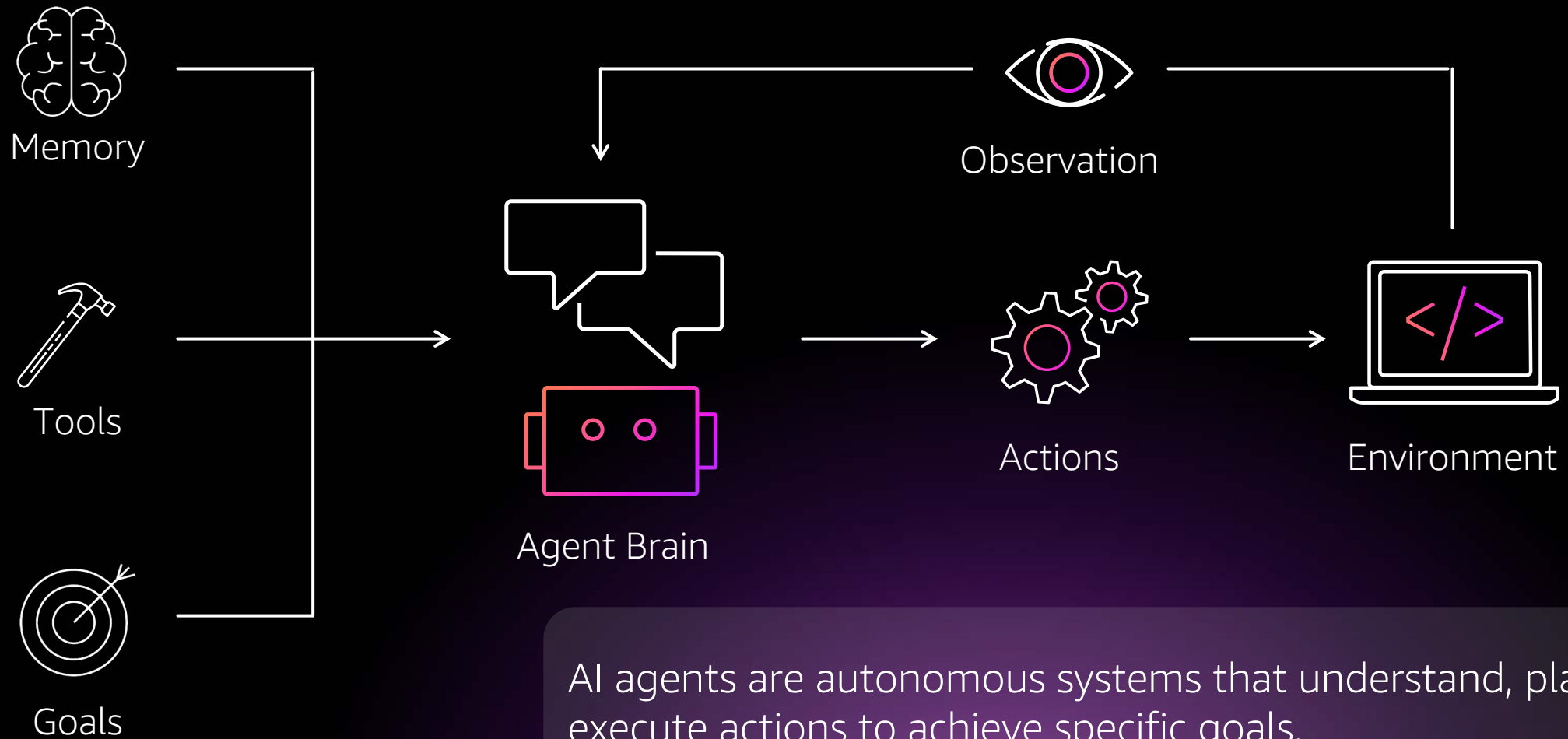# Amazon Bedrock Agents

Beyond Chatbots: How Amazon Bedrock Agents Drive Enterprise AI

Samuel Baruffi

Principal Solutions Architect
Amazon Web Services (AWS)

What is agentic AI?

AI agents are autonomous systems that understand, plan, and execute actions to achieve specific goals.

Enterprises are doubling down on agents

33%

of enterprise software apps will include agentic AI by 2028, up from less than 1% in 2024.

Gartner, "Top strategic Technology Trends for 2025," October, 2024.

15%

of day-to-day work decisions will be made autonomously through agentic AI by 2028.
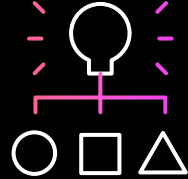
Gartner, "Top Strategic Technology Trends: agentic AI – The evolution of Experience" February 2025
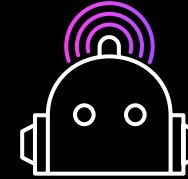
Evolution of Agentic AI

SIMPLE ASSISTANTS

- Basic query responses & actions
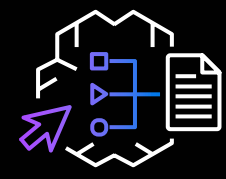- Single step tasks
- Model as Tool caller

DETERMINISTIC AGENTS

- Strict procedure adherence
- Plan is predetermined
- Model as Flow Router

AUTONONMOUS AGENTS

- Run time planning
- Multistep tasks
- **Expanded toolset – Computer/Browser**
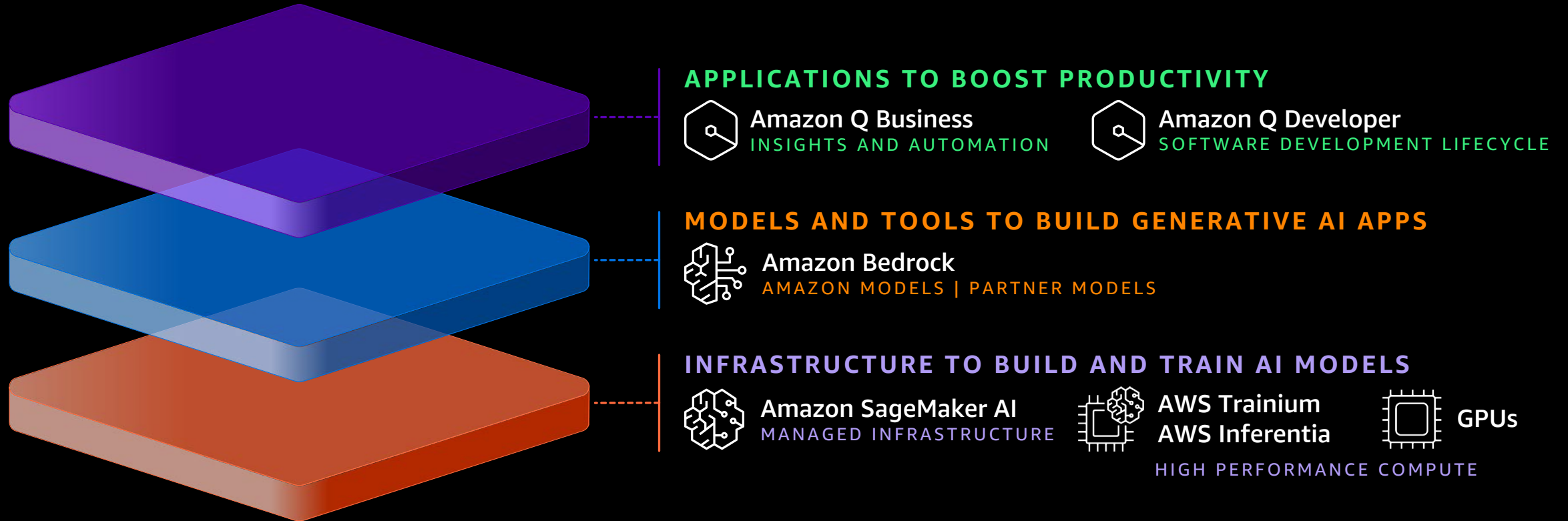- **Mimic human actions**

AGENTIC VIRTUAL WORKERS

- Multi-agent coordination
- Cross Org boundaries
- **Long running systems**
- **Mimic human teams**

INCREASING AUTONOMY AND BUSINESS IMPACT

AWS Generative AI Stack

APPLICATIONS TO BOOST PRODUCTIVITY

Amazon Q Business
INSIGHTS AND AUTOMATION

Amazon Q Developer
SOFTWARE DEVELOPMENT LIFECYCLE

MODELS AND TOOLS TO BUILD GENERATIVE AI APPS

Amazon Bedrock
AMAZON MODELS | PARTNER MODELS

INFRASTRUCTURE TO BUILD AND TRAIN AI MODELS

Amazon SageMaker AI
MANAGED INFRASTRUCTURE

AWS Trainium
AWS Inferentia

GPUs

HIGH PERFORMANCE COMPUTE

Amazon Bedrock

THE EASIEST AND FASTEST WAY TO BUILD AND SCALE GENERATIVE AI APPLICATIONS

TOOLS

Open source integration
- LangChain
- LangGraph
- LlamaIndex
- ...

Customize with your data
- Knowledge Bases
- Bedrock Data Automation
- Fine tuning
- Model Distillation

Orchestrate and execute
- Agents
- Flows

Developer experience
- Prompt management
- IDE
- Prompt optimization

Secure and responsible
- Security
- VPC PrivateLink
- Encryption
- No customer data to model providers, or to AWS
- Guardrails
- Automated Reasoning checks
- GDPR, SOC, ISO, CSA, HIPAA

MODEL CHOICE AND EVALUATION

Base foundation models
- amazon
- ANTHROP\C
- Meta
- Luma
- stability.ai
- AI21labs
- cohere
- MISTRAL AI_
- poolside

More models
- Bedrock Marketplace
- Custom model import

Evaluation
- Programmatic
- RAG
- Human
- LLM as a judge

INFERENCE AT SCALE

Flexible options
- On demand
- Provisioned throughput
- Batch

Optimized inference
- Prompt Caching
- Intelligent Prompt Routing
- Latency-optimized inference

Global reach
- Worldwide regions
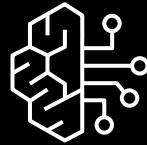- Cross-region inference

AWS offers a broad choice for deploying agents
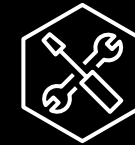
SPECIALIZED

Amazon Q agents for enterprise productivity and workflows

FULLY-MANAGED

Amazon Bedrock agents with built-in FM-powered orchestration

DIY

for expert developers using open-source frameworks
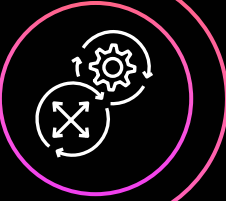
9

Amazon Bedrock Agents

FULLY-MANAGED

Amazon Bedrock Agents
with built-in FM-powered
orchestration

10

The reality of building production-ready AI agents

Development Barriers

- Rapidly evolving technology stack
- **Team learning curve**
- **Production readiness requirements**

Operational Complexity

- Multiple AI agents at **Scale**
- Complex workflow orchestration
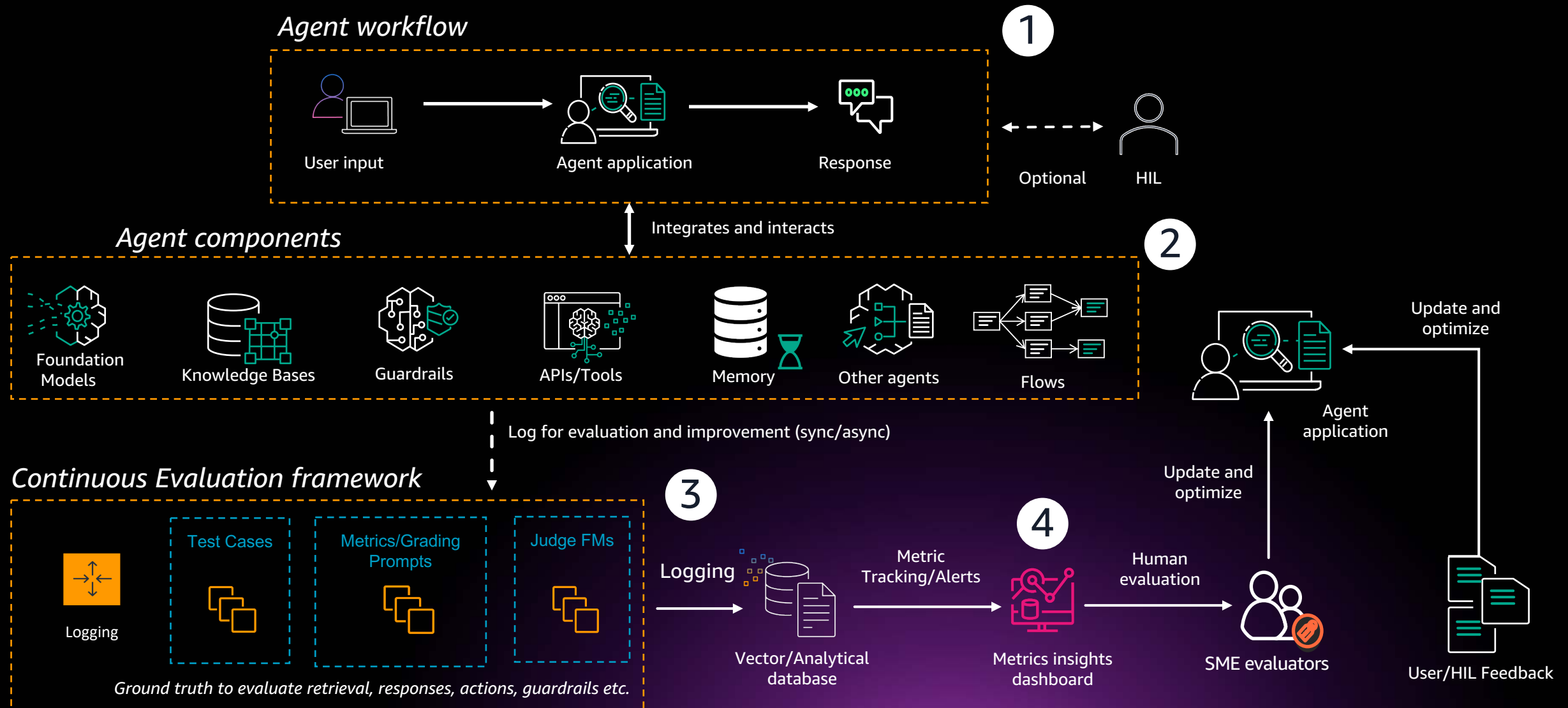- Collaborate across lines of businesses

AgentOps Requirements

- Governance needs
- Security & Compliance
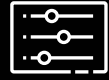- Observability & Evaluation

Innovation Hurdles

- Technology will evolve for years
- Framework integration complexity
- New model and OSS framework releases

What does an agentic system look like?

Amazon Bedrock Agents

Managed capabilities

- Choice of foundation models and reason techniques
- Tools: Action groups, knowledge bases, code interpreter, and Flows
- Memory management: session state and long-term retention
- Multi-agent collaboration for complex workflows
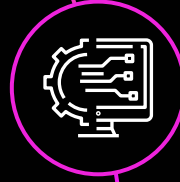- Comprehensive trace, debug, and observability
- Built-in guardrails, security, and compliance controls
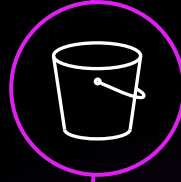
Amazon Bedrock Agents multi-agent collaboration

Scaling agentic experiences

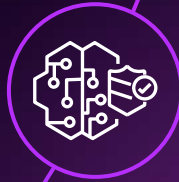Easily assemble agents and knowledge bases

Plan and execute complex tasks across agents

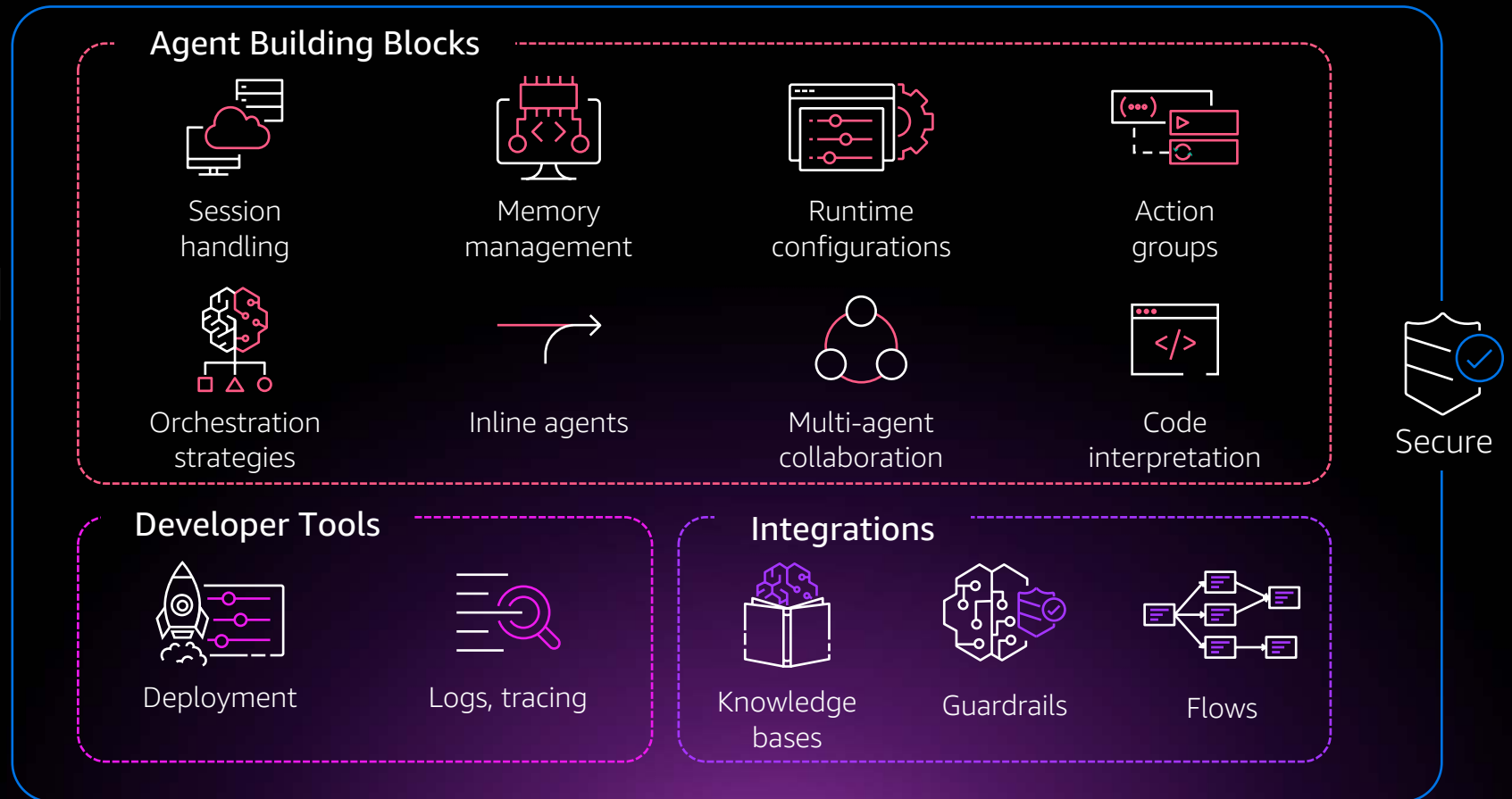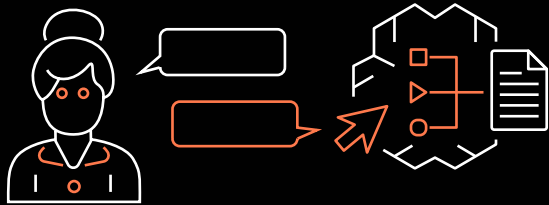Unify conversations across agents with built-in intent classification

Observability across multi-agent flows

Guardrails, security, and privacy

Enabling developers to build and scale reliable agents

Agent Building Blocks
- Session handling
- Memory management
- Runtime configurations
- Action groups
- Orchestration strategies
- Inline agents
- Multi-agent collaboration
- Code interpretation

Developer Tools
- Deployment
- Logs, tracing

Integrations
- Knowledge bases
- Guardrails
- Flows

Secure

Model Context Protocol (MCP)

What is MCP?

A standardized way for models to share and understand context with each other and connect to external data sources and tools, enabling more context-aware applications.

How Amazon Bedrock Agents supports MCP:

- Use Amazon Bedrock Inline Agent SDK to build MCP clients

- Add your MCP servers as Action Groups in Amazon Bedrock Agents

- Enables connecting agents to external tools and data sources via MCP servers

- Supports passing information between models and tools in multi-step workflows

Start building with
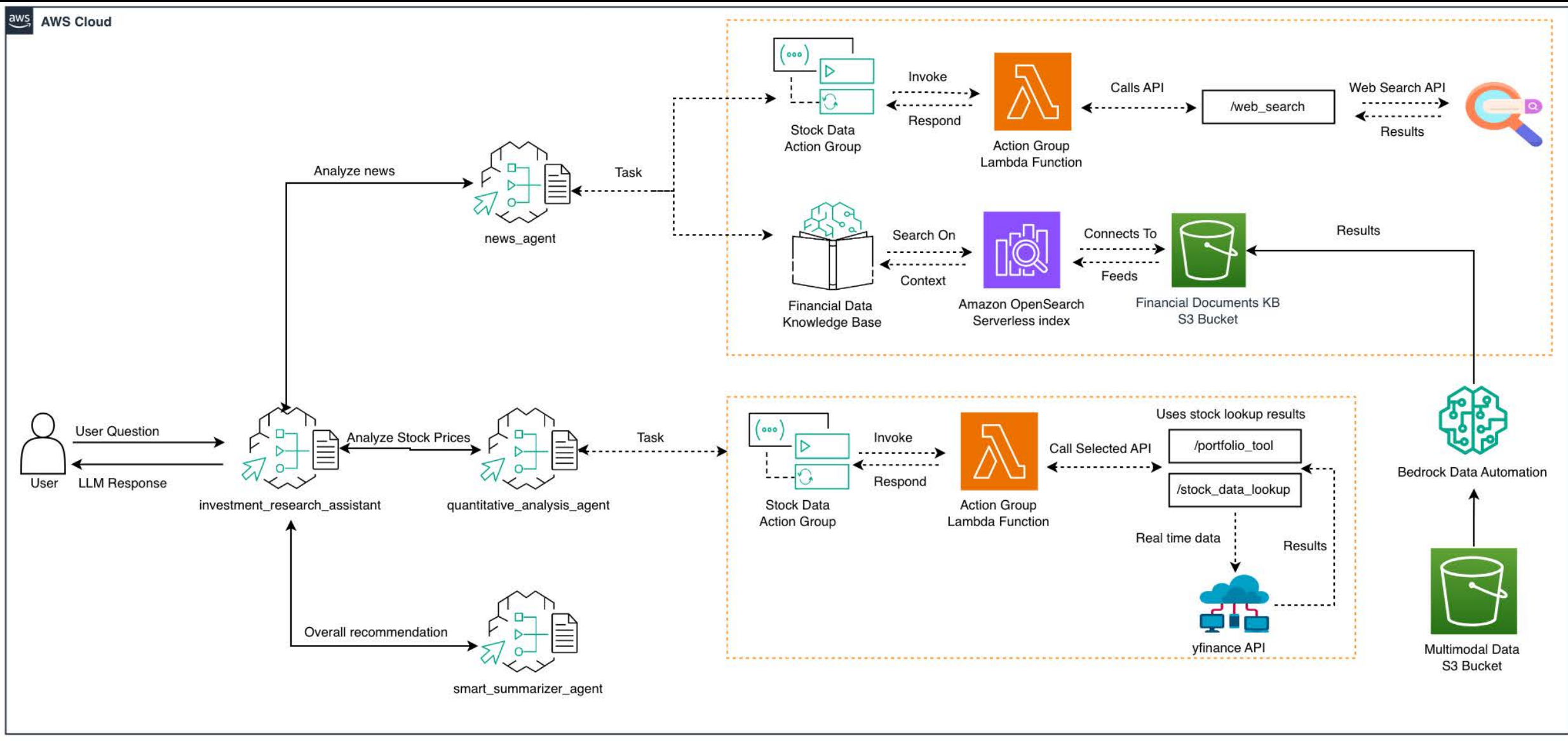# **Amazon Bedrock Agents!**

Explore Amazon Bedrock Agents capabilities

Request a customized workshop for your team

Learn at your own pace with our free course on Amazon Bedrock Agents

Investment Research Agent – Demo Architecture

DEMO

aws

Thank you!