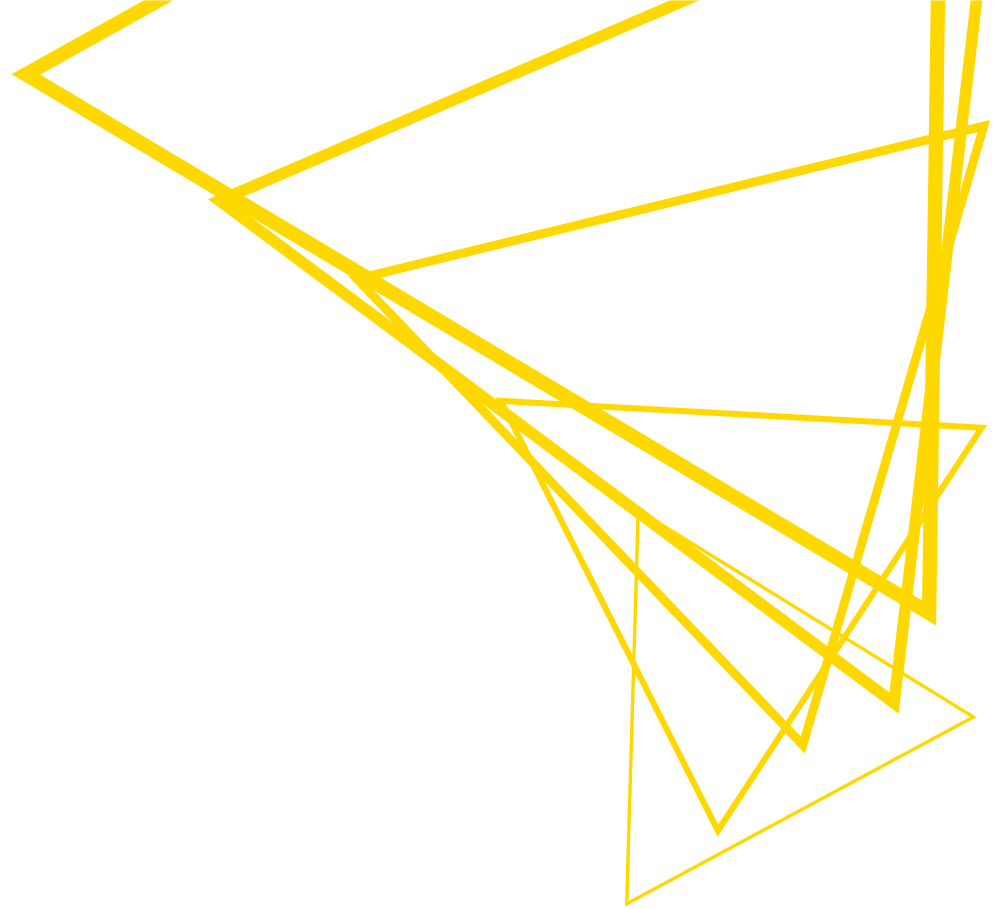


Data Aware Agentic AI

Cognitive, Control, and Data Flows

Michael Berthold

October, 22, 2025



My Agenda

- Demystifying Agents: Build Blocks for Agentic AI
- Working Agents: two real world Examples at KNIME
- Controlling Agents: How to allow Agents to use – but not abuse – Data*

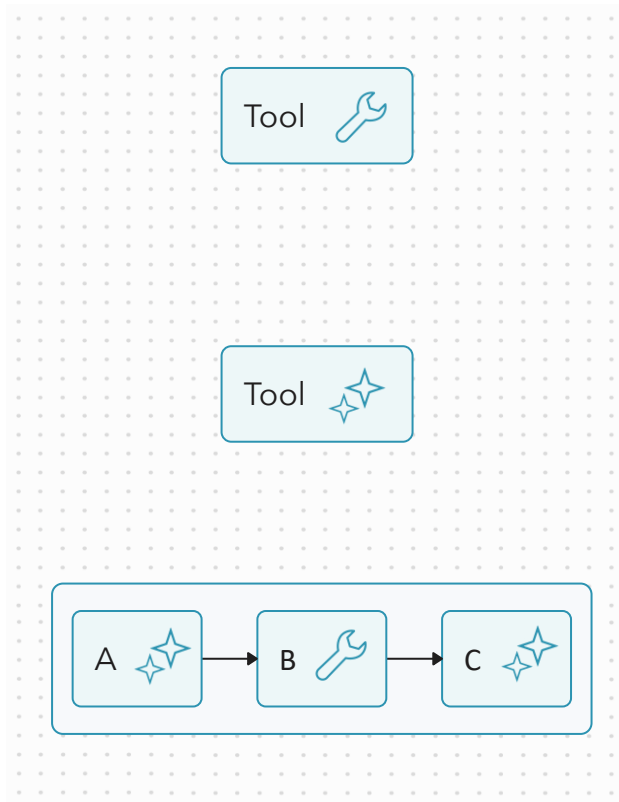
(*) or Devices, Robots, Rockets...

Building Blocks for Agentic AI



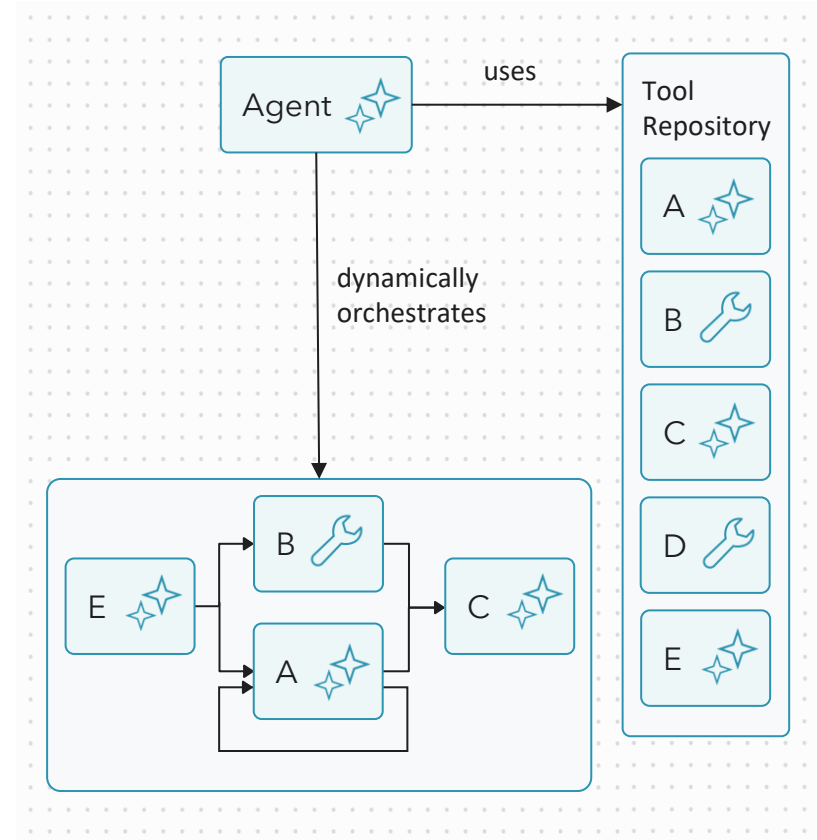
Agentic AI in a nutshell

- **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
- **Agentic Applications:** used by humans
- **Agentic Services:** used by other applications
 - Can be intelligent tools... (“Guardian Agents”?)



Agents & Tools – and KNIME Workflows

Tools:

- check tonality of a document
- translate text
- create image in the style of...



Workflows

Augmented Analytics

- get information about customer
- get user information
- get employee statistics



Workflows

Data Aggregations

- predict monthly growth
- forecast facility usage



Workflows

Predictive AI

- book travel
- schedule ads



Other Agents

Inhouse / as a Service

Agents & Tools – and KNIME Workflows

Data Apps 
Intelligent Apps



REST 
Intelligent Services



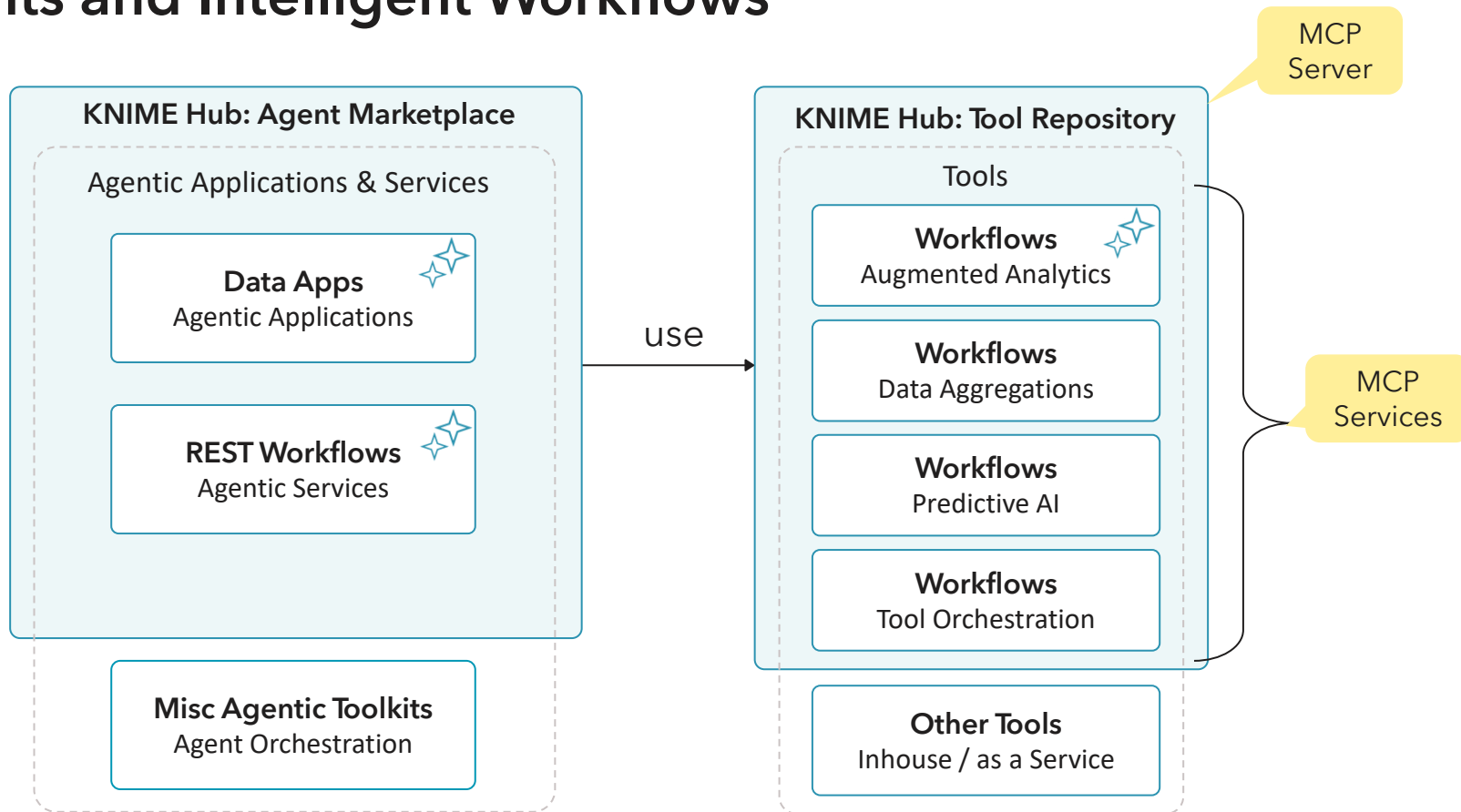
Workflows 
Agent Orchestration



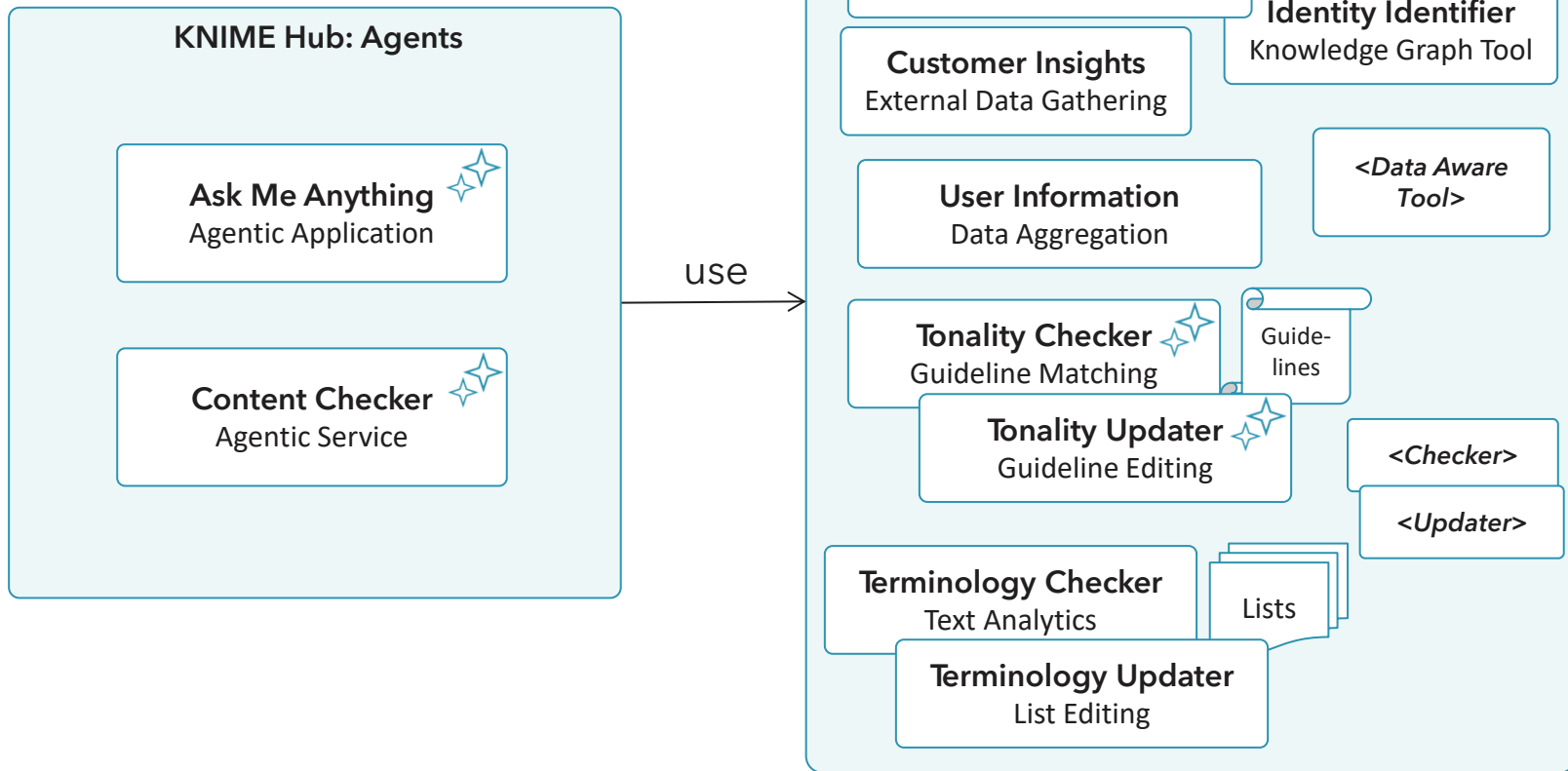
Agentic Apps & Services:

- Marketing Tonality Checker
- Article Summarizer
- Image Corrector
- News Aggregator
- Plan, Execute Plan, Revisit
- Do X, Y, Z in order

Agents and Intelligent Workflows



Agents - Examples



Abstract geometric lines in the top right corner of the slide, consisting of several overlapping triangles and polygons in a light yellow color.

A Real Life Example

The Ask Me Anything (about KNIME) Agent

The “Ask KNIME Anything” Agent



Conversation

What are you? Provide a brief overview of your capabilities.

I am a KNIME internal data agent designed to provide clear and concise responses to inquiries related to KNIME's internal data and tools. My capabilities include:

1. Retrieving company domain information for customer insights.
2. Accessing customer activity data from our CRM system.
3. Generating personalized email drafts based on user bios and usernames.
4. Providing information about KNIME employees, including their roles and locations.
5. Sharing recent topics from the KNIME Forum.
6. Offering detailed user biographies based on KNIME Forum and Community Hub activity.
7. Searching for publicly available information about entities.
8. Identifying top customers based on revenue contributions.

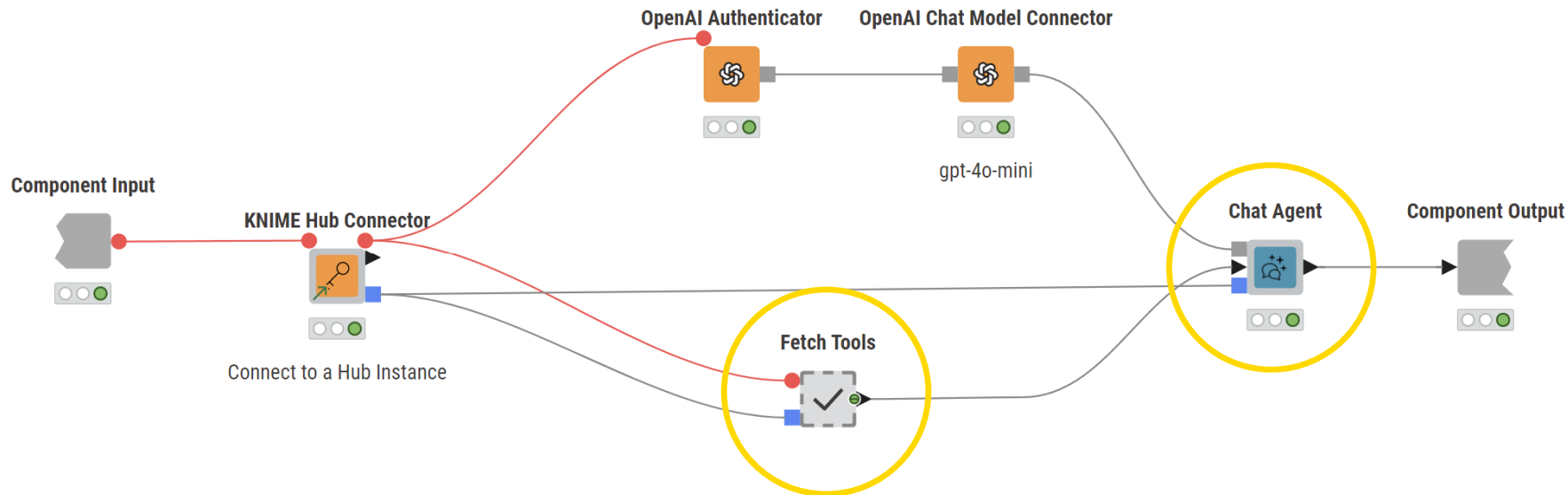
I leverage various internal tools to deliver accurate and relevant information efficiently.



Ask the AI Agent

☐ Advanced Settings

Inside the "Ask KNIME Anything" Agent



Prompt Options for the “Ask KNIME Anything” Agent

Option 1:

“You are a helpful assistant...
...you have access to the CRM System using tool “Salesforce”. You can also retrieve information about support tickets using tool “Zendesk”. You may also want to use the tool “Forum” to find additional information and maybe in using tool “Hubspot” you can also find valuable information around marketing automation. But if someone asks about users, you can...

Technology Centric

Lots of unnecessary detail
What happens if you switch?

Option 2:

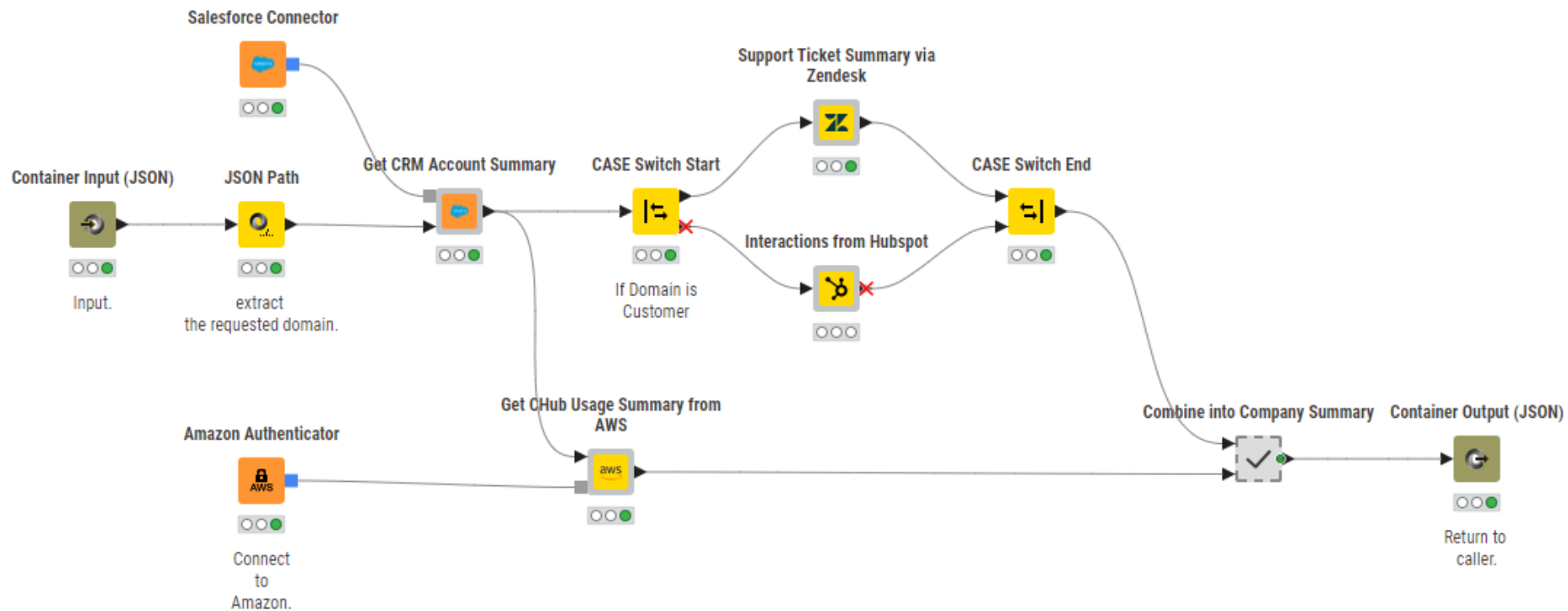
“You are a helpful assistant...
...you have access to information about customers using the tool “customers”.
You can also find information about individual users using tool “users”.

If you need information about KNIMERs,
use tool “employees”.
...

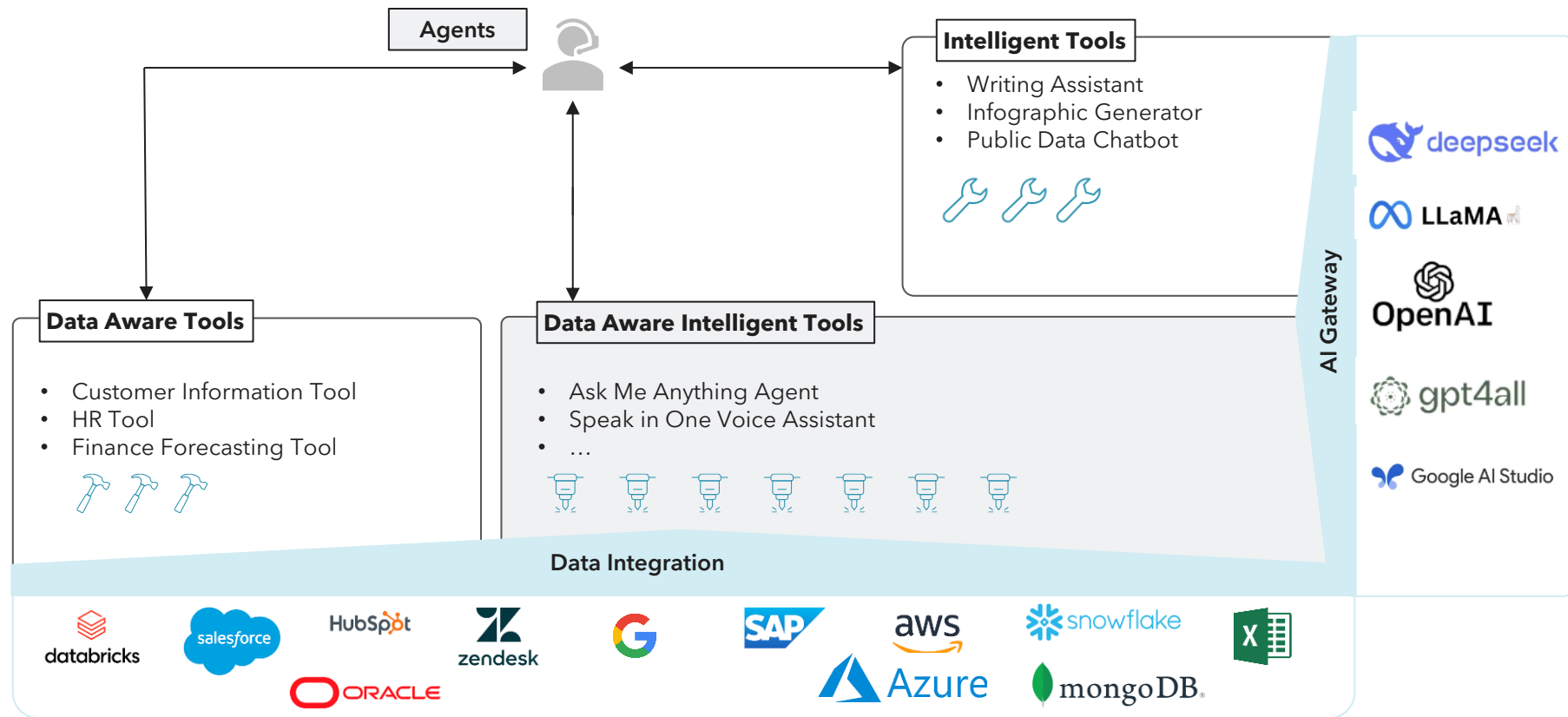
Information Centric

Focusses on relevant details
Easy to switch Technology.

The "Customer Information" Tool



Good data makes good tools ... and better agents



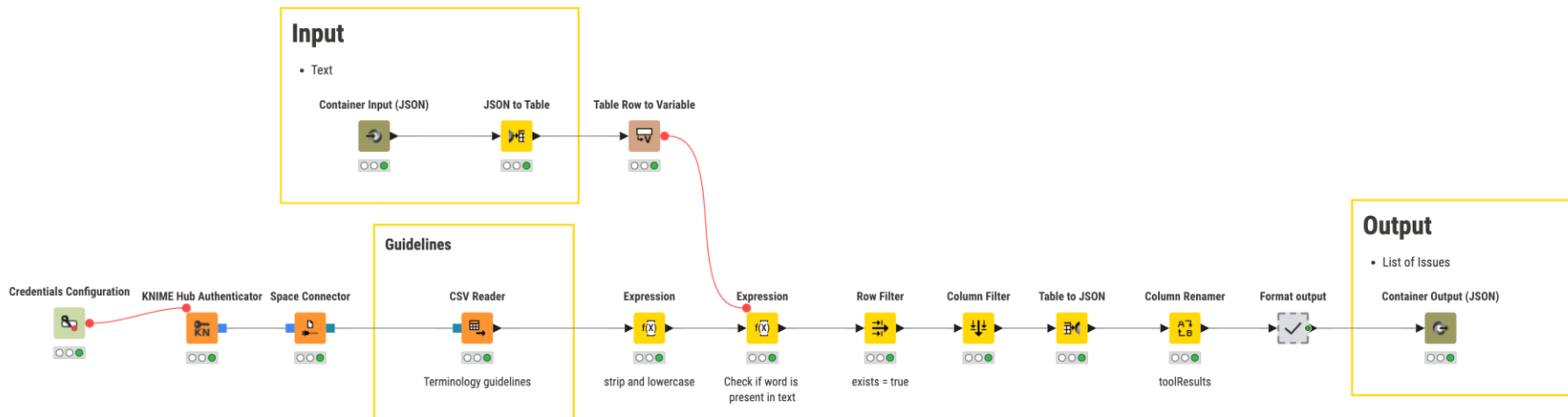
Abstract geometric lines in the top right corner of the slide, consisting of several overlapping triangles and polygons in a light yellow color.

Another Example (this time: bottom up)

Make KNIME speak in one voice

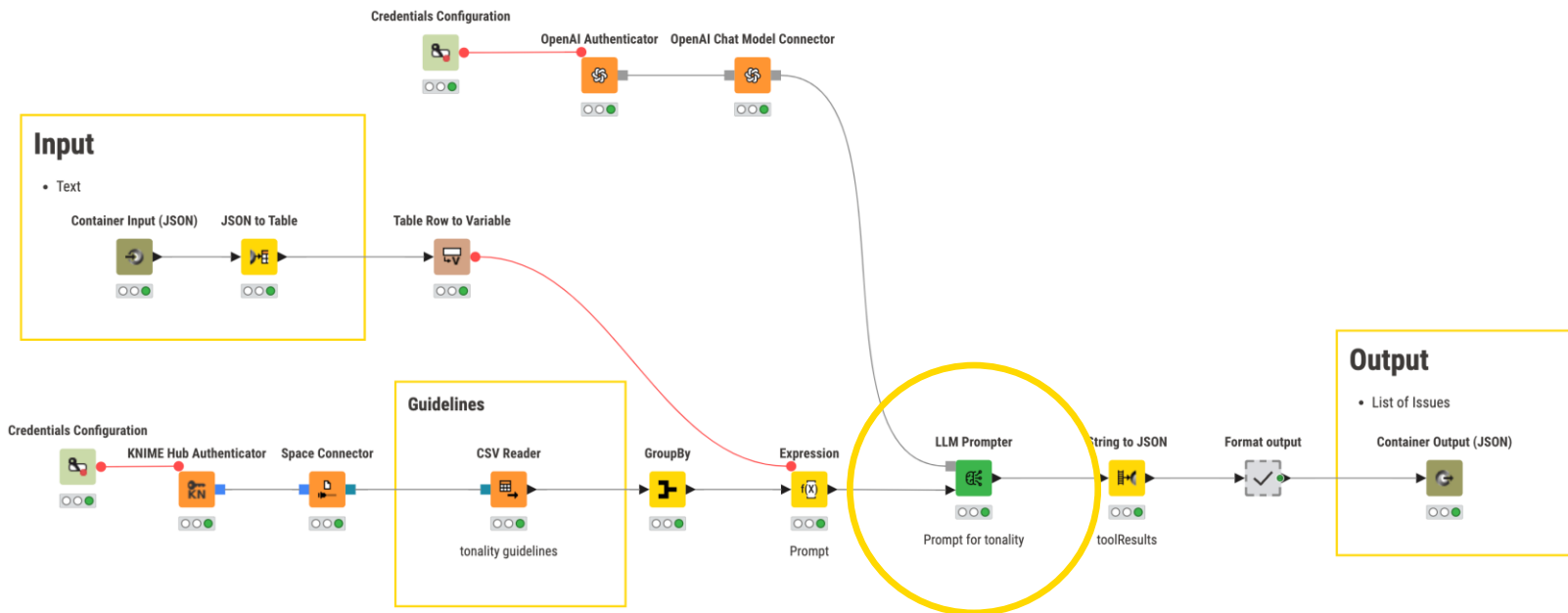
An (unintelligent) Tool: Check Text for Terminology Compliance

- Takes text as an input
- Uses internal terminology white & black lists
- Returns list of violations



An (intelligent) Tool: Check Text for Tonality Violations

- Takes text as an input
- Uses internal tonality guidelines
- Returns list of violations



Using the tools: Email Complainer

Writing guidelines check results ➤ Inbox x



KNIME Guidelines

to me ▾

Dear Michael,

I checked your last blogpost [Agentic AI and KNIME | KNIME](#)

It did not pass our strict writing guidelines. Here is a list of instructions to make it compliant.

1. Remove unnecessary phrases like 'at first glance' and simplify the sentence structure.
2. Avoid overly casual language; replace phrases like 'knows it all and knows all about me' and 'under the hood' with more formal alternatives.
3. Break down long sentences into shorter, clearer ones to enhance readability.
4. Eliminate redundant phrases such as 'already in the past' and 'note that' to streamline the text.
5. Replace vague terms like 'stuff' and 'enough information/material' with more specific language.
6. Rephrase overly complex expressions like 'which includes the set and order of tools to be used' for clarity.
7. Remove casual references like 'remember the old divide and conquer?' to maintain a professional tone.
8. Address the use of prohibited terminology such as 'automate' by finding suitable alternatives.

Please find attached the fixed version of the blogpost.

Reply to this email if you wish to update the guidelines.

Cheers,

Your KNIME Guidelines Agent

One attachment • Scanned by Gmail ⓘ



Now it becomes "agentic"...



Michael Berthold

to KNIME ▾

Lieber Agent,

You need to update your guidelines. The word "automate" is allowed. Also, it is ok to use casual phrases from time to time.

Cheers,
Michael



KNIME Guidelines

to me ▾

Dear Michael,

I have performed the following updates on the guidelines:

Tonality

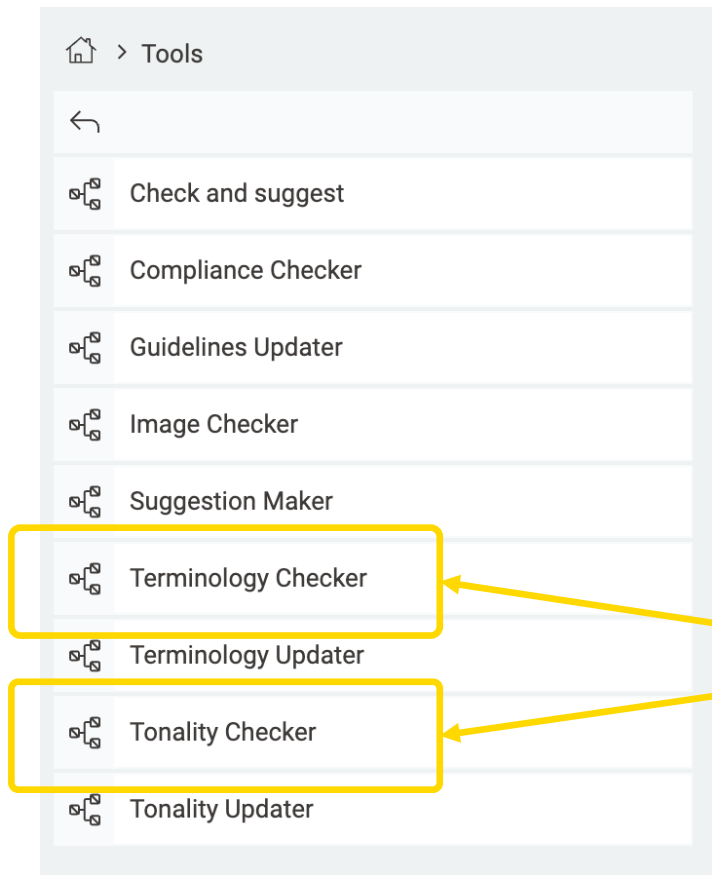
Old guideline: Avoid being overly robotic or too casual.

New guideline: Avoid being overly robotic, but allow casual phrases occasionally, while ensuring they remain appropriate for the context.

Terminology

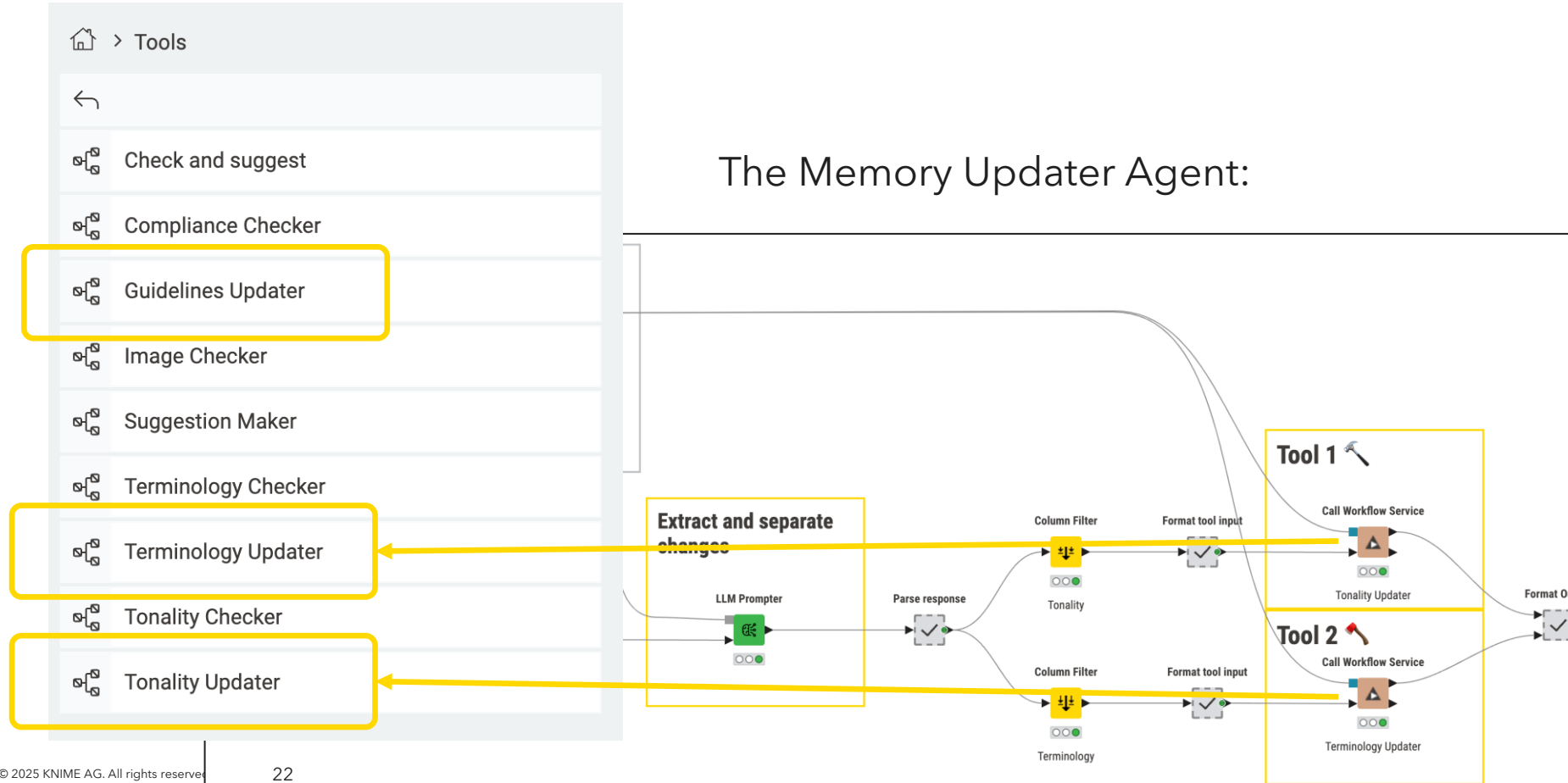
Removed forbidden words: Automate

Under the hood

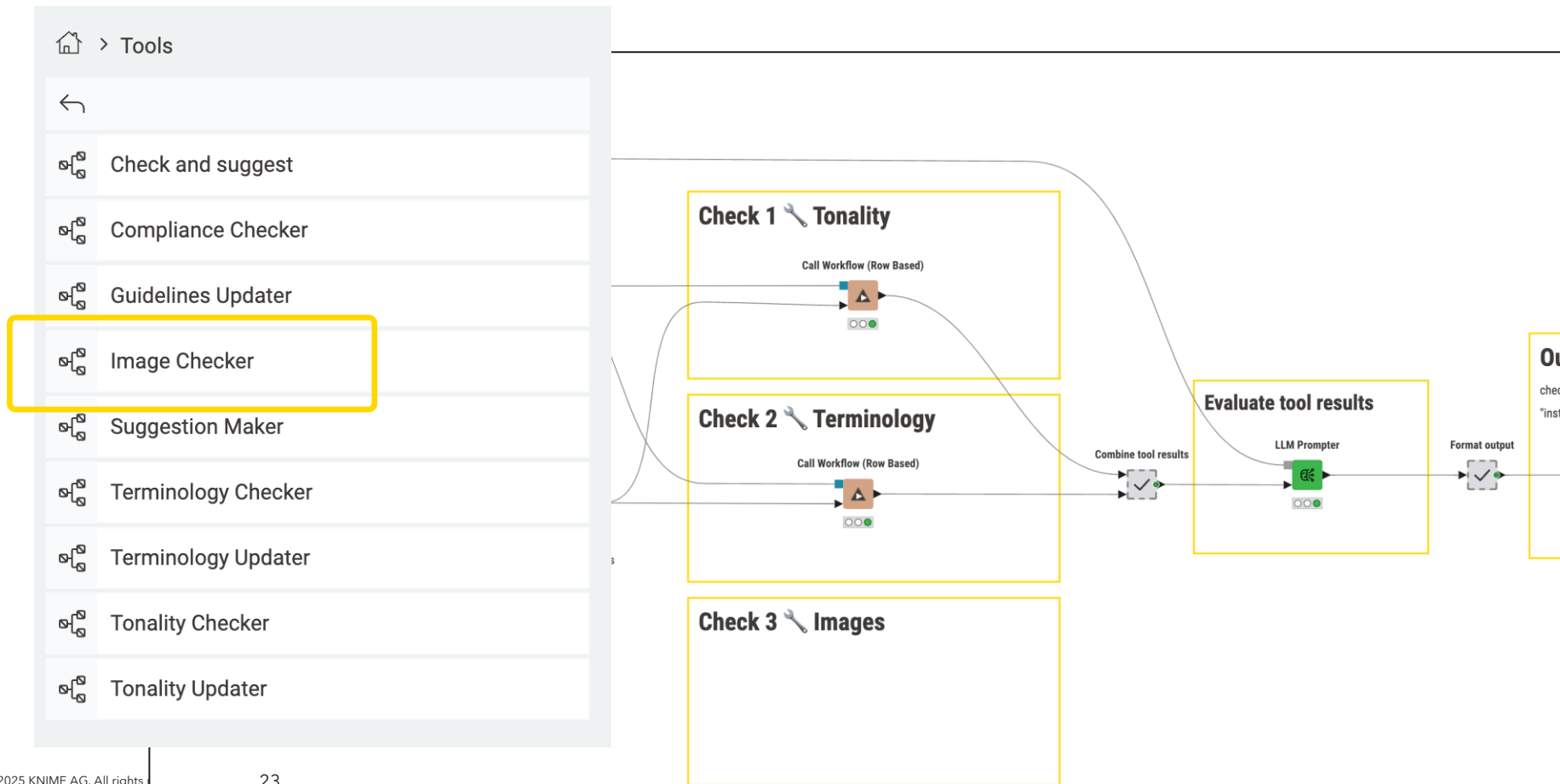


We have seen those two...

Under the hood



Adding Capabilities



Summary: Constantly Adapting Style Checker Agent

Where is this going?

- observer of all outward facing material
- quiet, reliable, and always-learning

Agentic Insights:

- Broadening scope and capabilities (=other modalities to check):
⇒ just add checker and updater tools
- Agentic System keeps and updates global memory

Summary: Data, Tools, and Workflows make Agents

- **Agent Systems are hybrid**

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

- **Agents start small**

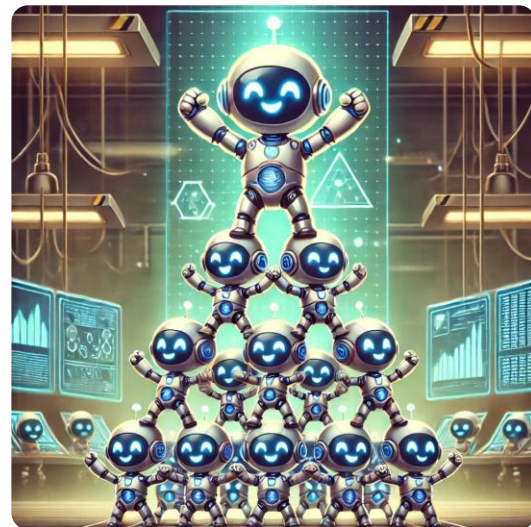
- start with more focused, less intelligent agents & tools
 - continuously add to the tool set
- ⇒ agents become more versatile and “smarter” over time

- **Remember?**

- Object Oriented Programming
- Micro Service Architectures

- **But with that increasing complexity come risks**

- transparency: can agents explain data-driven answers?
- trust: can we govern data access?



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
- No Trust

when explaining the path to results
with access to all of the data

Abstract geometric lines in the top right corner, consisting of several overlapping, thin, light yellow lines that form a complex, angular pattern.

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!

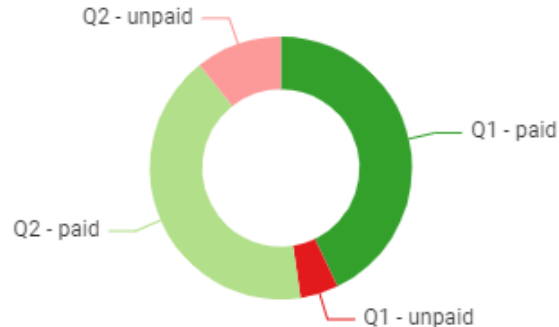
Let me have a look at the data...

...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

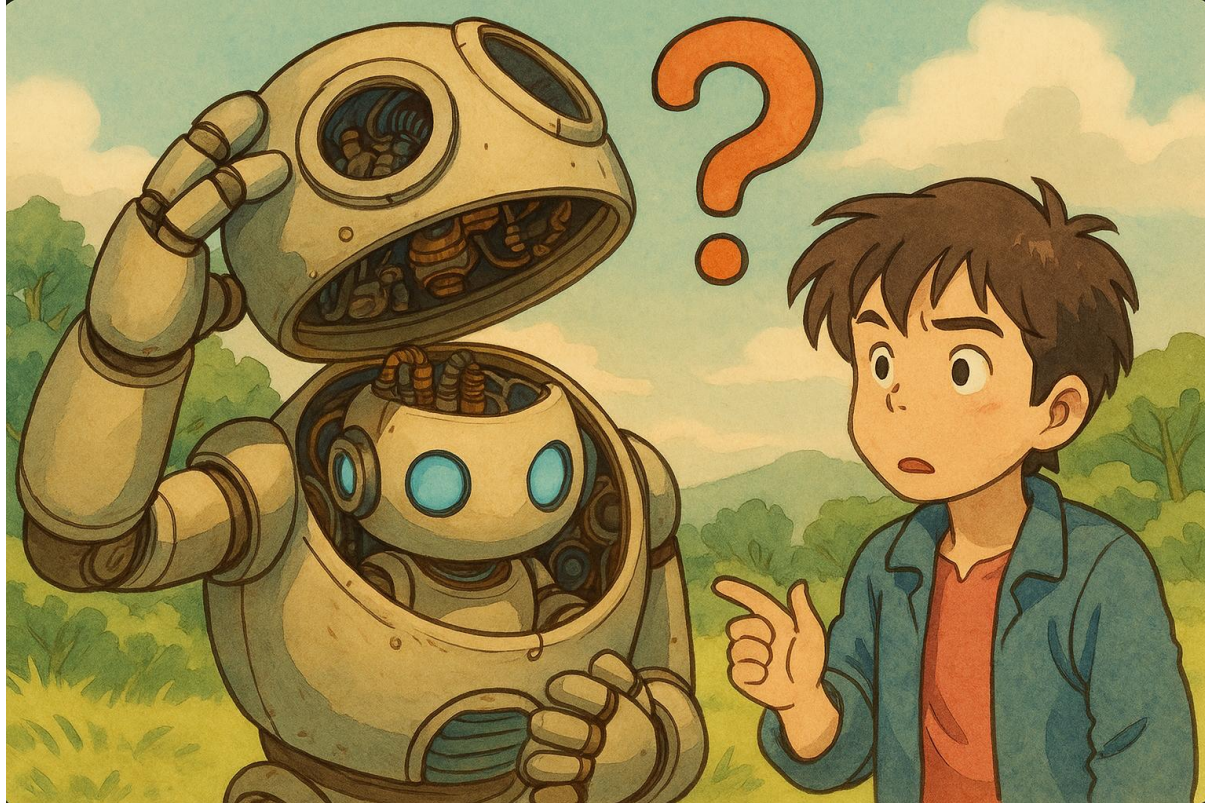
Communicating with the Agent

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

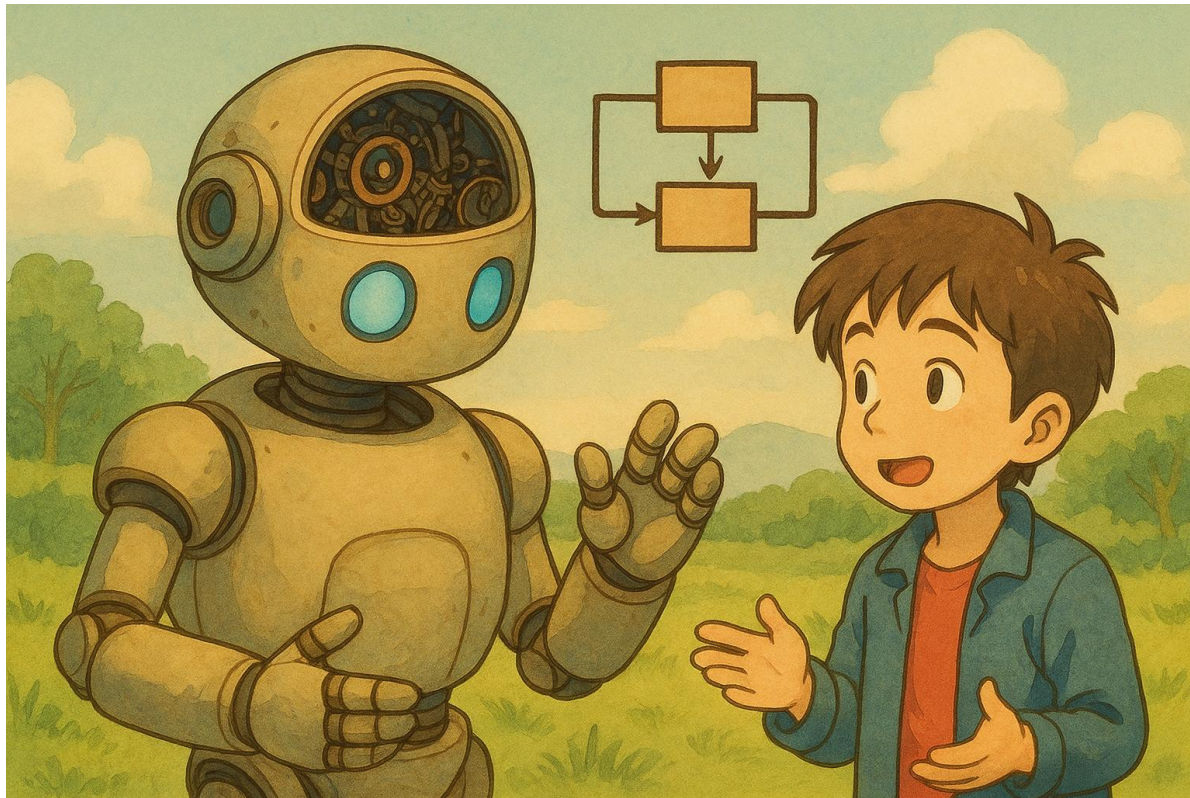
Of course, here is...:

???

How _do_ we talk about data work?



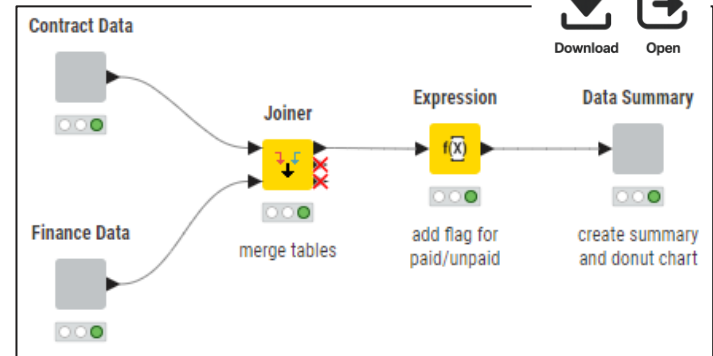
A Workflow says it all



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?)

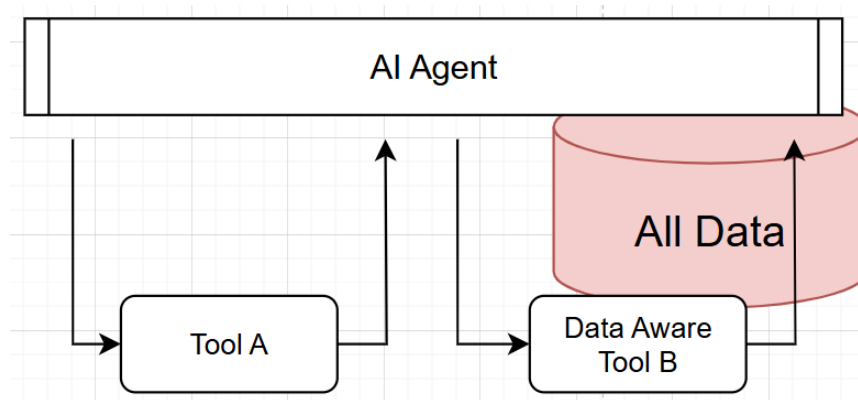
this helps **Transparency**.

"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?

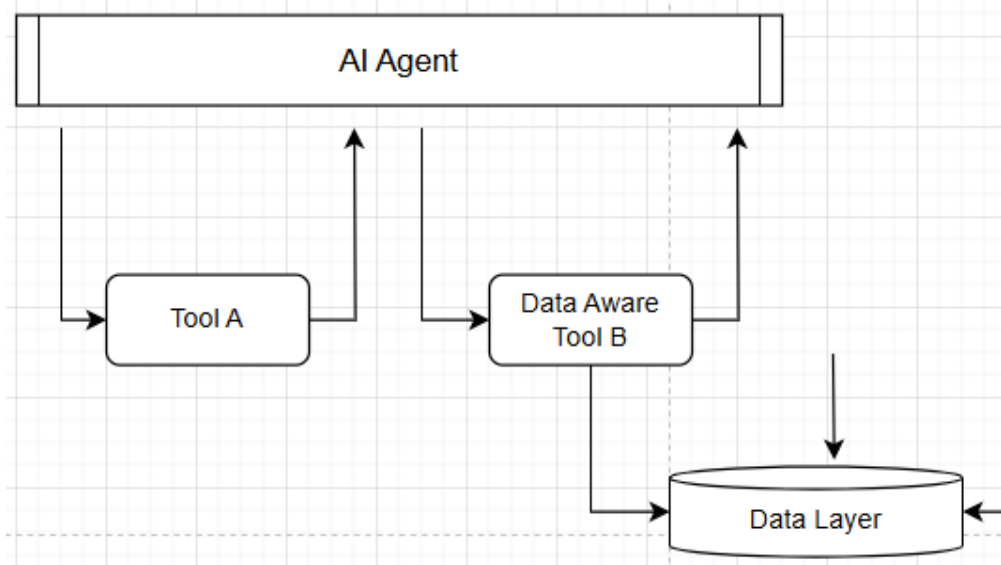


The dilemma:

- 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...

Adding a Data Layer



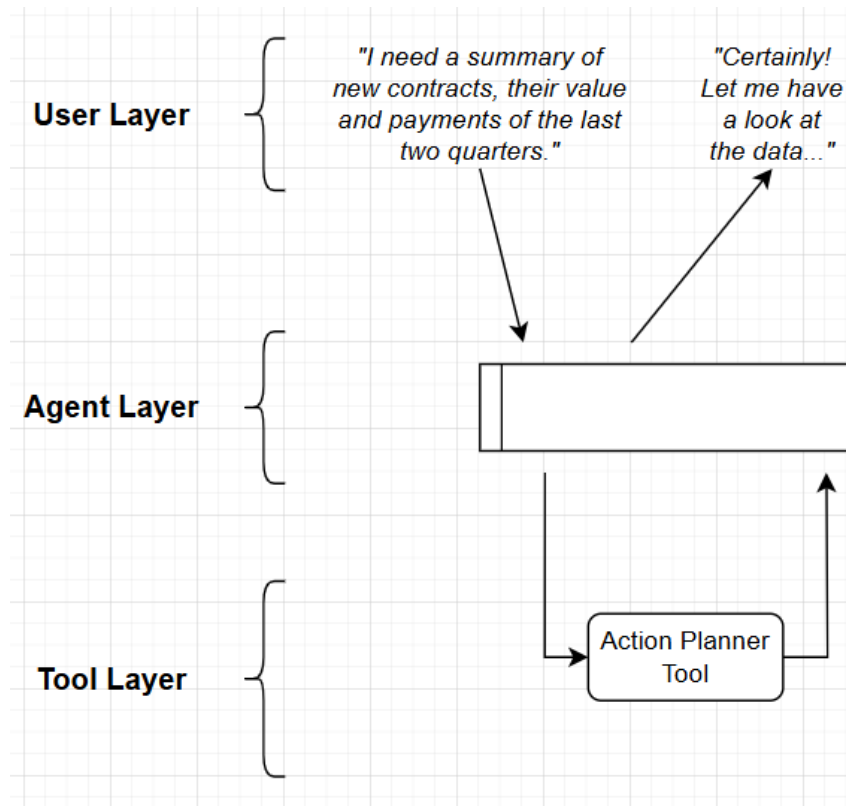
from UiPath: "You don't give agents direct access to data.
You give them access to tools, [...] and they are precise in nature.
They cannot be attacked."

Abstract geometric lines in the top right corner of the slide, consisting of several overlapping triangles and polygons in a light yellow color.

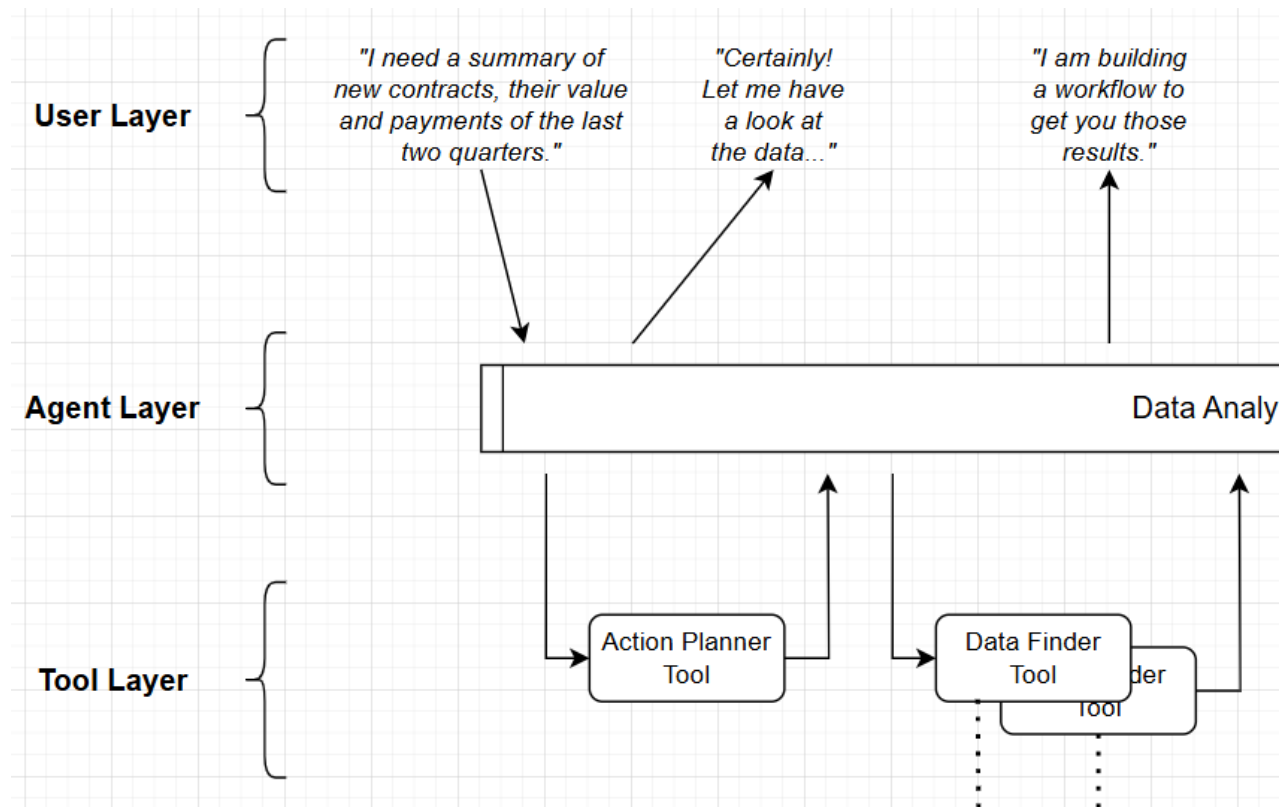
A Peek under the Hood:

How should Agents work with Data?

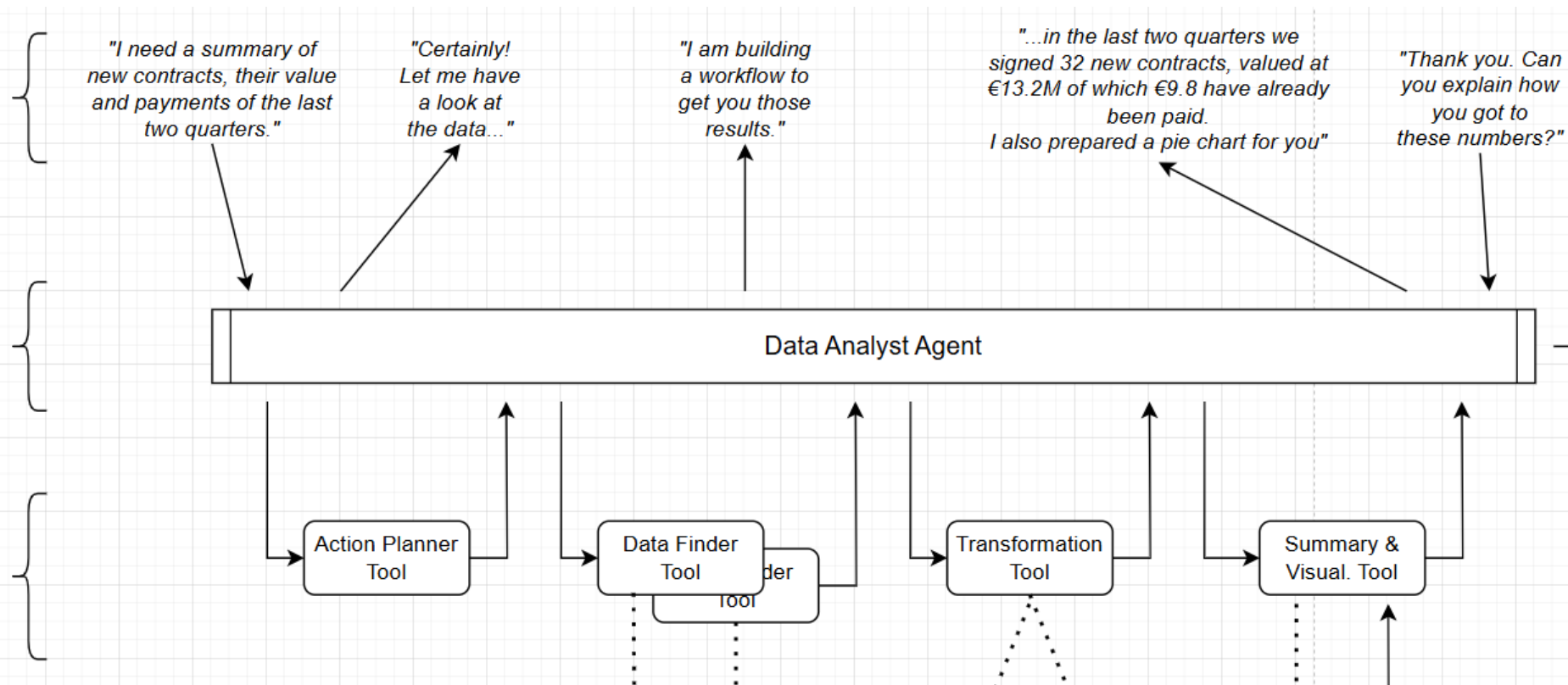
Agents, Tools, ...



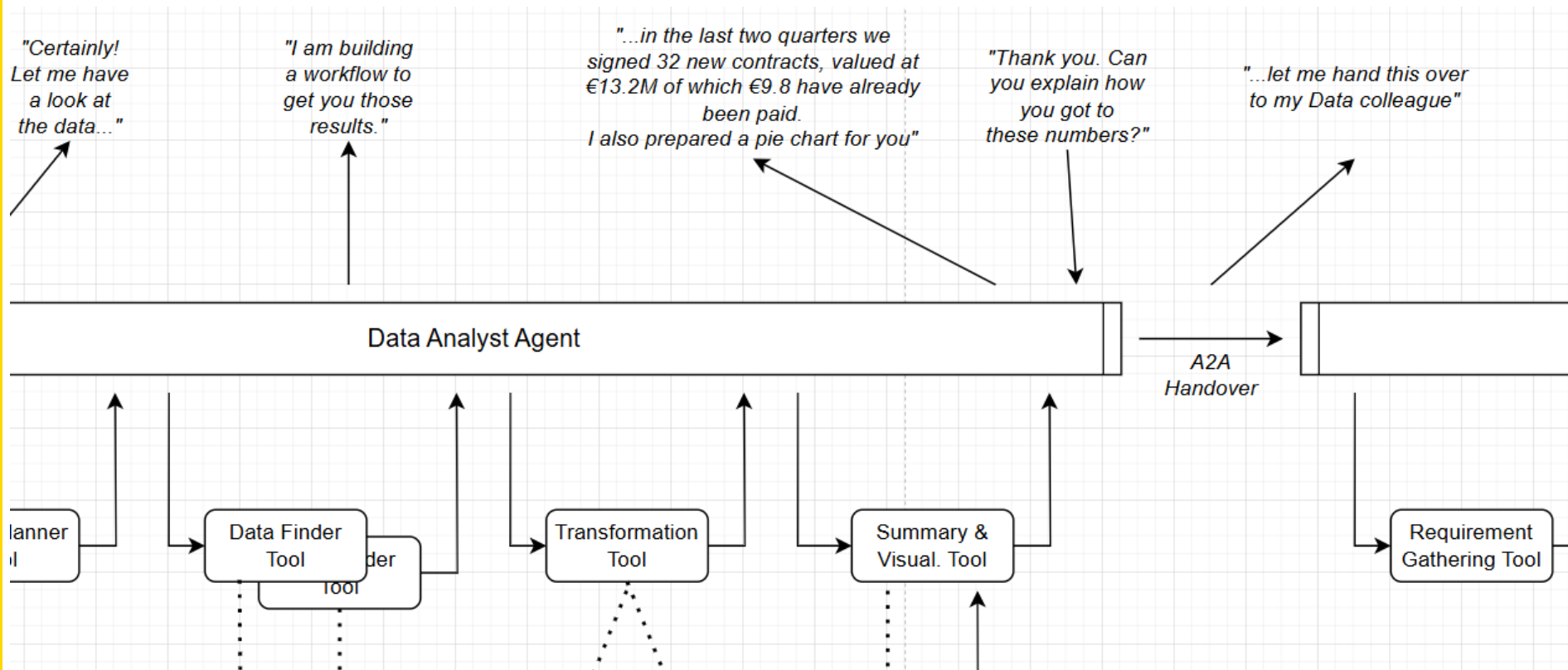
Agents, Tools, ...



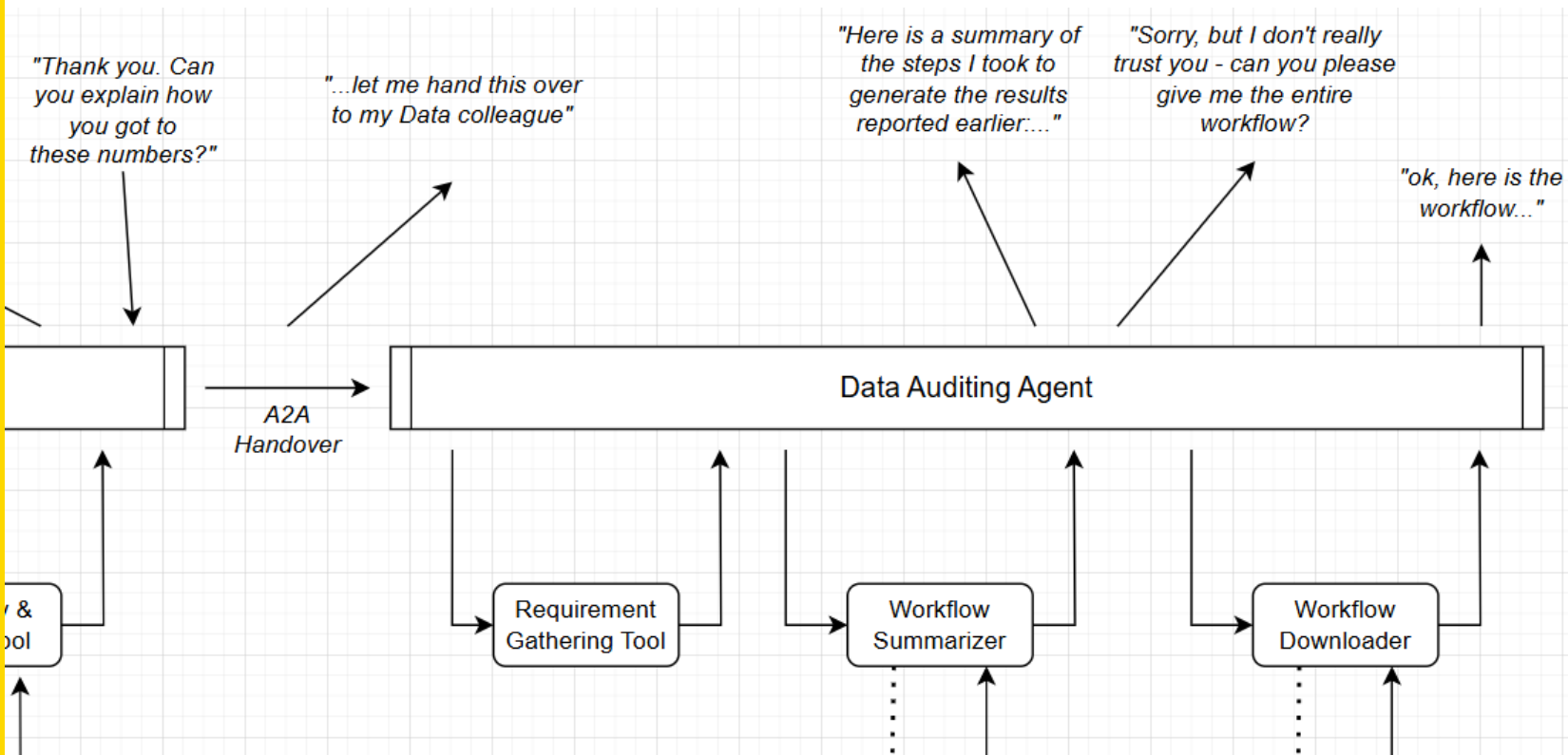
Agents, Tools, ...



Agents, Tools, ...

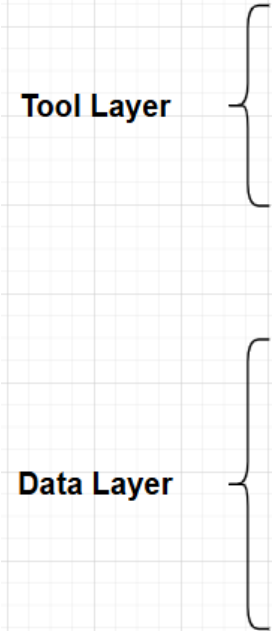


Agents, Tools, ...



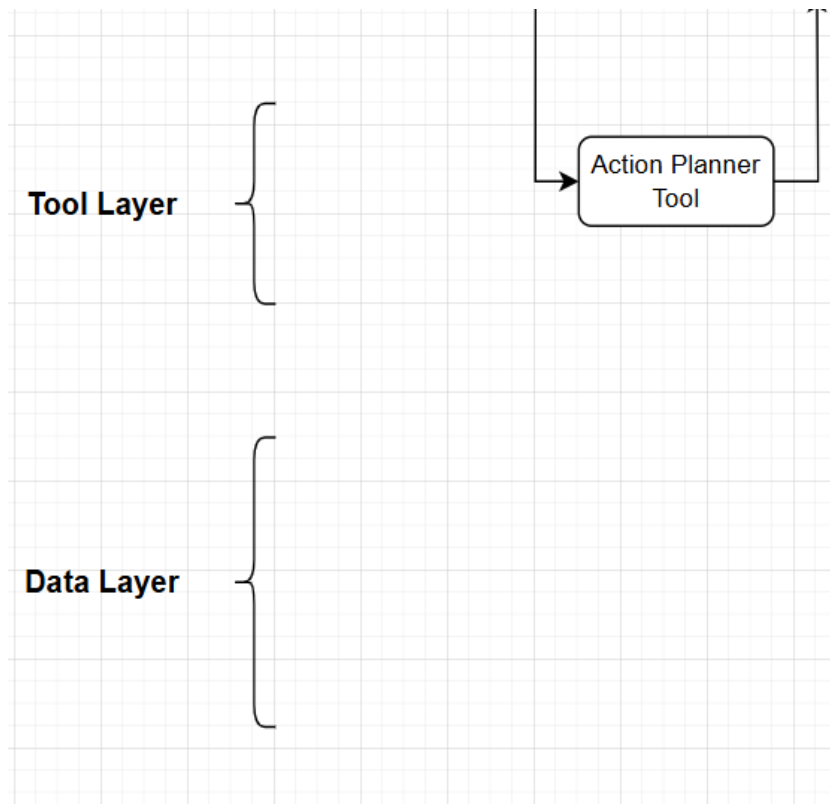
Agents, Tools, and Data!

Tool Layer

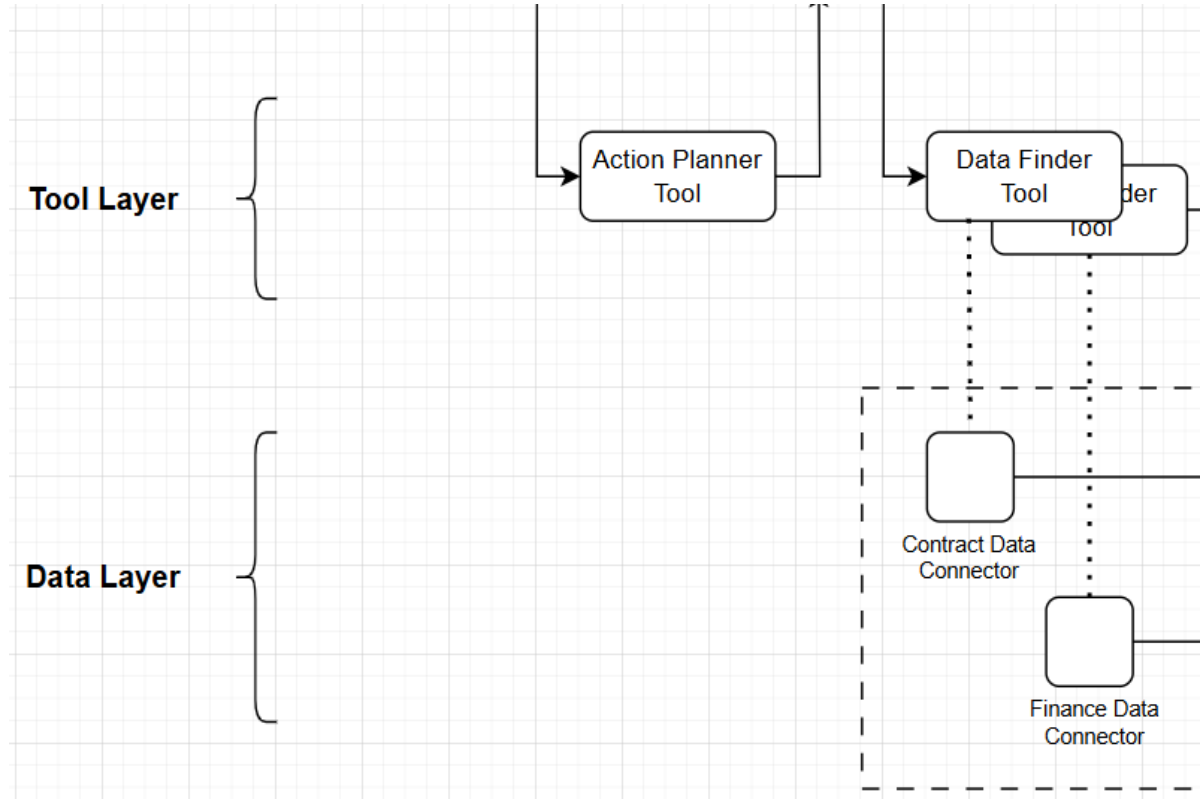


Data Layer

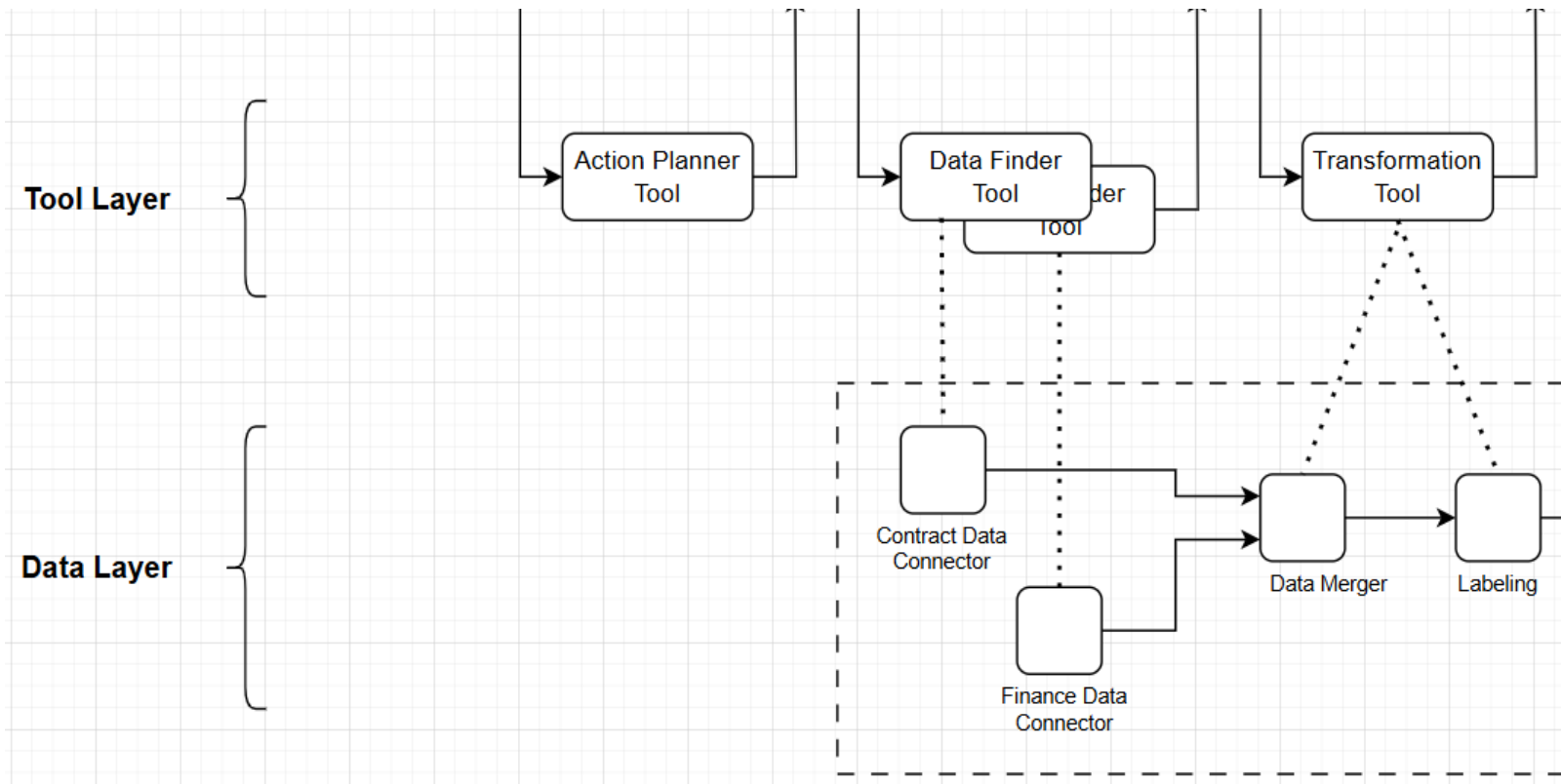
Agents, Tools, and Data!



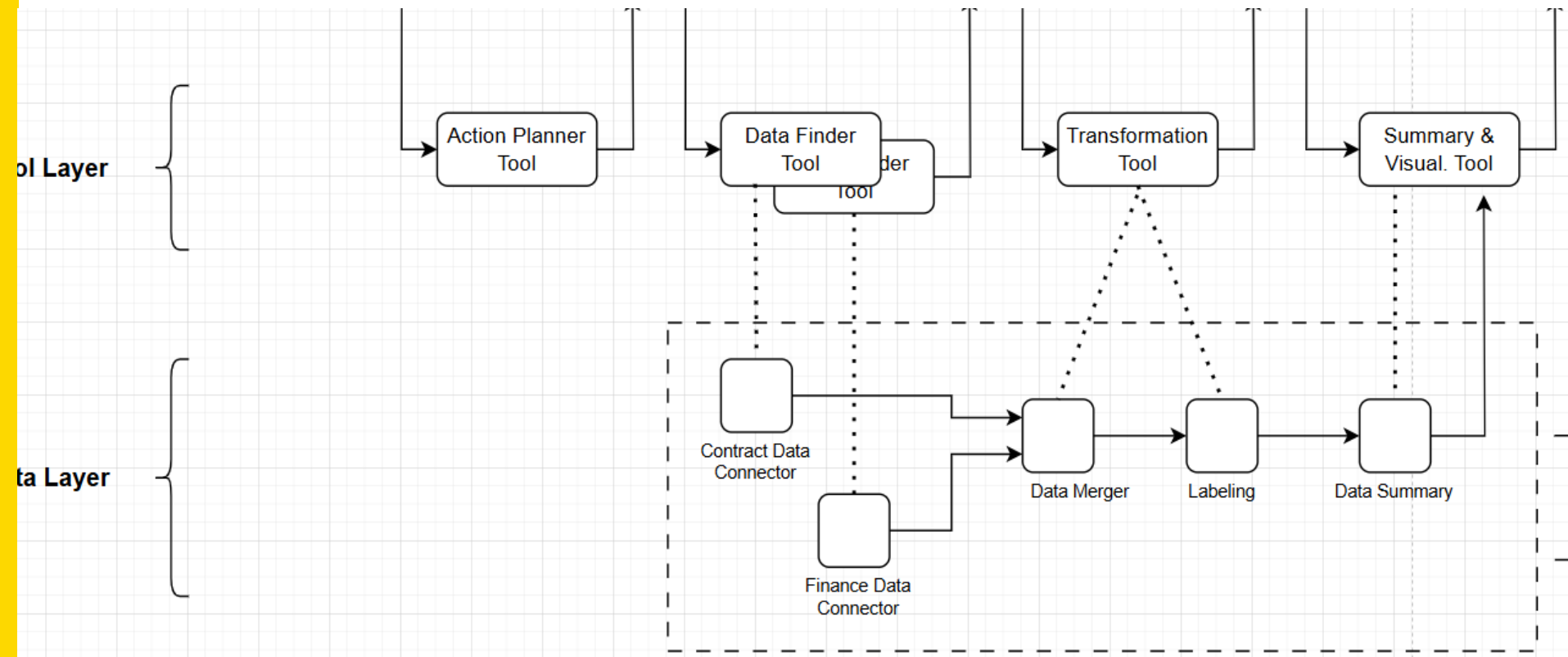
Agents, Tools, and Data!



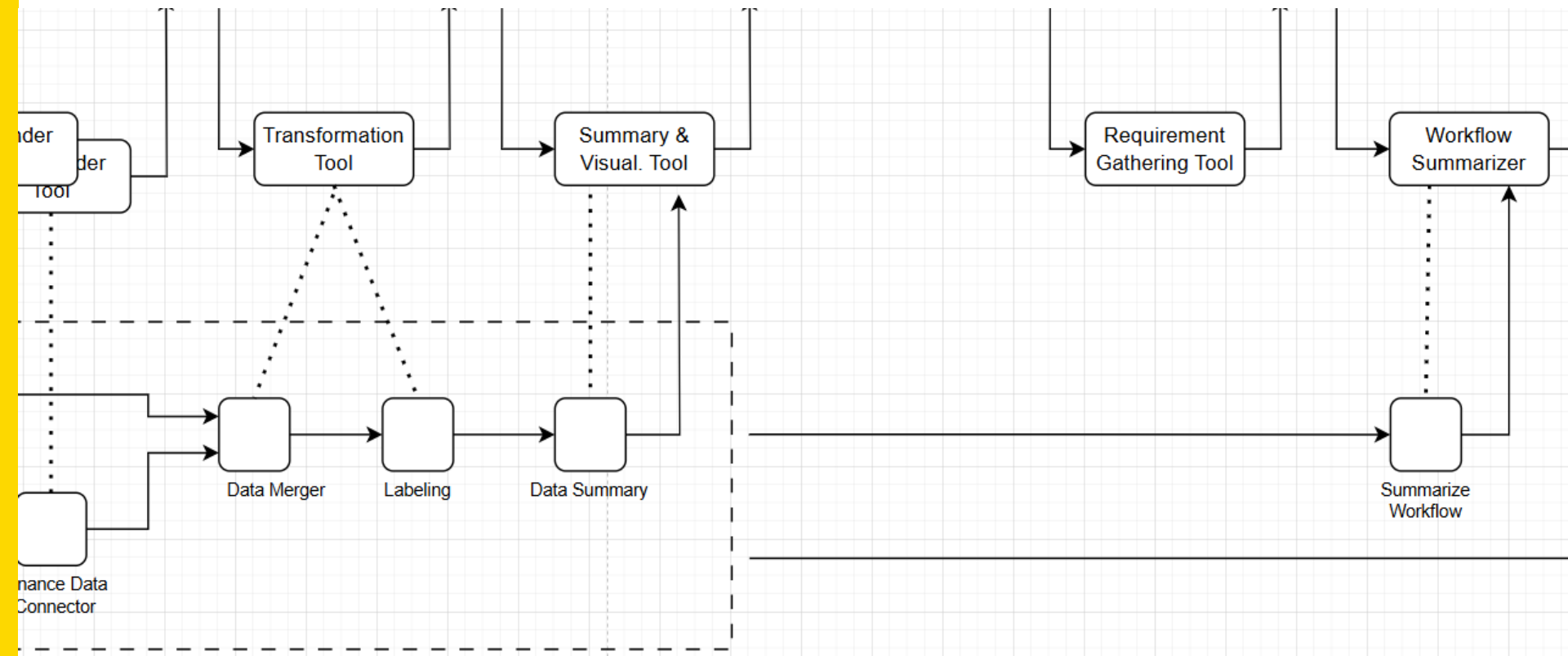
Agents, Tools, and Data!



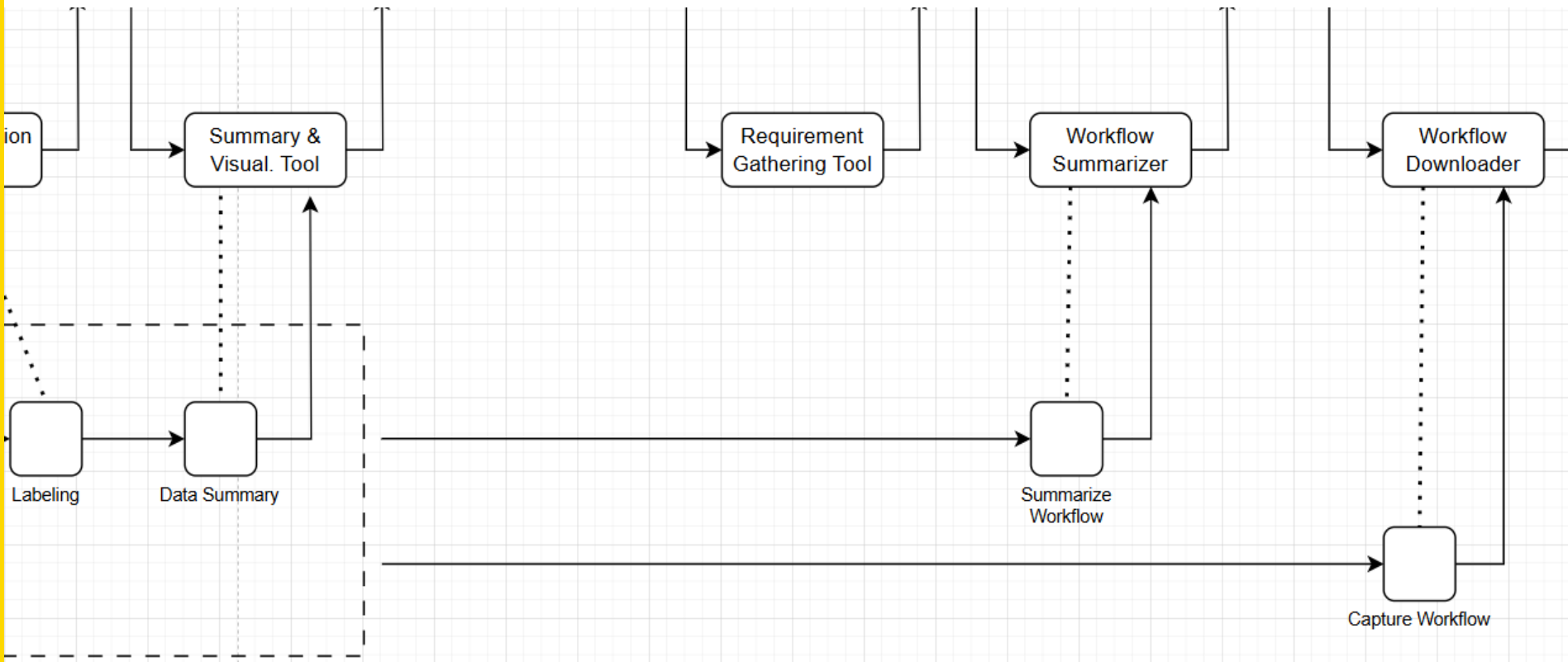
Agents, Tools, and Data!



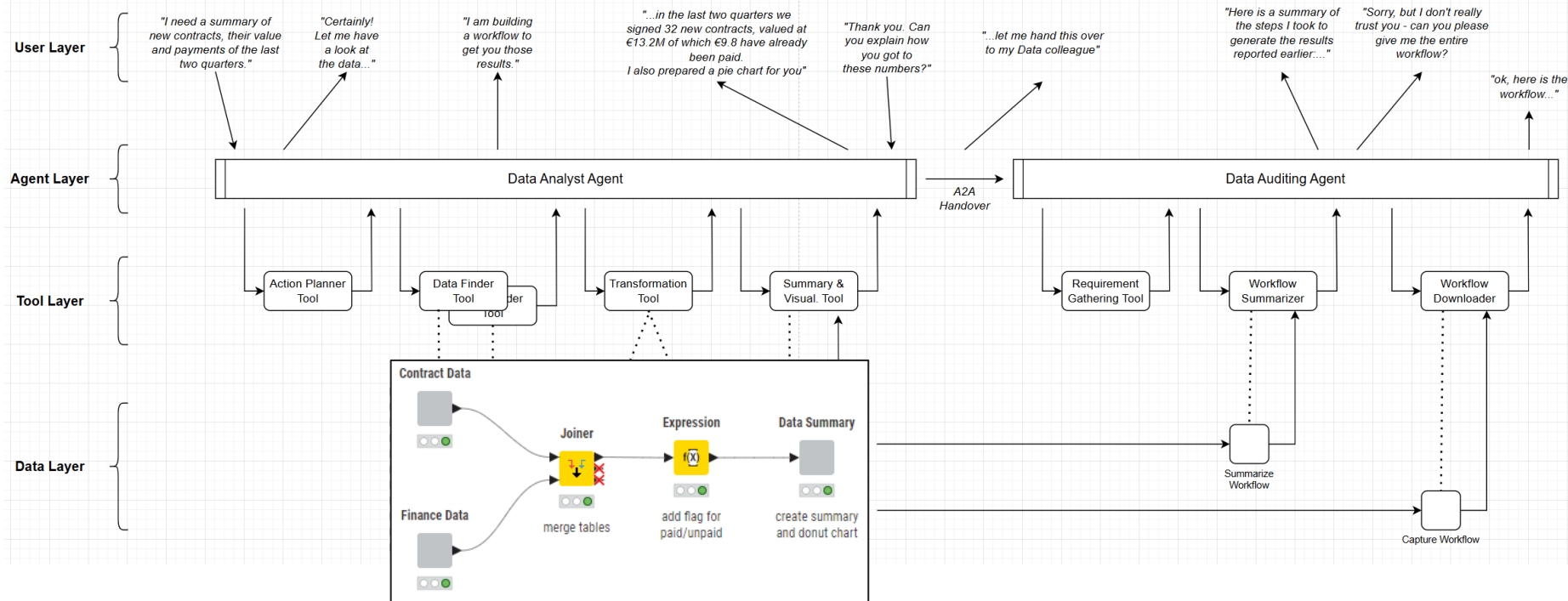
Agents, Tools, and Data!



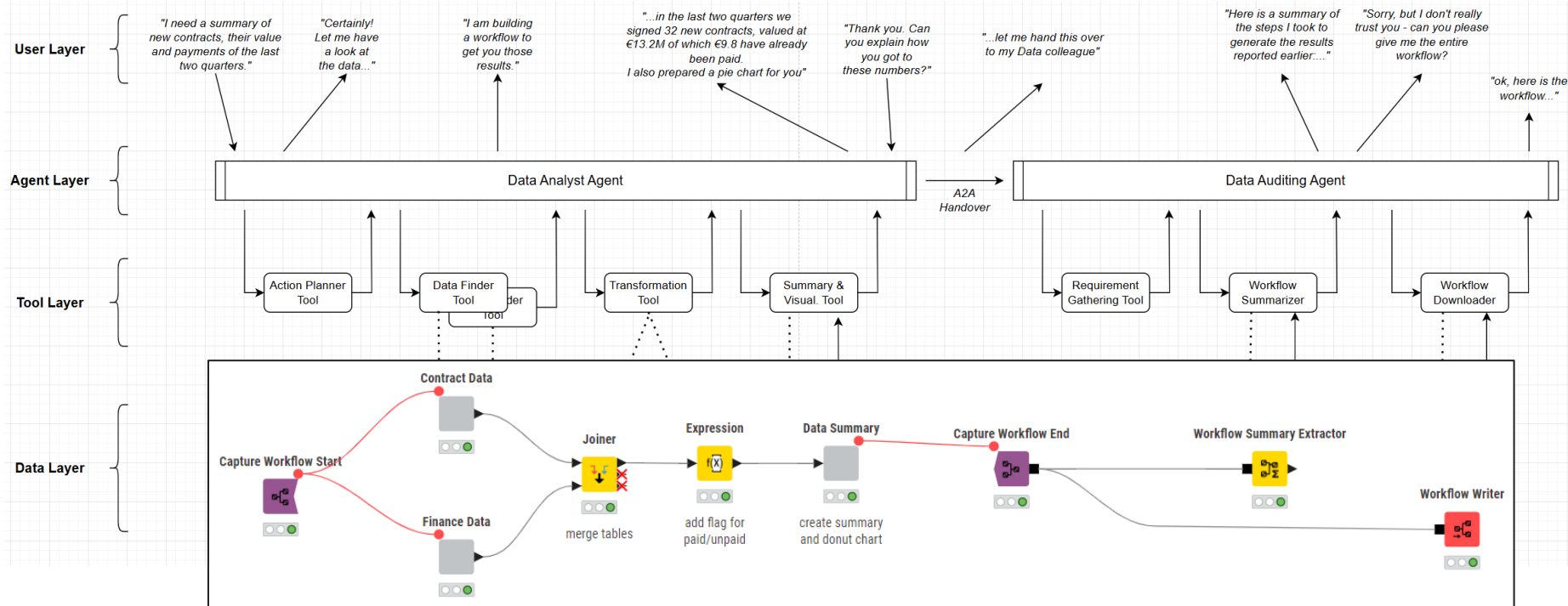
Agents, Tools, and Data!



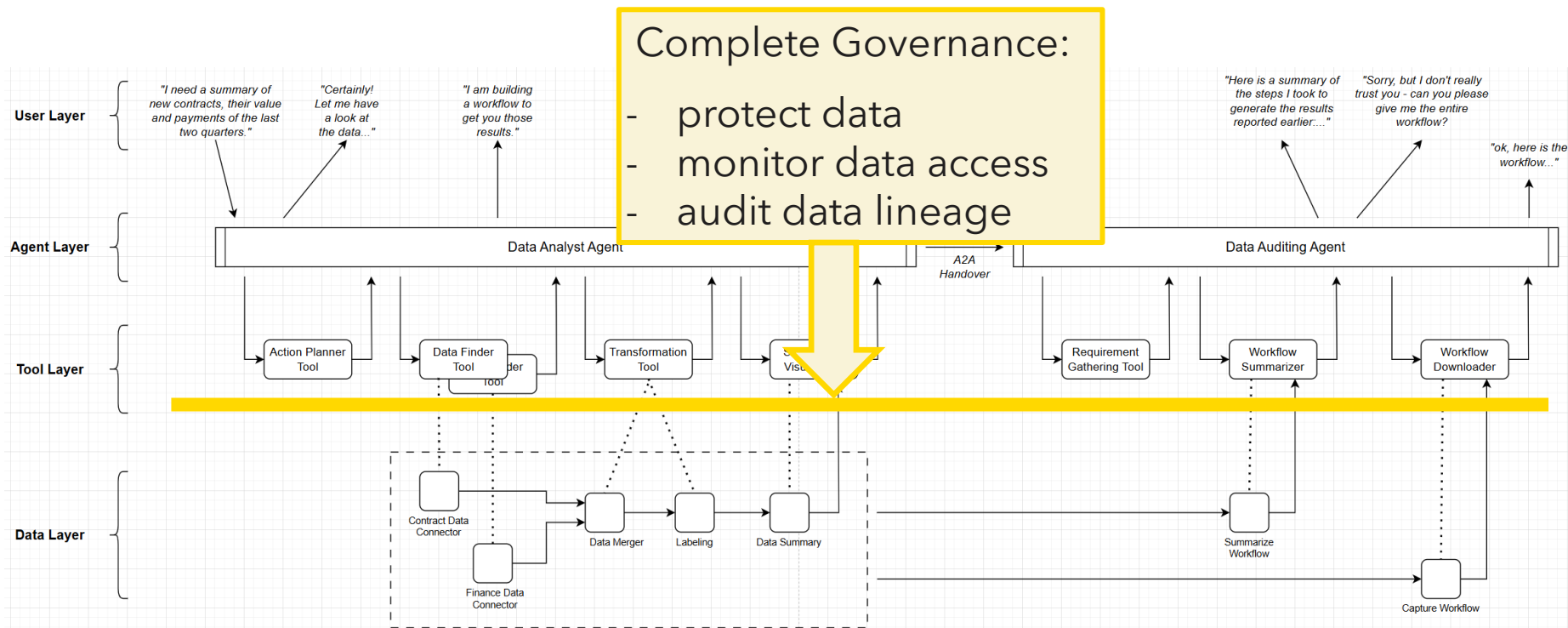
The Complete Picture



The Complete Picture



Clear Separation between Data and AI



Summary

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.