

Designing the Spectrum of *Intelligence*

How interaction patterns evolve as AI becomes more contextual, autonomous, and embedded into everyday experiences.



THE SPECTRUM

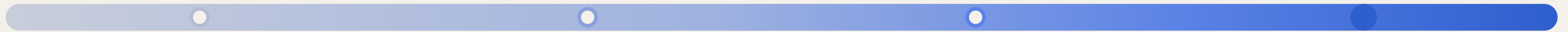
The way we interact with AI is evolving.

Conversational

Contextual

Agentic

Ambient



← User performs the work

System performs the work →

As systems become more capable, people shift from doing the work themselves to supervising outcomes.

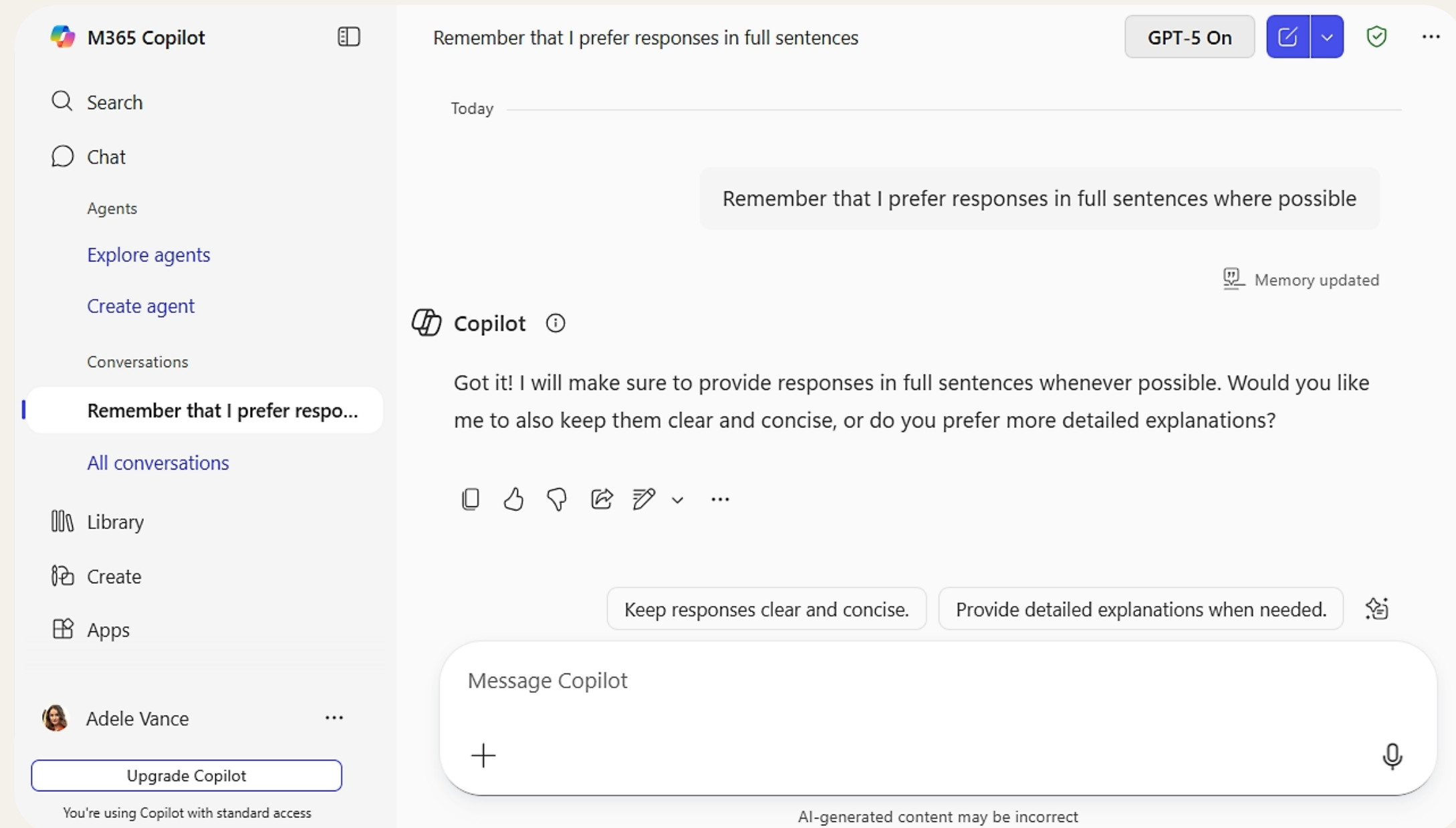
CONVERSATIONAL AI

Ask → Respond

Answer my question

The user provides the goals, the context, and the evaluation (voice or text).

The system answers, then waits for the next turn.



Conversational

Contextual

Agentic

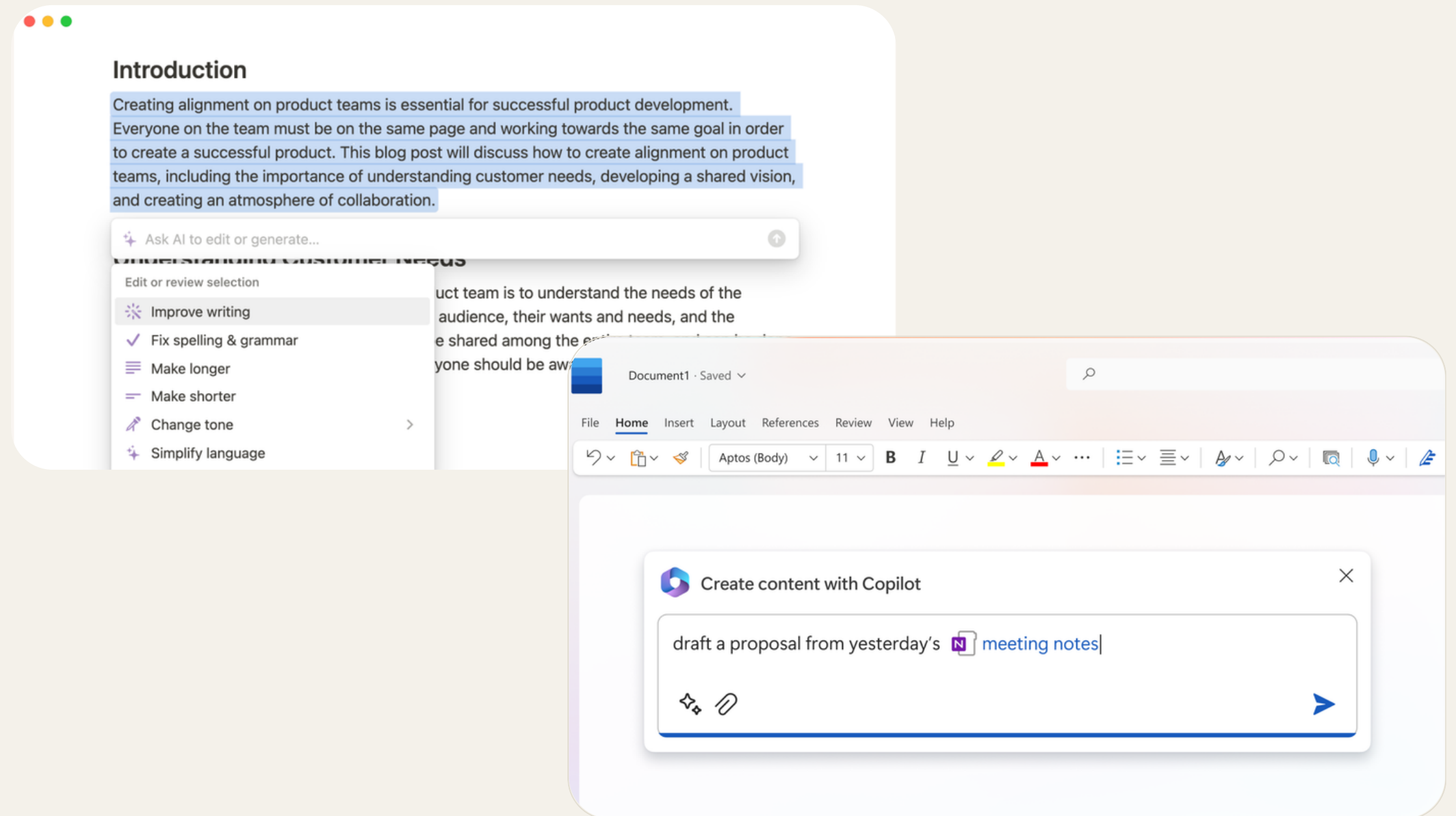
Ambient

Understand → Assist

Help me understand my task to be completed.

The system understands where the user is and what they are working on, and meets them inside the task.

Users no longer need to explain everything. The system already knows.



Plan → Execute

User initiated execution.

The system creates and executes a plan to achieve a goal, coordinating multiple steps on the user's behalf.

1. User initiates a question

Further investigate users experiencing MFA sign in issues.

2. Workflow kicks off

Workflow 5 of 5 complete

- ✓ Check for sign-in anomalies
- ✓ Create group and escalate to admins
- ✓ Temporarily restore access
- ✓ Patch vulnerability
- ✓ Simulate and update policy

3. Copilot outputs findings

Oct 20, 2024 3:56 PM

 **Copilot** 3:56 PM

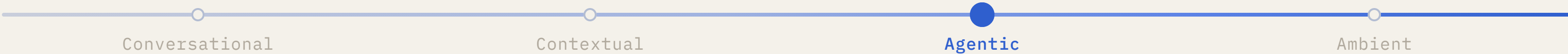
IT support agent generated and ran a step and found several related sign in issues. I've summarized the findings.

Detect sign-in anomalies ...

5 steps completed

 IT support agent  +1

View activity timeline ▾



Authorize → Protect

Autonomy begins with consent.

Before acting independently, the system makes its capabilities, permissions, and responsibilities visible.

Users understand what the agent can access, what it can do, and when it will act before choosing to enable it.

Conditional Access Optimization Agent (Preview) ×



The agent will scan all newly created users and apps from the last 24 hours and determine if they are in scope of at least one policy with multifactor authentication (MFA) or device compliance controls. It will suggest policy changes based on [Zero Trust best practices](#) and create new policies in report-only mode. It won't add new users to existing Conditional Access policies or turn on new policies without your approval. [Learn more about this agent](#)

Trigger

The agent will run once every 24 hours. You will also be able to run the agent manually at any time.

Permissions

- ✓ Read access for users, devices, and applications
- ✓ Read and write access for groups and Conditional Access policies

Identity

The agent will run using your identity. Agent authentication will expire according to your policies and need to be renewed. [Learn more about agent authentication](#)

Products

Conditional Access

Plugins

Microsoft Entra

Role-based access

Conditional Access Administrators, Security Administrators, Global Administrators. [Learn more about who can use the agent](#)

Once started, the agent will run in your tenant. You can remove the agent or customize the agent output.

Cancel

Start agent

Conversational

Contextual

Agentic

Ambient

Work moves from one-time execution to ongoing stewardship.

A horizontal spectrum diagram illustrating the progression of AI interaction levels. It consists of a horizontal line with four points marked by circles. From left to right, the points are labeled: 'Conversational', 'Contextual', 'Agentic', and 'Ambient'. The 'Ambient' label and its corresponding circle are highlighted in blue, while the others are in a lighter blue/grey. The background of the diagram is a light beige color.

1. **Create a new group for admins to manage:** Create a new group for admins to manage users affected by the same sign-in issue. This will allow other admins with higher permissions to easily handle policy assignments and app patching.
2. **Escalate to admins:** Notify and escalate these issues to the appropriate admins to resolve sign-in problems, address app vulnerabilities, and explore policy improvements.



Assign to agent

Manage

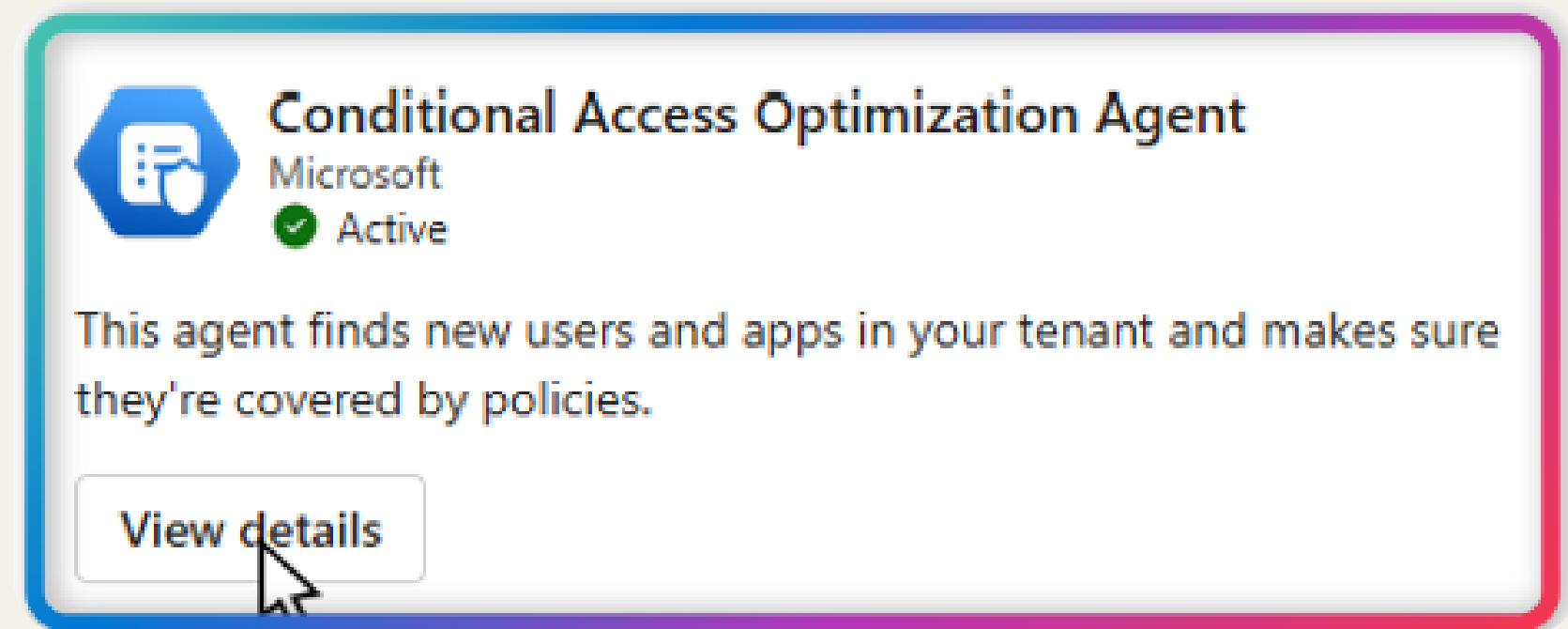


Browse more agents
that can help

Monitor → Maintain

Proactive intelligence

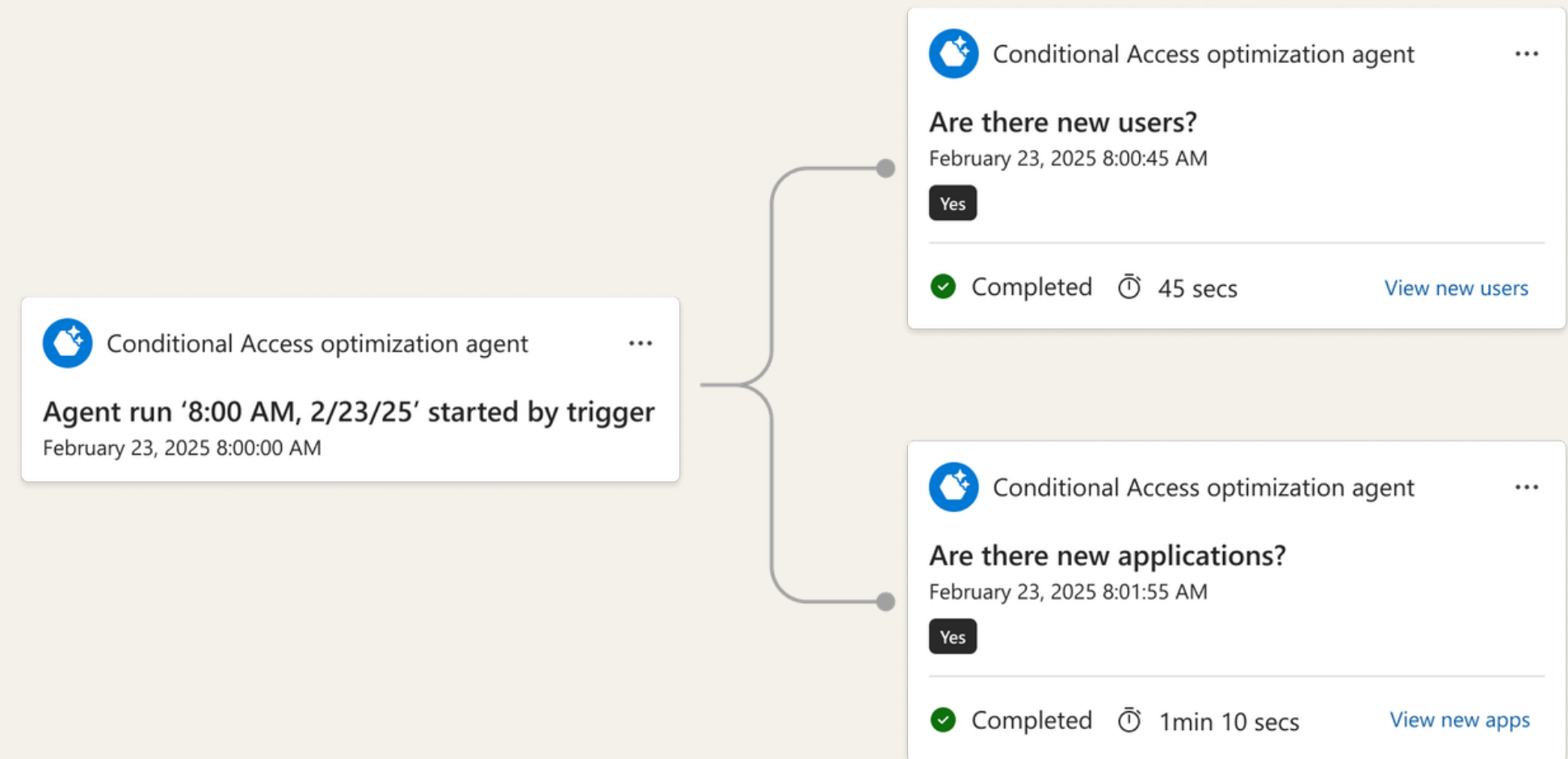
Intelligence becomes embedded into everyday experiences, quietly acting before you ever ask.



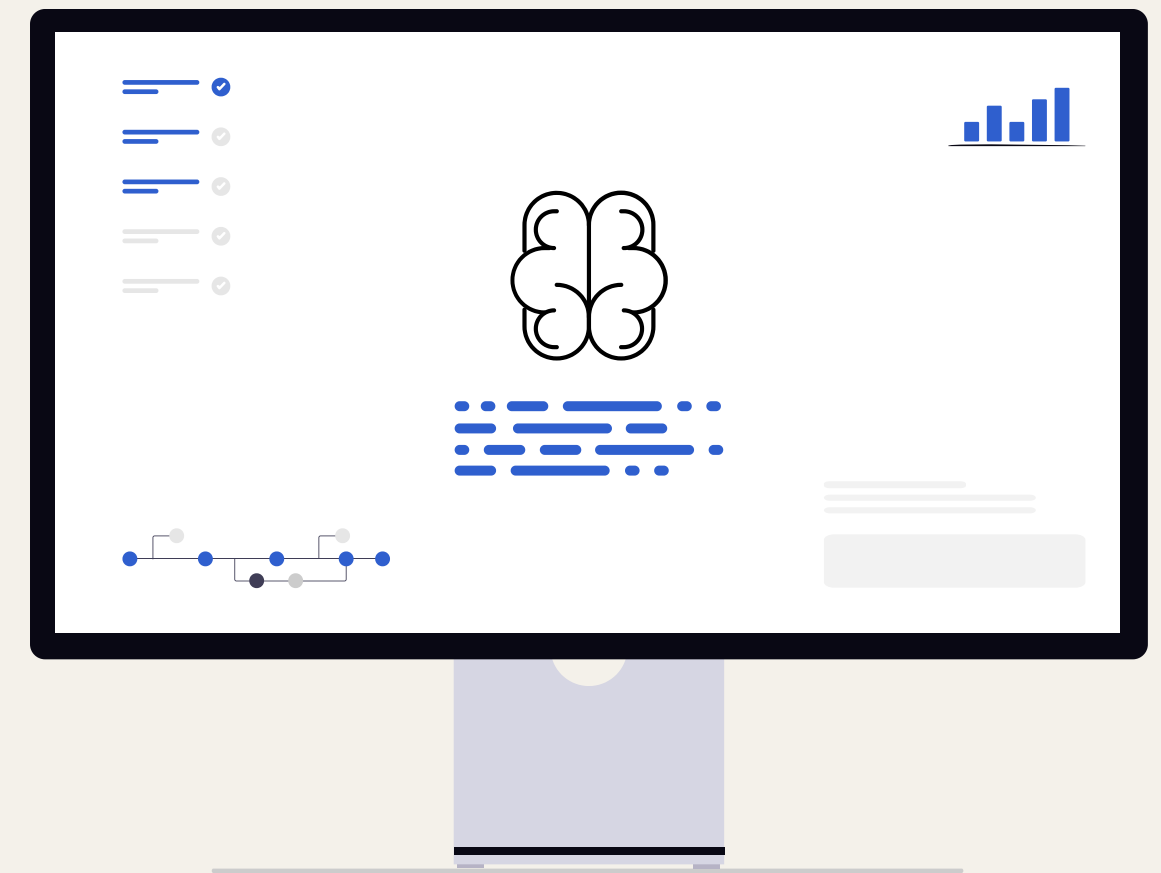
TRUST

Visibility evolves too.

As systems take on more responsibility, trust shifts from interaction design to visibility design.



As intelligence increases,
interaction decreases.



TRUST

Visibility evolves

People need to understand what happened, why it happened, and what happens next.

Explanations

why it did this

History

what happened before

Approvals

where you decide

Decisions

the choices made

Actions

what it actually did

TRUST

Clarity creates confidence.

CAPABILITY

What can it do?

TRIGGER

When will it act?

BOUNDARY

When will it ask?

FEEDBACK

How does it keep me informed?

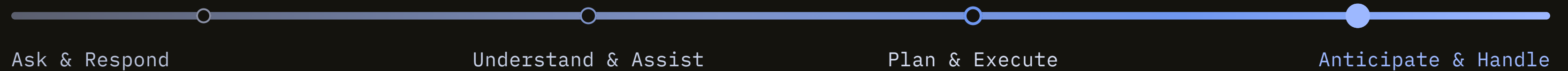
Trust grows when people understand capabilities, boundaries, and behavior.

New design questions.

- 01 What can the AI do *autonomously*?
- 02 What requires *approval*?
- 03 How is work *reviewed & verified*?
- 04 How do people maintain *awareness*?



The future of AI is a *spectrum* of interaction patterns.



The most important thing we design is the *relationship* people build with intelligent systems.

LET'S STAY IN TOUCH

Thank *you.*

Questions or ideas? Let's connect!

EMAIL

• mary.gansallo@gmail.com

LINKEDIN

• [in/mary-gansallo](https://www.linkedin.com/in/mary-gansallo)

