Getting Started with AI Agents

Ron Dagdag
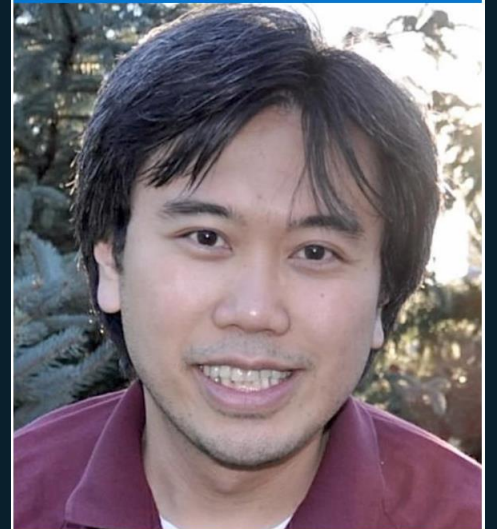
BEST SHERLOCK?

Agent as a Service

Ron Dagdag

R&D Engineering Manager

Ron Dagdag
R&D Engineering Manager

7-ELEVEN.

🚀 Code > Create > Coach > Repeat

"Opinions expressed are my own."

MVP Microsoft® Most Valuable Professional

Award Categories
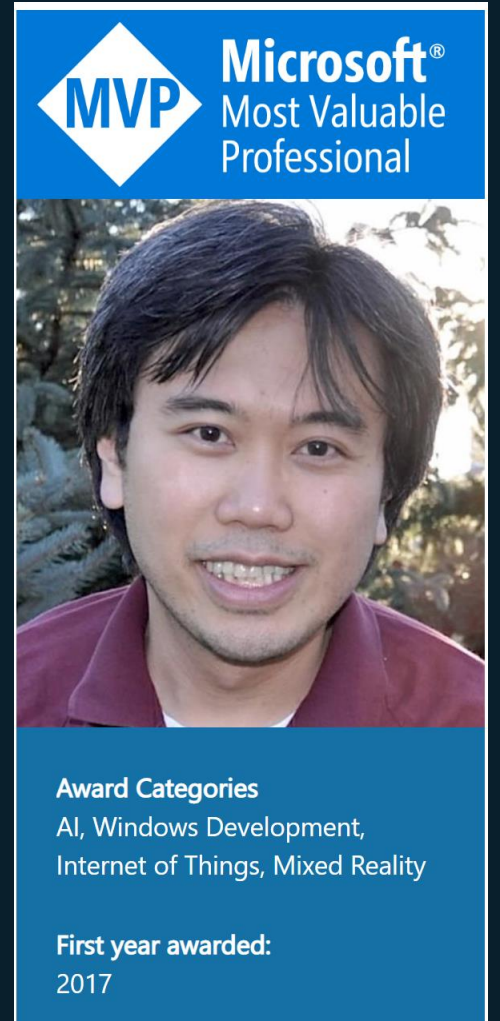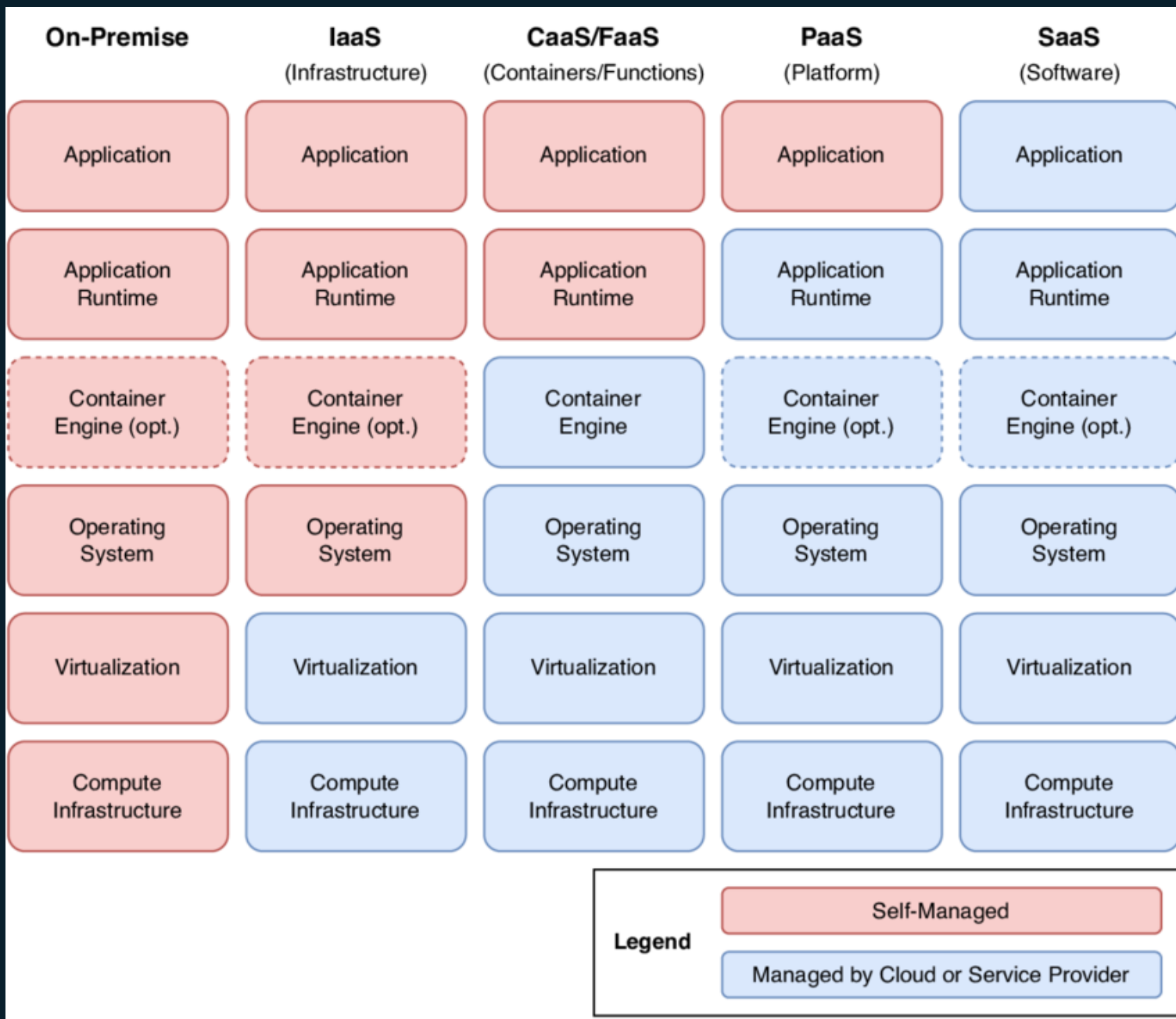AI, Windows Development, Internet of Things, Mixed Reality

First year awarded:
2017

On-Premise	IaaS (Infrastructure)	CaaS/FaaS (Containers/Functions)	PaaS (Platform)	SaaS (Software)
Application	Application	Application	Application	Application
Application Runtime	Application Runtime	Application Runtime	Application Runtime	Application Runtime
Container Engine (opt.)	Container Engine (opt.)	Container Engine	Container Engine (opt.)	Container Engine (opt.)
Operating System	Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Compute Infrastructure	Compute Infrastructure	Compute Infrastructure	Compute Infrastructure	Compute Infrastructure

Legend

Self-Managed

Managed by Cloud or Service Provider

Agents as a Service

On-Premise	IaaS (Infrastructure)	CaaS/FaaS (Containers/Functions)	PaaS (Platform)	AaaS	SaaS (Software)
Application	Application	Application	Application	AGENTIC Application	Application
Application Runtime	Application Runtime	Application Runtime	Application Runtime	Application Runtime	Application Runtime
Container Engine (opt.)	Container Engine (opt.)	Container Engine	Container Engine (opt.)	Container Engine (opt.)	Container Engine (opt.)
Operating System	Operating System	Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Compute Infrastructure	Compute Infrastructure	Compute Infrastructure	Compute Infrastructure	Compute Infrastructure	Compute Infrastructure

Legend

Self-Managed
Managed by Cloud or Service Provider

Chapter 1

Understanding
AI Agents

AI Agent

An agent in LLM-based applications is a semi-autonomous software entity leveraging large language models to perform specific tasks through natural language interaction.
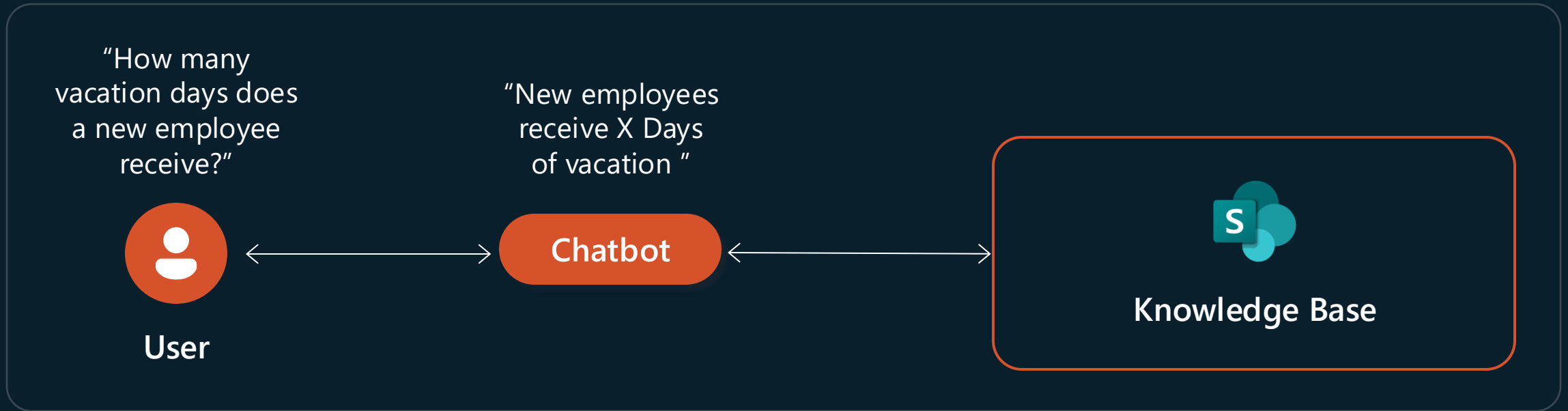
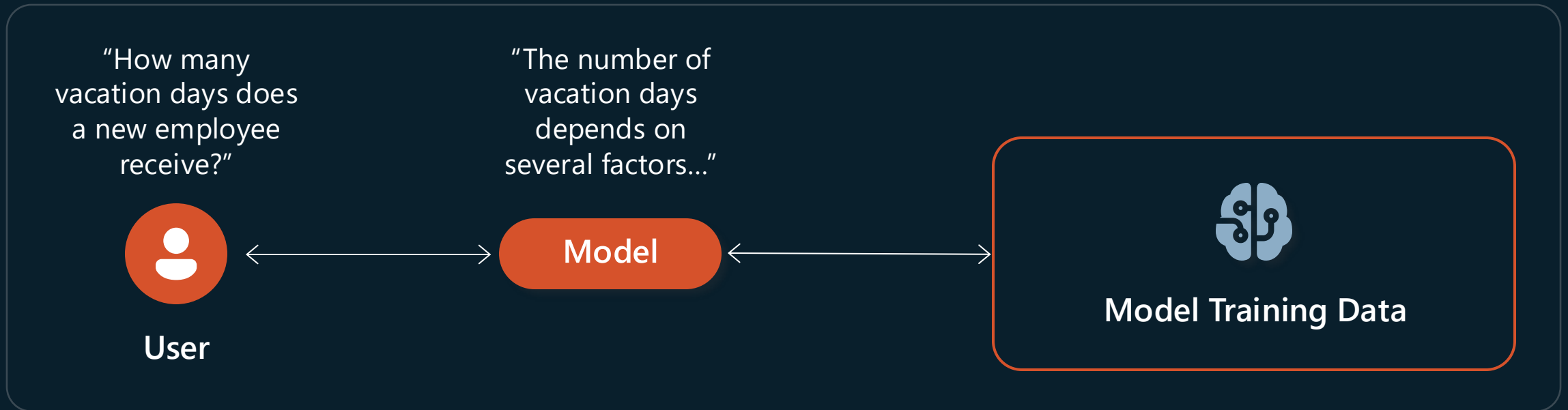| Create a plan | Retrieve context | Perform an Action |

A Chatbot Application

"How many
vacation days does
a new employee
receive?"

"New employees
receive X Days
of vacation "

Chatbot

Knowledge Base

User

⚠️ **Limitations**

Knowledge limited to connected data sources

Chatbots unable perform any action

Limited scope in response

A Generative AI Application without RAG
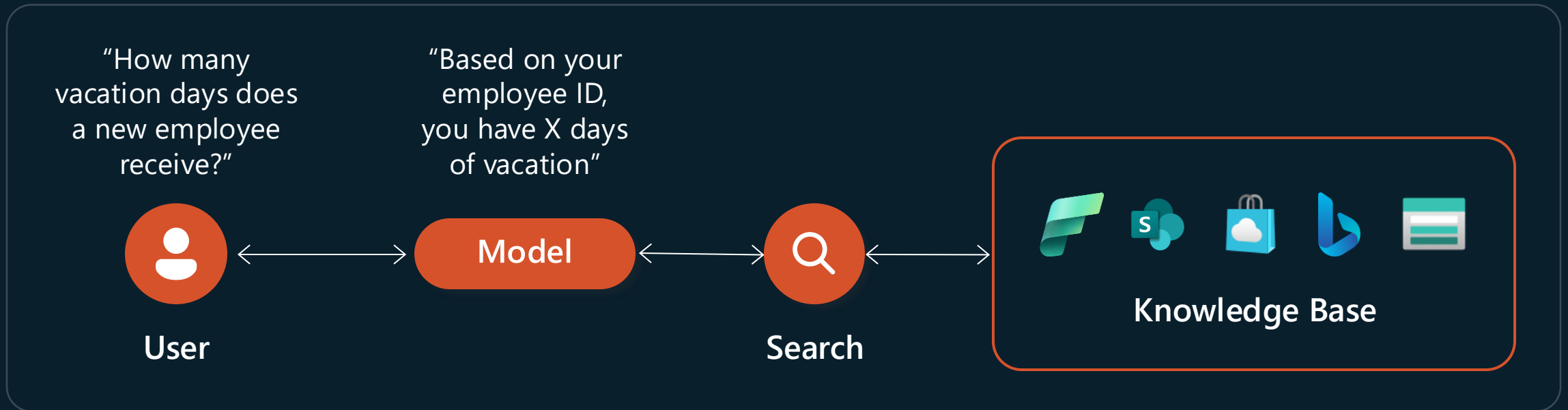
"How many vacation days does a new employee receive?"

"The number of vacation days depends on several factors..."

User

Model

Model Training Data

⚠️ **Limitations**

Responses not grounded in relevant data to the user

Responses are limited to the training data of the model

Higher probability for model to fabricate answers

A Generative AI Application with RAG

"How many vacation days does a new employee receive?"

User

"Based on your employee ID, you have X days of vacation"

Model

Search

Knowledge Base

⚠️ **Limitations**

Provides relevant responses for users but model is limited to data sources

Works well for information retrieval scenarios but not action based ones

Questions outside of the planned scope may not be effectively answered
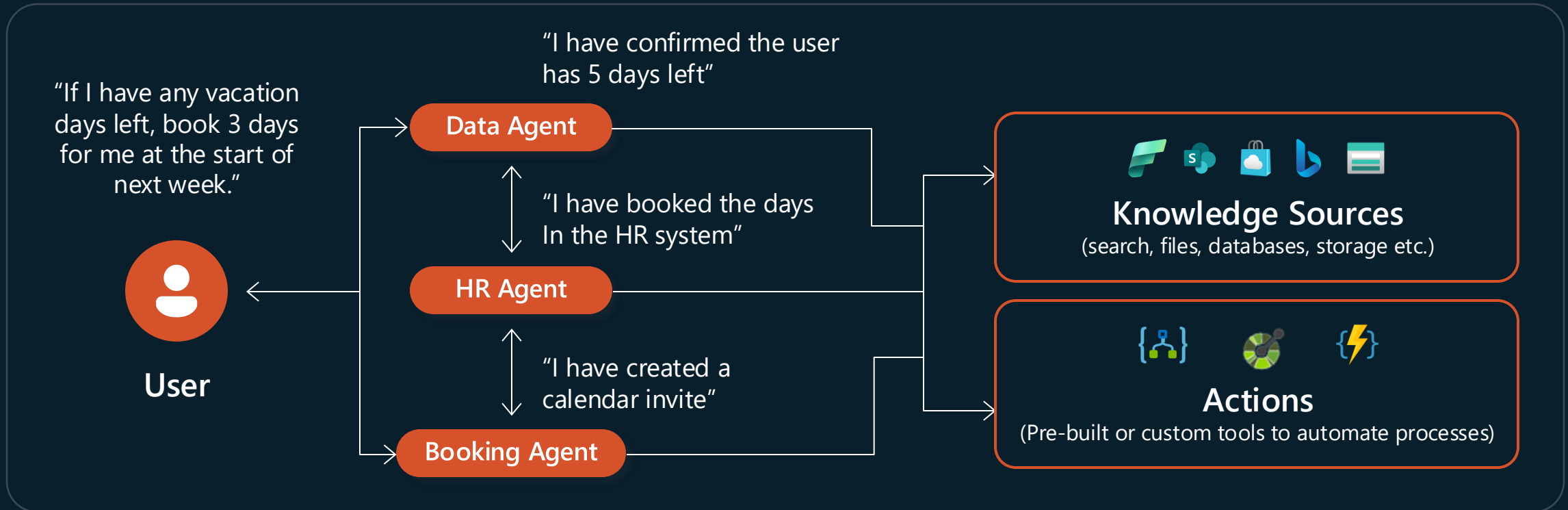
A Generative AI Application with Agents

"If I have any vacation days left, book 3 days for me at the start of next week."

User

"I have confirmed you have 5 days left, book 3 days in the HR system and added them to your calendar"

Agent

Knowledge Sources
(search, files, databases, storage etc.)

Actions
(Pre-built or custom tools to automate processes)

✓ **Benefits**

Agents perform complex tasks

Agents plan out actions based on user input

Agents use knowledge bases, defined business processes and tools

A Generative AI Application with Multiple Agents

"If I have any vacation days left, book 3 days for me at the start of next week."

User

"I have confirmed the user has 5 days left"

Data Agent

"I have booked the days In the HR system"

HR Agent

"I have created a calendar invite"

Booking Agent

Knowledge Sources
(search, files, databases, storage etc.)

Actions
(Pre-built or custom tools to automate processes)

✓ **Benefits**

Agents perform only specific assigned tasks

Agents are not overloaded with complex prompts

Agents only have access to specific tools and data it needs to complete its assigned task

Chapter 2

AI Agent
Use Cases

AI Agent Use Cases

Travel Booking & Expense Management

- Assists employees in booking business trips
- Integrates with Tripadvisor, Outlook, and SharePoint
- Books via Teams chat or email
- Uses OCR to gather receipts
- Automates expense report submission and tracking

Employee Onboarding

- Personalized onboarding assistant for new hires
- Uses LLMs grounded in HR data from SharePoint
- Provide relevant training materials
- Schedule orientations and set up software accounts
- Monitor task completion and ensure efficient onboarding

Personalized Customer Support

- Diagnoses issues by referencing history and product manuals
- Provides tailored solutions or escalates through automated workflows
- Creates tickets and schedules follow-ups
- Updates CRM records, enhancing future support

Data Analytics and Reporting

- Analytics data from data lake and data warehouse
- Responds to user requests in natural language
- Generates insights, visualization, and sends via Teams or email
- Automates data handling for real-time, effortless decision-making

Chapter 3

Building Agents

AI Agent Considerations

Knowledge
Providing agents with the right context

Actions
Giving agents access to the tools needed to complete tasks

Security
Ensuring agents have access to only to the data and services they need

Evaluation
Ensuring agents complete tasks correctly

AI Agent Considerations

Knowledge

Microsoft Fabric

Bing Search

Your own licensed data

Files (local or Azure Blob)

Actions

Azure Logic Apps

OpenAPI 3.0 Tools

Azure Functions

Security

Content Filters

Secure storage

User Authentication

Evaluation

Tracing and monitoring

Model Flexibility

Chapter 4

Azure AI
Agent Service

Azure AI Foundry

Public Preview

Azure AI Agent Service

Securely build, deploy, and scale AI agents with ease

| Rapid development and automation | Extensive data connections | Flexible model selection | Enterprise-grade security |

ai.azure.com

Using the AI Agent Service

Agent

Large Language Model with defined instructions and tools

Tool

Services and functions that extend the agent's ability

Threads

Manages and truncates Messages

Run

Activation of an Agent to perform tasks based on Thread contents and configured Tools

AI Agent Service in Action

Step 1
Create an Agent

Step 2
Create a Thread

Step 3
Run the Agent

Step 5
Check the Run status

Step 6
Display the
Agent's Response

Agent
Contoso Sales Agent

Instructions
You are an advanced sales analysis agent for Contoso, specializing in assisting users with sales data inquiries

Model

Your data (optional)
🔍 Azure AI Search

🗔 Files (local or Azure Blob)
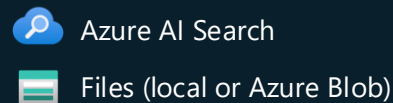
Tools (optional)
File Search
Code Interpreter
Function Calling
Bing Search
Microsoft SharePoint
Microsoft Fabric
Azure Logic Apps
Azure Functions
OpenAPI 3.0 specified tools

Thread
Sales analysis

User's message
Tell me the total sales by region

Agent's message
Here is the sales:
Europe: $15478.00
America: $78792.00

User's message
Show as a pie chart

Agent's message
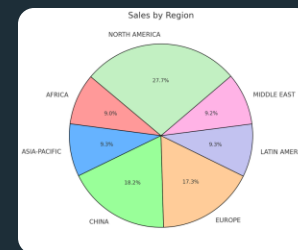
Run 1
1 — Function Calling Tool
Query SQLite DB

2 — Create message

Run 2
1 — Code Interpreter Tool
Create a pie chart

2 — Create message

Demo

Code interpreter tool

Ron Dagdag

Demo

Function calling

Ron Dagdag

Chapter 5

Exploring AI Agent Frameworks

Iteration — Scale — Product

1 Single-agent

Deploy agents with
Azure AI Foundry

Managed agent
micro-services

→

2 Multi-agent

Orchestrate them together with
AutoGen and Semantic Kernel

State-of-the-art
research SDK

Production-ready
and stable SDK

Ideation

Production

Chapter 6

Takeaways

Learnings and next steps

1 Define and identify your use cases where AI Agents can be effective

2 Take it to the next level with AI Agent Service to get function calling, code generation, file search, and more

3 Explore frameworks like Azure AI Agent service, Semantic Kernel and Autogen to implement advanced functionalities

4 Use UI or code to build your agent

Thank you

Ron Dagdag