proarch

Build Your First
Microsoft 365 Copilot Agent

MEET OUR PRESENTERS

Jim Spignardo

Director of Cloud Strategy
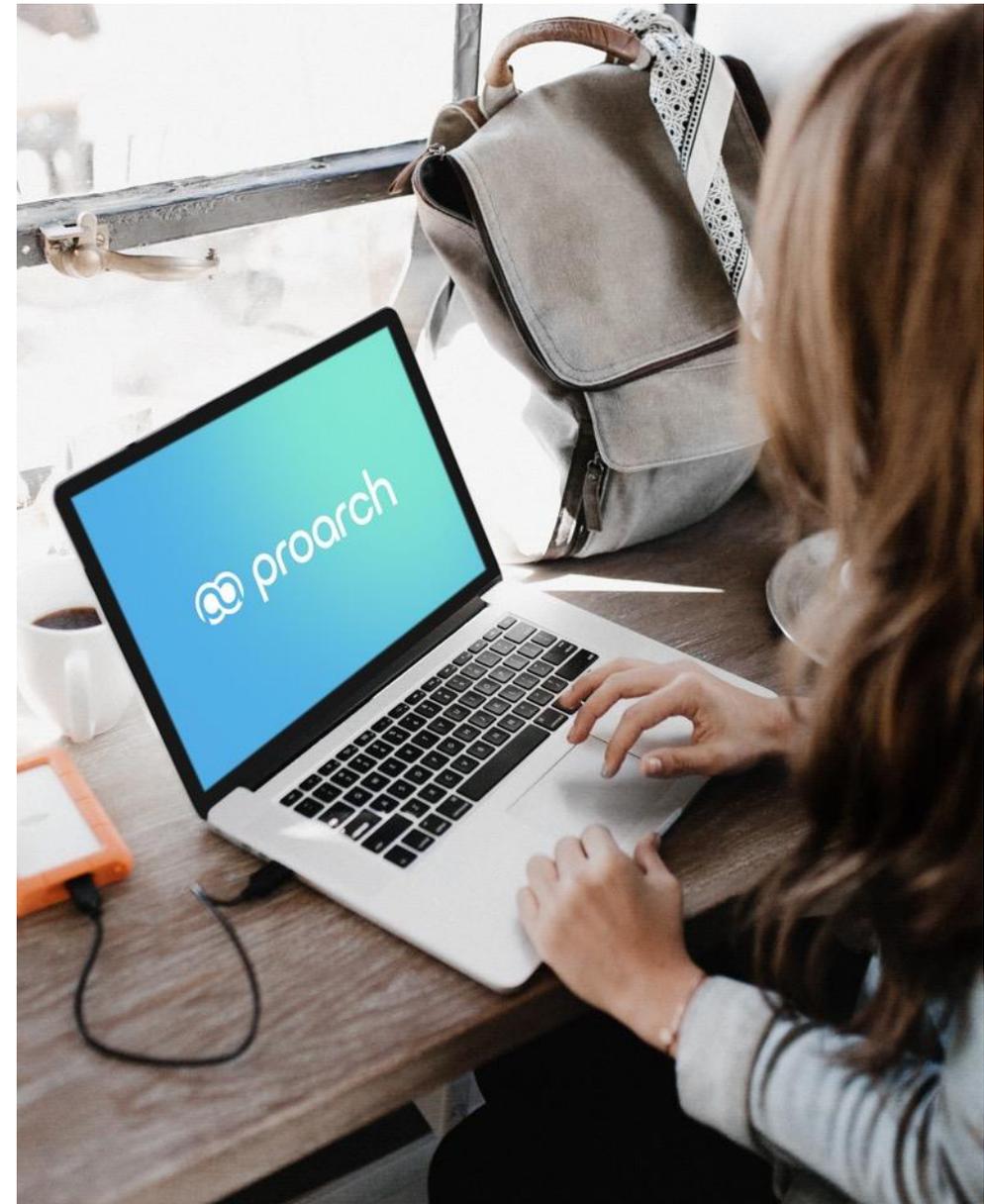and AI Enablement

Greg Dodge

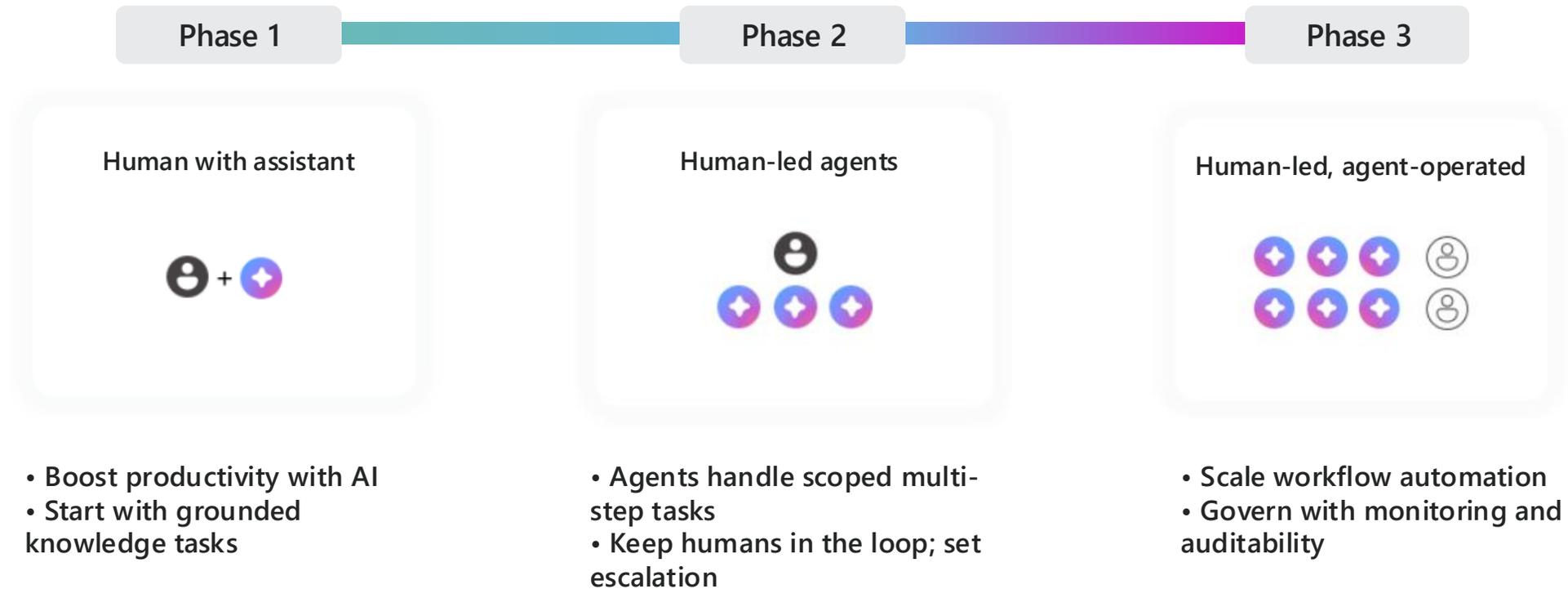Director of Solution Development,
Customer Advisor, and Technical Sales

Agenda

→ What is Agentic AI?

→ Declarative vs Custom Agents

→ Agent Maturity

→ Retrieval vs. Autonomous

→ Tips for Best Output

→ Demo: Building your First M365 Copilot Agent

Every company is on the journey to transform into a Frontier Firm

| Phase 1 | Phase 2 | Phase 3 |

Human with assistant

Human-led agents

Human-led, agent-operated

• Boost productivity with AI
• Start with grounded knowledge tasks

• Agents handle scoped multi-step tasks
• Keep humans in the loop; set escalation

• Scale workflow automation
• Govern with monitoring and auditability

Agents vs. Assistants: What's the Difference?

Assistant

Helps you do the work. Inform and accelerate decisions.

- Responds to prompts
- Drafts, summarizes, explains, and analyzes
- Suggests next steps
- Requires human review and action

Think:

A highly capable advisor sitting beside you

Best suited for:

- Knowledge work
- Decision support
- Writing, analysis, planning
- Individual productivity

Agent

Can take action on your behalf. Under rules.

- Executes predefined steps
- Can monitor, trigger, and follow workflows
- Operates within explicit constraints and approvals
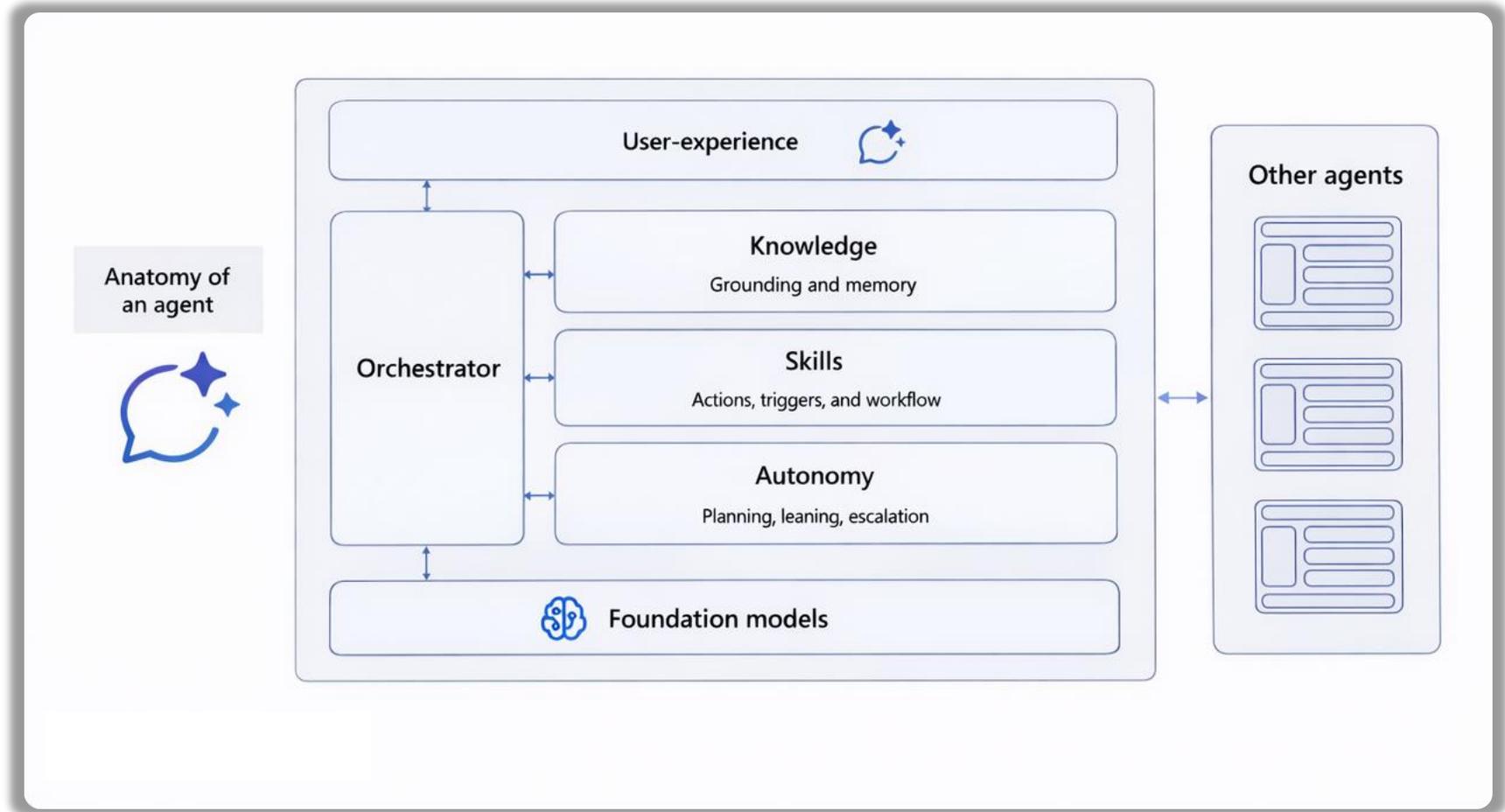- Requires stronger governance and oversight

Think:

A junior operator you delegate work to, with guardrails

Best suited for:

- Repetitive processes
- Cross-system coordination
- Monitoring, triage, and follow-up
- Automation with accountability

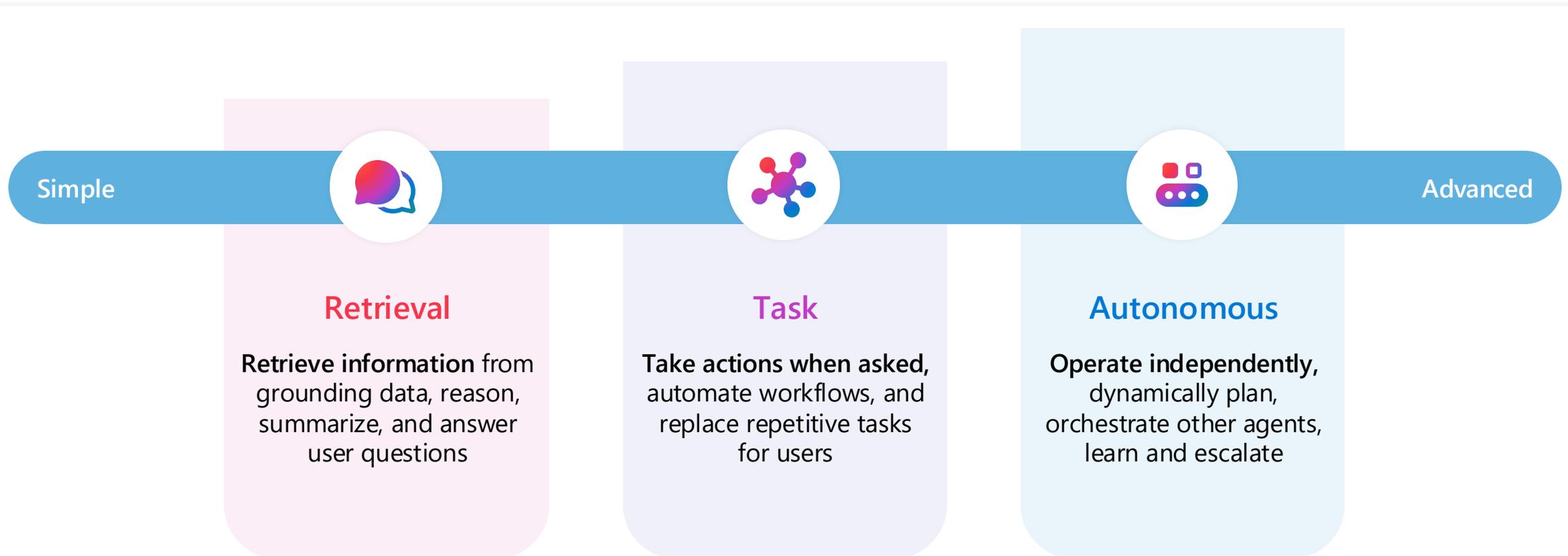**The difference is autonomy, risk, and responsibility.**

Microsoft 365 Copilot Agents act as AI assistants to automate and run business processes.

Types of Agents

Agents Exist on a Spectrum

Simple   Advanced

Retrieval

Retrieve information from grounding data, reason, summarize, and answer user questions

Task

Take actions when asked, automate workflows, and replace repetitive tasks for users

Autonomous

Operate independently, dynamically plan, orchestrate other agents, learn and escalate

Agents vary in levels of complexity and capabilities depending on your need

Copilot Agent Options

Declarative Agents
Platform-Managed

🛡️ **Declarative Agents**

What they are

AI agents that run **inside an enterprise platform**, inheriting identity, permissions, and **security by defaٮut**.

Best for

- Knowledge work
- Internal productivity
- Broad adoption at scale

Strengths

🚀 Fastest time to value

🛡️ Built-in governance and auditability

⬇️ Lower operational risk

Strengths

🚀 Fastest time to value

🛡️ Built-in governance and auditability

⬇️ Lower operational risk

Custom Agents
Orchestrated & Engine-Controlled

🔧 **Custom Agents**

What they are

AI agents built on **custom AI stacks** where the organization controls models, workflows, and runtime behavior.

Typically deployed across

- Enterprise productivity ⌨️
- Collaboration tools
- External or customer-facing scenarios

Trade-offs

- Higher build and maintenance cost
- Greater governance and security responsibility

Typically deployed across

- Line-of-business systems
- Custom web applications

Most organizations will use both.
Declarative agents for scale and safety.
Custom agents where differentiation and automation matter.

Key takeaways: Declarative agents

DO

- Define the goal, not the steps

- Keep workflows clean and readable

- Ground answers in trusted knowledge

- Add guardrails and boundaries

DON'T

- Write step-by-step scripts

- Grant unchecked permissions

- Allow open-ended requests

Designing Your Agent for Clarity & Trust

Tips for Building Reliable Agents

Start with one clear job

Pick a single task the agent is responsible for

Keep the design simple (at first)

Use basic steps or a single tool before adding complexity

If you have Microsoft 365 Copilot (paid) you have Copilot Studio

Write instructions like a job description

Define what success looks like and when

Choose tools that match the task

Only add tools the agent truly needs

Let the agent ask when information is missing

Guessing leads to bad outcomes

Test early, fix, and get feedback often

Small tests reveal problems fast

Secure and Govern M365 Copilot

Prepare your environment and implement Zero Trust strategy for secure Microsoft 365 Copilot adoption

Discover security, privacy, and safety risks with comprehensive visibility

Protect against emerging threats and safeguard sensitive data with end-to-end security

Govern Microsoft 365 Copilot usage and systems to comply with code-of-conduct and regulatory policies

Prepare

Discover

Generative AI

Govern

Protect

Protect Your Data and Users as You Embrace AI

Unify secure access for all users

- Multi-factor authentication (MFA)
- Conditional access policies
- Microsoft Entra ID P1 (cloud-based identity and access management)

Microsoft Entra

Protect data in the age of AI

- Sensitivity labels
- Data loss prevention (DLP)

Microsoft Purview

Microsoft 365 Copilot

Uncover Shadow IT, including AI apps

- Cloud app discovery
- Defender Endpoint Plan 1 (core protection capabilities)
- Microsoft Intune P1 (cloud-based device and app management)

Microsoft Defender

Microsoft Entra

Expand threat protection

- Microsoft Defender for Endpoint P1
- Microsoft Entra ID P1
- Microsoft Intune P1

Microsoft Defender

Microsoft Entra

Microsoft Intune

Copilot Agent Builder

The Copilot Agent Builder in Microsoft 365 Copilot enables you to build agents for Microsoft 365 Copilot easily and quickly.
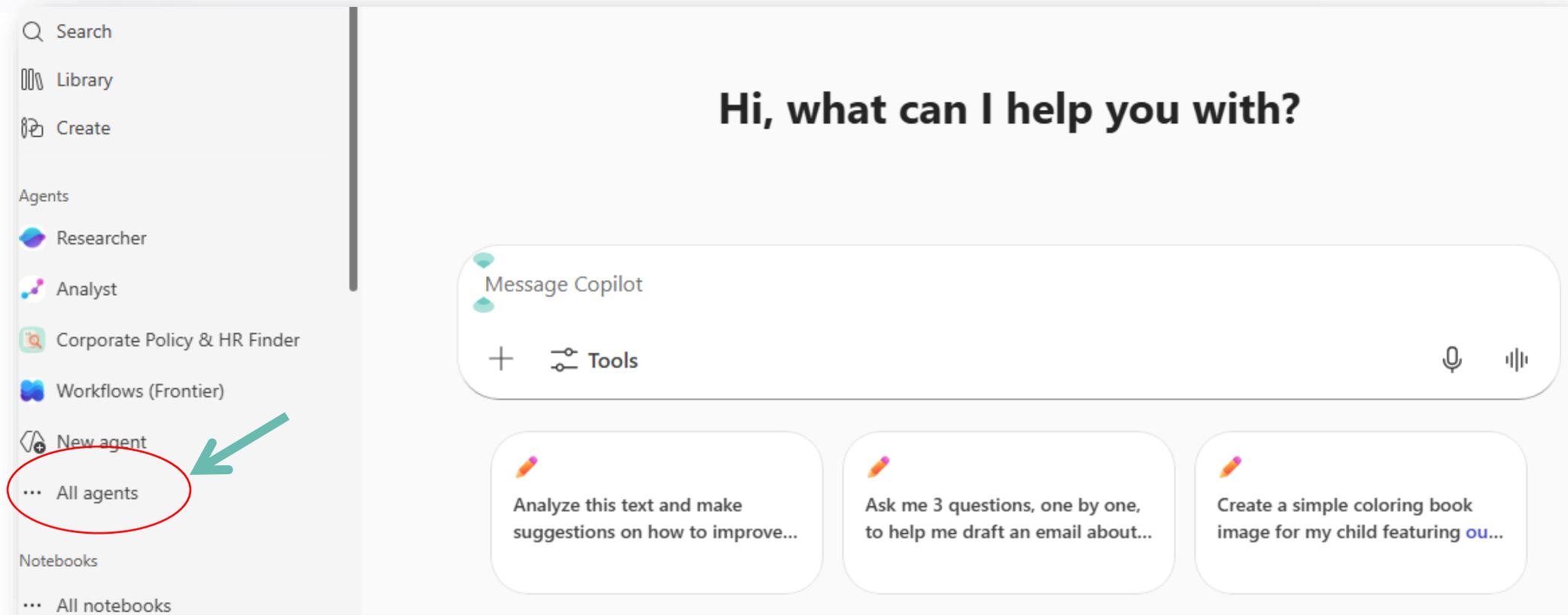
THANK YOU FOR JOINING US | PROARCH.COM