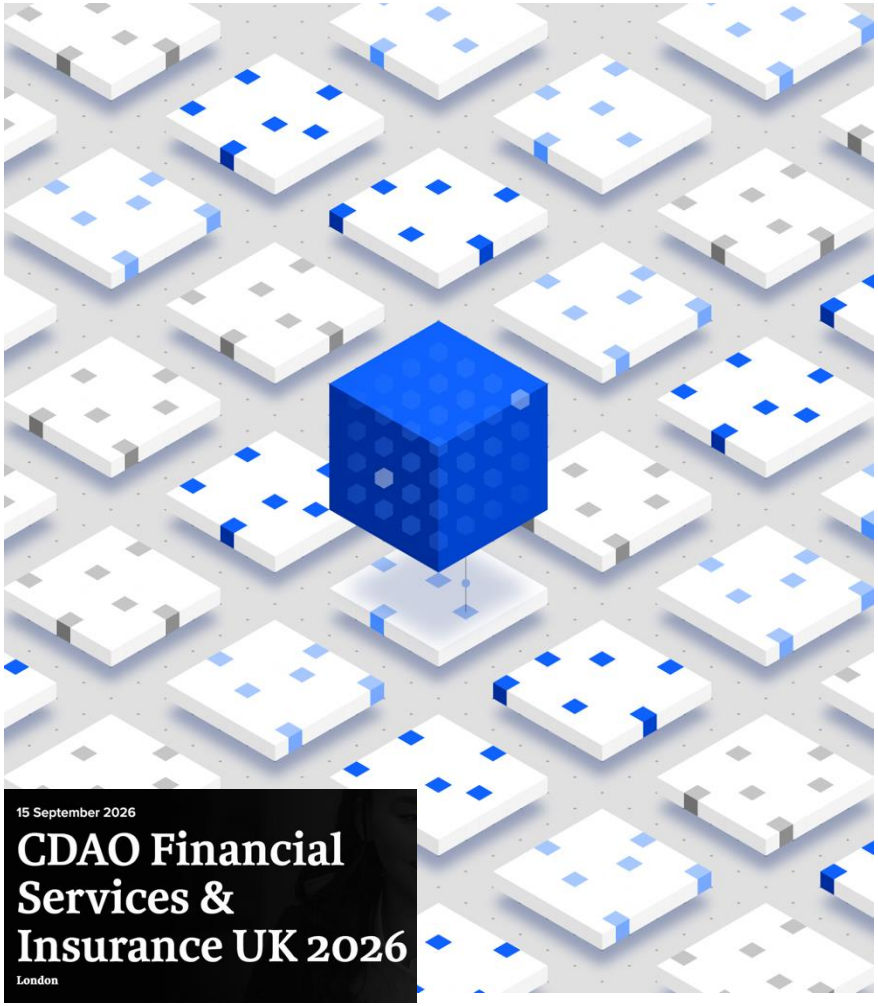
Putting in the right foundations required for successful AI adoption



Rob Woods
AI Platform Architect, IBM Technology

Tuesday 15th September 2026



Company data can provide a significant strategic advantage

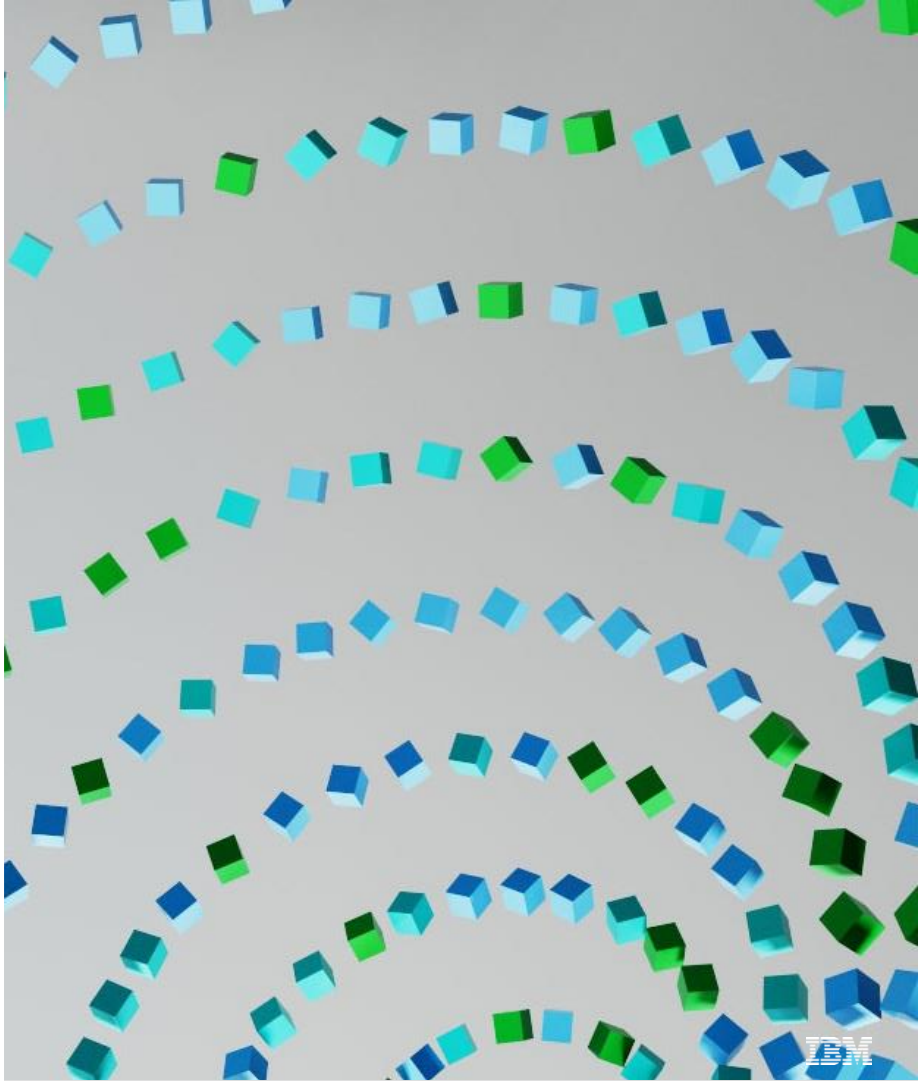
72%

of CEOs go so far as to say that their **company data** is key to **competitive advantage** and **unlocking the value** of AI.

but **only**

26%

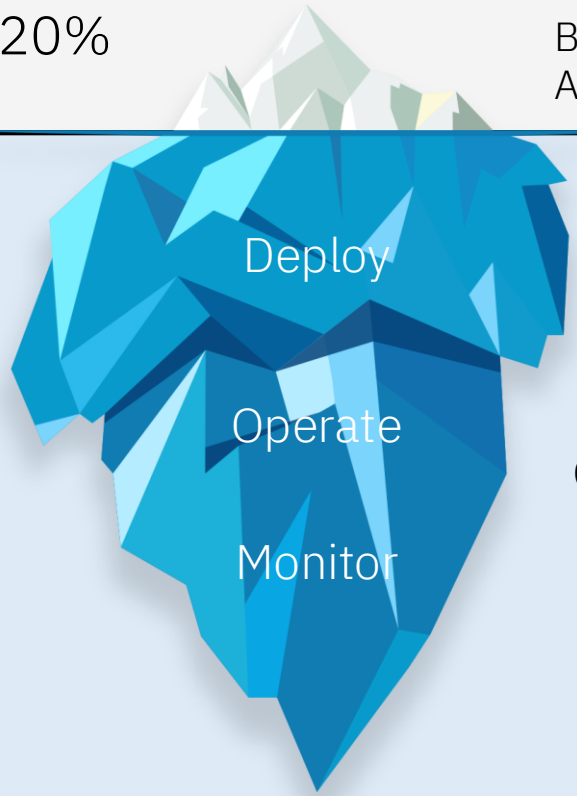
of CDOs are confident their data capabilities can support new AI enabled revenue streams



Building AI agents is just the beginning....

20%

Building AI Agents

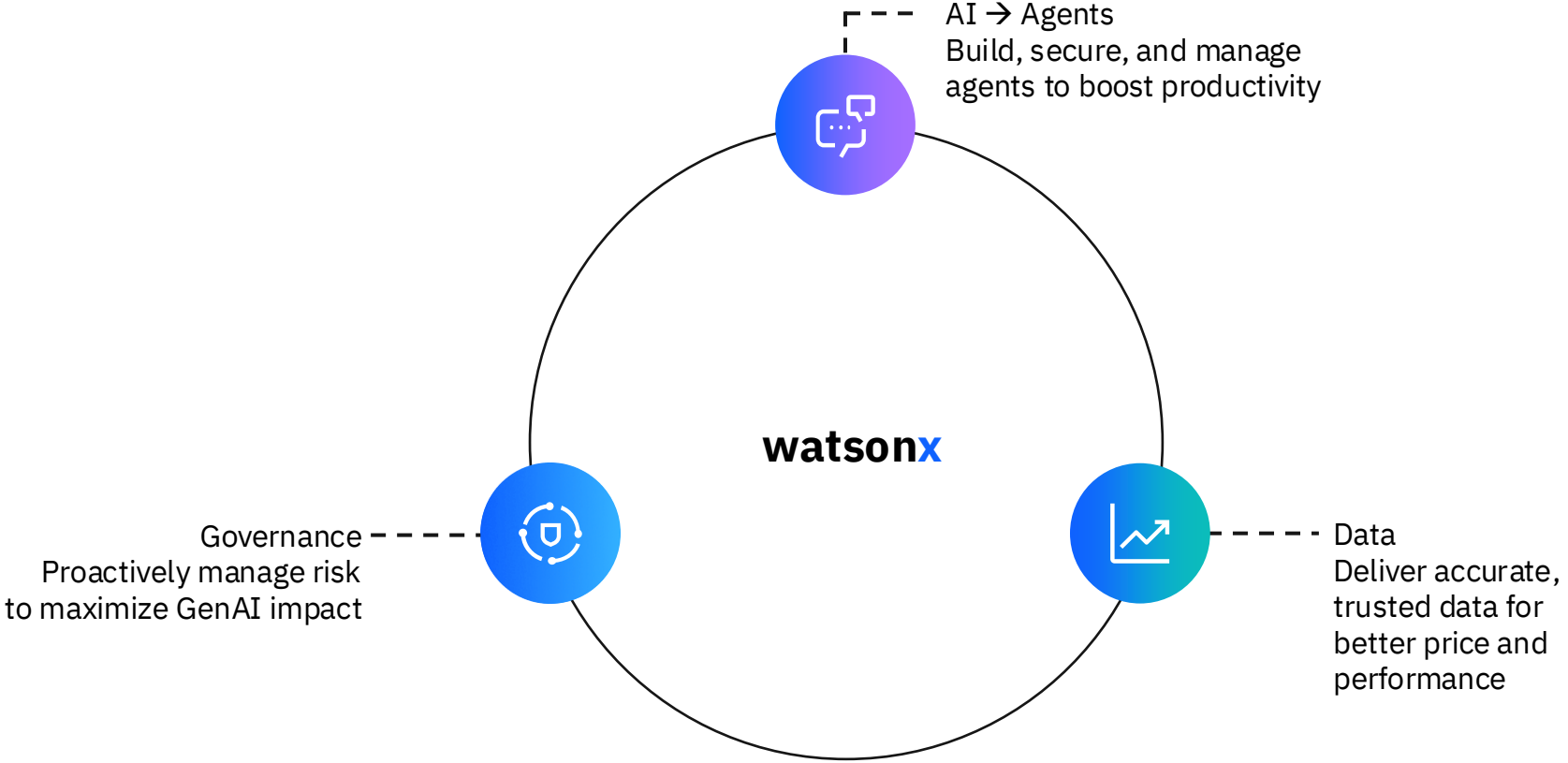


80%

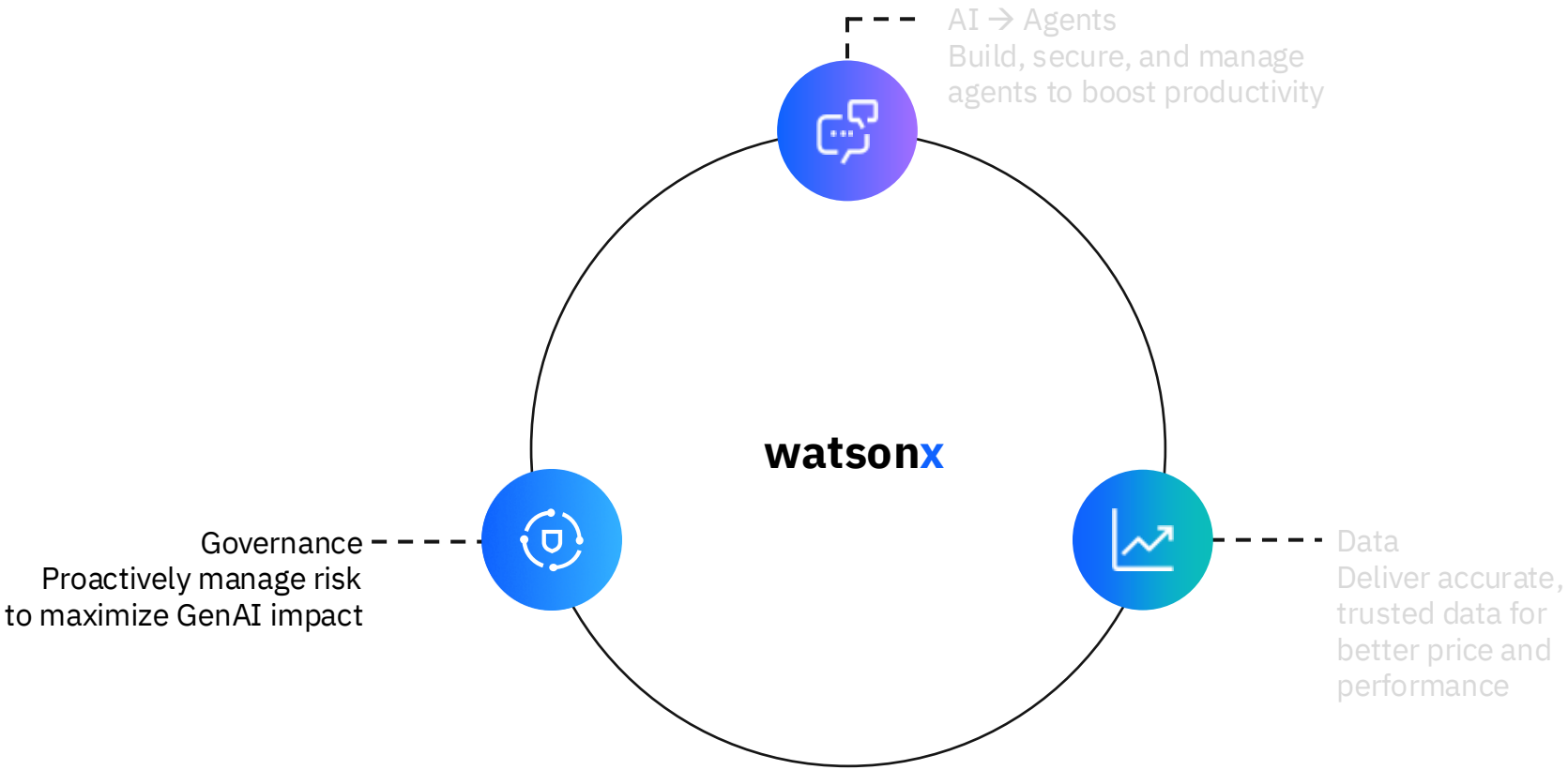
Control Plane

- Integration with back-end systems
- Evaluations & Deployment
- Monitoring & Observability
- Governance & Compliance
- Security & Access control
- Performance optimization
- Multi-agent coordination
- Continuous improvements

watsonx


AI → Agents
Build, secure, and manage agents to boost productivity
watsonx
Governance
Proactively manage risk to maximize GenAI impact
Data
Deliver accurate, trusted data for better price and performance

watsonx


AI → Agents
Build, secure, and manage agents to boost productivity
watsonx
Governance
Proactively manage risk to maximize GenAI impact
Data
Deliver accurate, trusted data for better price and performance

watsonx.governance

One unified, integrated AI Governance platform

Lifecycle Governance

Govern across the AI lifecycle. Automate and consolidate tools, applications and platforms. Capture metadata at each stage and support models built and deployed in 3rd party tools.

Risk Management

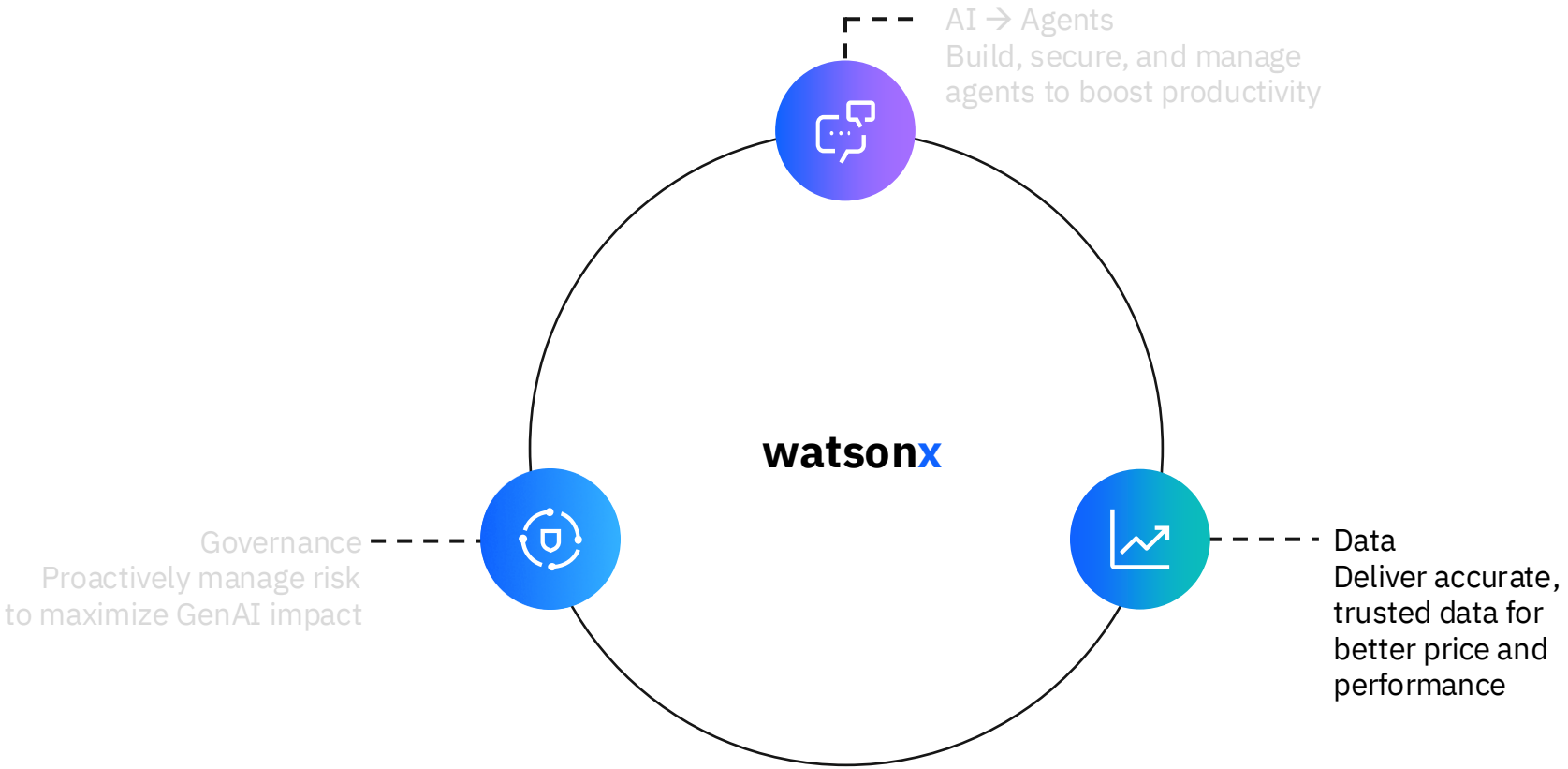
Manage risk and protect reputation by automating workflows to ensure quality and better detect bias and drift.

Regulatory Compliance

Adhere to regulatory compliance by translating growing regulations into enforceable policies.

Accelerate responsible, transparent and explainable AI

watsonx

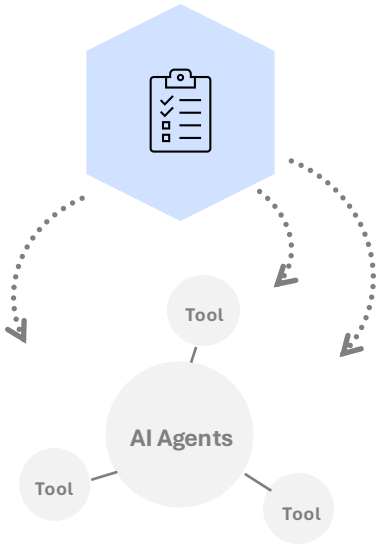

AI → Agents
Build, secure, and manage agents to boost productivity
watsonx
Governance
Proactively manage risk to maximize GenAI impact
Data
Deliver accurate, trusted data for better price and performance

What we're building and what it solves for our customers

Vision and Strategy for the Agentic Era: own the domain of governance and metadata management inside every enterprise through autonomous tools.

Data Compliance

CDOs are finding data compliance becoming increasingly complex and enforced by regulators.

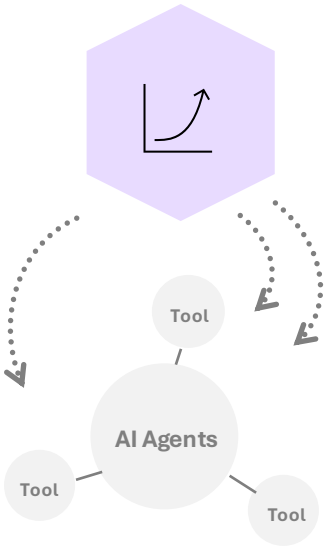


Market
Mature market - 3 major players (IBM, Informatica, Collibra)

Use Cases
Data Governance, Data Lineage, and Data Quality

AI-Ready Data

Data teams are tasked with driving 30%+ increase in organizational productivity through AI.



Market
Fast-growing and dynamic (Microsoft, AWS, Google)

Use Cases
AI-Ready Data

Pillars of the Strategy

Hybrid
Fully supporting on-premises, multi-cloud, and SaaS deployments across hybrid data estates.

Open
Integrating seamlessly across open ecosystems of products, tools, and agents.

AI Infused
Driving AI-powered automation to boost productivity across every interaction.

What the context layer must encode

Components of Context:

1

Meaning

Semantics + Relationships
Relevance and Accuracy grounded in Enterprise Reality
Context tied to a specific Business situation

Definitions, calculation logic, and authoritative glossary terms. Entity connections and cross-system mappings.

2

Trust

Lineage + Governance
Explainability and Auditability
Why did the agent make the decision it did, where it got the information and how it reasoned ?

Data origin and transformation history – enables audit. Sensitivity, compliance rules, and access – travels with the data.

3

Reality

Freshness + Signals
Realtime Temporal Reasoning
“what is true now,What changed recently, What is historically true”

Quality scores, pipeline health, and real-time reliability context.

Context must be machine-readable, governed, and delivered at inference time.

Data Intelligence: an AI transformation from static memory to reasoning and action



Autonomous data product creation

Agents discover, prepare, package, and ensure data meets quality and governance standards



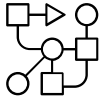
Automatic data quality issue remediation

Agents write data quality checks and resolve quality violations



Governance policy to enforcement

Written policy documents transform into executable data protection and quality rules



Auto data lineage documentation

Agents dynamically identify gaps of data pipeline documentation and augment their resolution

© 2025 IBM Corporation

Event driven Architecture

1 **Discover and catalog data in motion**
Continuously harvest metadata from streaming data stores and enterprise systems to create a shared catalog of trusted, discoverable data assets.

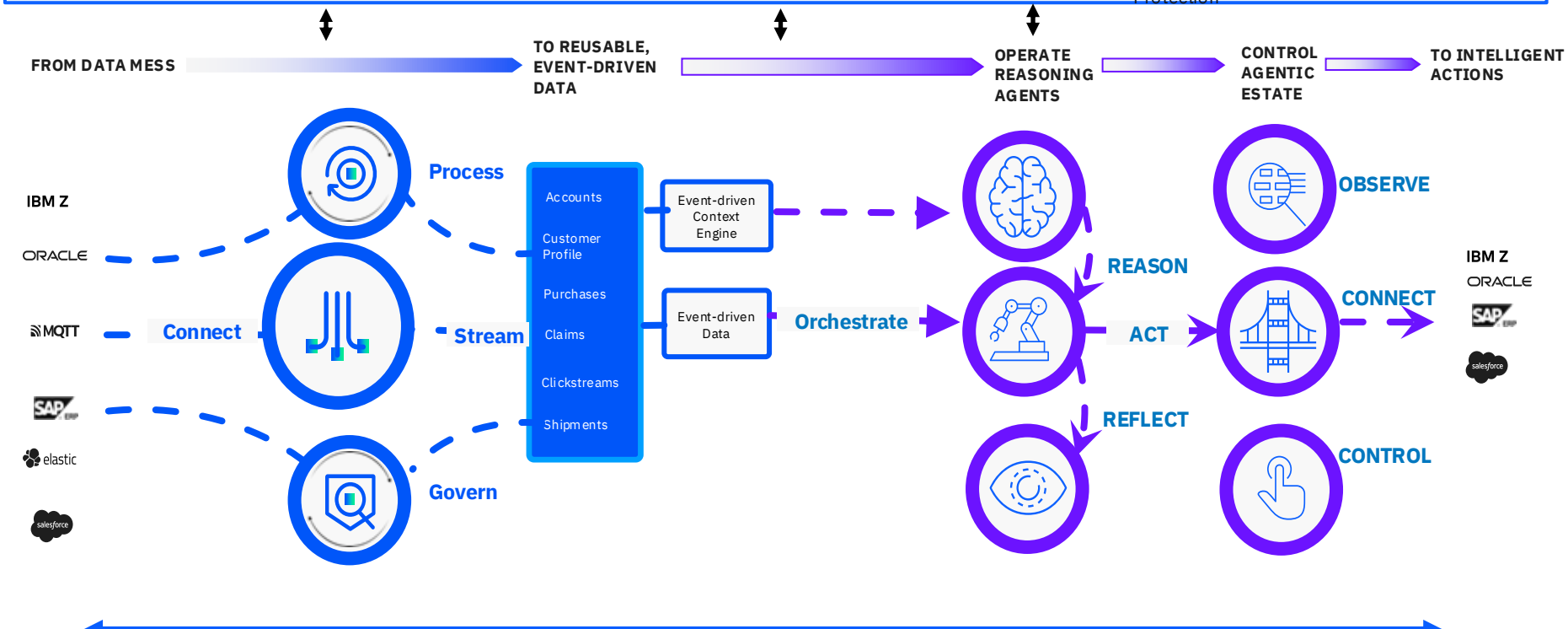
2 **Apply lineage, quality and policy controls**
Provide end-to-end lineage, automated data quality monitoring, and consistent policy enforcement across data.

3 **Deliver trusted, reusable data products**
Enable teams to find, understand and confidently use governed data products across analytics, AI and operational systems.

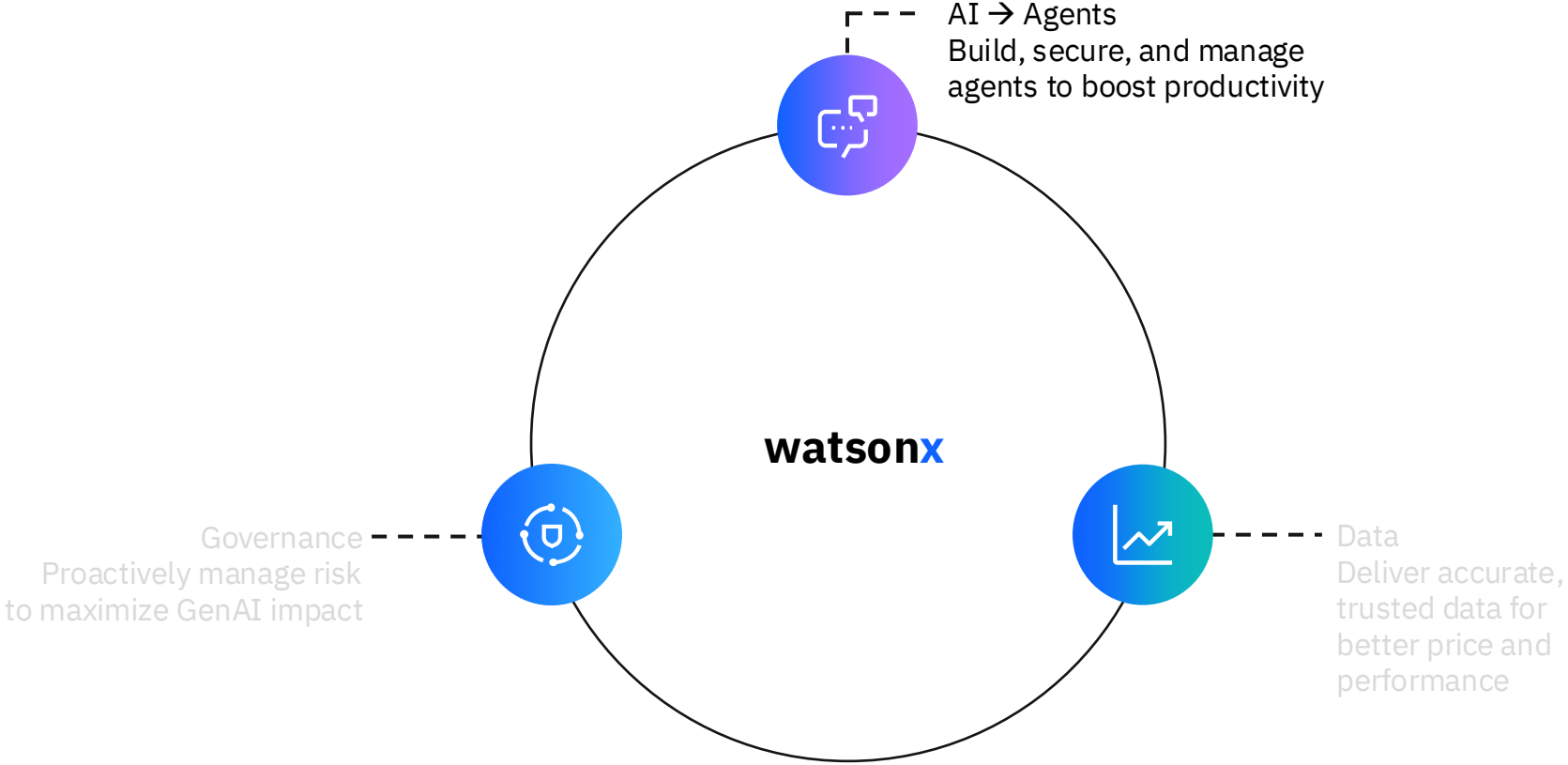
Business semantics
Standardized definitions and metrics

Lineage & auditability
End-to-end traceability

Compliance & security
Regulatory Controls and Data Protection



watsonx

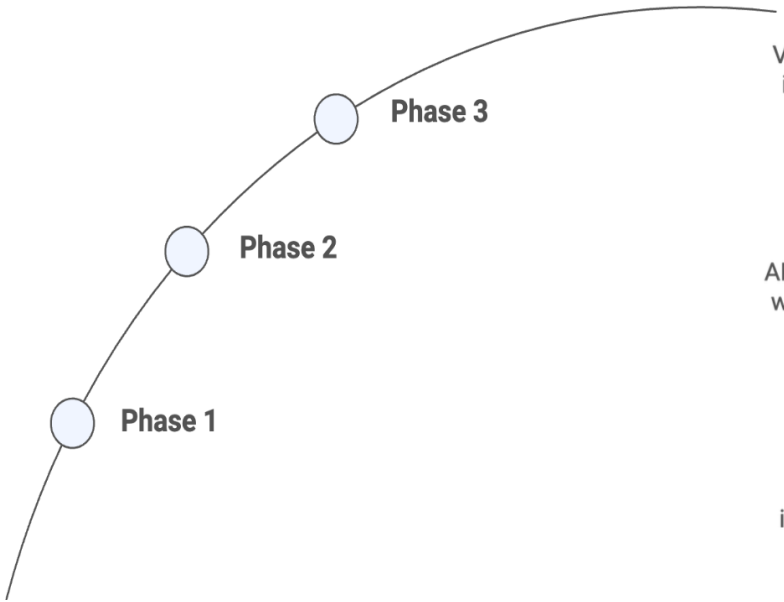

AI → Agents
Build, secure, and manage agents to boost productivity
watsonx
Governance
Proactively manage risk to maximize GenAI impact
Data
Deliver accurate, trusted data for better price and performance

Market Shift

Forrester's AI Market Evolution

Forrester formally recognized the agent control plane as a distinct enterprise technology market in December 2025, separating it from agent build platforms and workflow orchestration tools.

Forrester, 4th Dec 2025



Forrester frames enterprise agentic AI across three functional planes:

Agentic Control Plane

Vendor-agnostic control tower for inventory, policy, monitoring, risk, compliance, and intervention at scale

Orchestration Plane

APO embeds agents into business workflows with routing, decisions, and observability

Build Plane

Focus on models, frameworks, tools, RAG, evaluation, and infrastructure to build and deploy agents

IBM Agentic Control Plane is the Control Plane for Entire Agent Estate

Without changing where your agents run, who built them, or how end users access them

One registry with every agent



Register agents from any platform into a single platform's registry

Every agent is discoverable, auditable & visible regardless of where it runs or who built it

Federates with other existing control planes

Observability & controls across agents



Controls, observability, evaluations & audit trails extend to externally hosted agents without migration

Your existing agents stay exactly where they are but benefit from evaluation, policy controls & observability

Cross platform orchestration



External agents can participate as standalone agents or collaborators in multi-agent workflows

IBM

DEFINITION

What Is an Agentic Control Plane?

DEFINITION

An Agentic Control Plane is the software layer that governs WHAT AI agents can do, WHO can run them, HOW they behave at runtime, and WHAT they cost — enforced inline at every hop, observed end-to-end, and portable across every cloud, framework, and vendor.

Borrowed from the same separation that turned networking into SDN and containers into Kubernetes.

WHAT
they can do

POLICY & GUARDRAILS

Inline enforcement at every hop — LLM call · MCP tool call · A2A delegation · outbound API. Not a static doc; runtime policy decisions.

WHO
can run them

IDENTITY & ACCESS

Per-agent cryptographic identity · OBO delegation · on-behalf-of scope narrowing · sub-10-second kill-switch cascade.

HOW
they behave

OBSERVABILITY

Trace every call · eval scores against golden datasets · anomaly detection · audit-grade evidence trail. End-to-end, not per-tool.

WHAT
they cost

COST & FINOPS

Per-agent · per-LOB · per-cloud cost attribution. Resource-Unit metering · chargeback · cap and overage controls.

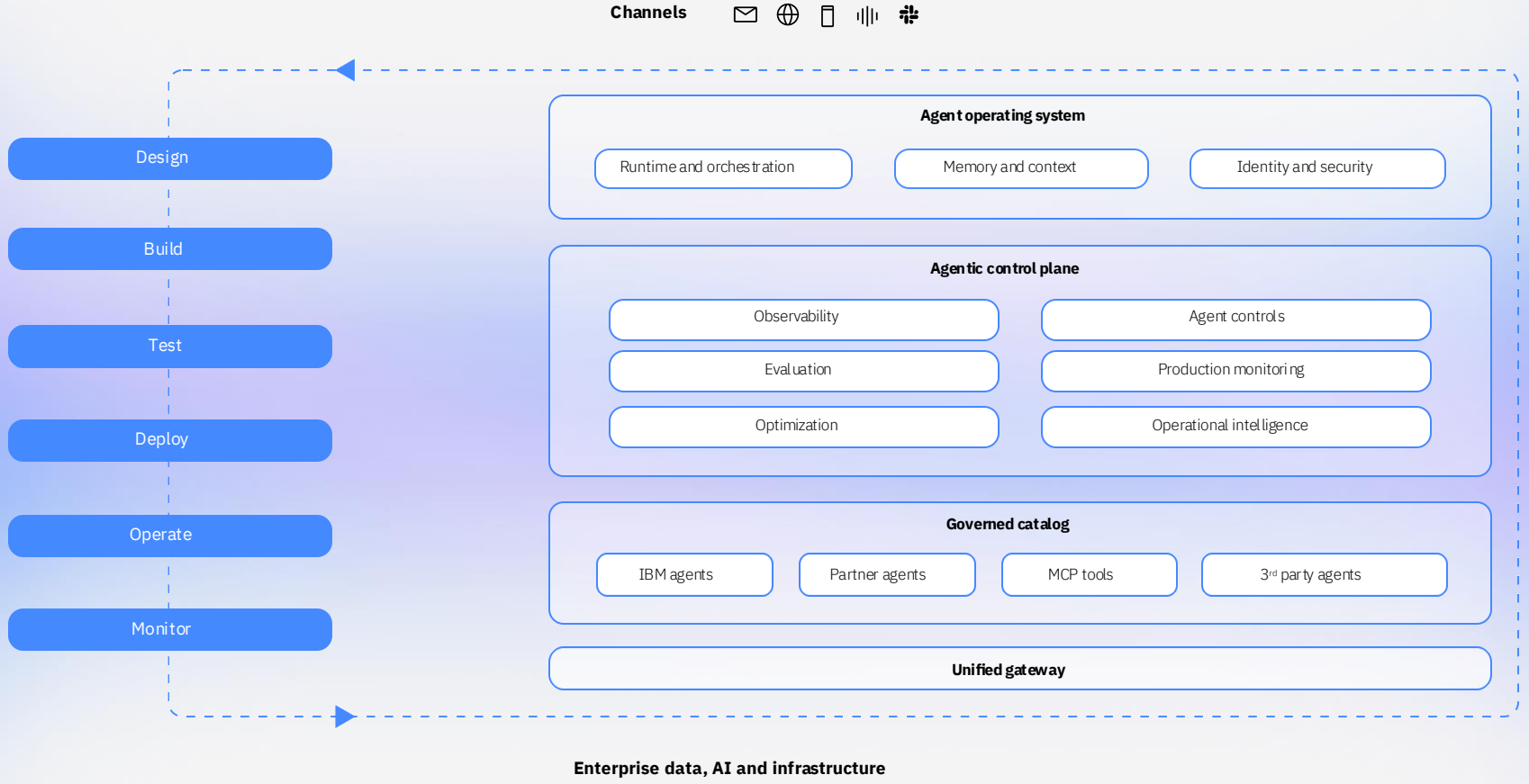
WHERE
it works

PORTABILITY

Cross-vendor (Bedrock · Foundry · Gemini · Salesforce · ServiceNow) · cross-cloud (SaaS · IBM Cloud · BYO · on-prem · air-gapped) · cross-framework.

Without one: ad-hoc agents · no inventory · no kill-switch · audit fails · costs spiral. With one: a governed agentic platform.

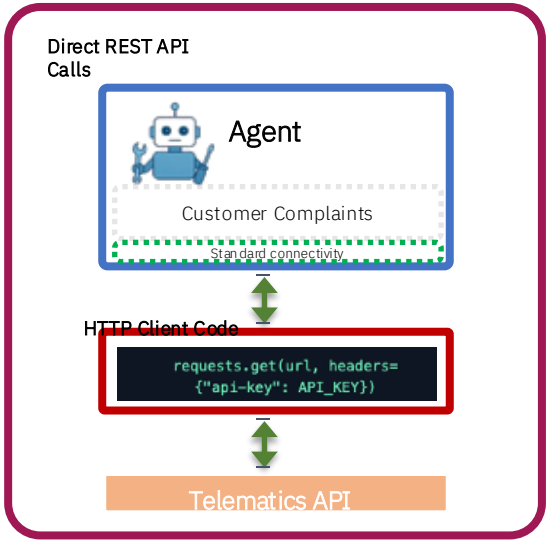
IBM watsonx Orchestrate The agentic control plane that runs, manages & governs your AI agents

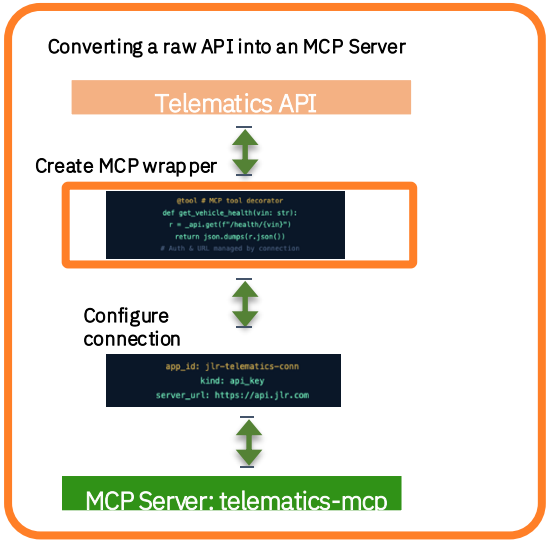


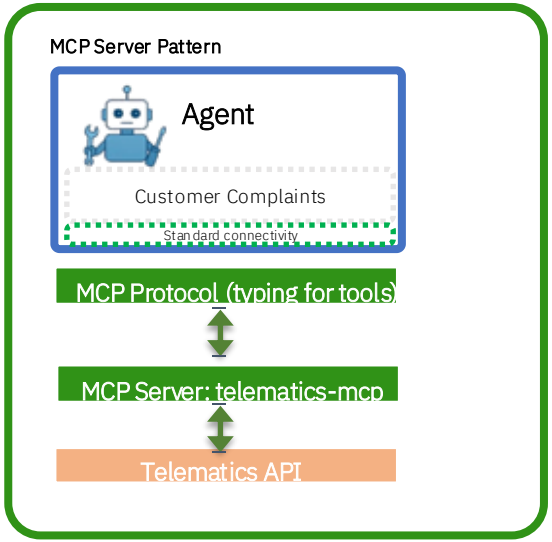
MCP Server versus APIs

Benefits and why use

MCP Servers are specifically built for Agents, APIs are not







Issues

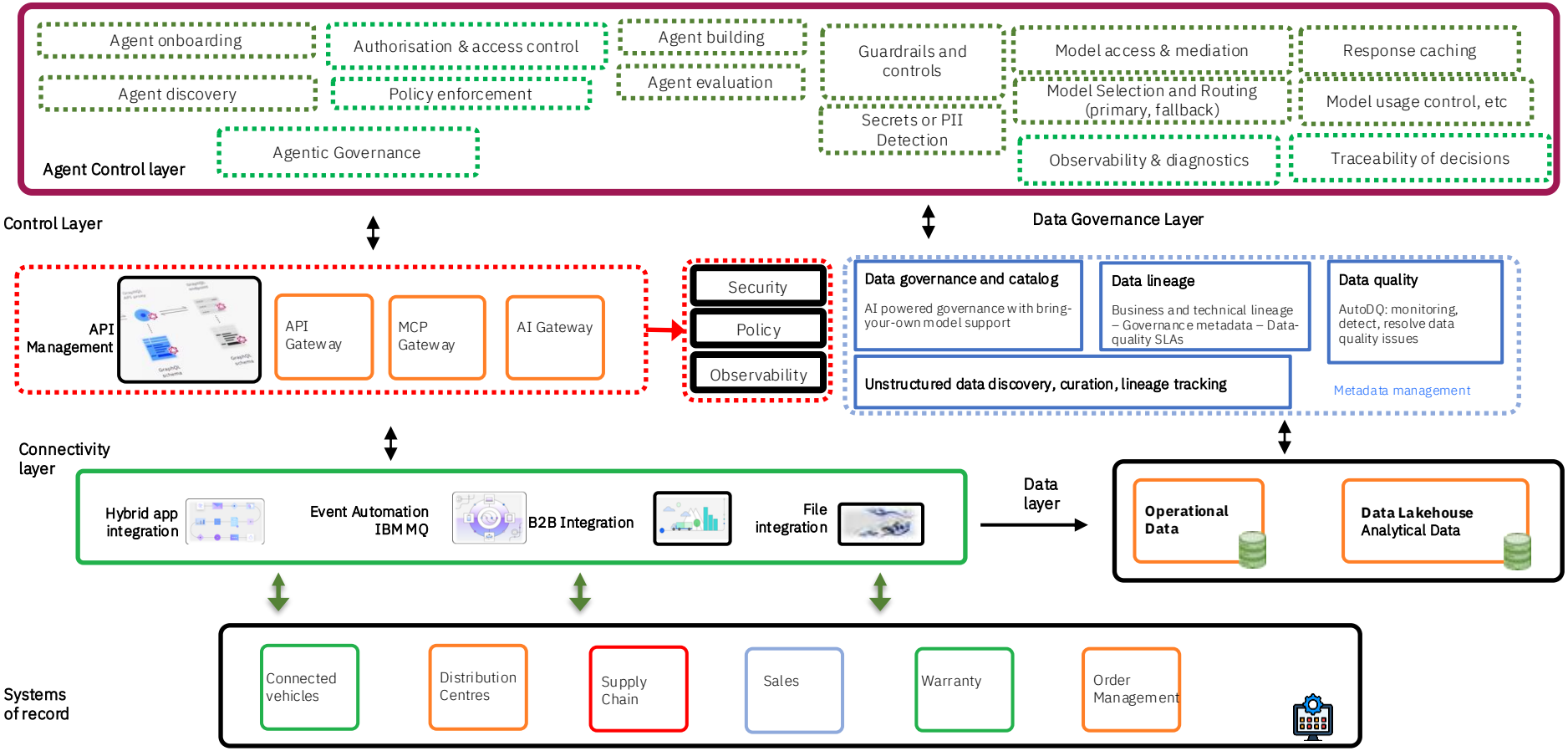
- Agent must handle HTTP errors directly
- No types schema for tools
- Endpoint url duplicated across tools
- No observability at tool call level

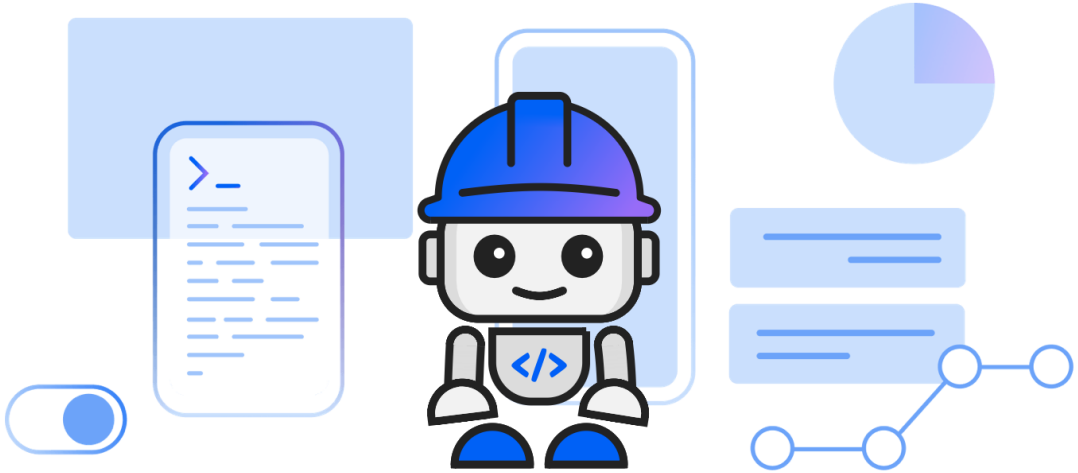
Benefits

- Agent and LLMs tuned to work with mcp server and tools
- Typed tool schema – LLMs understand
- Retries, timeouts and errors handled by server
- Secure handling of API Keys
- Tools support open telemetry for obsevability

So, what's new?

A reference Architecture





Welcome to IBM Bob:
Your AI-Powered Development Partner

Hi, I'm Bob! I'm here to work right alongside you in your codebase, and help you build quality software faster.

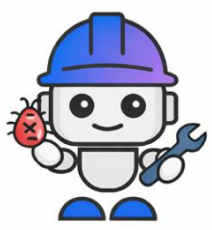
Introducing IBM Bob, your partner across the SDLC



Feature Development



Software testing



Bug Fixing



Security & Compliance
e.g. Vulnability Scan



DevOps & Automation
e.g. IaC, Observabillity



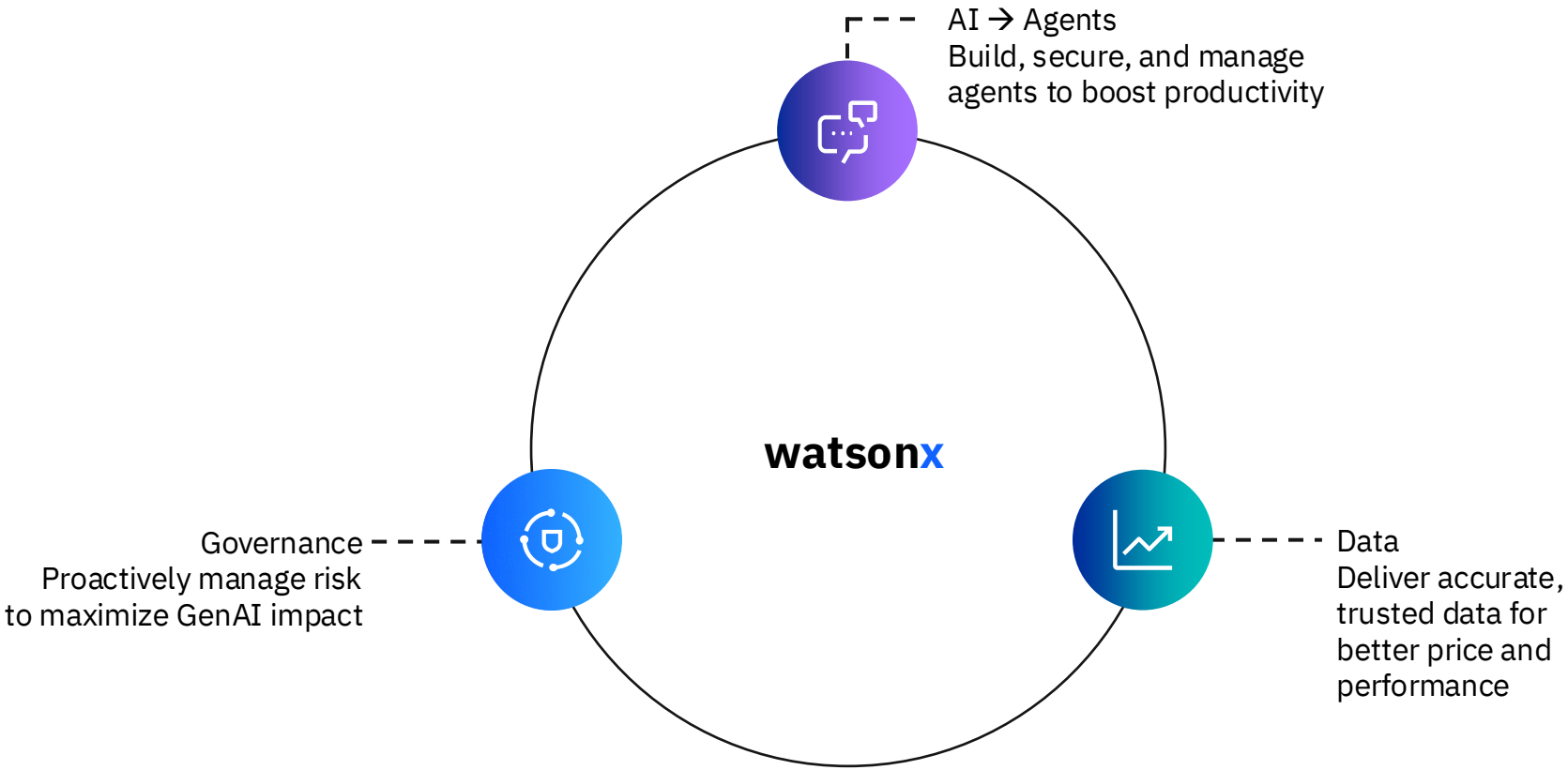
Documentation
e.g Business logic



Analysis & Insights
e.g Architecture Diagrams, Module Structure...



Modernisation
e.g. Refactoring


AI → Agents
Build, secure, and manage agents to boost productivity
watsonx
Governance
Proactively manage risk to maximize GenAI impact
Data
Deliver accurate, trusted data for better price and performance

IBM is the leader in AI Governance

Why is AI Governance needed?

As Enterprises build & run agents across multiple platforms they will need a unified way to register, discover or monitor them. This is essential to scale agents whilst managing operational risk.

watsonx and AI governance

Gartner® AI Governance Platforms Magic Quadrant™

Figure 1: Magic Quadrant for AI Governance Platforms



"IBM's long-term viability is critical for enterprise customers with complex needs. Its global presence, brand awareness, diversified portfolio and proven record as a trusted enterprise technology partner support client confidence, even in an emerging market."

Gartner Magic Quadrant Report, June 2026



