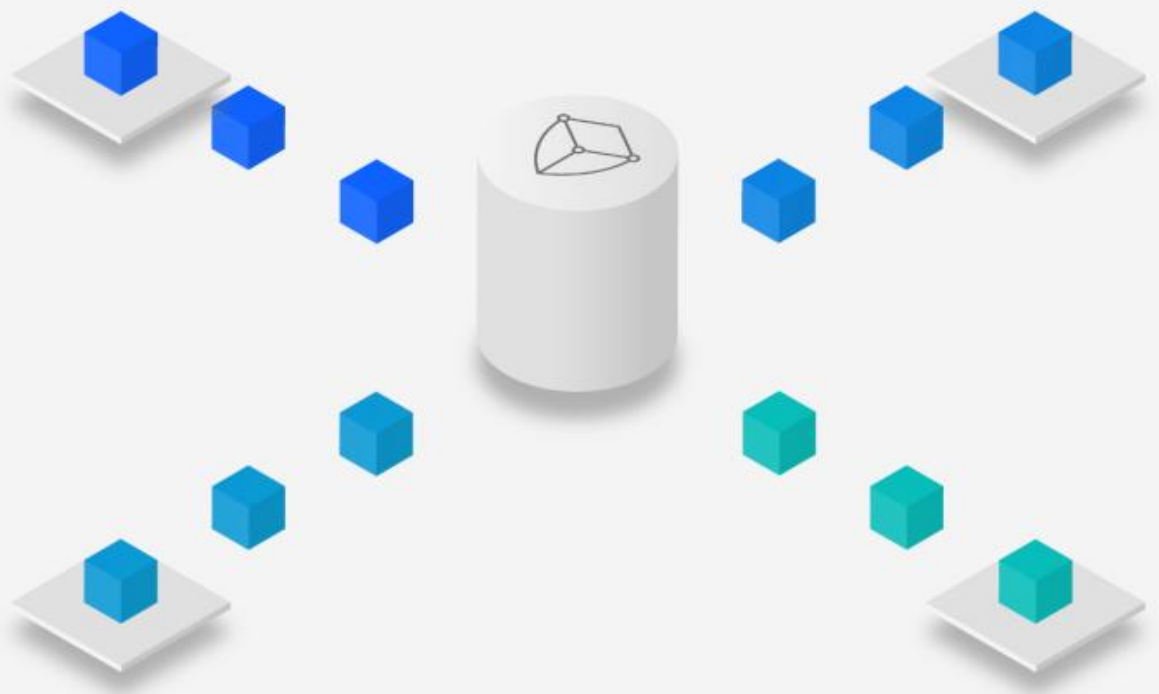
July 2025

IBM

Table of contents

Executive Summary

The enterprise is at the precipice of a seismic shift, moving beyond simple automation to an era of autonomous, intelligent action. This new frontier is powered by AI agents: sophisticated software that can reason, plan, and execute complex, multi-step business processes. Every major software and cloud provider, from SAP and Salesforce to AWS and Azure, is racing to embed these agents into their platforms, promising to redefine productivity across the business processes they support.

This creates both a monumental opportunity and a critical challenge. The opportunity is to create Agentic Applications, cohesive, end-to-end solutions that automate entire workflows, from finance to procurement, HR, supply chain and others, by orchestrating teams of specialized agents. These applications promise to solve long-standing "process, data, and technical debt" that has prevented AI from delivering value at scale.

The challenge, however, is a coming tsunami of complexity. Left unmanaged, the proliferation of siloed agents from different vendors will create a chaotic, insecure, and inefficient "digital workforce."

Enterprises that wish to harness this transformation successfully must invest in a dedicated Enterprise Agentic AI Platform. This platform serves as the central "operating system" and "control tower" for building, deploying, and governing all agentic activity. It provides the architectural backbone to orchestrate workflows across a heterogeneous mix of agents, whether they are embedded in your SAP ERP, part of your Salesforce CRM, or custom-built on a cloud platform like AWS, Azure or Google.

This point of view outlines the market dynamics driving this need, details the challenges of a fragmented approach, and makes the case for a unified platform. We will illustrate the power of this approach with concrete use cases in Finance and Supply Chain and provide a blueprint for the essential capabilities such a platform must possess. For business leaders, the message is clear:

> The race for competitive advantage will be won not by the company with the most agents, but by the company that can orchestrate them most effectively

Our AI Integration Services team at IBM Consulting is entirely focused on helping clients realize the full potential of Agentic AI by orchestrating and integrating end-to-end workflows across systems, platforms, and agents. Through our IBM Consulting Advantage for Agentic Applications platform, we provide the architectural backbone, governance tools, and pre-built application templates needed to scale Agentic Applications across core business functions. This IBM Consulting Advantage for Agentic Apps offers both the ease of use and productivity needed to scale your agentic AI, and empowers your technical and business leaders to adopt it confidently.

The new competitive frontier: Agent-Driven Business Transformation

For years, the promise of AI in the enterprise has been one of incremental gains, automating isolated tasks or providing analytical insights. The recent advancements in Generative AI and large language models (LLMs) has shattered this paradigm, ushering in an era of Agentic AI. This represents a quantum leap in business productivity, moving from AI assistants that merely respond to AI agents that take action autonomously.

These are not simple chatbots or scripted bots. An AI agent is a "digital coworker", an autonomous collaborator that can proactively execute business tasks by interacting with data, systems, and other agents. The vision shared by technology leaders is an AI-powered workforce that understands business context, collaborates across departments, and learns continuously.

This transformation is already underway. Every major enterprise software and cloud provider is racing to become the leading platform for delivering AI agents. They recognize that the true value lies not in a single, monolithic AI, but in orchestrating multiple, specialized agents to achieve automation at unprecedented speed and scale.

The Impact on Business Workflows

The implications for end-to-end business workflows are profound. Agentic AI promises to bridge the silos that have long plagued enterprise operations. Complex processes that once took hours or days of manual coordination across departments can be completed in moments by a team of collaborating agents.

> We are moving from systems of record and insight to "systems of intelligence" where AI agents act autonomously to orchestrate workflows across the entire enterprise.

Consider a few examples already in practice:

A billing dispute that typically requires hours of back-and-forth between finance, sales, and support teams can be resolved in seconds by an agent team that automatically analyzes the invoice, reviews customer communications, and processes the correction.

In customer service, a fully agentic application can autonomously resolve complex, multi-intent queries—such as tracking an order delay, issuing a refund, and updating the customer profile—without escalating to a human agent. It draws on multiple systems (CRM, logistics, billing) and coordinates actions across channels, significantly improving first-contact resolution and customer satisfaction.
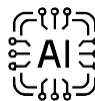
In IT and HR support, AI agents are delivering significant productivity gains and reducing operational costs by resolving a high percentage of service inquiries instantly and autonomously.

It is predicted that AI agents could soon handle a significant portion of the most-used business tasks within major ERP environments, offloading a vast amount of routine work from human employees. This is not merely automation; it is the re-engineering of work itself. We are moving from systems of record and insight to "systems of intelligence" where AI agents act autonomously to orchestrate workflows across the entire enterprise. Businesses that master this new operating model will gain a formidable competitive advantage in efficiency, agility, and customer experience.

The Platform land grab:
a double-edged sword

Recognizing this massive opportunity, technology vendors are aggressively positioning their platforms as the central hub for enterprise AI agents. This has led to a crowded and dynamic competitive landscape, creating a double-edged sword for enterprise leaders. On one hand, powerful new tools are becoming available; on the other, the risk of fragmentation and lock-in is growing.

The key players fall into two major categories:

1. **Enterprise Application (SaaS) Providers:** the giants of enterprise software, SAP, Salesforce, Oracle, and ServiceNow are embedding agentic AI deeply into their core platforms to automate processes within their domains.

◆ Joule	**SAP's Joule** is positioned as a "conductor" native to its vast ecosystem, orchestrating teams of agents across finance, supply chain, and HR. Its strength lies in leveraging decades of contextual business process data stored within SAP systems, giving its agents high efficacy for ERP-centric tasks.
Agentforce	**Salesforce's Agentforce** approaches from the customer-facing side, offering an "autonomous AI" for sales, service, and marketing teams built on its rich Customer 360 data. Salesforce emphasizes a robust "Trust Layer" and customization, allowing companies to bring their own AI models while benefiting from its governance framework.
servicenow.	**ServiceNow's AI Platform** stands out by leveraging its powerful workflow engine. Its strategy focuses on orchestrating not only its own agents but also third-party agents, using its "AI Control Tower" and "AI Agent Fabric" to manage and connect agents from any source across IT, HR, and customer service domains.
ORACLE	**Oracle** is integrating AI agents into its Fusion Cloud Applications to automate and optimize processes across finance, HR, and supply chain. Its focus is on embedding intelligent assistants and agents natively into its applications, leveraging its Redwood UX and unified data model to deliver consistent and contextual decision support across business functions.

2. **Hyperscale Cloud Providers:** the cloud giants, Microsoft, AWS, and Google view agentic AI as a natural extension of their cloud services, offering flexible frameworks for building and deploying custom agent solutions.

	Microsoft's Azure AI Foundry is an "AI factory" providing a unified platform to build, deploy, and manage agentic applications at scale. Its strengths are its deep integration with the Microsoft 365 and Power Platform ecosystems and an open-source-friendly SDK (Semantic Kernel) that supports multi-agent coordination.
	Amazon's Agents for AWS Bedrock appeals to developers by offering a managed service that simplifies the creation of agents that can execute multi-step tasks across company systems. It emphasizes ease of use, security, and tight integration with the broader AWS ecosystem, allowing agents to use AWS Lambda functions as tools to perform actions.
	Google Cloud leverages its leadership in AI research and state-of-the-art models (like Gemini) through platforms like Vertex AI. While its unified agent platform marketing has been less direct, its tools provide powerful capabilities for building agents that can use tools and integrate tightly with Google Workspace.

Each vendor wants to be the primary platform for managing an organization's digital workforce While this competition drives innovation, it confronts the enterprise with a critical strategic question:

> How do you prevent this explosion of capability from becoming an explosion of complexity?

The orchestration dilemma: a coming tsunami of complexity

The rise of agentic AI presents a powerful opportunity, but also a fundamental paradox. The very trend meant to dissolve process silos is, if left unchecked, is going to create a new and more insidious layer of fragmentation. As AI agents proliferate across SaaS applications, cloud platforms, and internal development teams, organizations face a looming orchestration crisis.

Without a unifying strategy, enterprises will soon find themselves with:

– SAP Joule agents managing finance and supply chain processes
– Salesforce Agentforce agents handling customer service workflows
– ServiceNow agents automating IT and HR operations
– Custom agents built in-house on platforms like Azure, AWS, or GCP to address specific business needs

Each of these ecosystems offers powerful capabilities, though they operate in silos, with their own tools, governance models, and orchestration logic. This fragmented agent landscape leads to a chaotic digital workforce that is difficult to manage, secure, scale, and govern.

This fragmentation raises a set of critical challenges:

1. Cross-Platform Orchestration:
There is no native way to orchestrate workflows that span across different agent platforms. How do you ensure agents from SAP, Salesforce, and AWS can coordinate actions, share context, and maintain transaction integrity while handling asynchronous communication, retries, or escalations?

2. Security, Control, and Monitoring:
Each platform comes with its own approach to access control, observability, and compliance. Enterprises must figure out how to centrally enforce role-based access, ensure auditability, apply guardrails, and monitor agents acting across different systems with varying levels of visibility and maturity.

3. Vendor Lock-In and technical incompatibility:
As vendors embed agents deeper into their platforms, the risk of lock-in to proprietary orchestration models, Agentic Tools and and APIs increases. Enterprises may find it difficult or sometimes even impossible to replace or extend agents, leading to brittle architectures and limited flexibility to evolve their automation strategy.

4. Inconsistent Data Context and Memory:
Without a shared data backbone, agents lack unified access to business context and history. This limits their ability to reason across functions or learn from previous interactions, making intelligent cross-domain orchestration nearly impossible.

5. Fragmented Governance:
Enterprises are left without a single control plane to manage agent behavior, apply usage policies, conduct evaluations, or ensure regulatory compliance across their entire digital workforce.

In short, enterprises risk rebuilding the very silos Agentic AI was meant to dismantle, only this time with LLMs and agents rather than legacy code and workflows.

Moreover, the technologies in this domain are evolving at an accelerating pace, making it challenging for organizations to keep up. This rapid change leaves them consistently at a crossroads, questioning whether new developments are fleeting trends or fundamental shifts requiring serious consideration.

To truly unlock Agentic AI's transformative potential, organizations must look beyond adopting individual agents. Instead, they must invest in a unified platform that provides end-to-end orchestration, robust governance, and seamless interoperability. Such a platform will cut through complexity to build a cohesive automation fabric, while remaining flexible enough to adapt to emerging technologies and the evolving technical landscape."

The strategic imperative: Why Adopt an Enterprise Agentic AI Platform

The proliferation of AI agents embedded across enterprise platforms is not enough to deliver transformational value. The strategic opportunity lies not in adopting individual agents, but in enabling a new class of intelligent solutions: Agentic Applications. These are not simply add-ons to existing processes; they represent a fundamental shift in how enterprise workflows are architected, executed, and experienced.
To make Agentic Applications real and scalable, enterprises must invest in a dedicated Enterprise Agentic AI Platform, a foundational control layer that allows organizations to design, orchestrate, govern, and continuously evolve agent-powered workflows across a fragmented and multi-vendor environment.

What Is an Agentic Application?

An Agentic Application is a reimagined, AI-native business workflow that spans systems, platforms, and organizations. It introduces a new application architecture designed around three core principles:

1. A New User Experience for Work
The traditional UX trapped inside ERP or CRM systems is replaced with a generative, conversational interface tailored to the user's role and context. Employees interact with the Agentic App through natural language, embedded directly in the tools they already use; Teams, Slack, Outlook, without switching contexts or navigating legacy screens.

2. An Orchestrated Workflow of Agents and Logic
Behind the scenes, the business process is executed by a blend of autonomous AI agents and deterministic logic, orchestrated securely across multiple systems, e.g., SAP, Salesforce, AWS, internal APIs. The orchestration dynamically routes tasks, manages dependencies and agent communication, and handles exceptions in real time.

3. Intelligent Context from Data Products
The workflow is grounded on governed Data Products that provide both operational inputs and contextual memory. These data artifacts ensure that agents and assistants have access to accurate, real-time, and trusted information to make decisions and take action.

In short, Agentic Applications are not about injecting AI into yesterday's processes, they are about designing a new kind of process, with a new experience, executed by a new digital workforce.
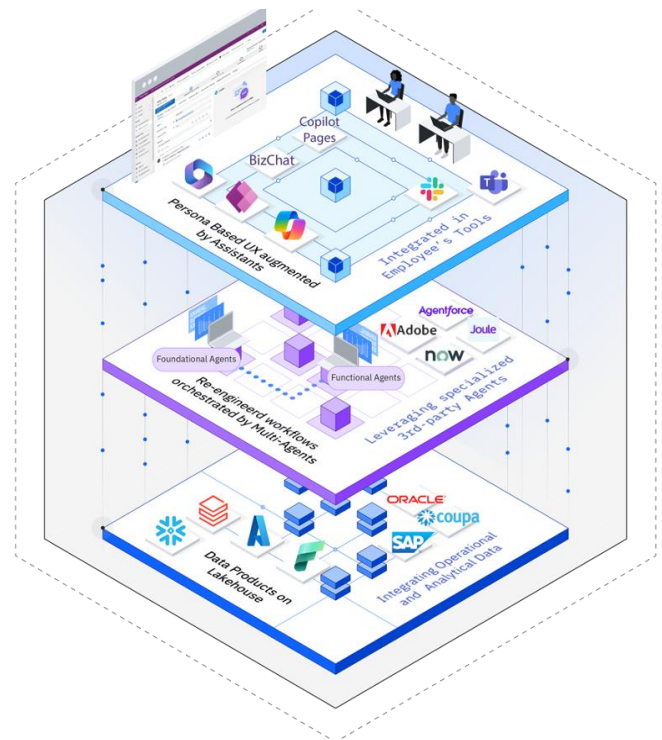
Why an Enterprise Agentic AI Platform is essential

Building such Agentic Applications is not possible with traditional tools or isolated agent environments. Only a purpose-built platform can address the orchestration, security, governance, and integration challenges outlined in the previous section.

The Enterprise Agentic AI Platform acts as the control plane for this new application layer. It provides:

1. Cross-Platform Agent Orchestration:
A unified engine to coordinate agent teams across vendor platforms (e.g., SAP Joule, Salesforce Agentforce, Azure Foundry), ensuring coherent workflows, reliable execution, and policy-based handoffs.

2. End-to-End Governance and Trust:
Centralized controls for authentication, access, observability, auditability, and human-in-the-loop escalation, ensuring secure and compliant deployment of autonomous agents.

3. Interoperability across vendor silos:
Open standards (e.g. MCP and A2A) and integration frameworks to prevent vendor lock-in, enabling enterprises to mix and match agents, models, and systems as their needs evolve.

4. A scalable Fabric for Agentic Apps:
Tools, templates, SDKs, and lifecycle management capabilities that let teams build, deploy, and iterate on Agentic Applications efficiently and safely across business domains.

5. Data Product Creation and Integration:
Embedded capabilities to define, govern, and integrate Data Products that serve as contextual memory and decision inputs for agents. These modular, reusable data assets provide real-time, trusted information across systems—enabling AI agents to reason effectively and act with precision in complex workflows.

Without such a platform, Agentic AI becomes a fragmented collection of disconnected tools. With it, enterprises can finally transform their business operations, not by incrementally improving legacy processes, but by designing intelligent, dynamic, and secure workflows that redefine how work gets done.
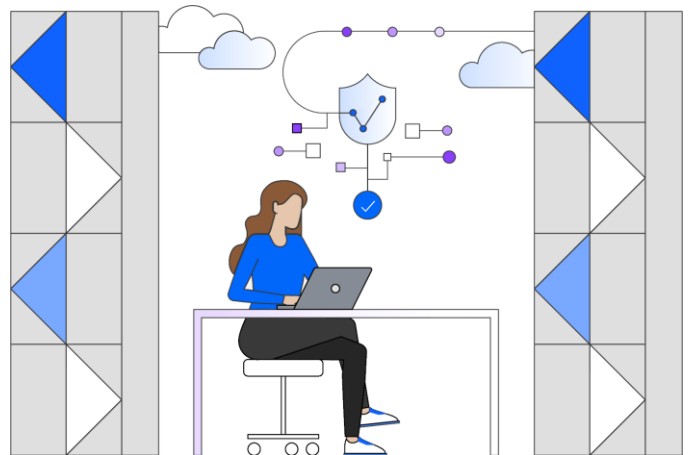
Agentic Apps in Action: Finance, Supply Chain, Talent, Operation and many more

To illustrate the power of an Enterprise Agentic AI Platform, consider the following examples of real-world, cross-functional workflows. These Agentic Applications demonstrate how enterprises can orchestrate specialized AI agents across platforms like SAP, Salesforce, ServiceNow, AWS, Azure, and Google Cloud to reengineer critical business processes. By integrating data, context, and automation, these use cases showcase how Agentic AI can unlock speed, accuracy, and scale across complex decision-making workflows.

Use Case 1: Autonomous Procure-to-Pay Anomaly Resolution (Finance)

Process:

A critical finance process is resolving discrepancies between purchase orders (POs), goods receipts, and supplier invoices. This traditionally requires significant manual effort from the accounts payable (AP) team.
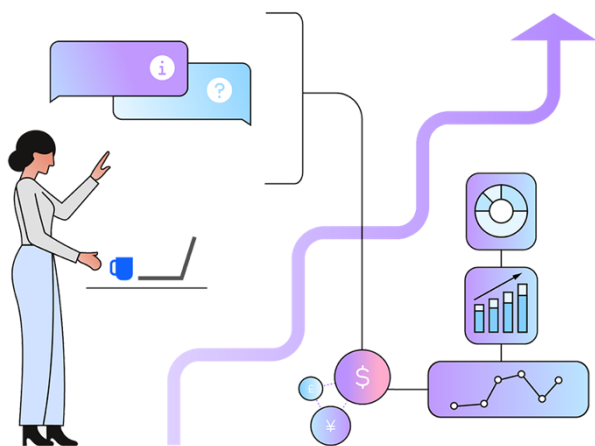
Agentic App Workflow:

1 A custom "Invoice Ingestion Agent" built on AWS Bedrock continuously monitors an inbox for supplier invoices. Using LLMs, it extracts invoice data and matches it against PO data pulled from SAP S/4HANA via a tool accessed through MCP.

2 The agent detects a mismatch: an invoice for $10,000 where the PO was for $9,500 due to an unapproved freight charge.

3 Instead of just flagging it for a human, the Bedrock agent triggers a specialized SAP Joule "Dispute Resolution Agent". This agent queries the SAP system to confirm the PO terms and checks if the goods receipt was logged correctly.

4 The Joule agent confirms the PO did not include freight. It passes this information back to the Bedrock agent.

5 The AWS Bedrock agent, now with full context, orchestrates the final steps: it drafts an email to the supplier rejecting the invoice and citing the specific discrepancy, creates a task in the AP team's workflow tool for tracking, and logs the entire interaction for audit purposes.

Use Case 2: Intelligent Talent Mobility & Retention (HR)

Process:

Large organizations struggle to proactively retain top talent and mobilize skilled employees across business units. Decisions on internal job transfers or retention bonuses typically involve fragmented processes across HR systems, managers, and finance controllers.

Agentic App Workflow:

1 An agent on SAP SuccessFactors continuously monitors employee engagement signals, performance reviews, and attrition risk indicators. When a potential flight risk is detected, it triggers a "Talent Retention Agent."

2 The SAP agent queries open internal roles across geographies and matches them with the employee's profile and aspirations, also referencing skills taxonomies managed on a third-party learning platform (e.g., Degreed or Workday).

3 A custom Azure-based AI agent pulls compensation benchmarks and initiates a review with the compensation planning team, while an orchestration agent manages approvals from HRBP and business leaders via Microsoft Teams.

The entire process, from detection to personalized retention offer, is completed autonomously with human-in-the-loop checkpoints and full audit logging across systems.

# Use Case 3: Regulatory Change Impact Analysis (Legal & Risk)

Process:

Legal and compliance teams must assess how new or updated regulations (e.g., data residency, ESG reporting, sectoral requirements) affect enterprise operations, contracts, and policies.

Agentic App Workflow:

1 A Google Vertex AI-powered Regulatory Intelligence Agent continuously monitors government portals and legal databases for updates.

2 Upon detecting a new regulation, the agent triggers a Legal Review Agent that uses and agentic RAG (retrieval-augmented generation) to assess affected clauses in contracts stored in a SharePoint repository and linked to metadata in a Salesforce contract management system.

3 A ServiceNow agent creates compliance tasks, assigns responsibilities, and initiates approvals across business units.

The app provides a unified dashboard showing which business functions are at risk, what updates are in progress, and which contracts need renegotiation.

These use cases are just simple examples to illustrate the core value of an Enterprise Agentic AI Platform: it enables seamless orchestration of agents across platforms (e.g., AWS and SAP), provides governed access to shared data and business context, and ensures that autonomous actions are executed securely, audibly, and in the right business flow. Without such a platform, this multi-agent workflow would remain siloed and unscalable, trapped within the limitations of individual vendor ecosystems. The platform turns a one-off automation into an enterprise-grade Agentic Application
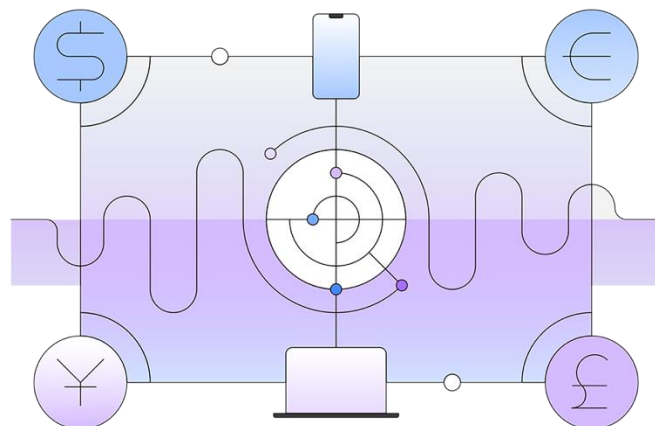
Blueprint for Success: Key Capabilities of an Enterprise Agentic AI Platform

To power the kind of cross-functional Agentic Applications described above, an Enterprise Agentic AI Platform must provide a cohesive set of capabilities. It is not a single product, but a holistic architecture designed for orchestration, governance, and scale. The following image provides a high-level overview of an Enterprise Agentic AI Platform Architecture.
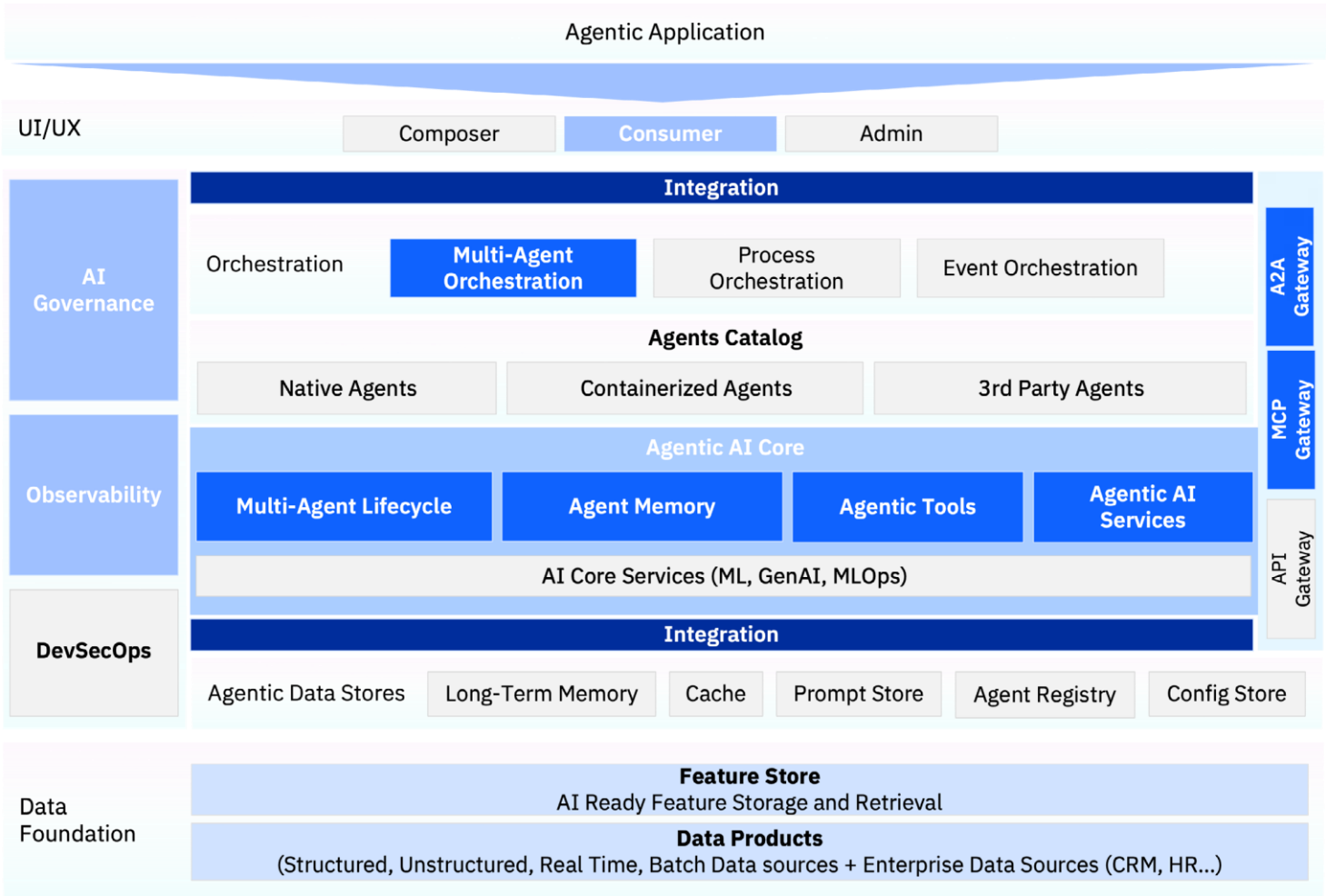
The essential components include:

A Unified Orchestration Engine

Definition:
The orchestration engine is the core runtime of the platform. It coordinates the execution of complex workflows involving both autonomous agents and deterministic systems. It manages sequencing, routing, task decomposition, data flow, and communication across agents operating in different environments.

Key Capabilities:
– Multi-agent orchestration: manage collaborative tasks between foundational and functional agents.
– Task decomposition and planning: break complex goals into structured, sequenced steps.
– Deterministic + AI agent integration: orchestrate both rule-based logic and autonomous agents in one flow.
– Cross-platform execution: bridge execution across SAP, Salesforce, AWS, ServiceNow, etc.
– Execution controls: manage timeouts, retries, error handling, escalation logic.
– Embedded governance: enforce security policies, access controls, evaluation checkpoints, and audit logs.

Value Provided:
The orchestration engine enables reliable, scalable execution of cross-functional workflows, turning fragmented AI agents into a cohesive automation fabric. It ensures that actions are taken in the right order, with the right context, by the right agent, under full enterprise control. This is the backbone for realizing Agentic Applications at scale.

A Centralized Agent Catalog

Definition:
As AI agents multiply across vendors and internal teams, the Agent Catalog becomes the enterprise's system of record for AI agents. It provides a unified registry to manage all available agents, whether built in-house, sourced from third-party SaaS platforms, or provided by cloud vendors.

Key Capabilities:
– Unified, searchable registry of agents from across platforms (SAP, Salesforce, Azure, AWS, internal)
– Rich metadata management: task type, interface, owner, status, version, dependencies
– Version control and lifecycle tracking (e.g., draft → tested → approved → deprecated)
– Usage telemetry and performance metrics for each agent
– Support for Agent-to-Agent (A2A) communication protocols, including:
  • Agent Cards: declarative metadata about what the agent can do, its input/output formats, and security requirements
  • A2A Server: enables secure discovery, negotiation, and communication between agents
  • Collaboration templates: predefined workflows for multi-agent task orchestration
– Role-based publishing, approval, and deprecation workflows

Value Provided:
The Agent Catalog prevents duplication, sprawl, and unmanaged agent usage by offering a single source of truth. It enables reuse, simplifies compliance, and accelerates the delivery of new Agentic Applications by making agents discoverable, trustable, and composable across teams and platforms.

An Agentic Application Builder

Definition:

The Agentic Application Builder is the end-to-end design and development environment within the Enterprise Agentic AI Platform. It enables teams to create cross-functional Agentic Applications by composing user experiences, workflows, agents, and data logic into a single, coherent solution.

Why It's Needed (and Why SaaS Isn't Enough):

While tools like SAP Joule, Salesforce Agentforce, or ServiceNow Studio provide agent creation and configuration capabilities, they are tightly bound to their respective platforms. They are ideal for domain-specific automations, but cannot or struggle to support:

– Workflows that span multiple enterprise systems
– Interoperability across vendor ecosystems
– Central governance of agents and apps
– Integration with enterprise-wide Data Products

To deliver end-to-end Agentic Applications, enterprises need a vendor-agnostic, platform-level builder that can integrate and orchestrate agents from across the stack, including those from SaaS, cloud, and internal teams.

Key Capabilities:

– Low-code/no-code environment to compose workflows involving AI agents, APIs, and deterministic logic
– Visual orchestration canvas to map out agentic workflows across SAP, Salesforce, ServiceNow, and custom cloud agents
– Agent discovery and reuse via integration with the Central Agent Catalog
– Configuration of GenAI-powered UX, embedded into collaboration tools like Teams, Outlook, or Slack
– Pre-built agentic templates for common processes (e.g., dispute resolution, onboarding, order fulfillment)
– Integration of Data Products as context and memory providers for workflow accuracy
– Native support for MCP and A2A protocols
– Cross-platform execution: bridge execution across SAP, Salesforce, AWS, ServiceNow, etc.
– Execution controls: manage timeouts, retries, error handling, escalation logic.
– Embedded governance: enforce security policies, access controls, evaluation checkpoints, and audit logs.

Value Provided:

The Application Builder provides the enterprise-scale abstraction layer needed to standardize how Agentic Apps are created—regardless of underlying agent technologies. It allows organizations to scale development beyond siloed platforms, reduce redundant effort, and ensure all applications conform to shared security, UX, and governance policies.
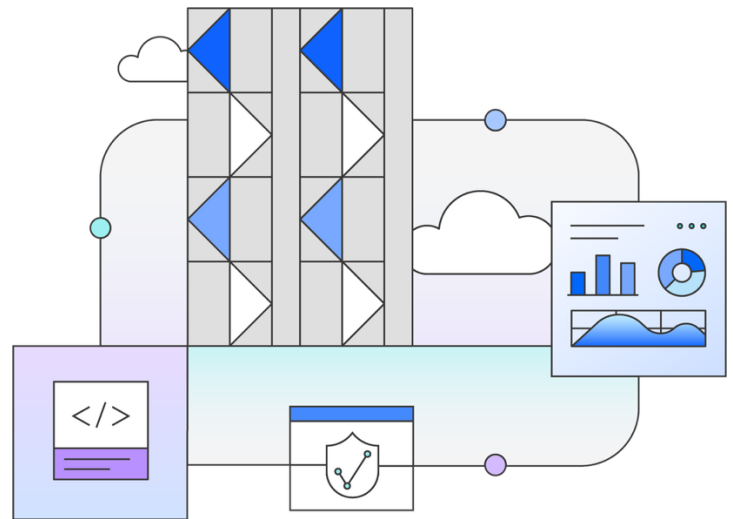
A Comprehensive AgentOps

Definition:
AgentOps is the comprehensive framework and set of tools for managing the entire lifecycle of AI agents, from design, build, and deployment to monitoring, control, and continuous improvement. It provides the enterprise-grade rigor needed to develop reliable, secure, and performant agents at scale.

As AI agents evolve from isolated proofs of concept to mission-critical digital workers, enterprises need structured processes and tooling to ensure they are built safely, deployed consistently, and operated with full governance. Without a robust AgentOps capability, organizations risk introducing fragmented, poorly performing, or non-compliant agents into production environments.

Key Capabilities:

Design & Build
– Templates and SDKs for foundational and functional agents
– Integration with internal and external tools for skill/function packaging (e.g., RAG, API connectors, deterministic logic)
– Agent Cards for standardized metadata, capability declaration, and interoperability

Deploy
– Promotion workflows from dev → staging → prod
– Versioning, rollback, and compatibility management
– Integration with Agent Catalog, MCP Gateways and A2A Server

Run & Monitor
– Real-time observability (latency, success rate, confidence scores, agent interactions)
– Alerting and diagnostics for failure patterns or drift

Evaluate & Improve
– Evaluation benchmarks (accuracy, relevance, bias, hallucination)
– Human feedback capture and fine-tuning triggers
– Continuous improvement pipelines

Govern & Control
– Role-based access and permissions
– Guardrails, output validation, and action constraints
– Full audit trail of agent behavior and decisions

Value Provided:
AgentOps ensures that every Agentic Application along with the agents used to transform the workflow, is built and deployed with efficiency, confidence, control, and accountability. It enables organizations to move from ad-hoc development to repeatable, industrialized agent production, ensuring quality, compliance, and performance at scale.
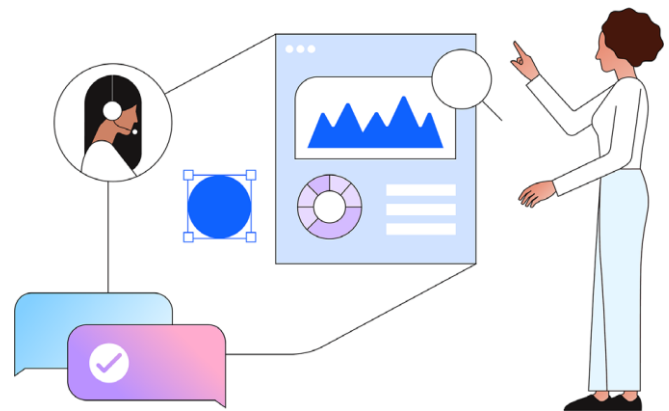
An Enterprise Data Foundation and Integration

Definition:

The data foundation is the intelligent fabric that connects AI agents and workflows to the enterprise's most valuable resource: its data. It provides structured, governed, and reusable Data Products that serve as both memory and context for agent decision-making, across systems, business domains, and time.

Agents are only as effective as the context they operate with. Without access to clean, trusted, and timely data, they hallucinate, make incorrect decisions, or break business logic. More critically, in cross-platform workflows (e.g., Salesforce + SAP + app built on AWS), agents need shared state and understanding, a challenge that traditional data lakes, warehouses, or API calls alone cannot solve.
The Enterprise Agentic AI Platform addresses this by embedding a data abstraction layer built around domain-specific Data Products, accessible to agents, assistants, and deterministic logic alike.

Key Capabilities:

– Data Product Layer: Modular, governed data components (e.g., Purchase Order, Customer Profile, Case History) exposed as reusable assets
– Context Injection: Real-time delivery of data snippets to agents to ground actions in business context
– Support for Advanced Retrieval: Integration with Retrieval-Augmented Generation (RAG), vector databases, and enterprise search
– Knowledge Graphs & Memory Stores: For long-term agent memory, relationship awareness, and personalized workflows
– Data Governance & Trust: Lineage, masking, access controls, and SLA enforcement

Value Provided:

This component ensures agents have the right data, in the right format, at the right time—without relying on brittle system-specific queries. It creates a shared memory layer that spans platforms, fuels reasoning, and reduces redundancy, while enforcing governance, security, and consistency across workflows.

A robust Governance, Observability and Security Layer

Definition:

This layer provides the enterprise-wide control plane for enforcing governance, compliance, and security across all agentic activity, spanning users, agents, data, and workflows. While AgentOps governs individual agent behavior at runtime, this layer establishes the global guardrails for how agents are deployed, accessed, and audited across the organization. It ensures the platform aligns with enterprise policies and regulatory requirements from day one.

Key Capabilities:

– Centralized policy enforcement for data privacy, action restrictions, region constraints, etc.
– Role-based access control and identity propagation for agent actions (e.g., inheriting user context)
– Platform-wide observability dashboards (security, usage, policy violations)
– Integrated FinOps tools to track:
  • Per-agent and per-application LLM/API usage
  • Cost attribution by workflow, team, or business unit
  • Budget thresholds, alerts, and optimization insights
– Audit logging and traceability for compliance reporting
– Integration with enterprise IAM, SIEM, and cost management platforms

Value Provided:

This layer ensures that Agentic AI operates not only safely and compliantly—but also transparently and efficiently. By embedding FinOps into governance, enterprises can scale agent usage while controlling cost exposure, avoiding budget overruns, and making informed design decisions.

An Open Standards and Integration Framework

Definition:
This component ensures the platform is open, interoperable, and future-proof, supporting standard APIs, agent-to-agent (A2A) protocols, and enterprise integration frameworks like the Modular Composition Platform (MCP) to compose workflows across heterogeneous systems and tools.

It prevents vendor lock-in and enables agents from different ecosystems, SAP, Salesforce, Azure, AWS, and internal apps to interact securely and meaningfully. By leveraging MCP and A2A standards, enterprises can compose complex, cross-platform workflows with confidence, flexibility, and governance.

Value Provided:
It gives enterprises the architectural freedom to scale agentic automation across platforms and time—ensuring continuity, control, and strategic independence.
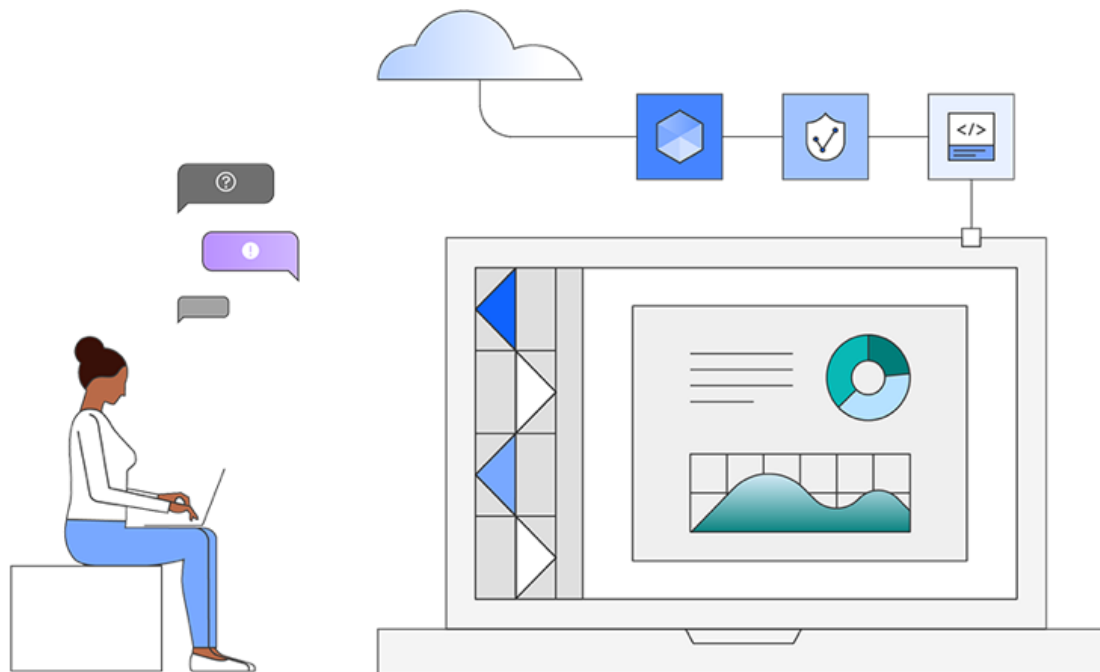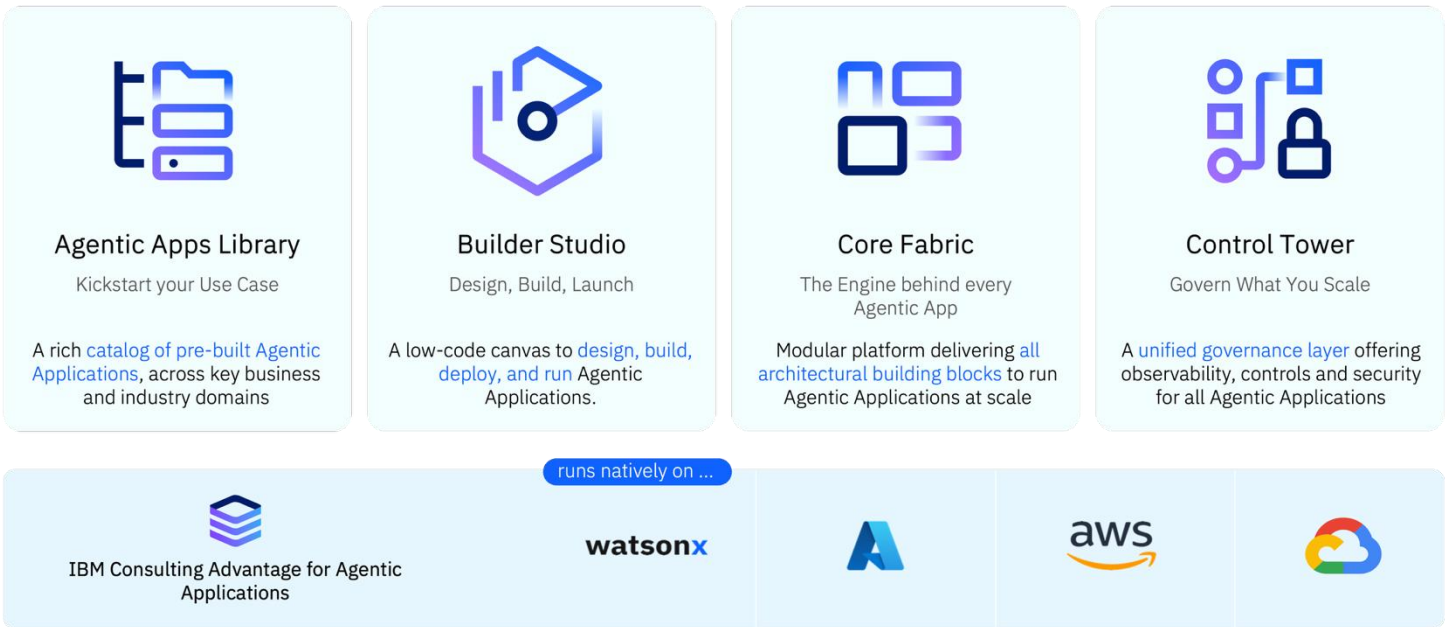
Powering the Enterprise Agentic AI Platform with IBM Consulting Advantage for Agentic Applications

Together, all these components form the architectural backbone of an Enterprise Agentic AI Platform. They are not optional features, they are essential capabilities that enable organizations to design, deploy, and govern agentic applications at scale. By establishing this foundation, enterprises can move beyond isolated agent pilots to create a secure, interoperable, and future-ready automation fabric that drives real business transformation.

Our IBM Consulting Advantage for Agentic Applications is the execution engine for building the Enterprise Agentic AI Platform. It provides the full lifecycle tooling across design, orchestration, governance, and observability needed to create, run, and scale Agentic Applications. Built to work natively with leading hyperscaler platforms and open standards like A2A and MCP, it accelerates the path from concept to enterprise-grade automation.

The following image provides a high-level overview of the key components of IBM Consulting Advantage for Agentic Applications.

Agentic Apps Library
Kickstart your Use Case

A rich catalog of pre-built Agentic Applications, across key business and industry domains

Builder Studio
Design, Build, Launch

A low-code canvas to design, build, deploy, and run Agentic Applications.

Core Fabric
The Engine behind every Agentic App

Modular platform delivering all architectural building blocks to run Agentic Applications at scale

Control Tower
Govern What You Scale

A unified governance layer offering observability, controls and security for all Agentic Applications

runs natively on ...

IBM Consulting Advantage for Agentic Applications — watsonx — Azure — aws — Google Cloud

Conclusion: Orchestrating Your Future

The era of agentic AI is no longer a distant vision; it is a present-day reality and the next major driver of competitive differentiation. We have moved beyond simple automation into a world where autonomous, collaborative "digital workers" can execute complex, end-to-end business processes with superhuman speed and efficiency.

However, this transformation comes with a critical mandate for enterprise leaders. The proliferation of powerful but siloed agent offerings from every major software and cloud vendor threatens to create a new layer of fragmentation and complexity, undermining the very value it promises to deliver. A strategy of simply acquiring disparate AI tools is destined to fail.

The path to scalable success lies in orchestration

The strategic imperative is to invest in a comprehensive Enterprise Agentic AI Platform. This platform is the essential control plane for the modern enterprise, providing the architecture and governance needed to build, deploy, and manage a cohesive digital workforce. It is the factory for creating Agentic Applications, transformative solutions that re-engineer workflows by harmonizing the actions of agents built and deployed on any platform to a unified, intelligent system.

This approach allows you to:

– Overcome Complexity: Tame the chaos of a multi-vendor agent landscape with a single point of control and orchestration.
– Ensure Governance and Trust: Deploy autonomous agents with confidence, knowing their actions are secure, compliant, and auditable.
– Drive Scalable Value: Move beyond isolated pilots to industrialize AI-driven automation across every business function.
– Future-Proof Your Enterprise: Build an agile, interoperable automation fabric that can adapt and evolve as AI technology advances.

For business and technology executives, the time to act is now. Leading this transformation requires a holistic vision and a strategic investment in the foundational platform that will enable organizations not just to use AI agents, but to orchestrate them into a powerful force multiplier for achieving the most critical business goals.

About the authors

Francesco Brenna
VP & Senior Partner
Global Leader AI Integration Services

IBM Consulting

Rabeela Janorious
IBM Distinguished Engineer
Global CTO AI Integration Services

IBM Consulting