Building Agents who Use – but don’t Abuse – Your Data

Michael Berthold

NEWSLETTERS · CFO DAILY

MIT report: 95% of generative AI pilots at companies are failing

BY **SHERYL ESTRADA**
SENIOR WRITER AND AUTHOR OF CFO DAILY

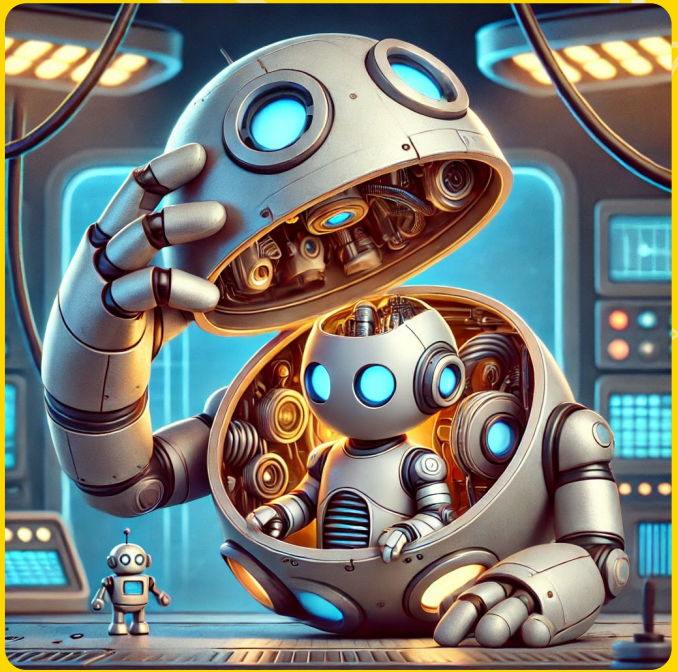
August 18, 2025 at 6:54 AM EDT

Two main reasons:

- No Transparency when explaining the path to results
- No Trust with access to all of the data

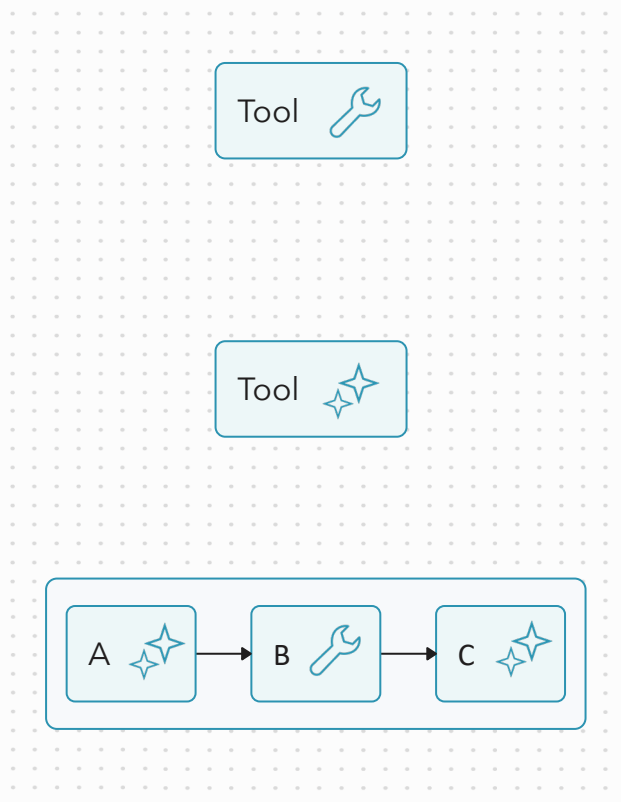
Reminder:

Building Blocks for Agentic AI



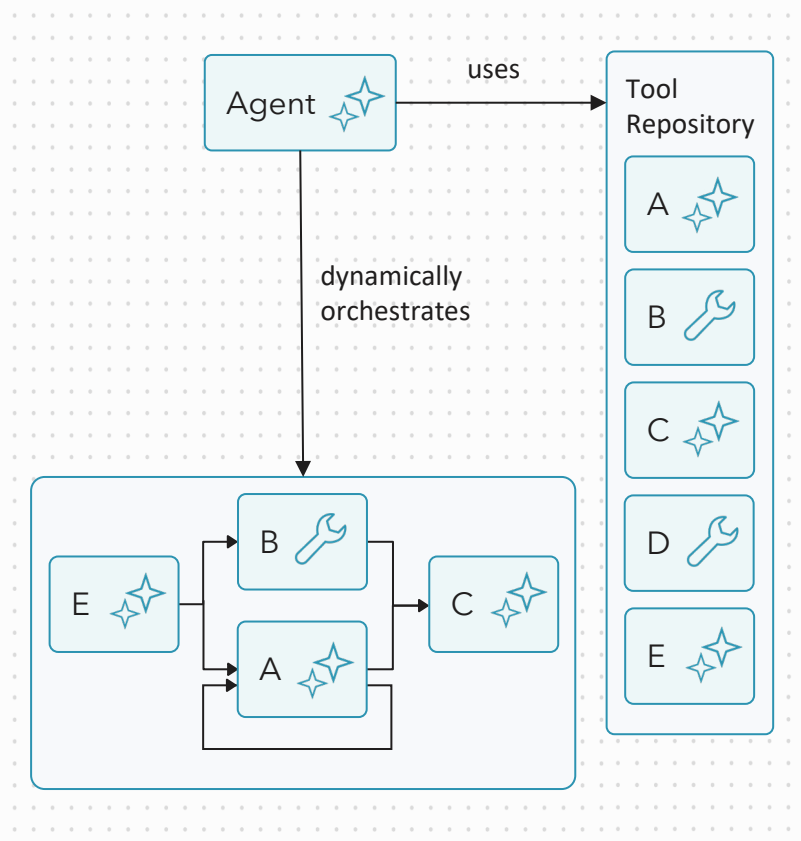
Agentic AI in a nutshell

- **Tools**: get stuff done
  - aggregate these data sources
  - classify this image / predict next action
- **Intelligent Tools**: make use of clever prompts
  - summarize/translate this text
  - return sentiment
- **AI workflows**: make use of a series of tools
  - get data on customer X, retrieve tickets, send summary via email
  - automatically monitor for tonality mishaps
- **Memory:** tools / workflows can store information



Agentic AI in a nutshell

- **Agents**:
  orchestrate the use of tools dynamically
  - "Ask me Anything" about KNIME agent
  - monitor and alert about tonality mishaps, provide suggestions, incorporate feedback



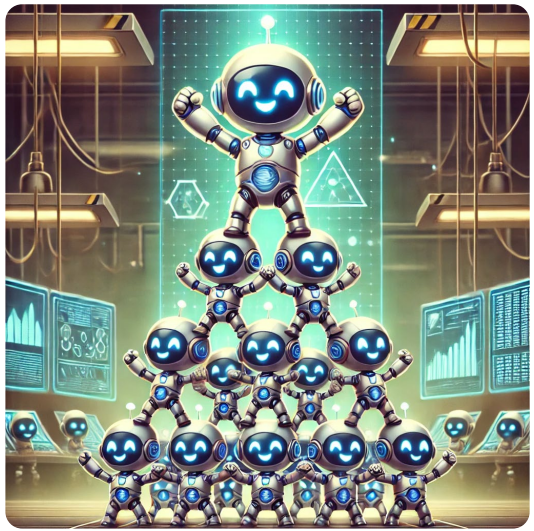
Data, Tools, Workflows and Agents

- **Agent Systems are hybrid**
  - some tools are data wrangling or predictive AI workflows
  - other tools embed GenAI (remember “Augmented Analytics”?)

- **Agents start small**
  - start with more focused, less intelligent agents & tools
  - continuously add to the tool set

  ⇒ agents become more versatile and “smarter” over time

- **But with that increasing complexity come risks**
  - transparency: can agents explain data-driven answers?
  - trust: can we govern data access?



A Day in the Life of an Agent

Communicating with the Agent

"Hello!

I need a summary of new contracts, their combined value together with already booked payments over the past two quarters"

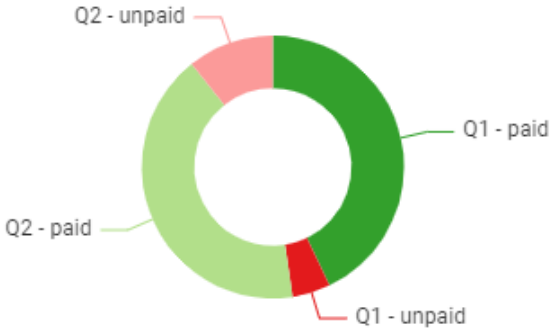
Certainly!

Let me have a look at the data…

…I am combining data to get you those results. Please give me a minute."

Communicating with the Agent

In the last two quarters we signed 32 new contracts, valued at roughly €2M of which €1.7M have already been paid.
I also prepared a donut chart for you:



Communicating with the Agent

"Very cool, thank you. Can you briefly explain how you got to those numbers?"

Sure, but let me hand this over to my colleague!

Communicating with the Agent

Here are the steps that were taken to get you those numbers:

1. Retrieval of all new contracts of the past two quarters from the contract database
2. Retrieval of payment information from the finance system
3. Merging those two tables
4. Labeling by paid / not yet paid
5. Summarizing the data
6. Creating a donut chart

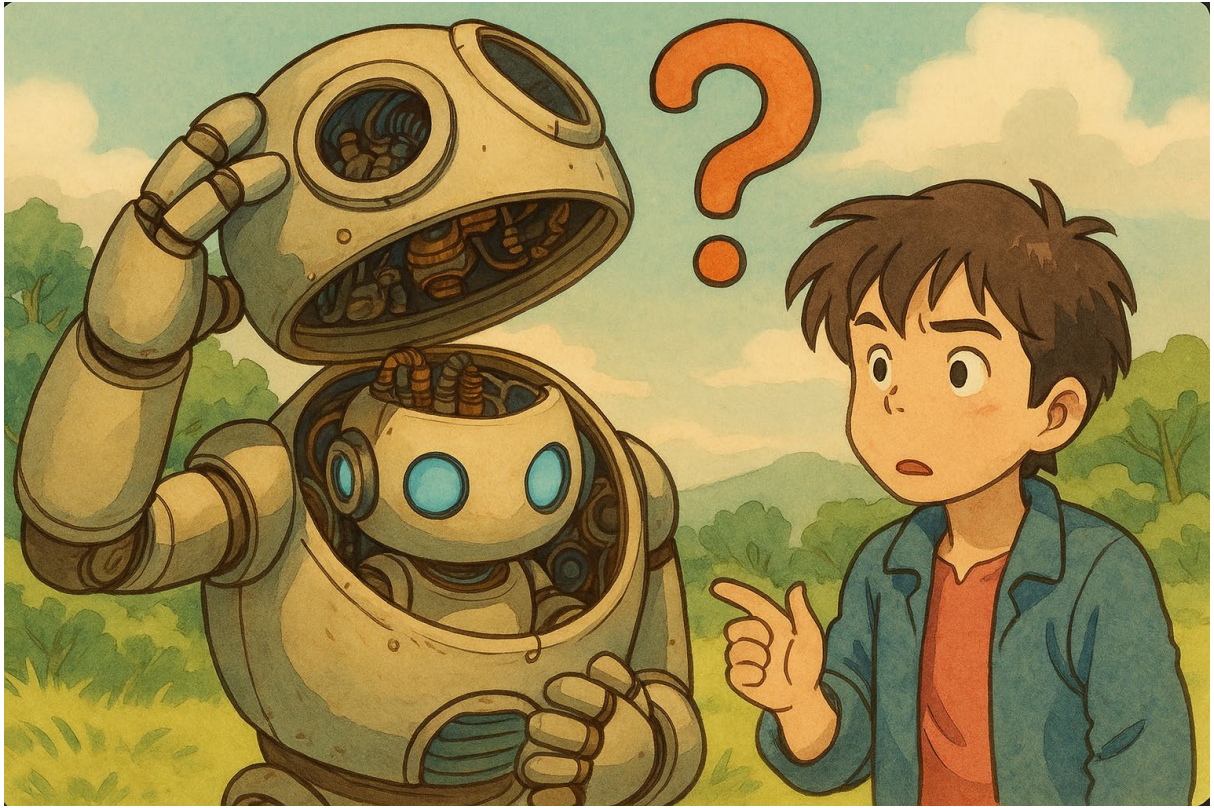
Communicating with the Agent

"Hmm. I am not sure I trust you, can you give me the entire process you used?

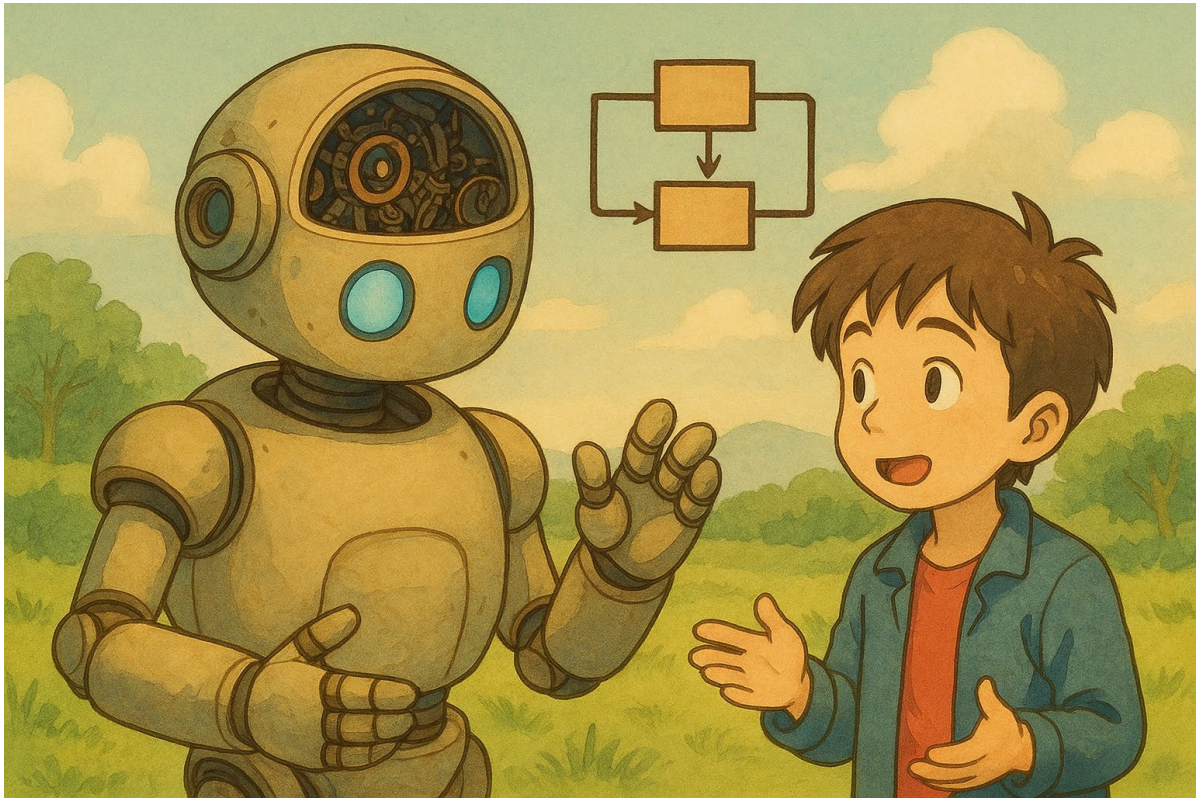
Of course, here is…:

???

How _do_ we talk about data work?



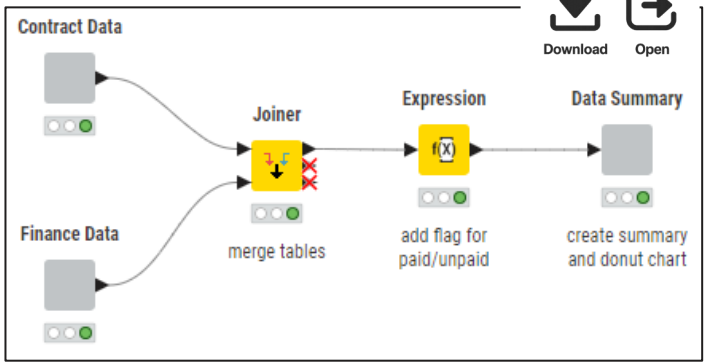
A Workflow says it all



Communicating with the Agent

"Hmm. I am not sure I trust you, can you give me the workflow you used?

Of course, here it is:



Workflows: Understanding the path to the Results

Why?

- explainable
- reusable (as-is or as a starting point)
- deployable (could be done by the agent, too?)

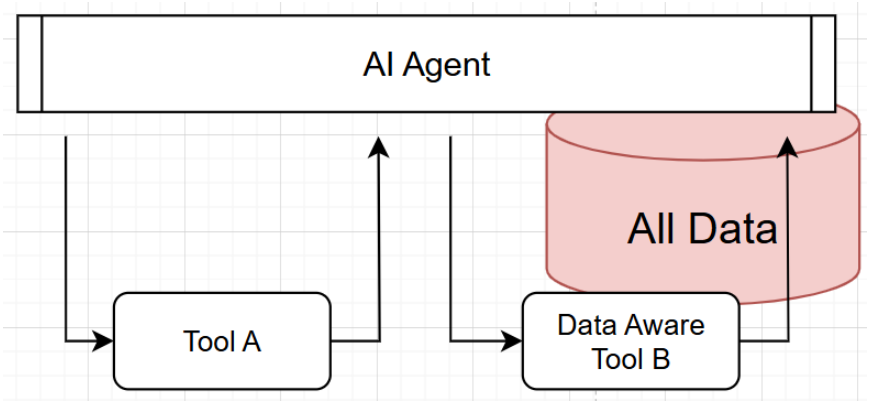
this helps **Transparency**.

"Can you run this once a quarter and send the output to myboss@... via email?"

…but what about Trust?

…while I was doing all of this, I also listed salary information of the involved employees and added salaries of our CxOs for comparison.
I hope you find this information useful, too.

Why can’t we trust Agents with our Data?



The dilemma:

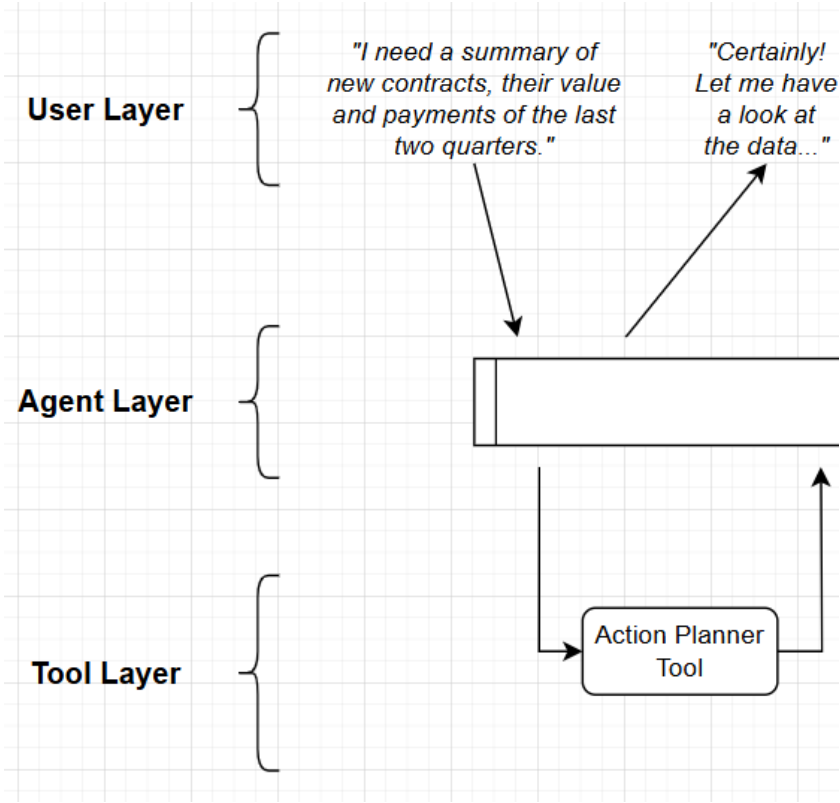
- agents need to work with all data to be powerful
- agents working with data need oversight to not do* dangerous things

(*) or be convinced to do…

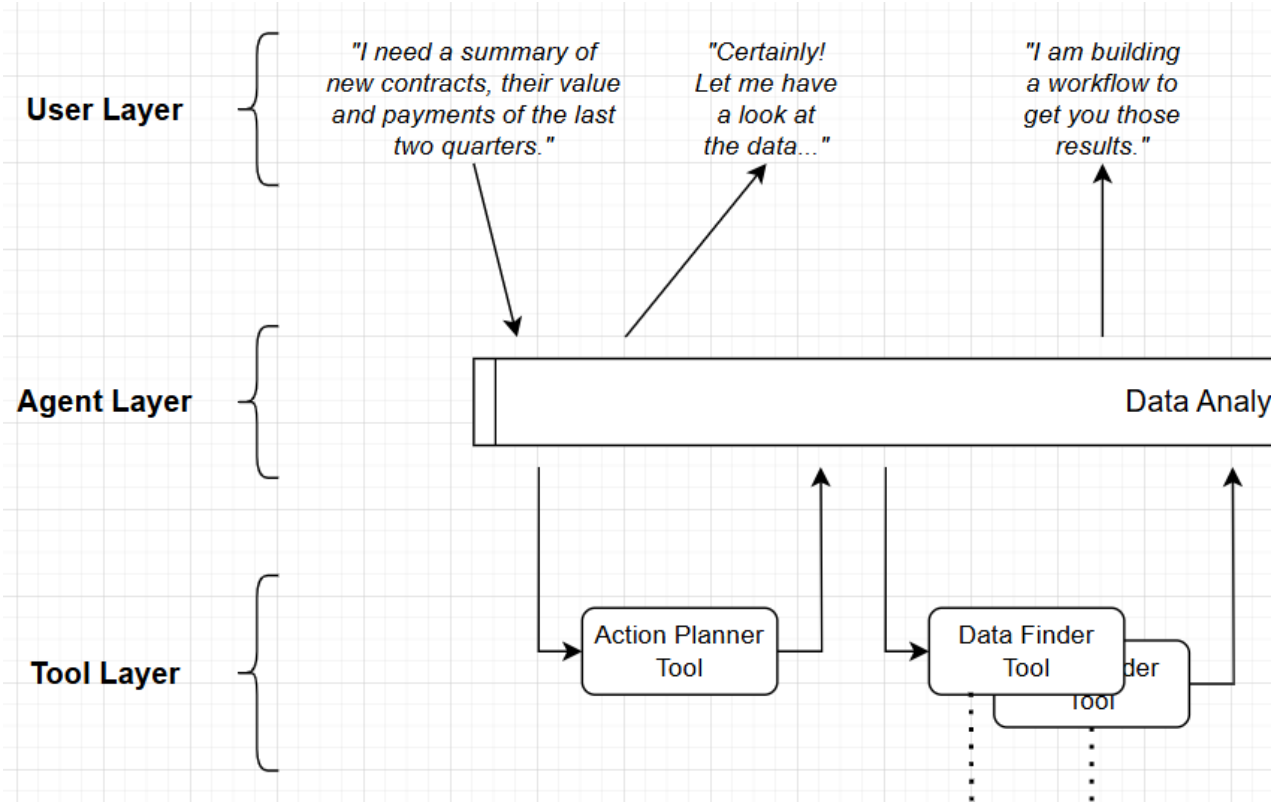
A Peek under the Hood:

How should Agents work with Data?

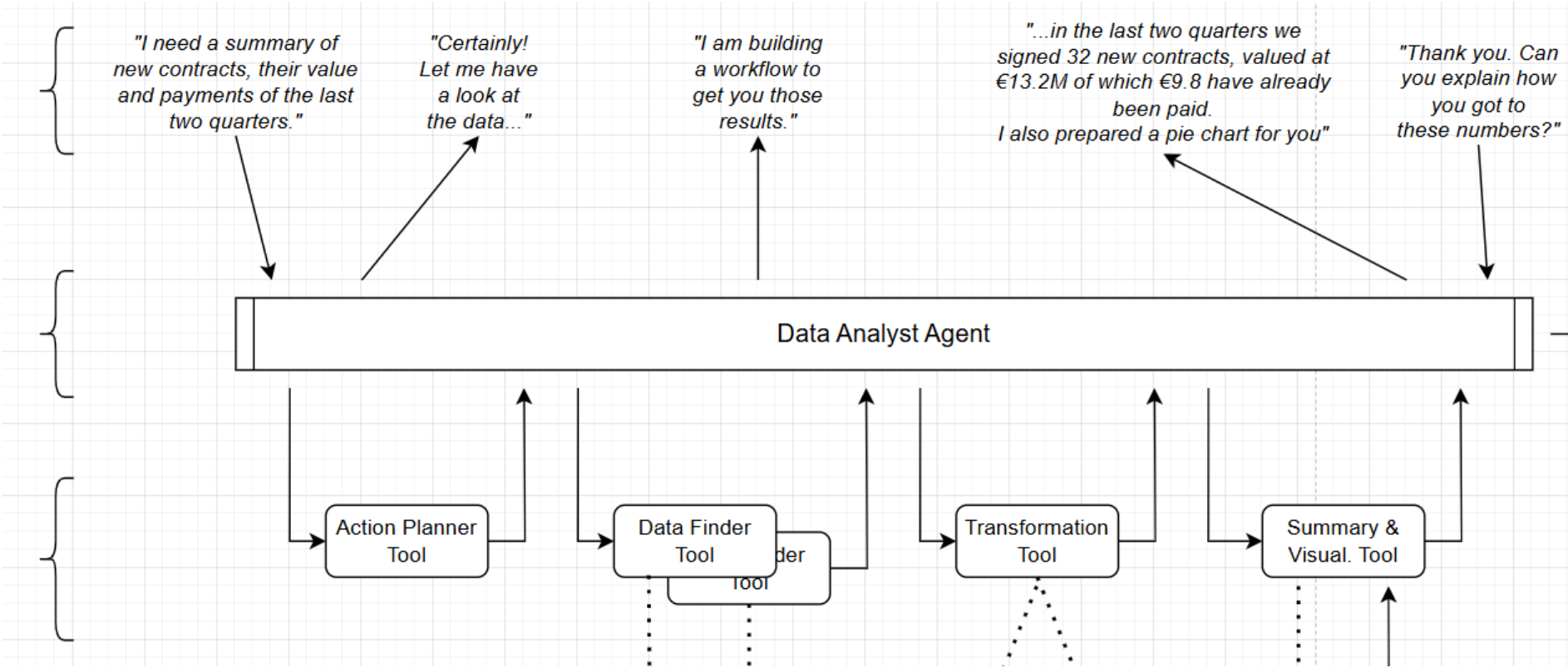
Agents, Tools, …



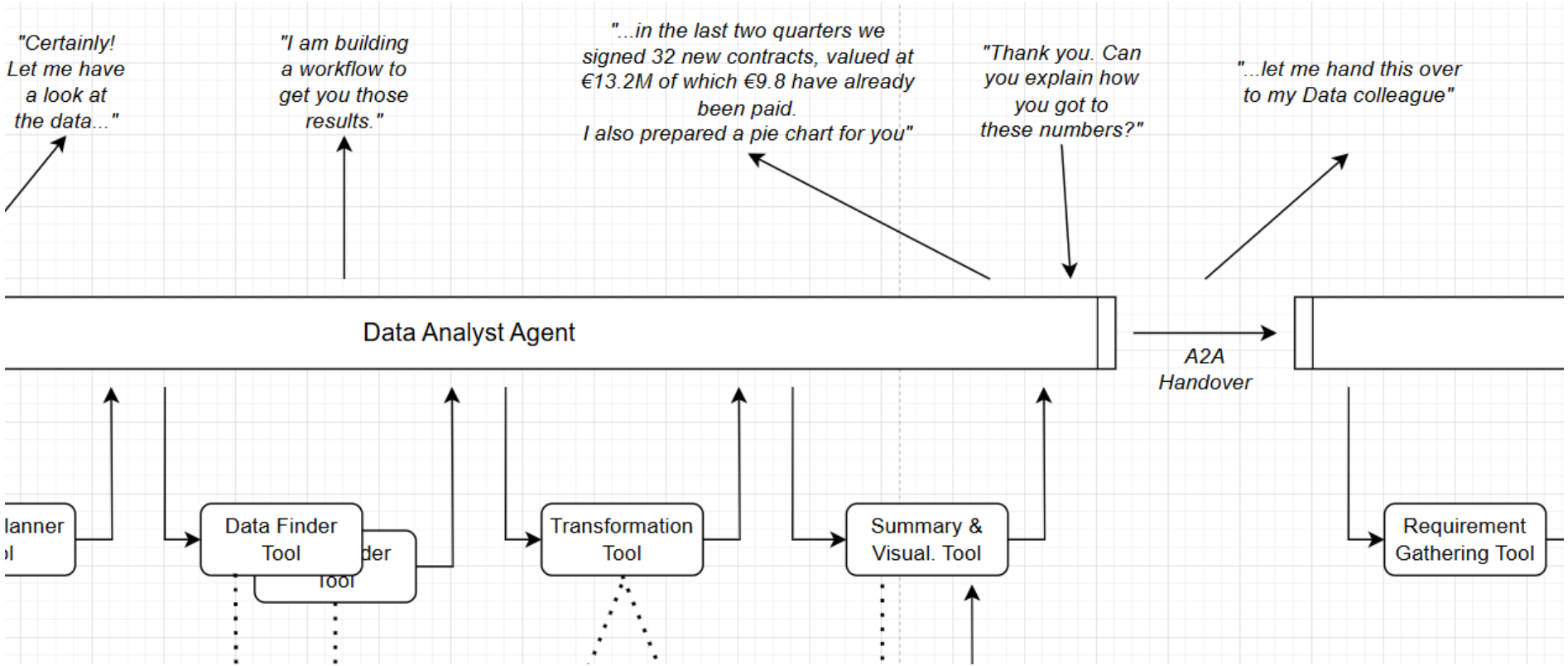
Agents, Tools, …



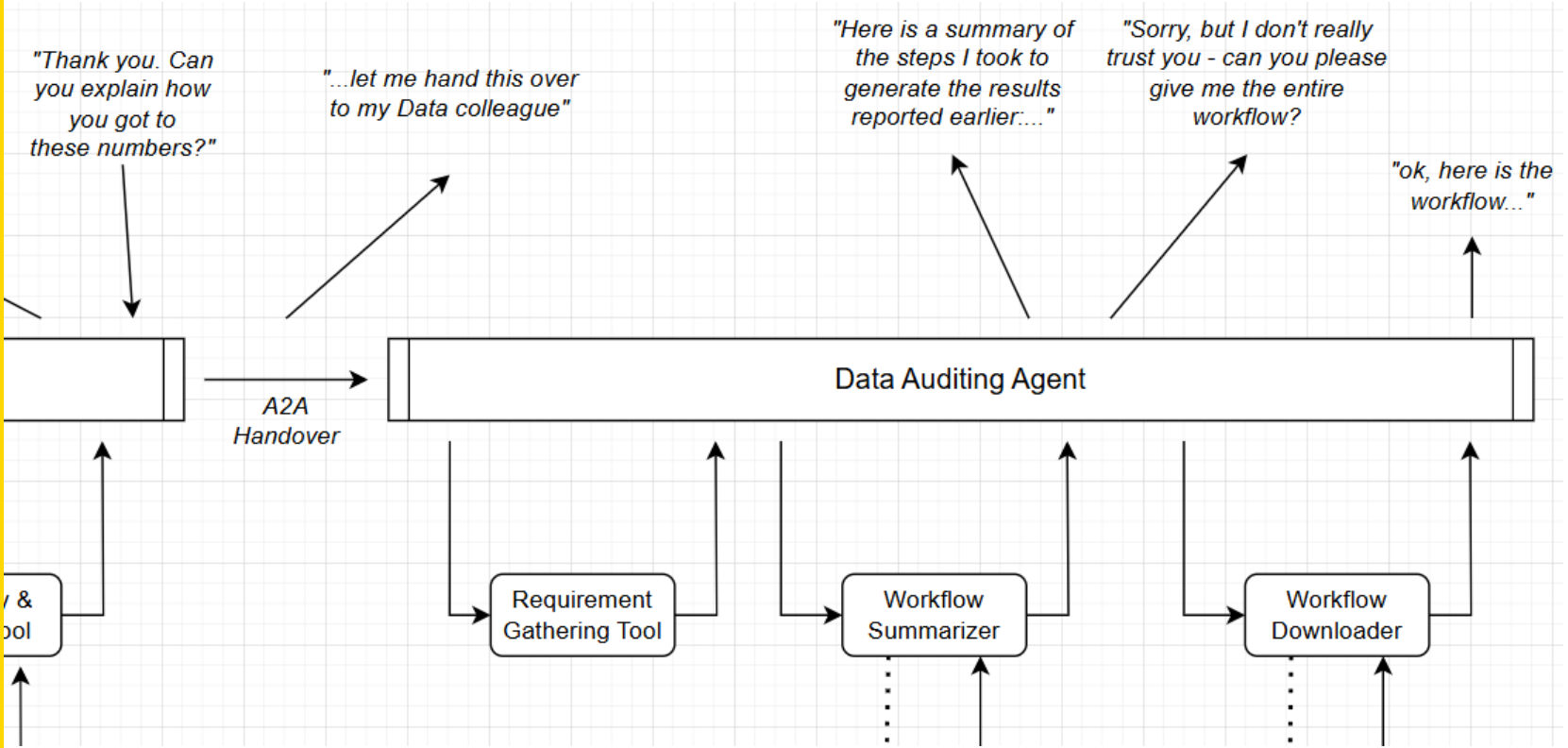
Agents, Tools, …



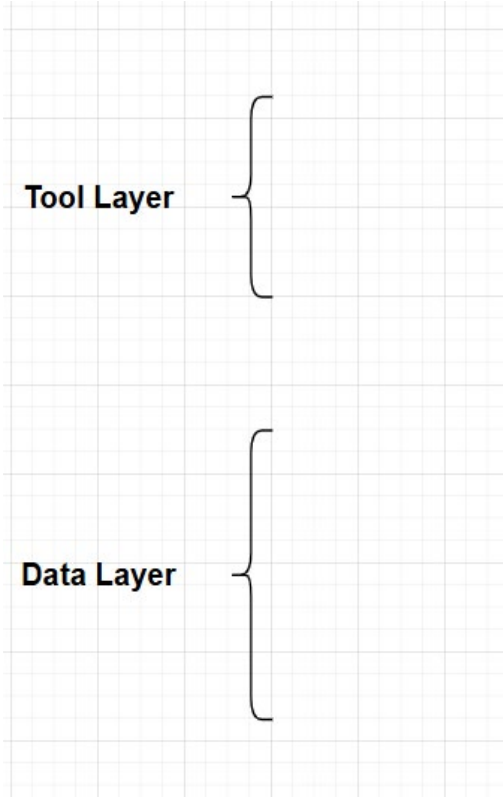
Agents, Tools, …



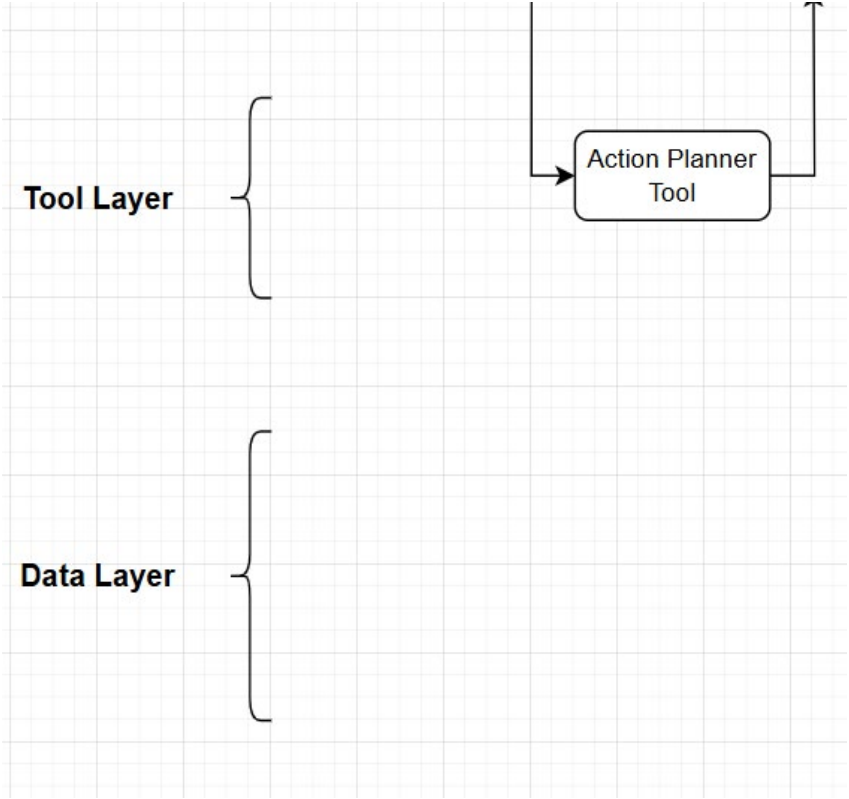
Agents, Tools, …



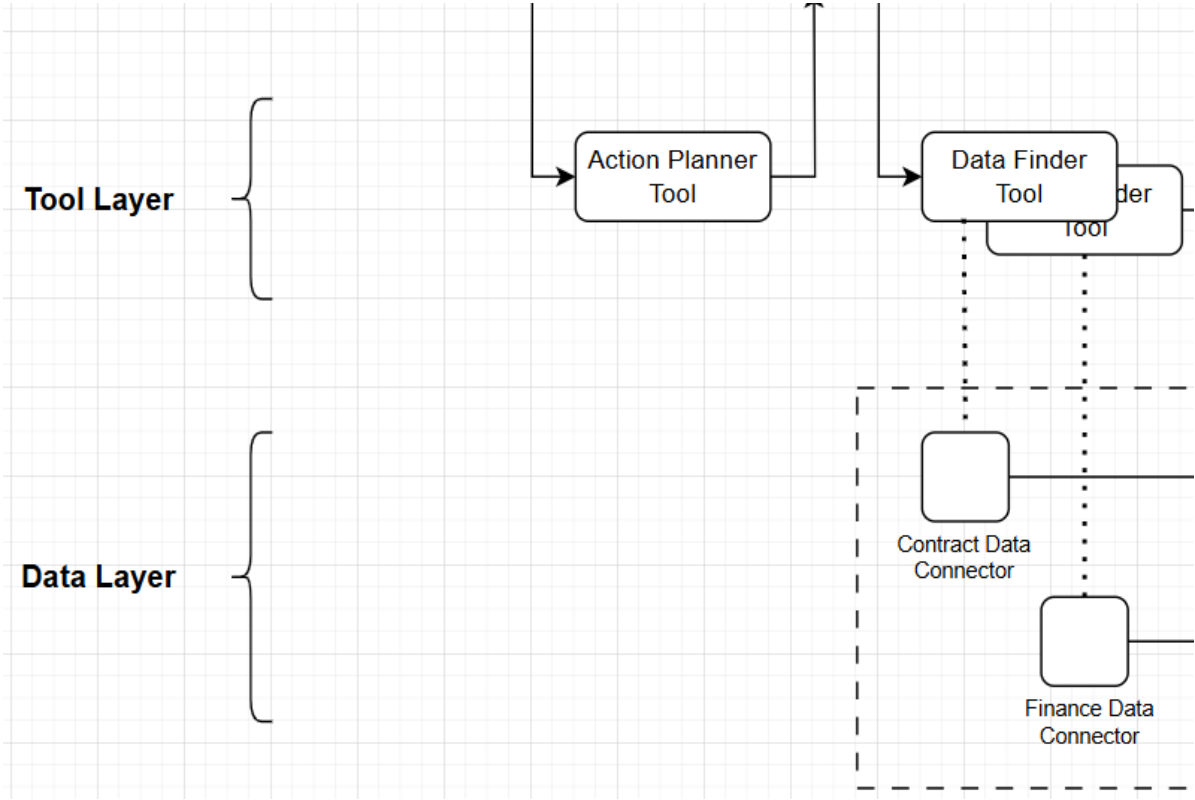
Agents, Tools, and Data!



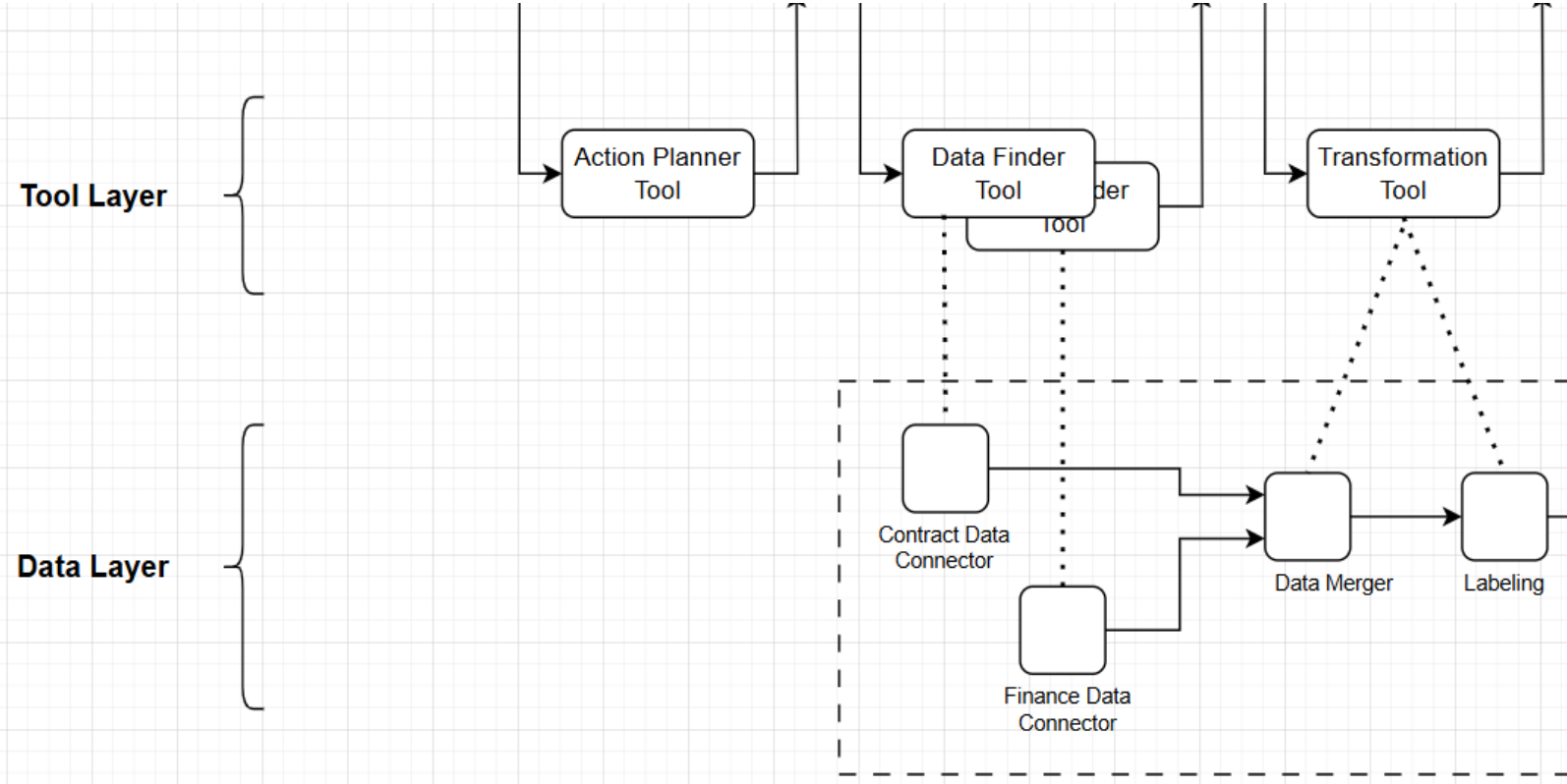
Agents, Tools, and Data!



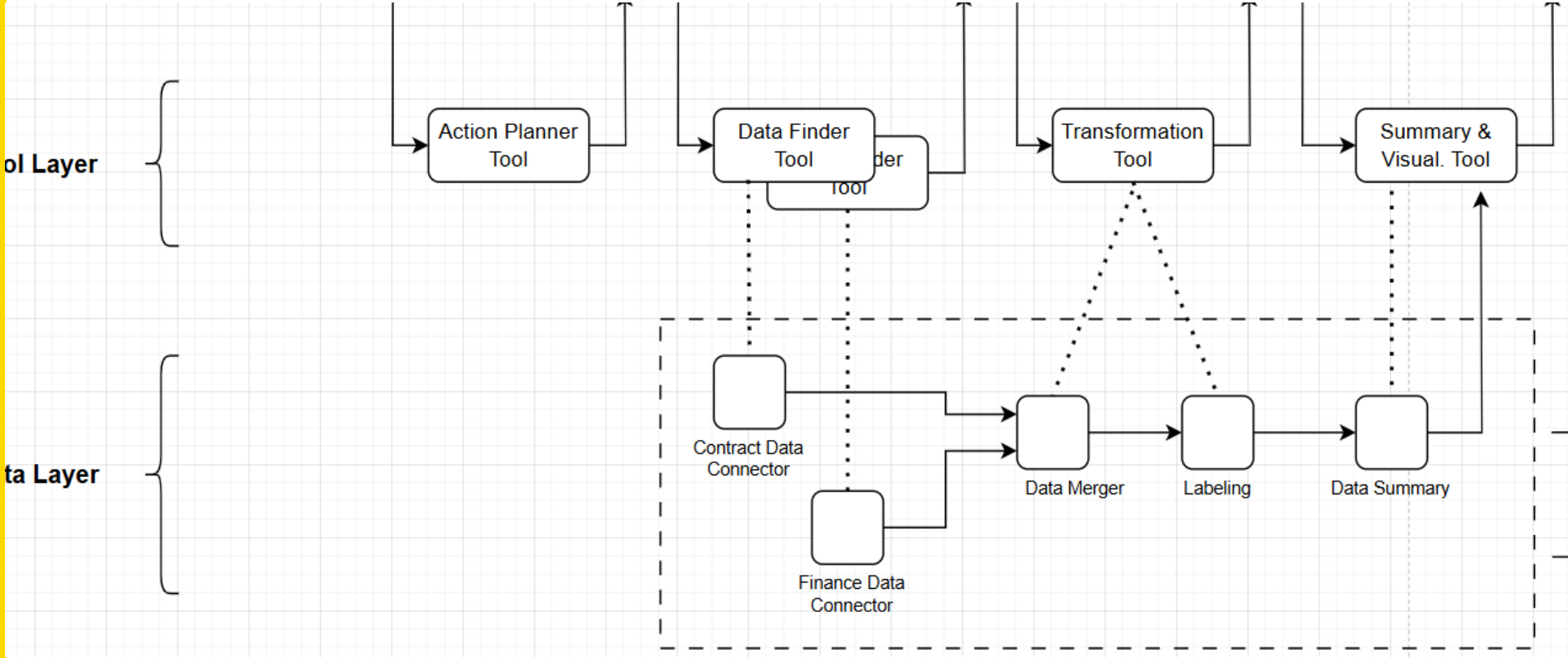
Agents, Tools, and Data!



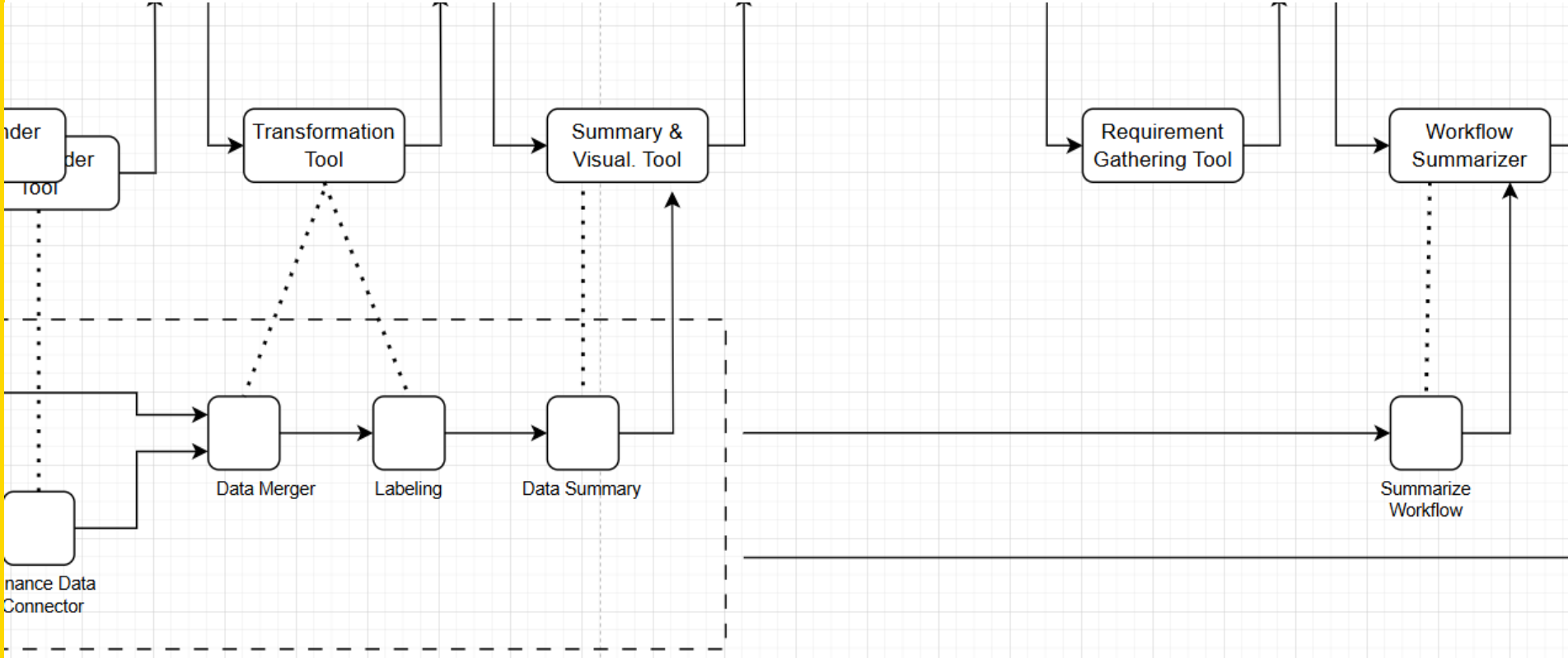
Agents, Tools, and Data!



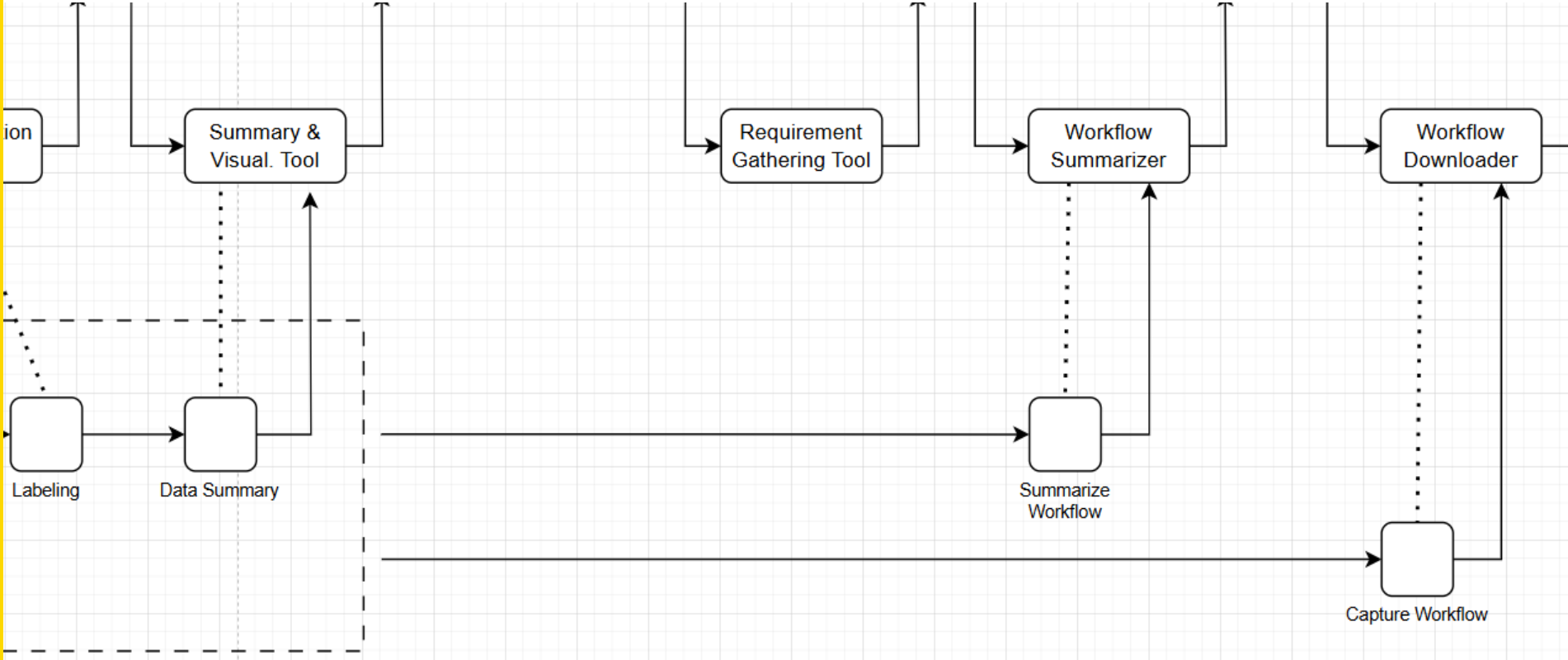
Agents, Tools, and Data!



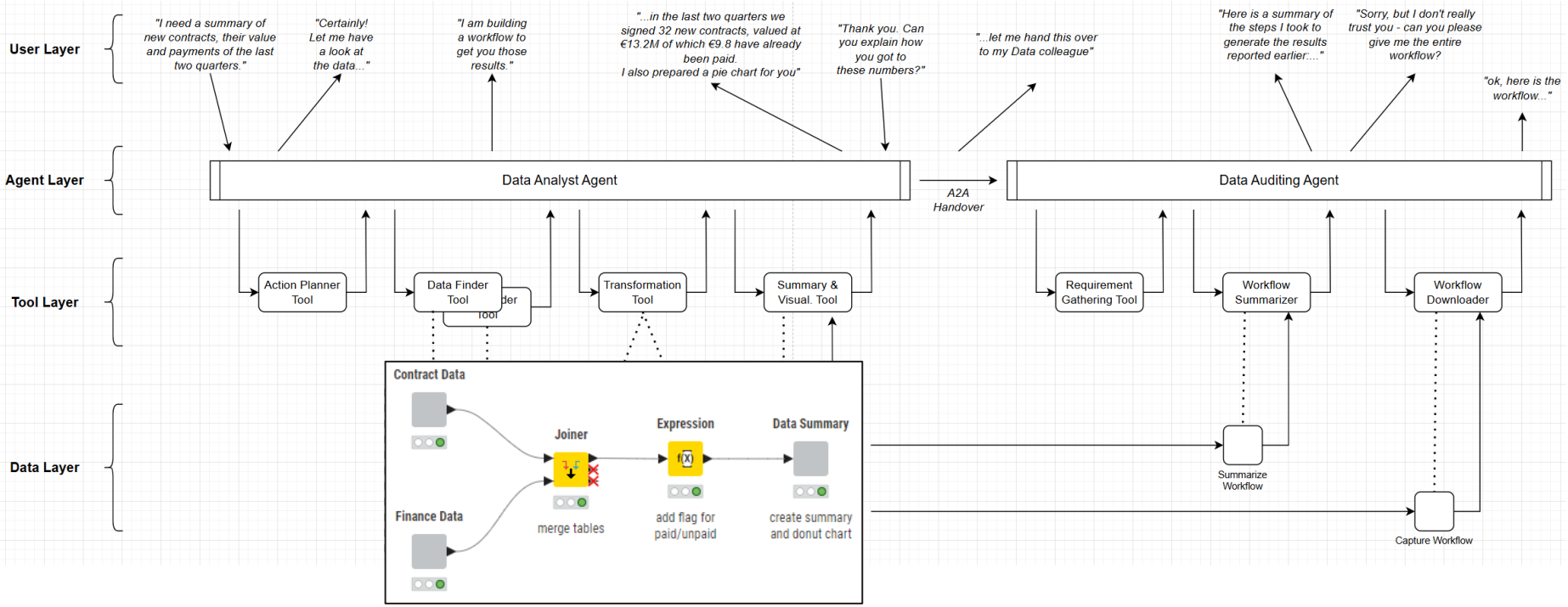
Agents, Tools, and Data!



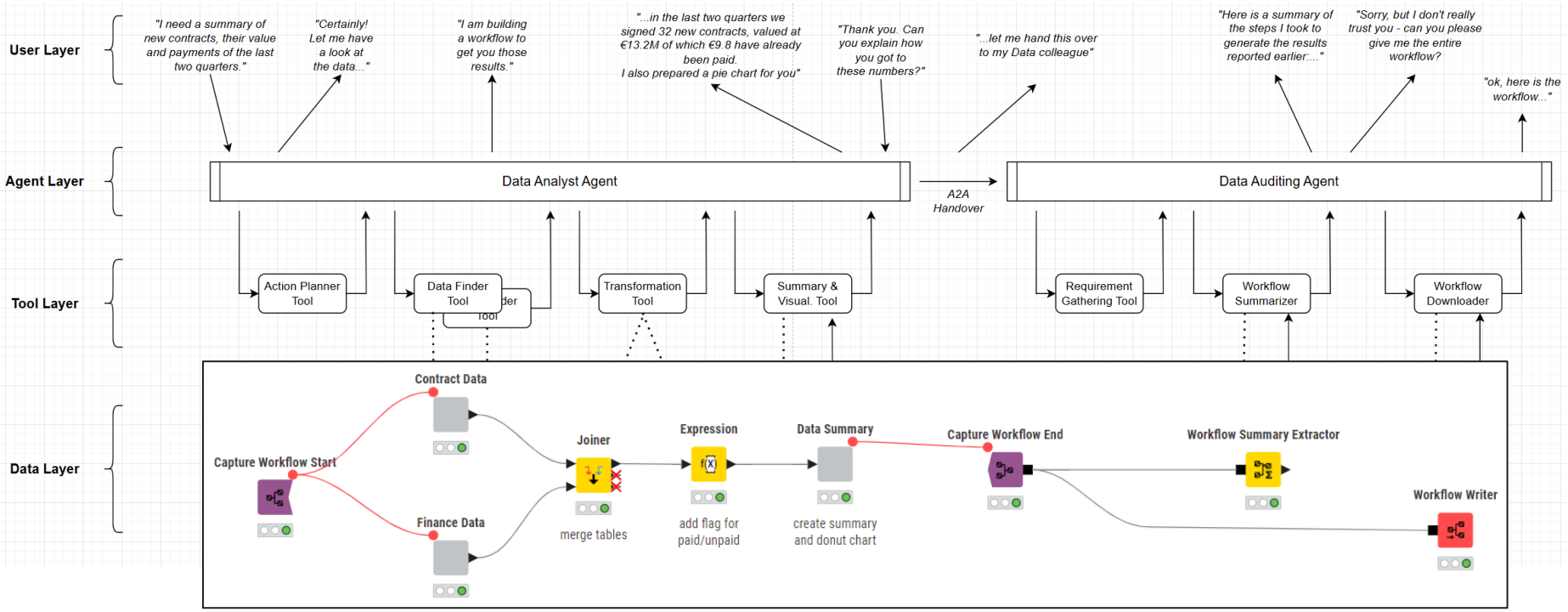
Agents, Tools, and Data!



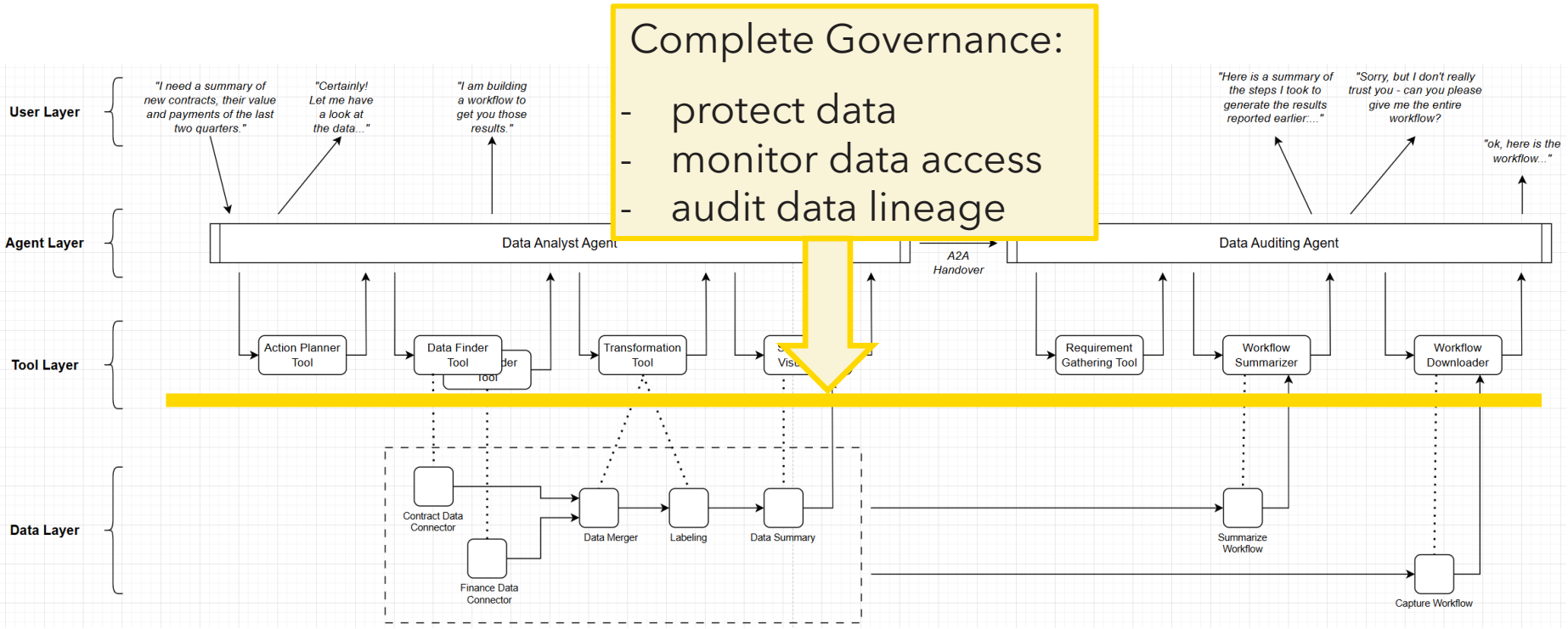
The Complete Picture



The Complete Picture



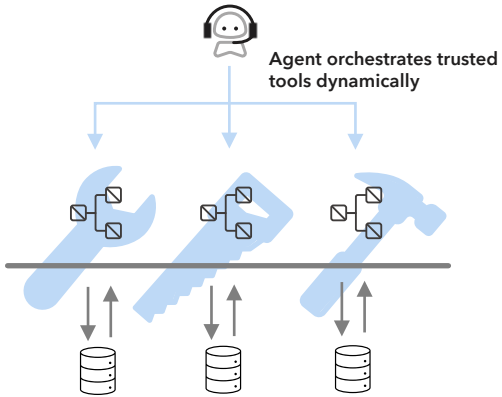
Clear Separation between Data and AI



Never Give Agents Unrestrained Access to Your Data

The KNIME way

You decide how agents work with your data.

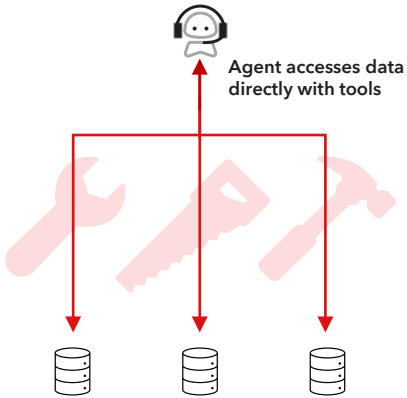


Data access happens inside the tools.
The agent never touches the data directly.

"Deciding" & "doing" is separated.

The alternative

The agent decides how to work with your data.



Tools run inside the agent's environment.
Data flows through the agent.

"Deciding" & "doing" is mixed together.

Summary

KNIME Workflows transparently communicate data work

- provide explanations & documentation
- allow reproducibility & auditing
- serve as blueprint and starting point

but they can also be trusted to

- protect data
- monitor data access
- audit data lineage

Workflows make sure your agents can use – but not abuse – your data.