FME

WEBINAR

MCP Meets Governance: Safely and Securely Connect Your AI Agents to Data



Meet the Presenters

Safe Software



Sanae Mendoza

Customer Solutions Specialist



Aaron Hillier

Technical Support Specialist, FME Flow

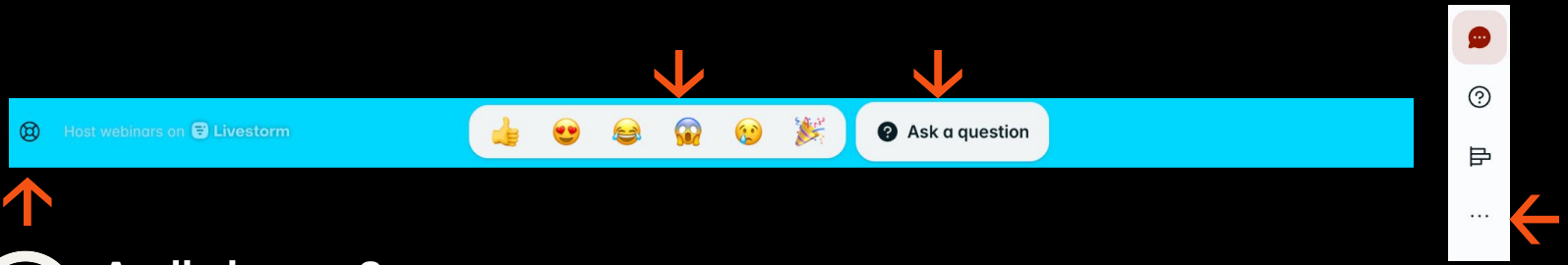


Rylan Maschak

Director, Product Management

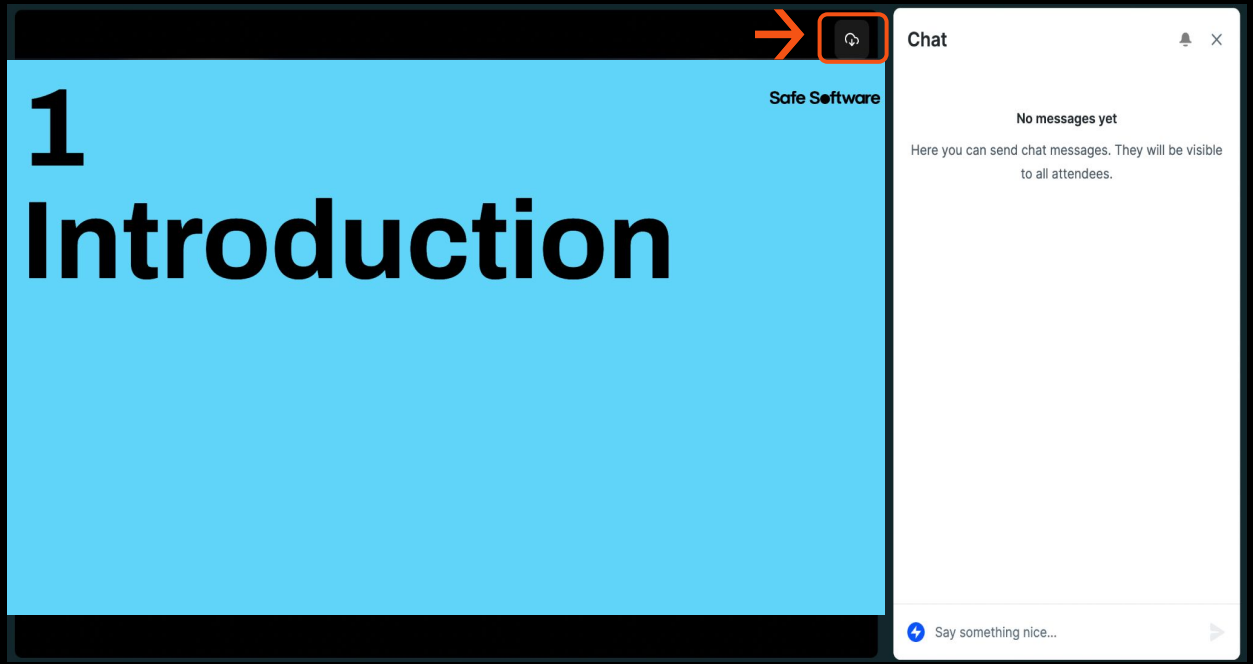
Welcome to Livestorm.

A few ways to engage with us during the webinar:



Audio issues?
Click here for 4 simple troubleshooting steps.

How to download slides.



1. Hover over the slide deck in the webinar room
2. Click **download** button

Agenda

Safe Software

1. Introduction
2. Safe by Design: Where the Controls Live
3. Best Practices: Tool Design & Testing
4. Best Practices: Tool Descriptions & Chaining
5. Conclusion
6. Resources
7. Next Steps
8. Q&A



Safe Software

1 Introduction

Safe Software

Safe MCP starts with three questions.

Authentication

Who is asking?

Every tool call should trace back to a verified person or service.

Access control

What can they reach?

Signed in isn't the same as allowed. Grant only what the task needs.

Data sovereignty

Where does it go?

Where data lives, where it runs, and where the answer lands all matter.

Safe Software

MCP in 60 seconds



AI application

Claude, Copilot, ChatGPT or your own agent. It holds the MCP client.



Tools

Named actions with inputs. In FME, each tool is a workspace.



List, then call

The agent finds tools with tools/list, then runs one with tools/call.



MCP server

Publishes the tools and decides who may call them. Safety lives here.

Safe Software

MCP is an enterprise integration layer.

The Protocol

Model Context Protocol. Open standard from Anthropic. Lets AI agents call tools and retrieve data securely.

The Strategic Shift

For years, you built integrations for applications. Now you build them for AI. Same problem. New urgency.

The Compounding Effect

Every data source you connect through MCP becomes available to every AI model you adopt - now and in the future.

Safe Software

From Esri to AI: Create an MCP Server in 7 Minutes with FME

SCAN TO WATCH



Don Murray

Safe Software



Sanae Mendoza

Safe Software



Dmitri Bagh

Safe Software

Safe Software

MCP and the Power of Choice: Expanding Your AI and System Reach

SCAN TO WATCH



Don Murray

Safe Software



Stewart Harper

Safe Software



Sanae Mendoza

Safe Software

Safe Software

32

years of governing where data goes.

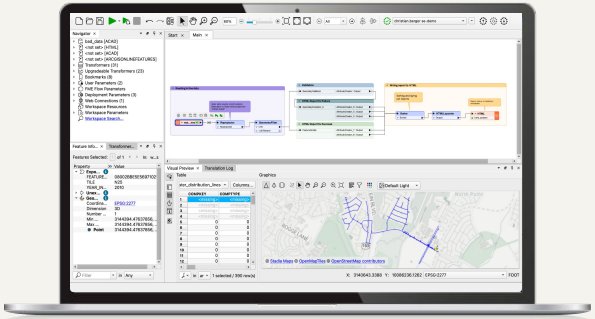
FME has always let you choose which records move, in what shape, and where they land. With MCP, AI is the newest destination.

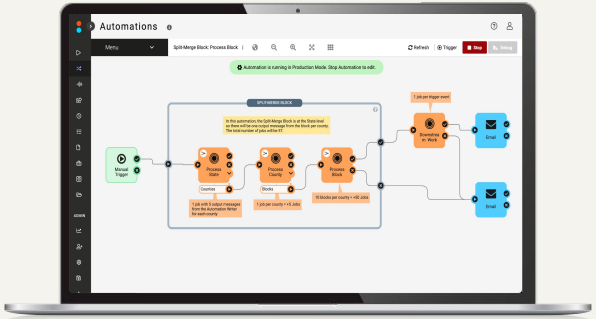
1993	Founded - spatial data integration
2000s	CAD, BIM, 100+ formats supported
2010s	Cloud, IoT, enterprise systems, real-time data pipelines
2020s	Orchestration, automation at enterprise scale
2025+	**Exposing all of it to AI, on your terms**

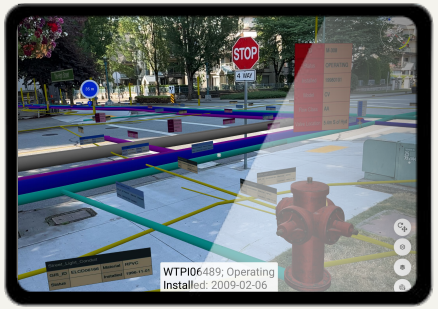
Safe Software

FME Enterprise Integration Platform

The only All-Data, Any-AI Platform.







FME Form

Data Movement and transformations *workflows* are built here.

FME Flow

Brings life to FME Form *workflows*.

FME Flow Hosted
Safe Software SaaS Version of FME Flow

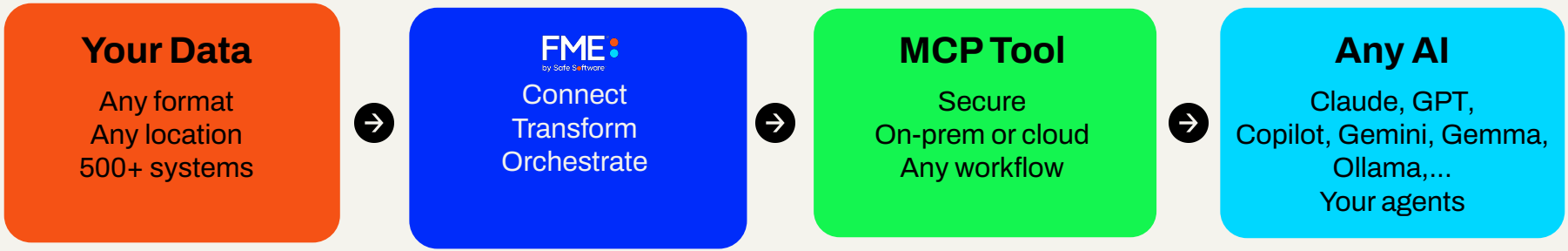
FME Realize

Experience data in real world context, in real time.

fme.safe.com/platform

Safe Software

FME is the layer between all your data and MCP.



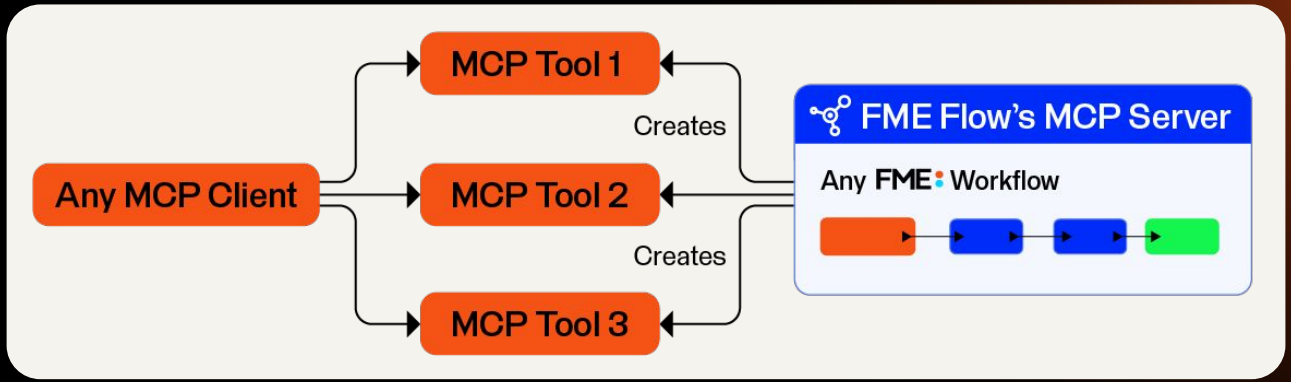
Build once. Works with every AI model. On-prem, cloud, or both.

Safe Software

FME Flow's MCP Server

Turn any FME workspace into an AI-ready tool.

- Workspaces become tools: parameters in, structured results out.
- Host multiple MCP servers on a single FME Flow.
- Any MCP-compatible client can connect: Claude, OpenAI, Copilot, FME…



Safe Software

One server. One context.

ACCURACY

Agents pick the right tool

Small sets of related tools keep selection sharp. Accuracy drops as unrelated tools pile up.

CONTEXT COST

Lean context, better answers

Every tool description loads into the model's context. Unrelated tools waste tokens and attention.

SECURITY

Least privilege by design

Each server has its own OAuth 2.0 sign-in and permissions. Finance tools reach finance users only.

GOVERNANCE

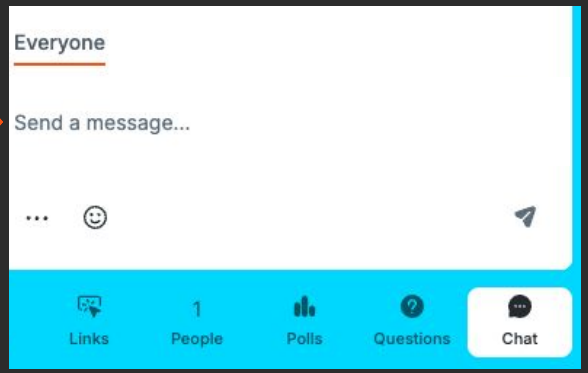
Clear ownership, safe change

Each team owns and versions its own server. One change can't break another team's agents.

Chat Storm

Safe Software

Which system would you connect an AI agent to first, and which should it never touch?



2

Safe by Design: Where the Controls Live

MCP makes organizational tools easier for agents to use.



Monday



MCP connected the agent to everything in 5 minutes.

Monday



MCP connected the agent to everything in 5 minutes.

Friday



MCP connected the agent to everything in 5 minutes.

Safe Software

Easy, until it isn’t!

- Connections can grant more access than a task needs
- Some records and columns cannot be used with AI
- Returned content can influence the next action
- Requests and outcomes need to be traceable



The Five Safes

Established questions for sensitive data access

1

Safe people

Who may use it?

2

Safe projects

Is the use approved?

3

Safe settings

Where is access controlled?

4

Safe data

How is confidentiality protected?

5

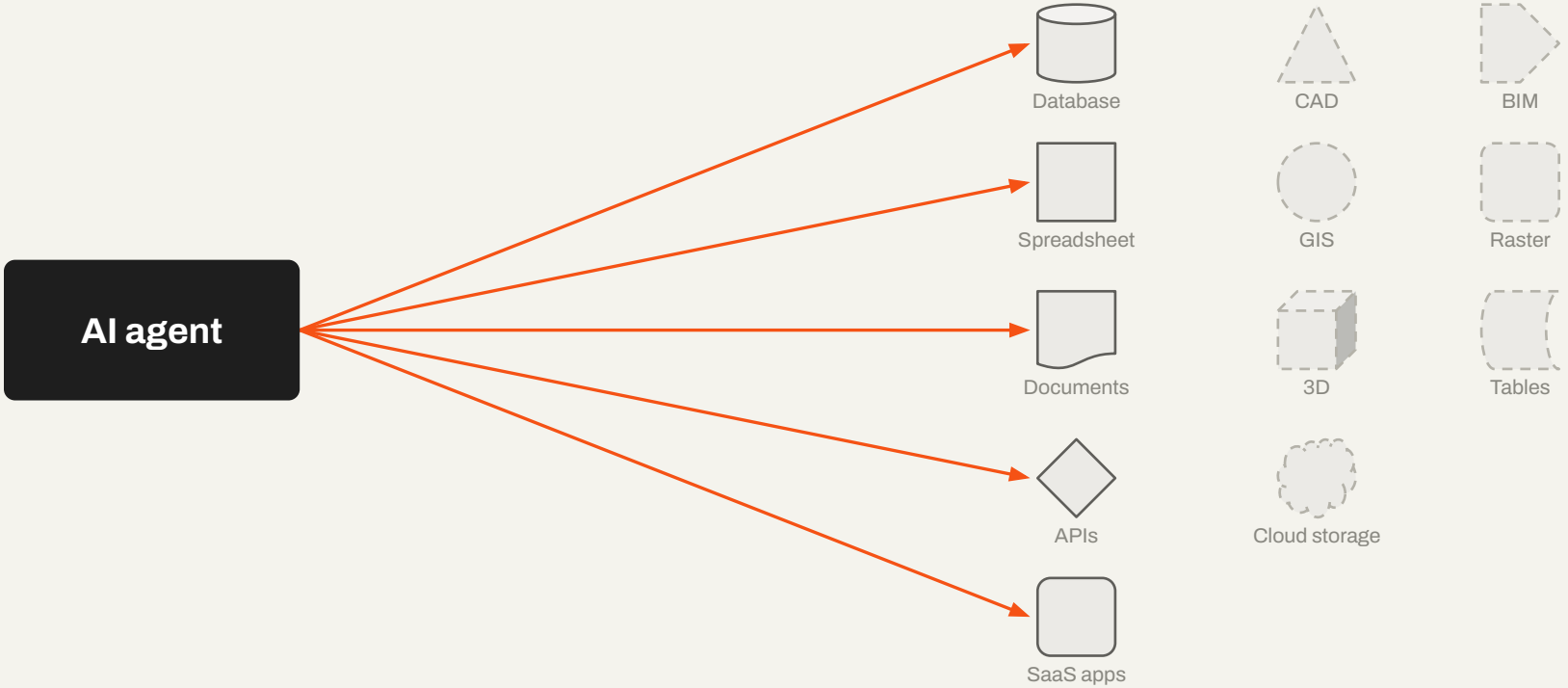
Safe outputs

What is safe to release?

A data-access framework from the UK Office for National Statistics, used by the UK Data Service.

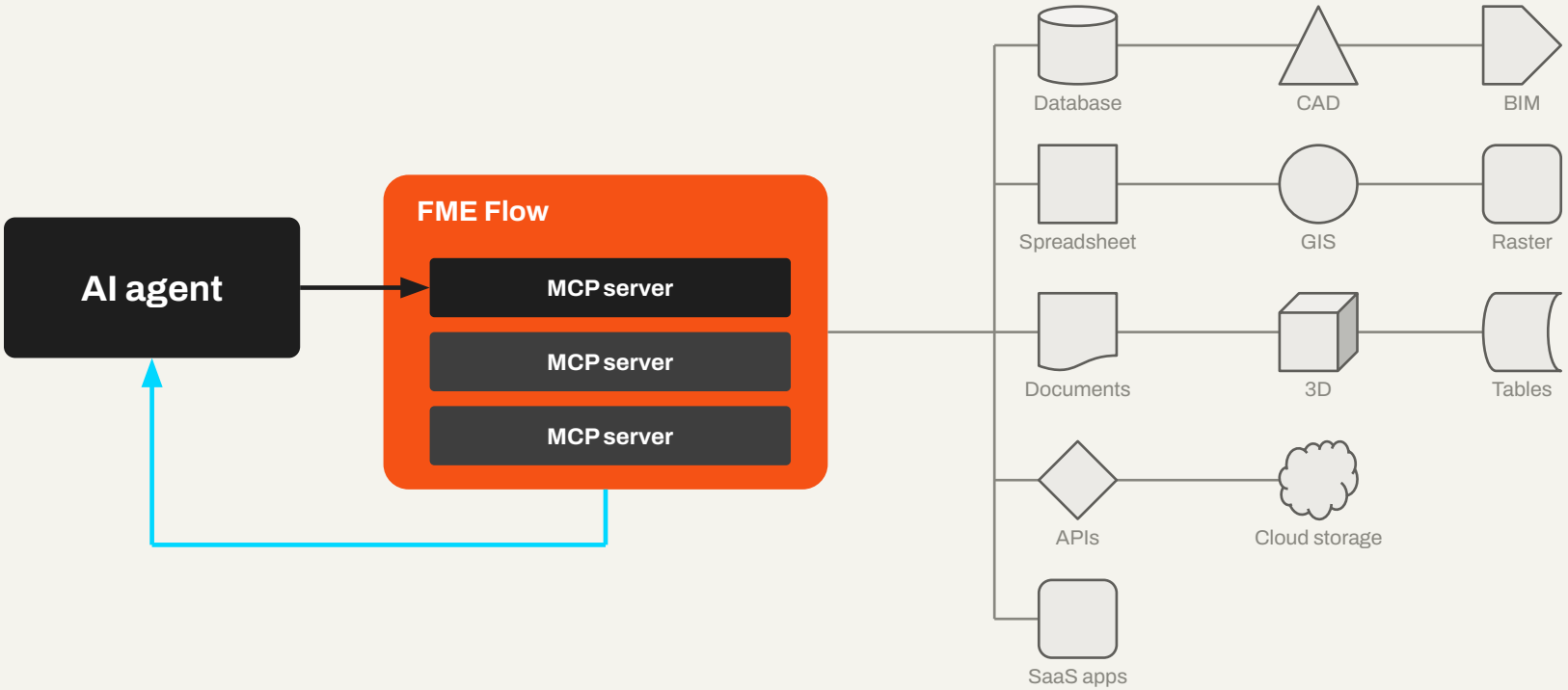
Safe Software

Wired directly, an agent gets the easy data uncontrolled (and the hard data not at all)



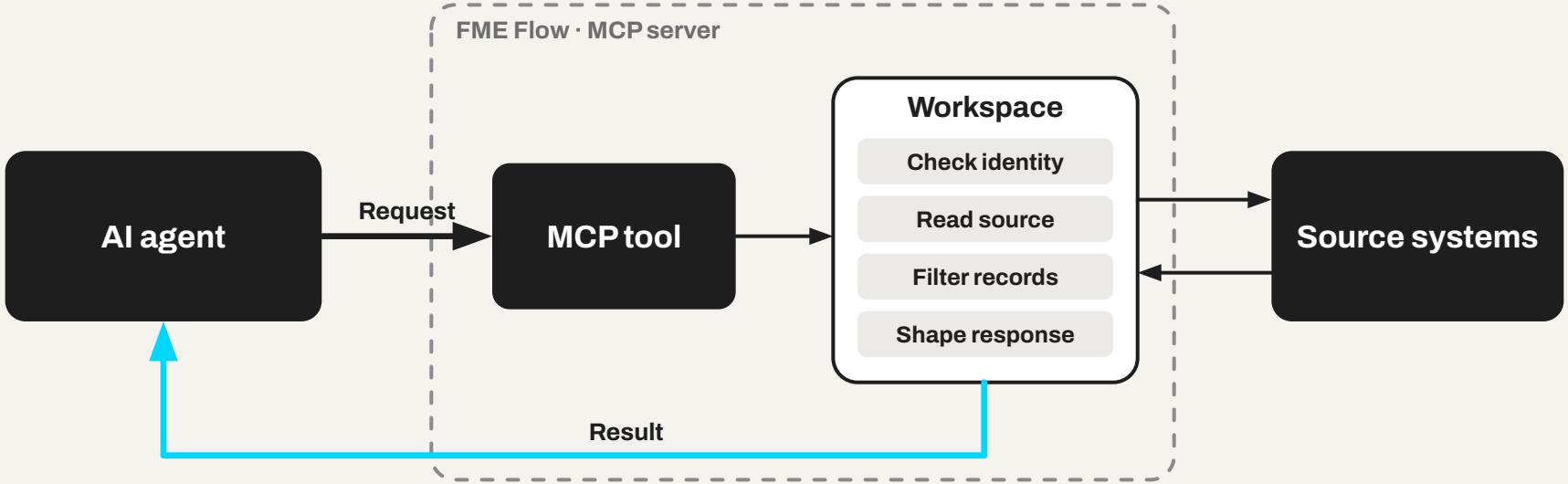
Safe Software

A managed integration behind every tool.



In FME, a tool is a workflow, not a connection.

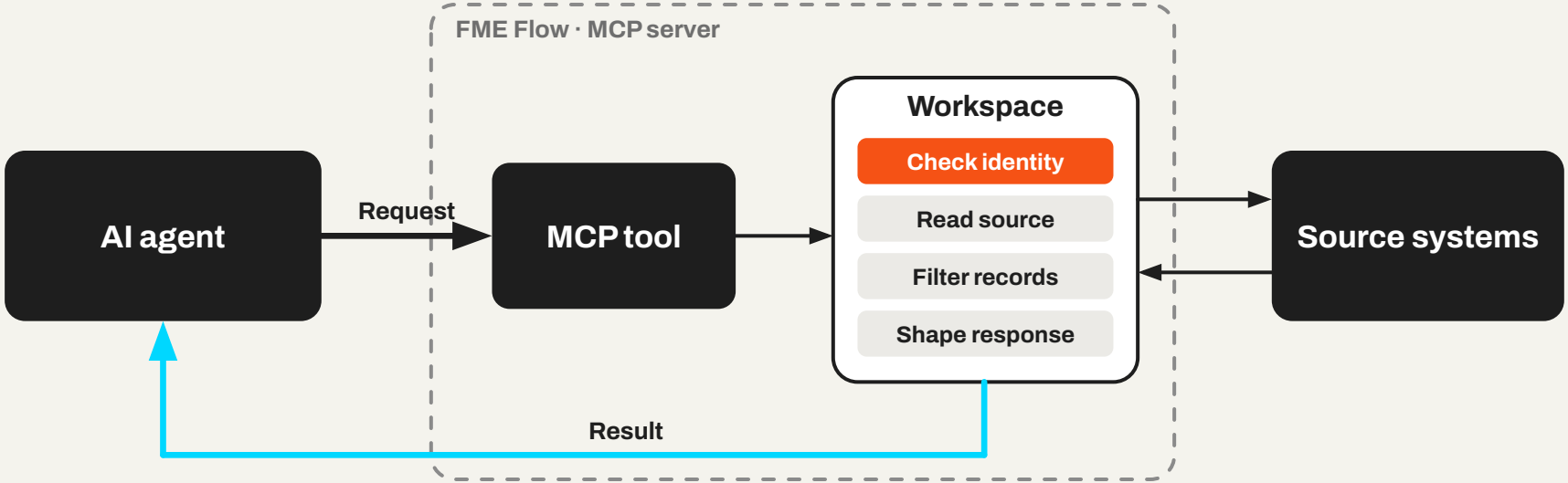
You design the workspace, control what it can access, and monitor its execution.



Safe Software

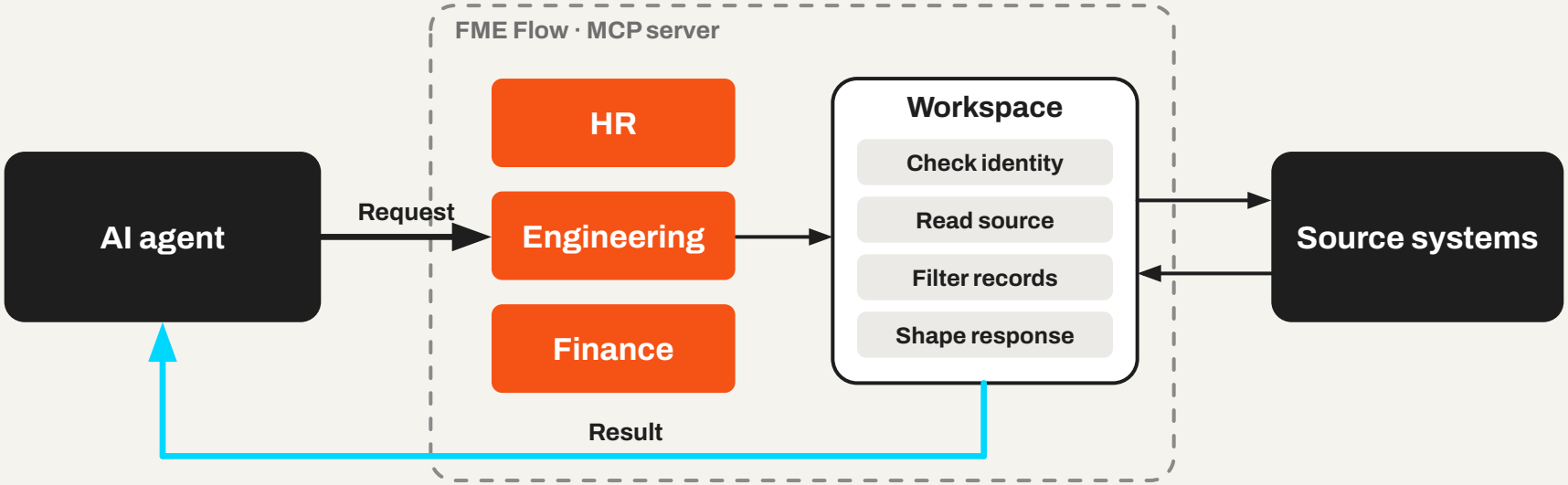
Who may use it?

Identity arrives with the request and is checked before anything runs.



What purpose is the data approved for?

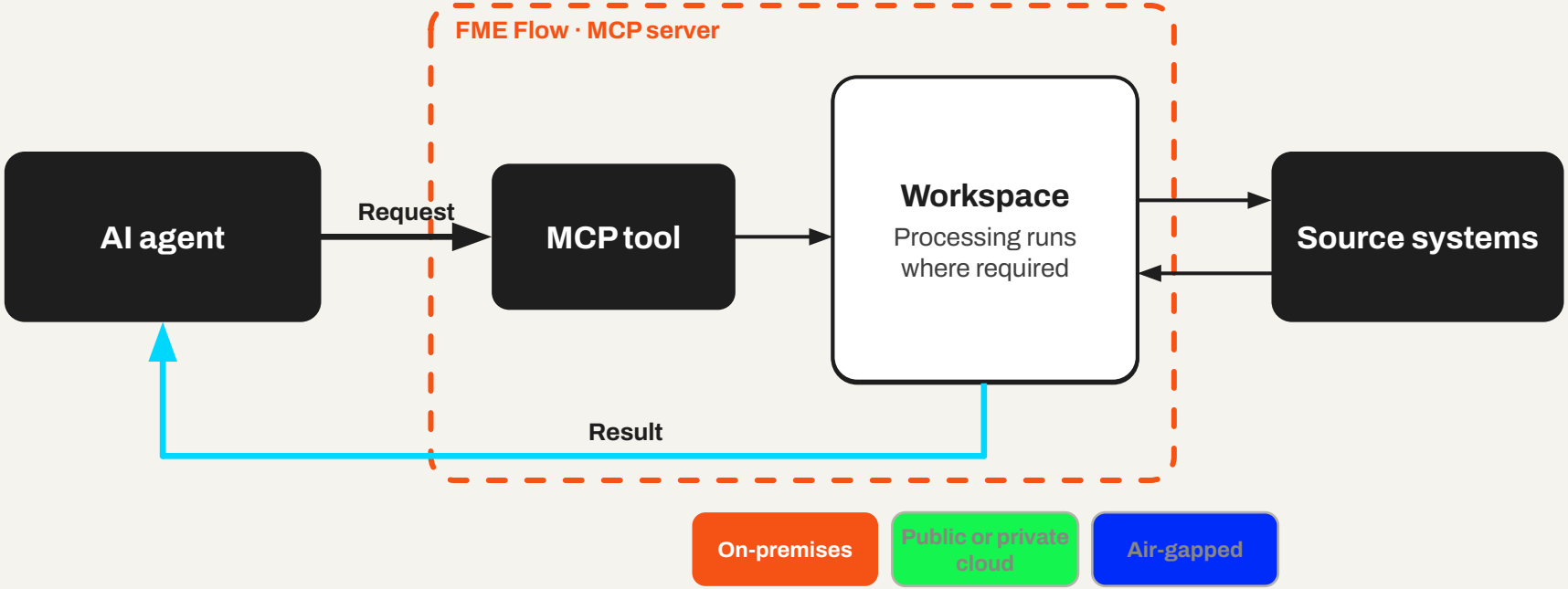
Group tools into MCP servers for specific domains, and restrict each workflow to its approved operations.



Safe Software

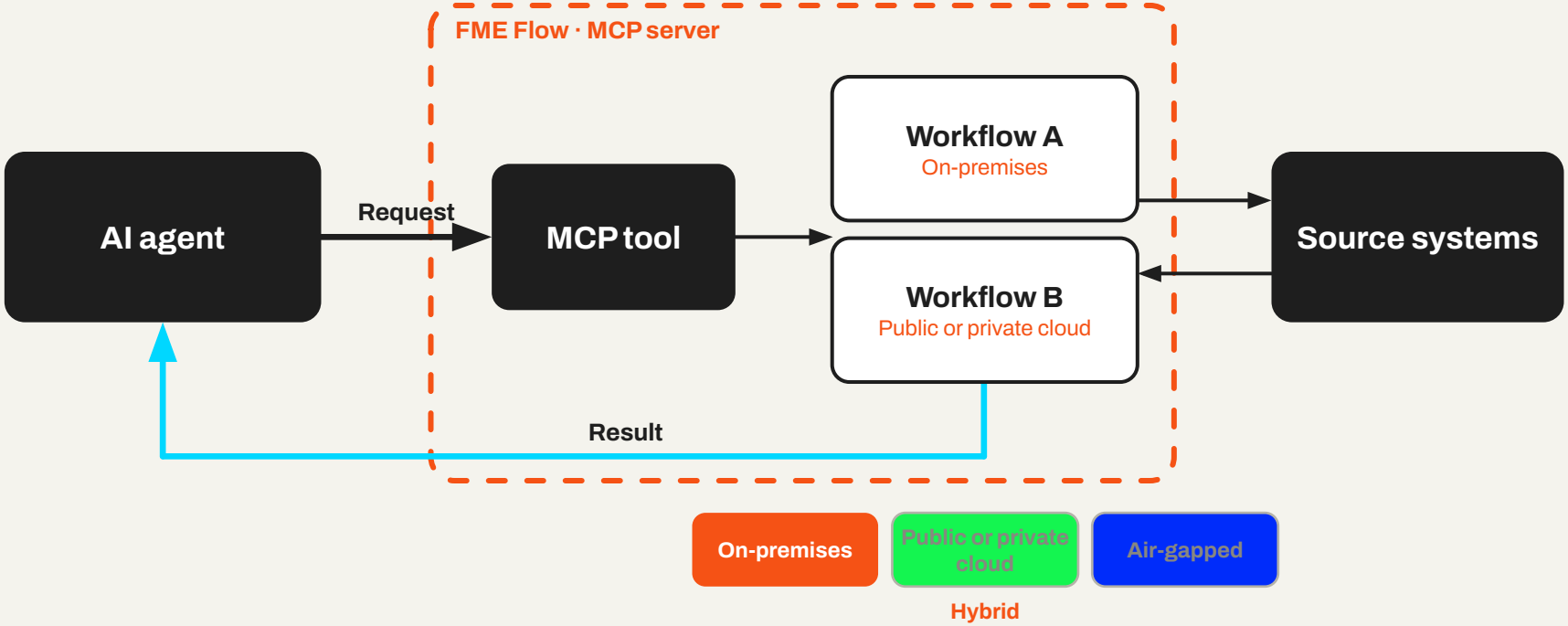
Where is access controlled?

The server runs where its data needs it, and the response goes where the model is.



Where is access controlled?

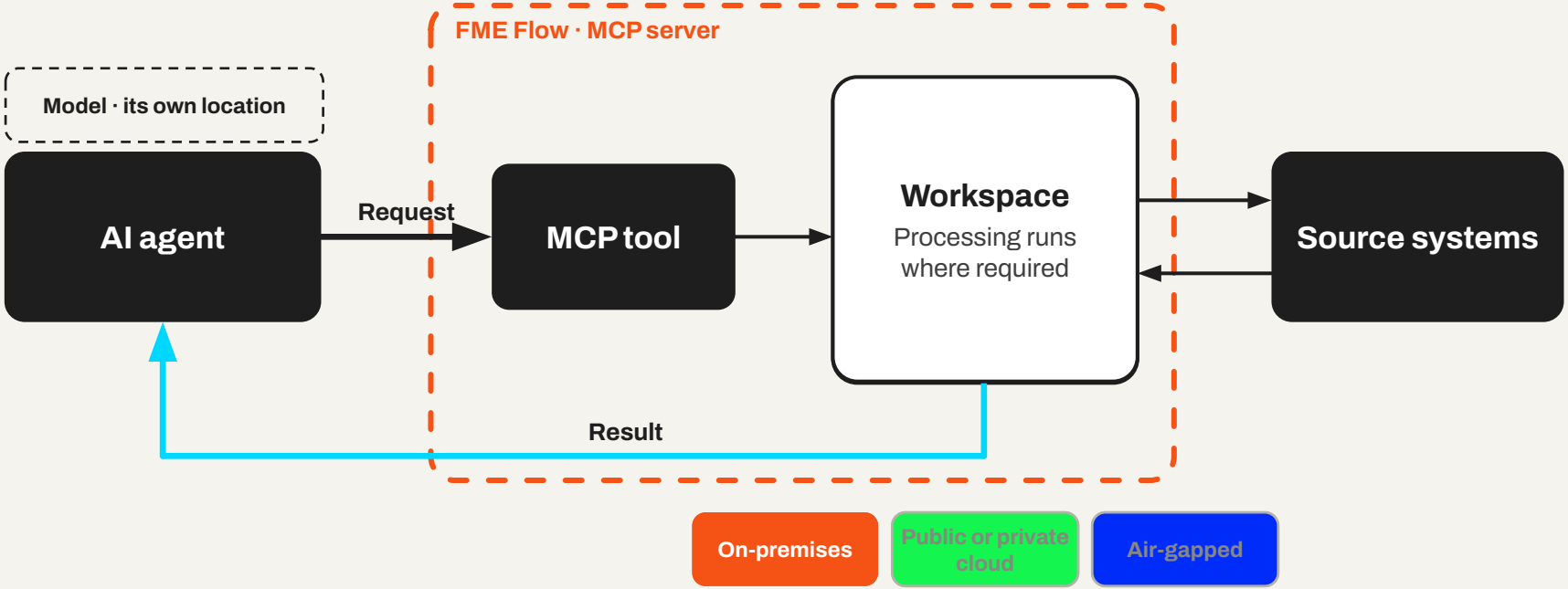
The server runs where its data needs it, and the response goes where the model is.



Safe Software

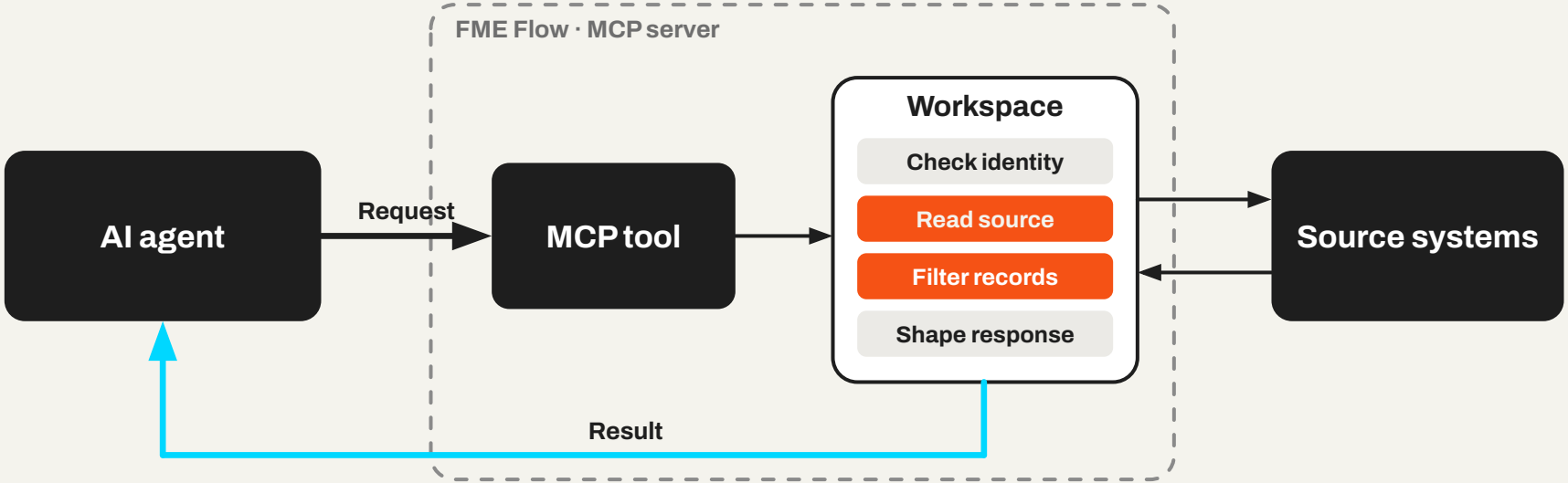
Where is access controlled?

The server runs where its data needs it, and the response goes where the model is.



How is confidentiality protected?

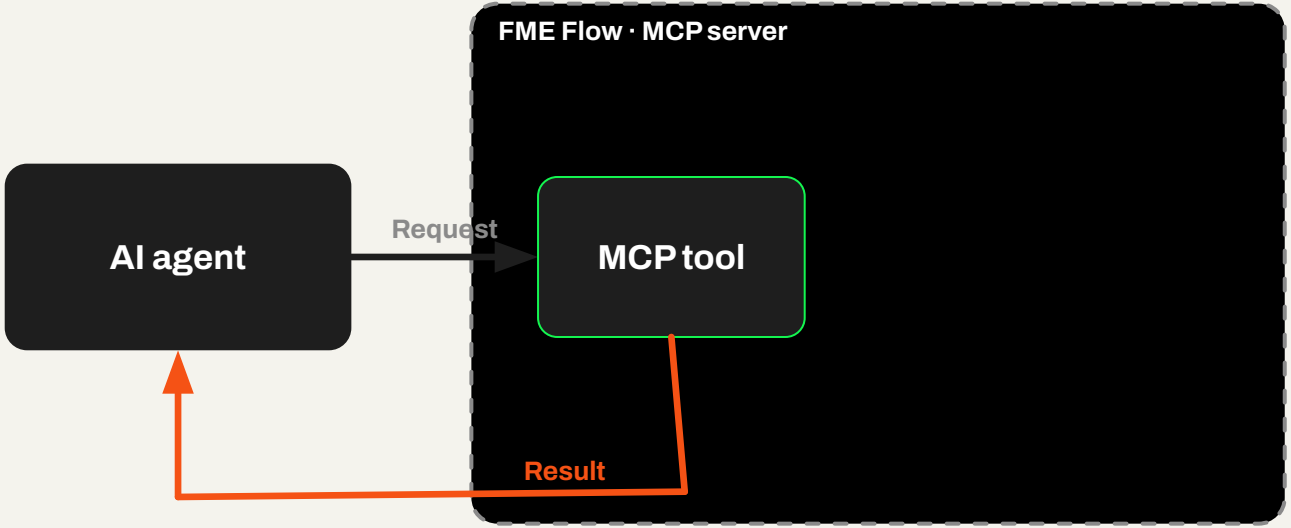
The workspace filters and shapes before anything leaves FME.



Safe Software

What is safe to release?

Inspect the response before a model sees it, and keep the record of every call.



The Five Safes

Established questions for sensitive data access

1

Safe people

Identity checked before anything runs

2

Safe projects

Tools do only what they were published to do

3

Safe settings

The server runs where the data needs it

4

Safe data

The workspace filters before anything leaves

5

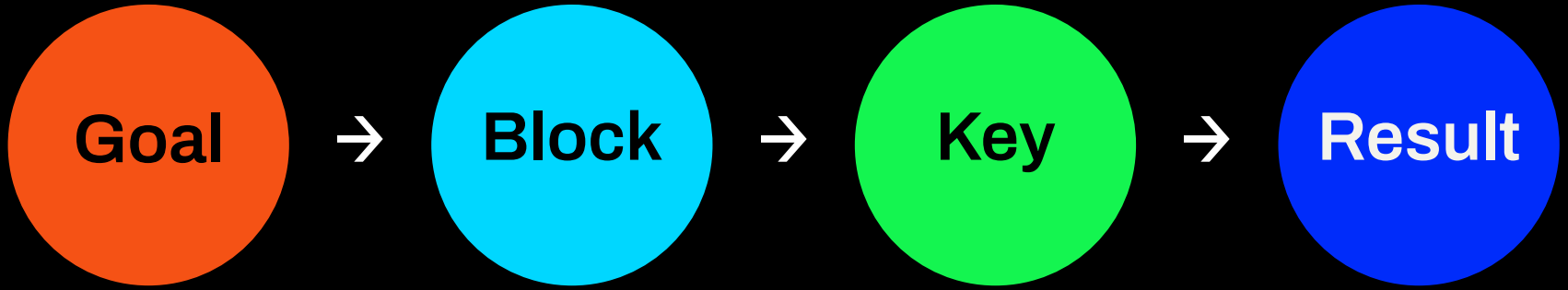
Safe outputs

Inspected responses, recorded calls

A data-access framework from the UK Office for National Statistics, used by the UK Data Service.

Safe Software

The Magic Data Bus: Tracing one MCP request



Answer a discharge coordinator's question from two systems, without the agent ever learning who a patient is.

The systems sit in different places with different owners. Connecting an agent to both normally means exposing everything in them.

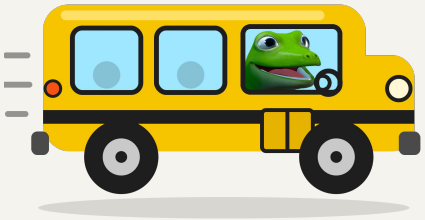
One read-only Flow tool. It checks who's asking, reads both systems, removes anything that identifies a patient, and writes the answer.

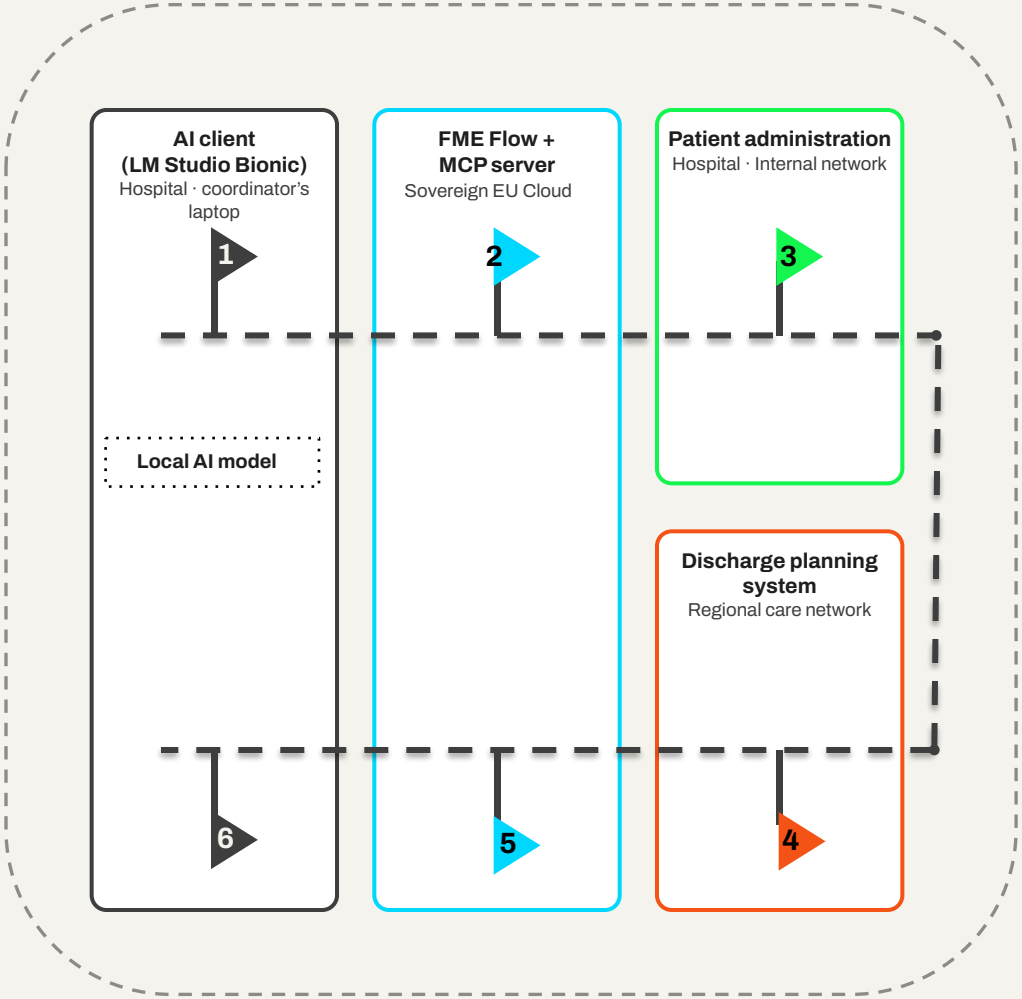
Eleven blocked patients, listed by ward and bed, with the reason for each. Eight seconds. The model never saw a name, ID, diagnosis or insurance number.

Safe Software

The Magic Data Bus

Six stops. 4 places. Zero exits from the EU.

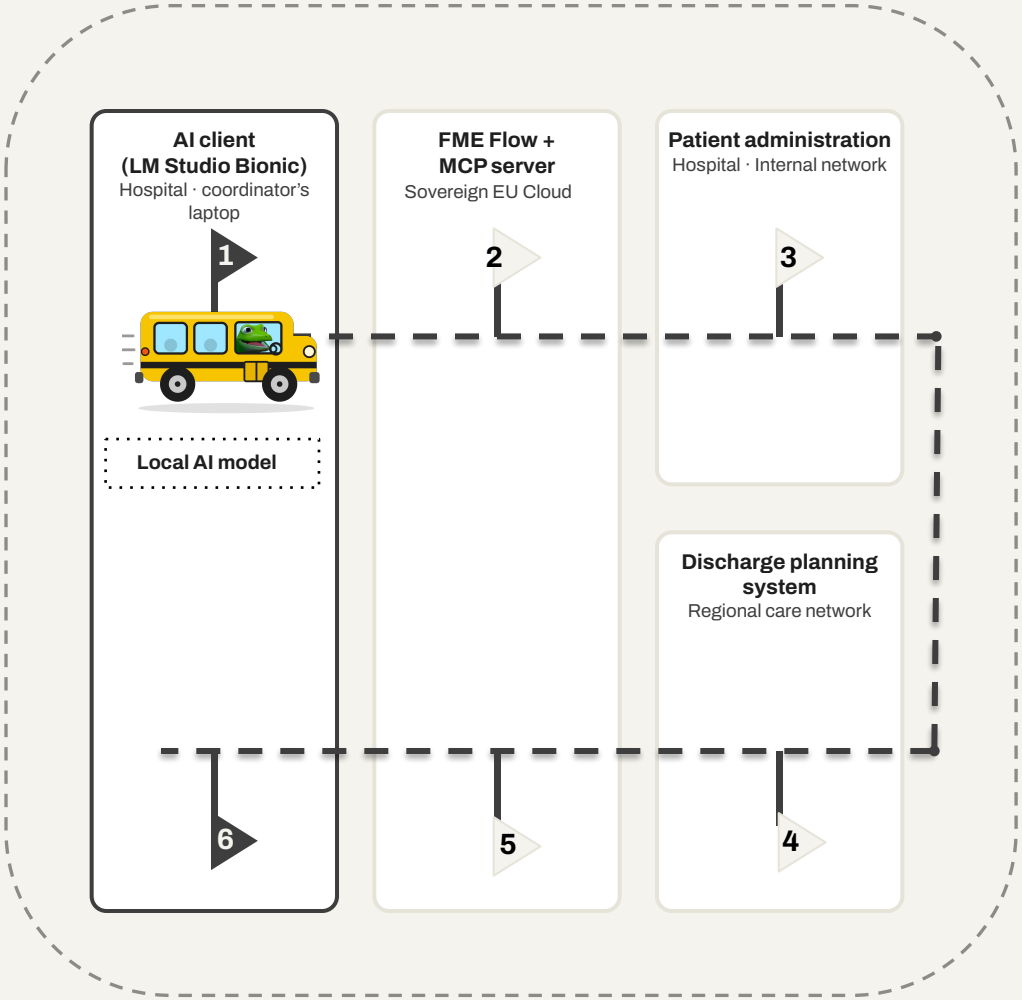




Safe Software

The user asks...

Which patients on the surgical wards are blocked from discharge, and what's holding them up?



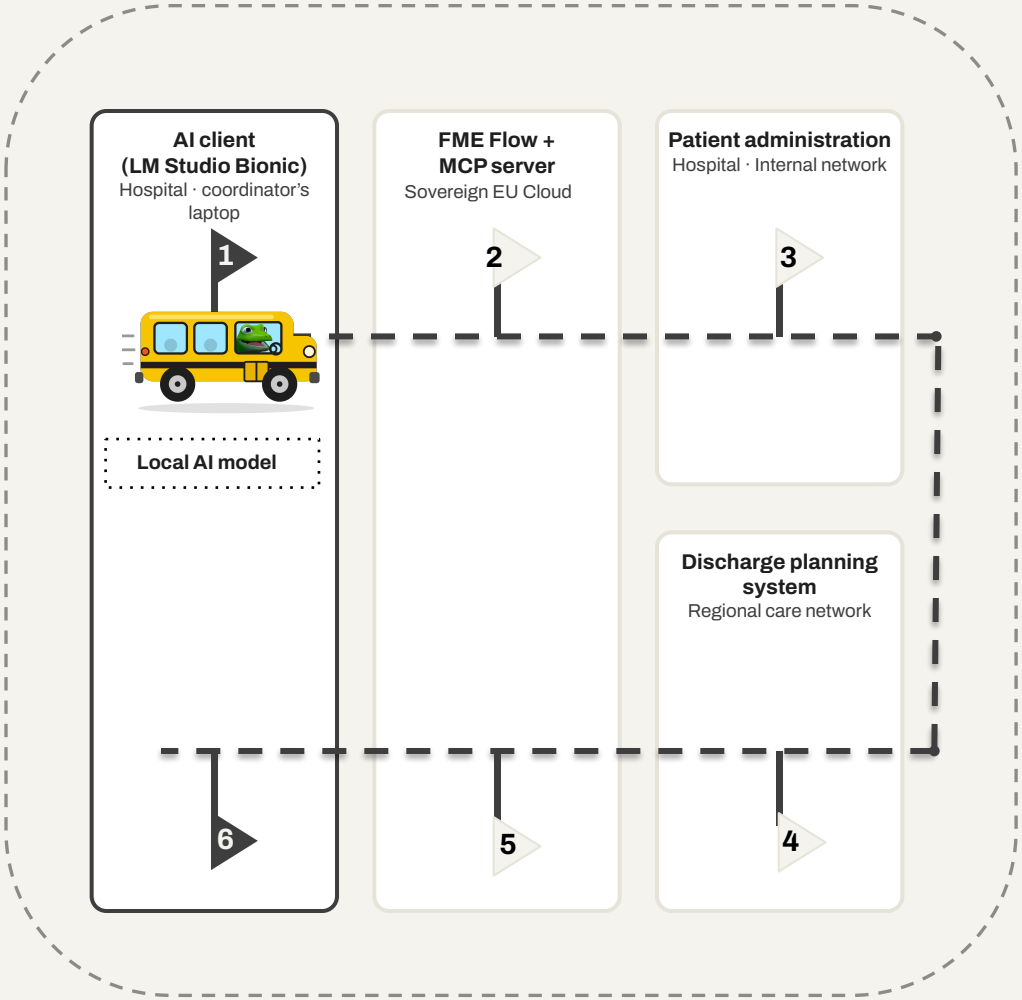
Safe Software

The user asks...

Which patients on the surgical wards are blocked from discharge, and what's holding them up?

What gets sent...

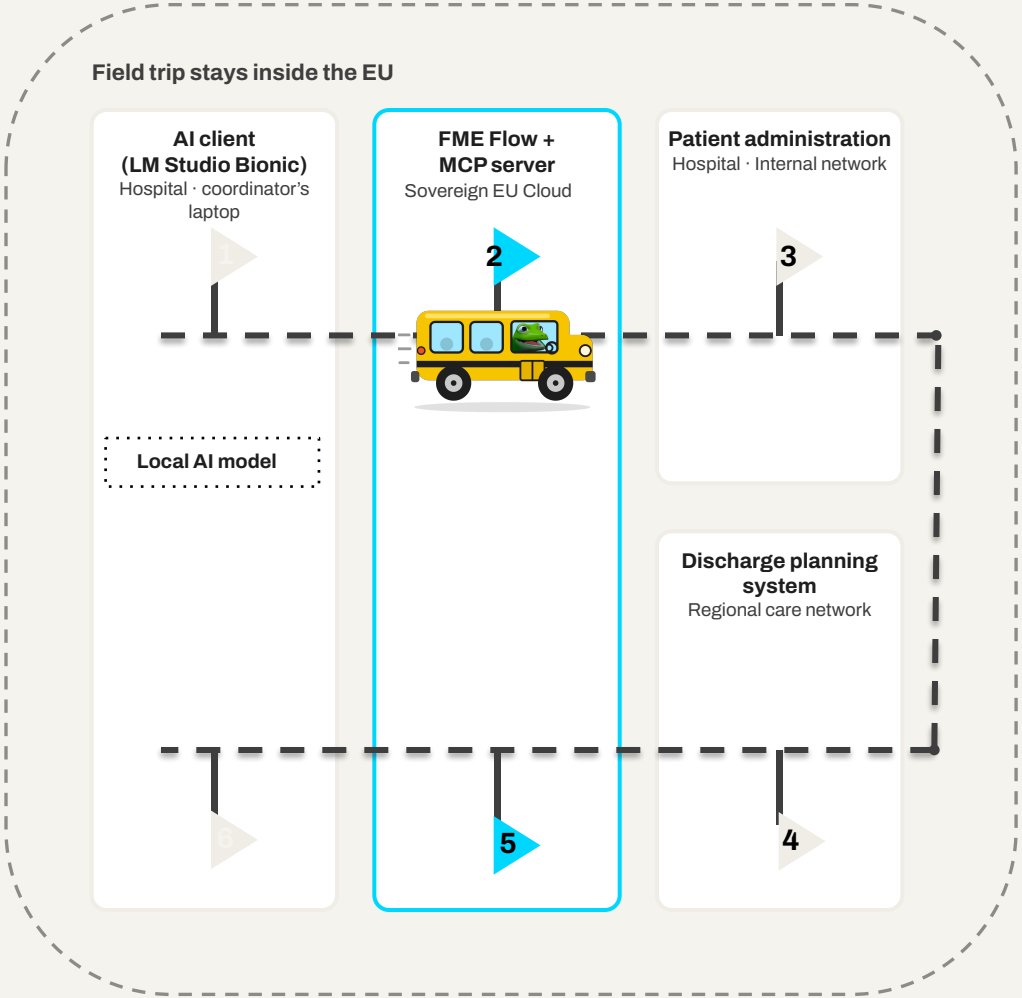
```
> tools/call
>   discharge_blockers
>   {"ward_group": "surgical"}
```



Safe Software

FME Flow: Whos asking?

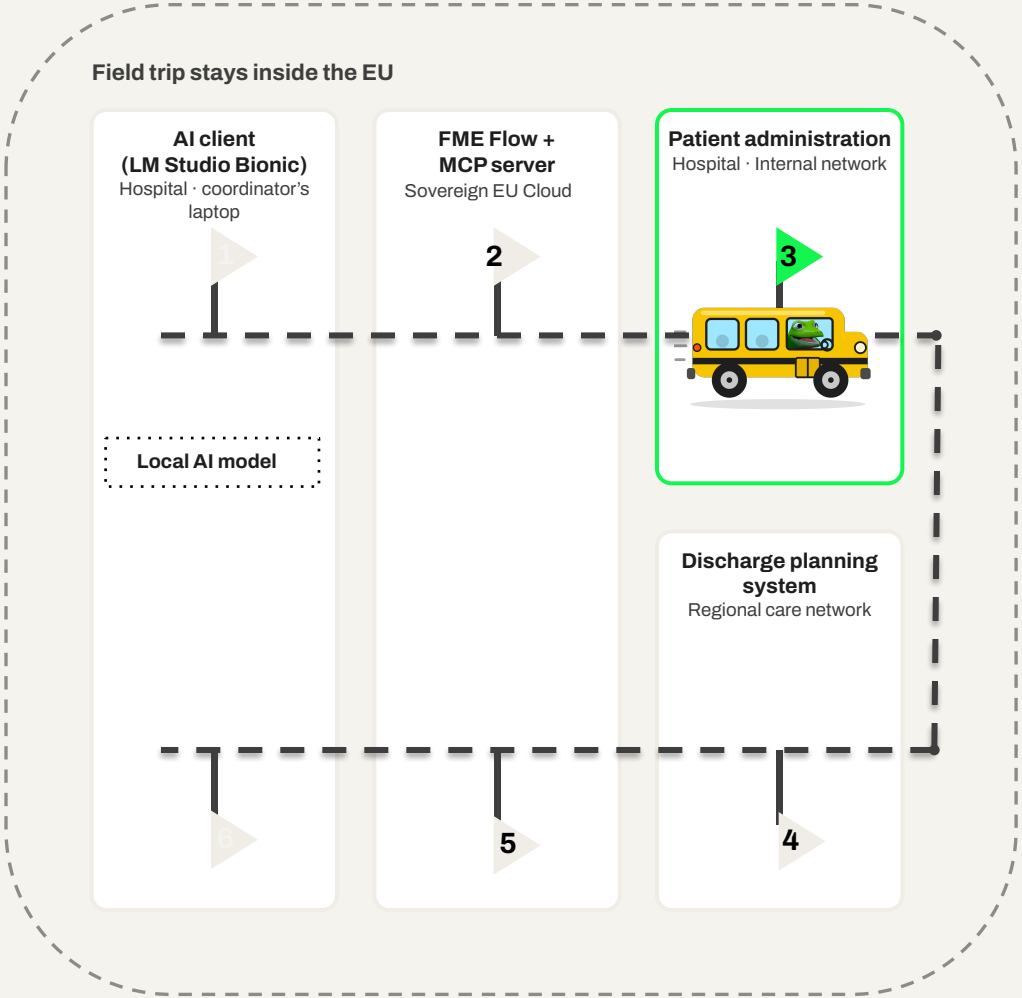
```
✓ Identity m.weber@klinikum-example.de (SAML)
✓ Role discharge-coordinators
      → may call discharge_blockers
✓ Running job 48112
· source: MCP
· 09:41:07 → discharge_blockers.fmw
```



Safe Software

Everything the hospital knows...

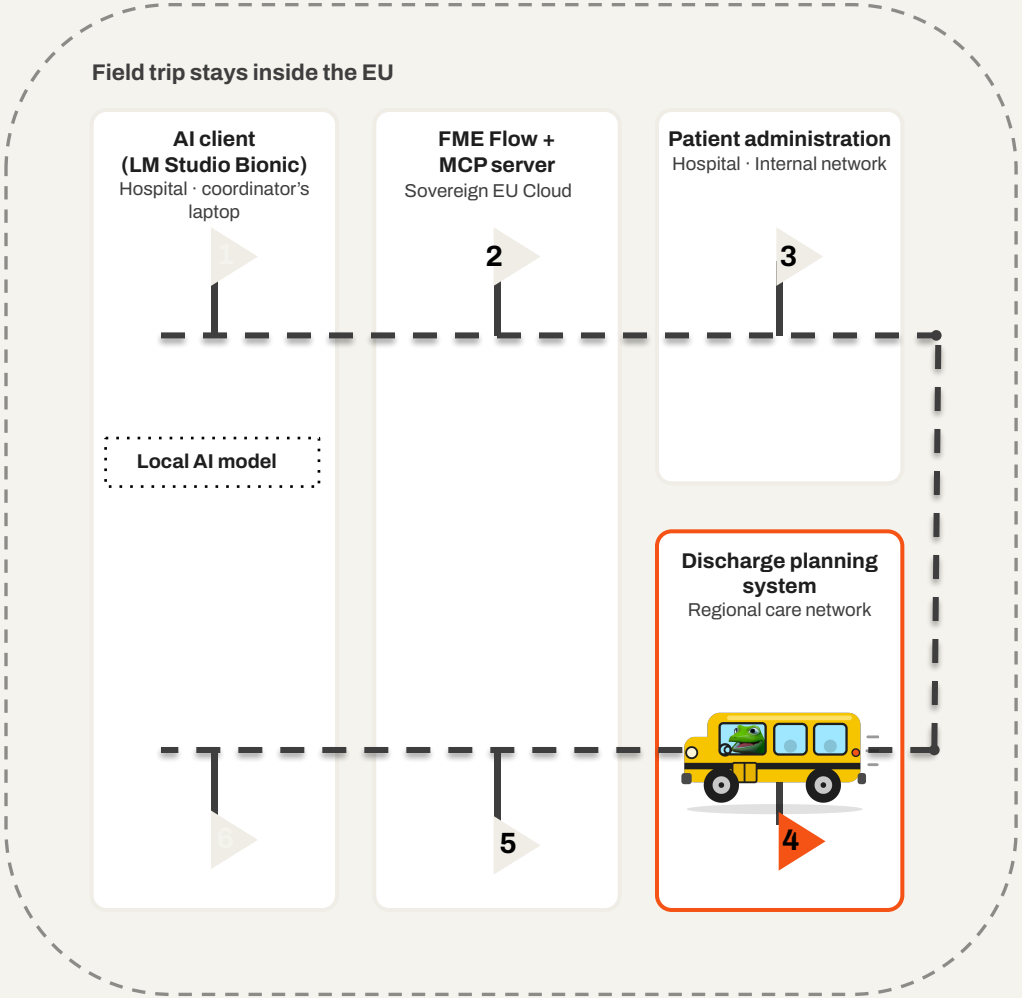
```
name · dob · insurance_no
ward · bed · admitted · diagnosis
Mustermann, Erika · 1948-03-12
  A123456789 · CH2 12-B · hip
fracture
… 14 more rows
```



Safe Software

Whos stuck and why...

```
patient_id · fit_date · reason
care_level · pending · notes
P-10231 · care-home place · 3
  "daughter can't take her…"
… 11 more rows
```

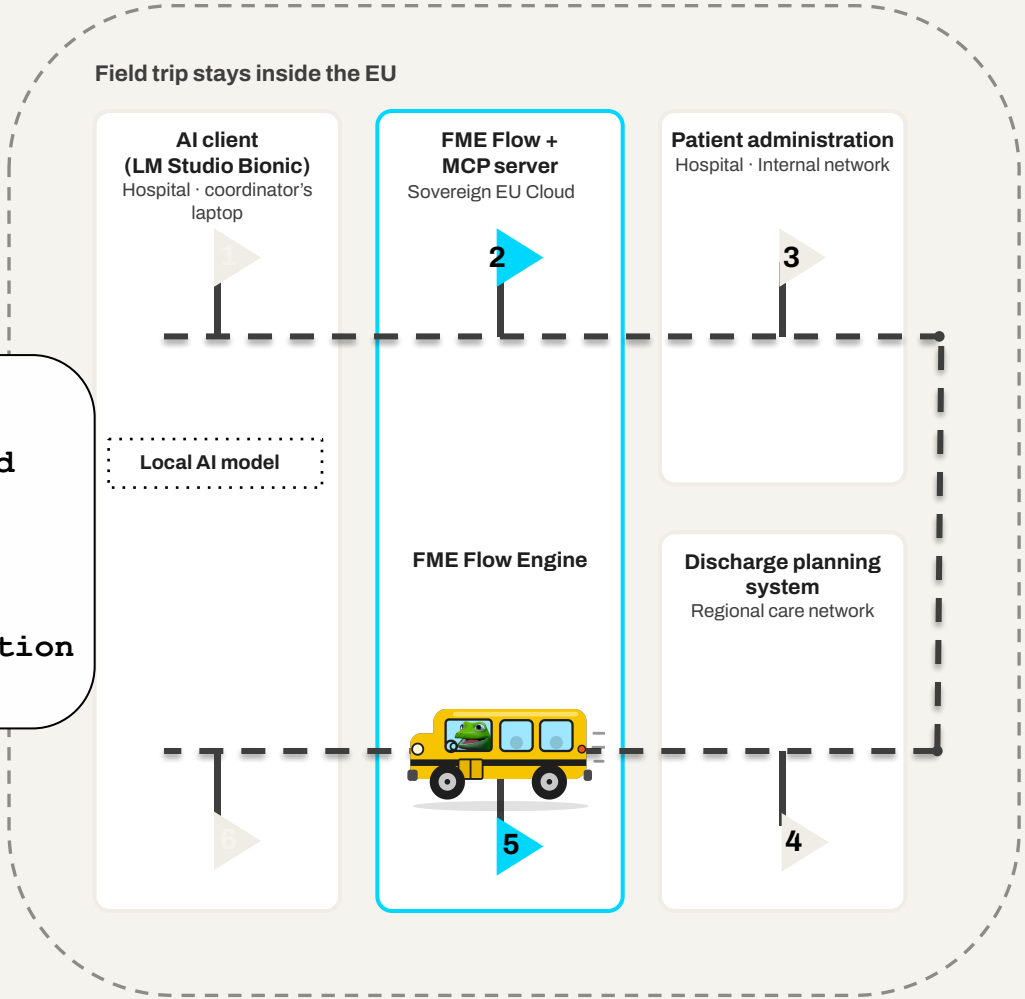


Safe Software

Sensitive data unloads the bus...

Gets off: `name · dob · insurance_no diagnosis · notes · patient_id`

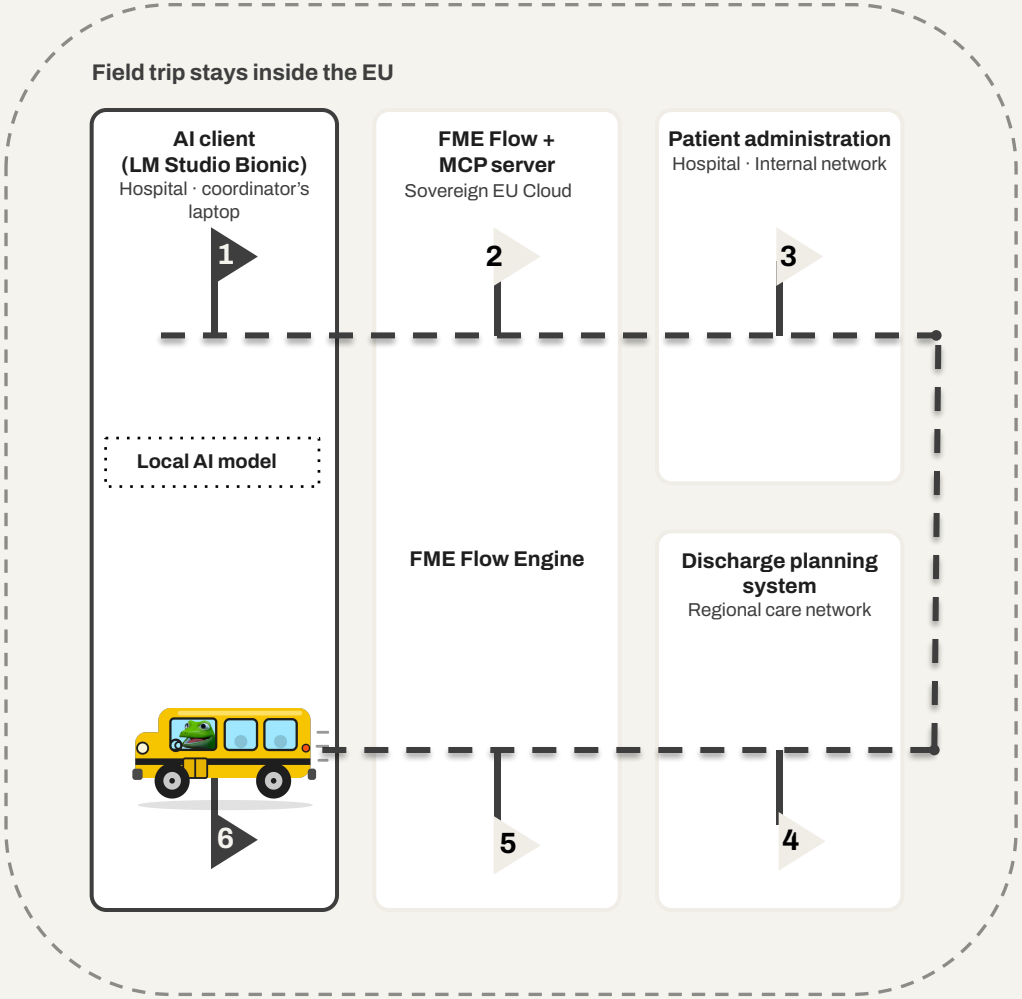
Stays on: `ward · bed · days_waiting blocking_reason · care_level pending_assessments · next_action`



Safe Software

What gets sent back..

```
CH2 bed 12-B · 23 days
  care-home place · care level 3
  2 assessments pending
  next: social-work review in 2 days
… 10 more
```



Safe Software

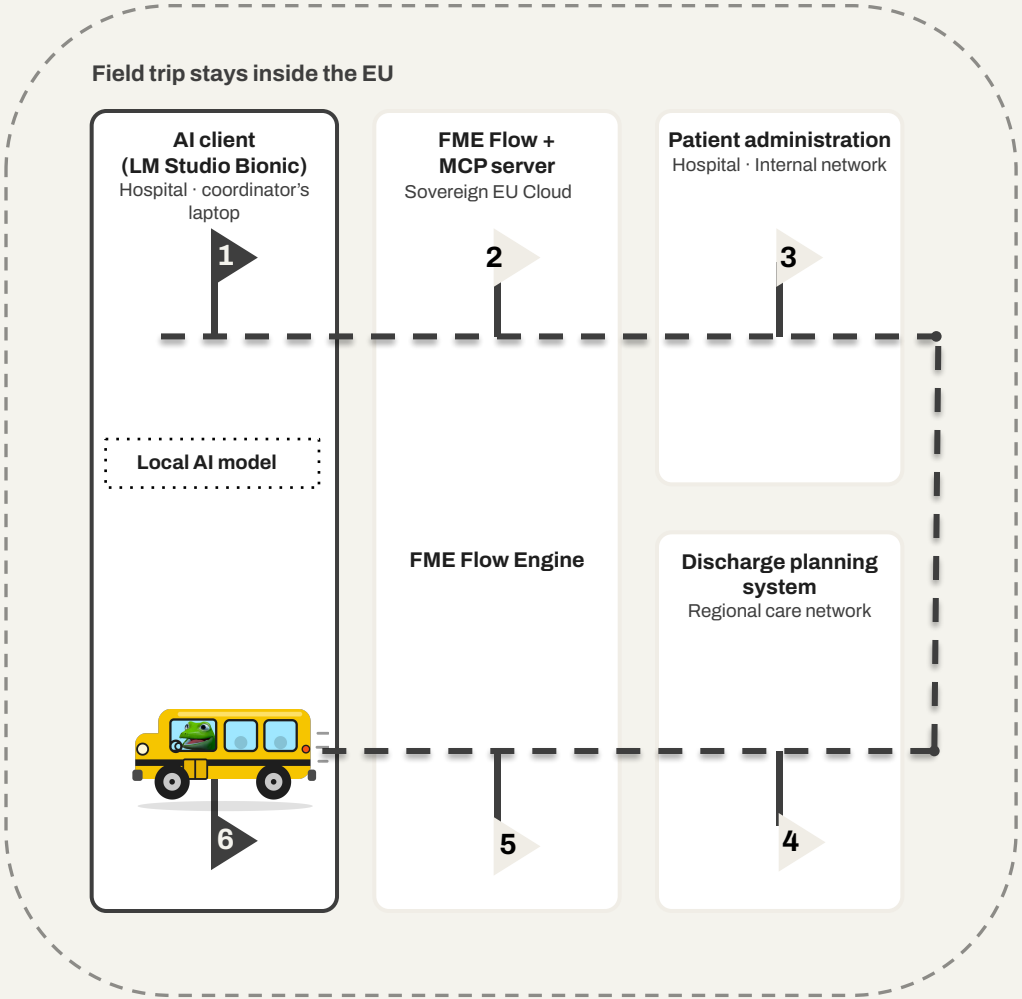
What gets sent back..

```
CH2 bed 12-B · 23 days
  care-home place · care level 3
  2 assessments pending
  next: social-work review in 2 days
… 10 more
```

What the user sees >

11 patients on the surgical wards are blocked from discharge: 7 waiting on a care-home place, 3 on home care, 1 on equipment.

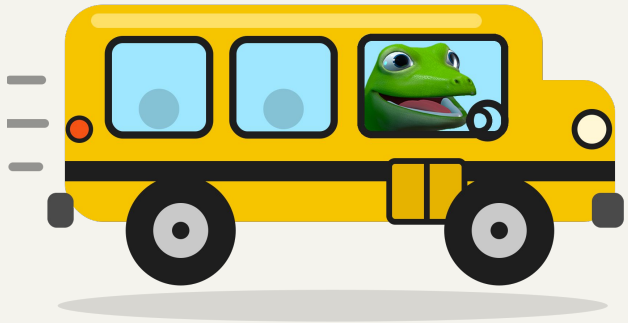
The longest wait is 23 days (ref 7f3a…). Blocked on a care-home place, care level 3, two assessments pending. Next step is the social-work review on Thursday.



Demo

The Magic Data Bus: Key Takeaways

- Decide who can use each tool
- Limit each tool to its approved purpose
- Know where processing happens and where responses go
- Return only the data the task needs
- Inspect responses and keep execution traceable



Safe Software

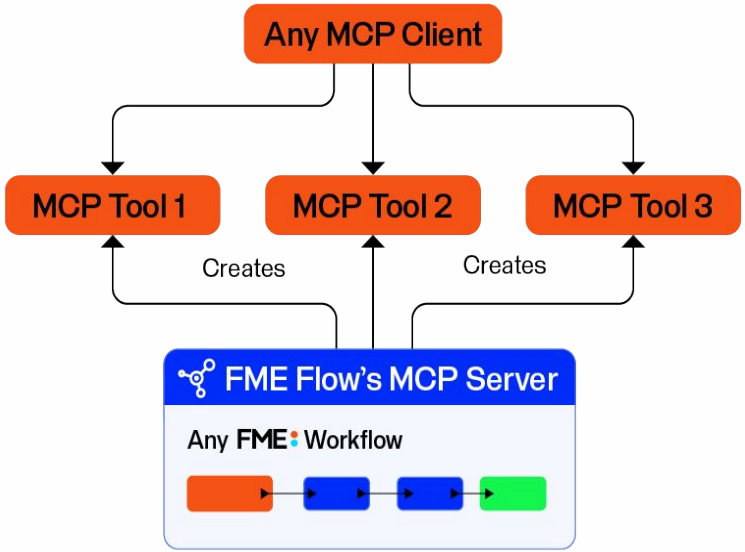
3 Best Practices: Tool Design & Testing

FME is the Data Guardian

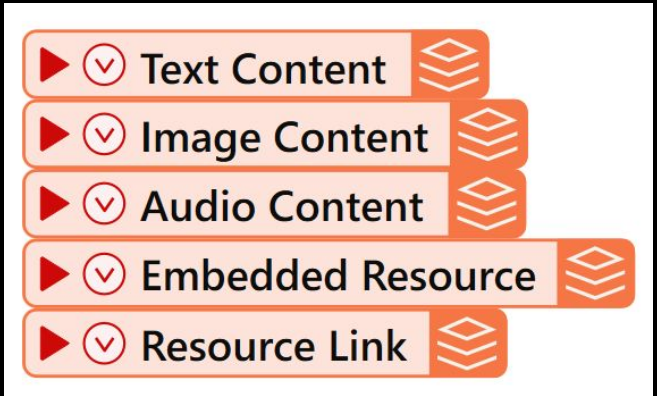
Workspaces are the filter between your AI agent and your data

- Filtering, querying, attribute management, etc...

*Your AI only sees the outputs that **you** decide to show it - no more, no less*



MCP Writer



The “**last line of defence**” - by the time your data reaches this point, it should be ready for your MCP client!

Workspace authors aren’t perfect, so how can we expect perfect workspaces every single time?

Mistakes will happen… we just need to do our best to ensure they happen in the safest possible environment!

Tool Testing Approaches

Testing with Agentic AI

Difficult to interpret the raw response, and can be unpredictable from one model to another when workspaces/tools are still in development

Testing with non-AI Clients

Easily inspect the raw JSON, and can always run safely within a private network on-premises

Postman, MCP Inspector, etc...

Run it before the agent does

- ✓ Allowed request returns only the intended data
- ✗ Unauthorized request is denied
- ✗ Missing policy or approval stops execution
- ✓ Completed or failed call can be traced
- ✗ Revoked access blocks further requests

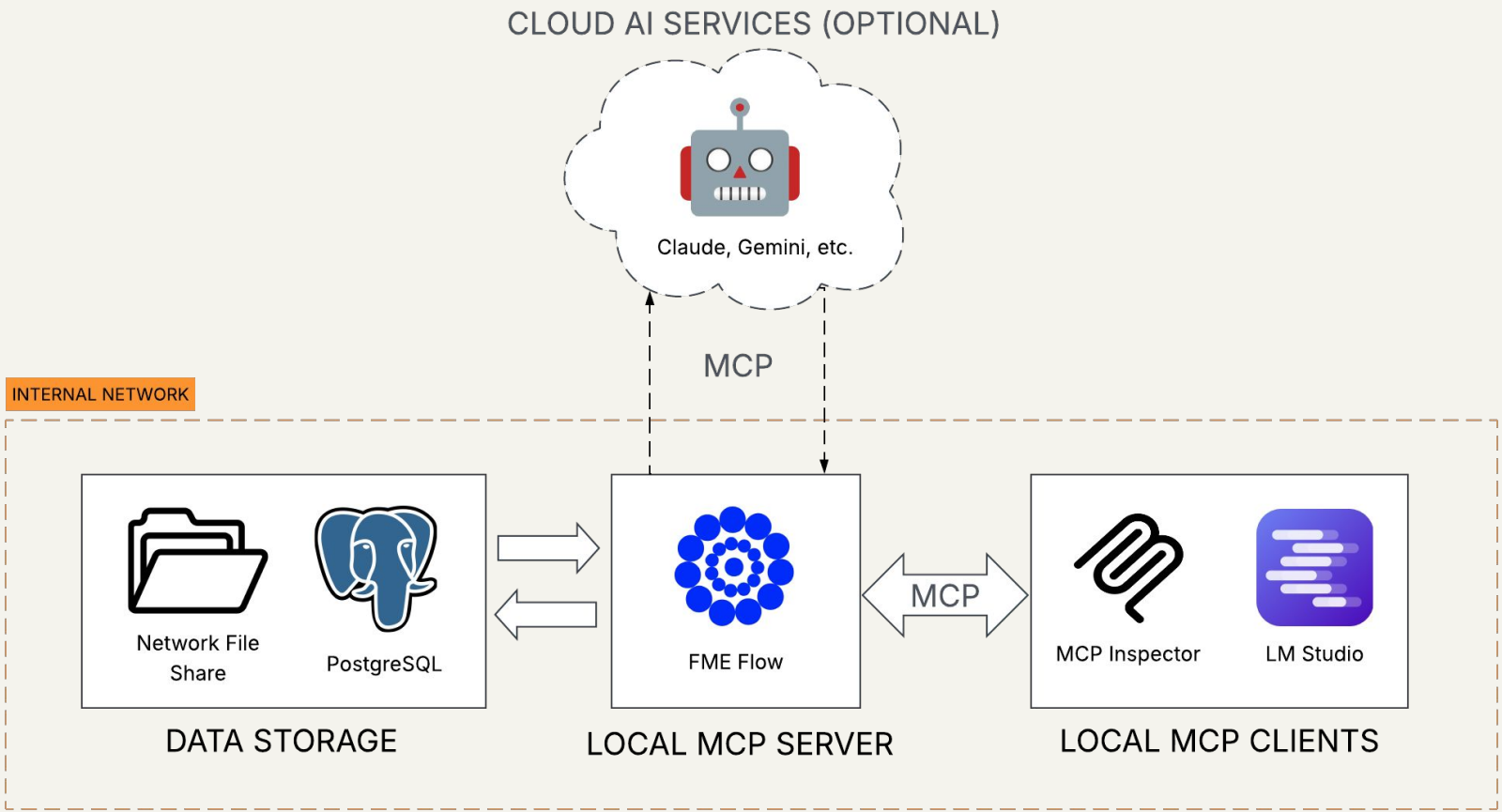
Testing and execution records show whether the rules hold.

Ticks are what should succeed; crosses are what should be refused.

MCP client tools/call · building_summary **200 · response**


```
{
  "jsonrpc": "2.0",
  "id": 1,
  "result": {
    "content": [
      {
        "type": "text",
        "text": {
          "building_id": "[…]",
          "floor_area_m2": [__],
          "approved_summary": "[…]",
          "permitted_records": [__]
        }
      }
    ],
    "isError": false
  }
}
```


Inspect the raw response before a model sees it


CLOUD AI SERVICES (OPTIONAL)
Claude, Gemini, etc.
MCP
INTERNAL NETWORK
Network File Share
PostgreSQL
DATA STORAGE
FME Flow
LOCAL MCP SERVER
MCP
MCP Inspector
LM Studio
LOCAL MCP CLIENTS

Flash Demo

MCP ≠ AI

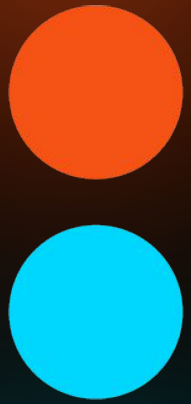
Local, non-AI clients are a great tool for testing MCP workflows

Any potential security issues with our workspaces can be uncovered and addressed from the privacy of our own network!



Safe Software

4 Best Practices: Tool Descriptions & Chaining



Good tool descriptions are a must when it comes to MCP - plain and simple!

But what do we mean by a “good” tool description?... Verbose? Brief?

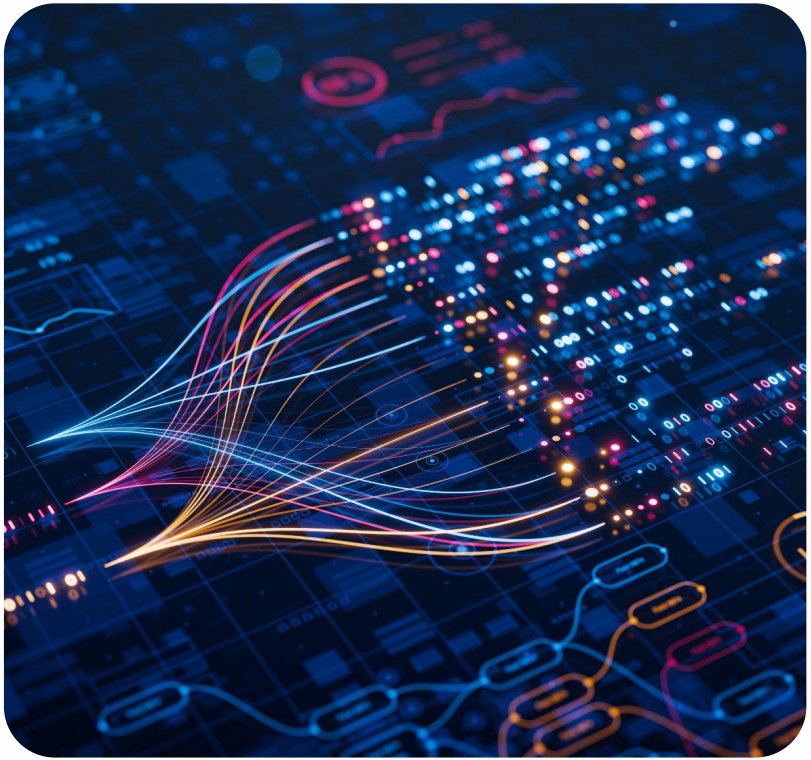
Good Tool Descriptions Should…

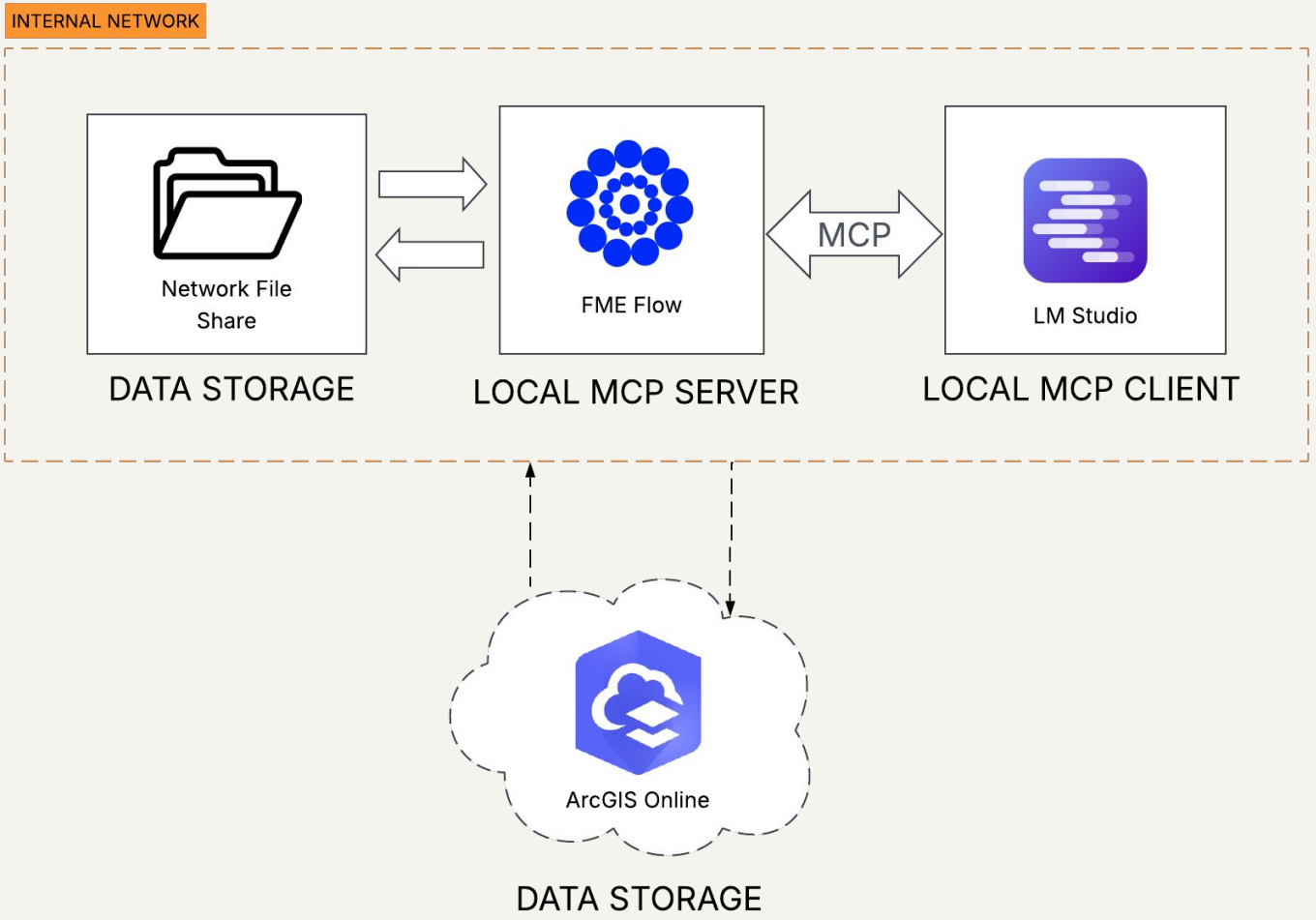
- Be clear and concise
- Clearly state the tool's purpose and expected output
- Highlight any specific tool limitations
- Align with any tool parameter descriptions
- Align tools with the "5 Safes" framework (safe projects and settings)

Chaining Tools

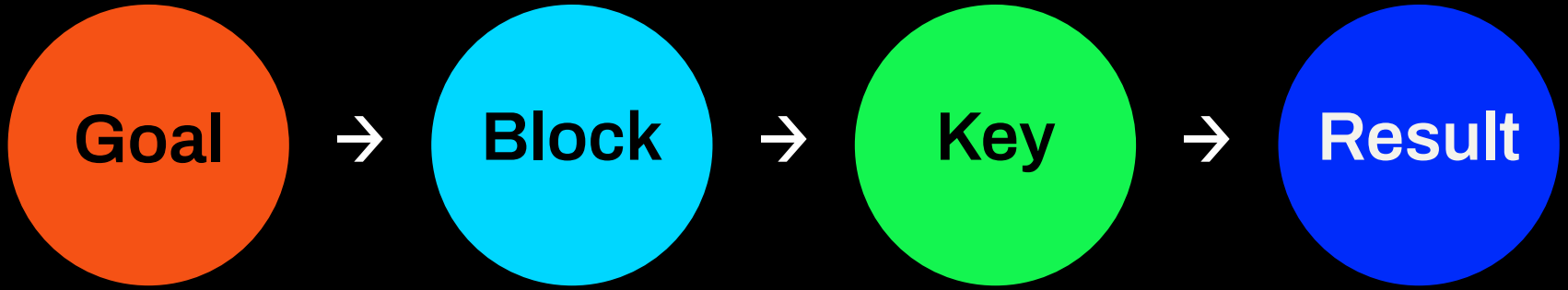
Tool descriptions can be used to chain tools in sequence

- Useful, but should be used with caution
- Consider using “human in the loop” checks to ensure that no unintended actions are taken




INTERNAL NETWORK
Network File Share
FME Flow
MCP
LM Studio
DATA STORAGE
LOCAL MCP SERVER
LOCAL MCP CLIENT
ArcGIS Online
DATA STORAGE

Feature Service Fiasco…



Perform multiple tasks with a single prompt to our AI agent

A single tool/workspace with no description is not an effective strategy

Break the workspace into multiple tools, with a HITL check in the middle

A more predictable, repeatable, and safer data workflow!

Demo

Some key takeaways…

- Tool descriptions are crucial - your agent knows nothing about your tools unless you provide it with context!
- Smaller, specialized tools are often more useful (and predictable) than large tools with multiple steps
  - Especially true when chaining tools together!
  - HITL checks help to ensure data integrity and security (server-side and client-side)

5 Conclusion

Safe Software

Safe Software

Three questions, answered in FME.

Authentication

Who is asking?

OAuth 2.0 sign-in, mapped to your SAML identities. Checked before anything runs.

Access control

What can they reach?

An MCP server per domain, per-tool permissions, and workspaces that filter what returns.

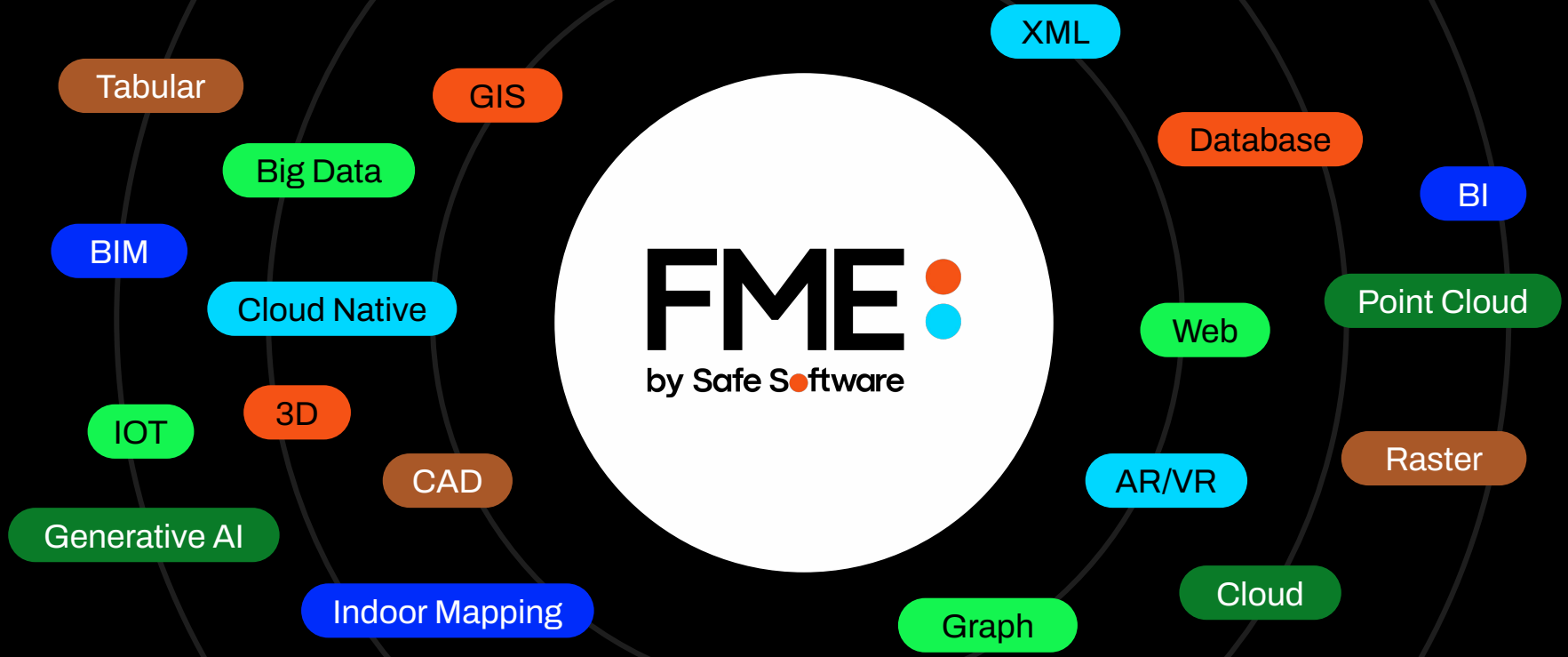
Data sovereignty

Where does it go?

FME Flow Hosted in your region, on-prem, or fully internal with a local model.

Unrivalled Data Support

Safe Software



With 500+ supported data types in FME.



Safe Software

30+
years of solving data challenges

128
countries with FME customers

25K+
organizations worldwide

30K+
FME Community members

200K+
users worldwide

140+
global partners with FME services

bsi ISO/IEC 27001 Information Security Management CERTIFIED

A-LIGN SOC 2

Certified B Corporation

Personal Information Protection and Electronic Documents



FME is a **Leader for On-Premise Data Integration, Data Virtualization, iPaaS, ETL Tools, and Reverse ETL** in G2's Fall 2026 Reports.













fme.safe.com/g2

Safe Software

The Power of Choice

Expanded to give you the ability to choose what AI sees.



Deploy Anywhere

On-premises, any cloud, hybrid, edge and more. Your infrastructure. Your rules.



Any Data Source

1000s of formats. Systems built before APIs existed. If it holds data, FME reads it.



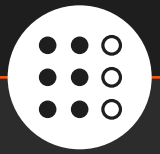
Full Governance

Sensitive data never leaves your perimeter. Compliance is architecture, not paperwork.



Any AI Model

OpenAI today, something else tomorrow. Your data layer does not care who wins.



Data Exposed to AI

Choose the data AI sees. Pick the rows. Pick the columns. Obfuscate anything else.

6 Resources

Resources

- FME with MCP: Bring Choice and Control to Enterprise AI
- Getting Started with MCP in FME
- Turning FME workspaces into MCP tools: Connecting ArcGIS to AI
- How to give AI access to sensitive data without letting it leave your network



Resources

Safe Software



Get our Ebook

Spatial Data for the Enterprise

fme.ly/gzc



FME Academy

Guided learning experiences at your fingertips

academy.safe.com



Knowledge Base

Check out how-to's & demos in the knowledge base

support.safe.com



Webinars

Upcoming & on-demand webinars

safe.com/webinars

7
Next Steps

Safe Software

Safe Software

Contact Us

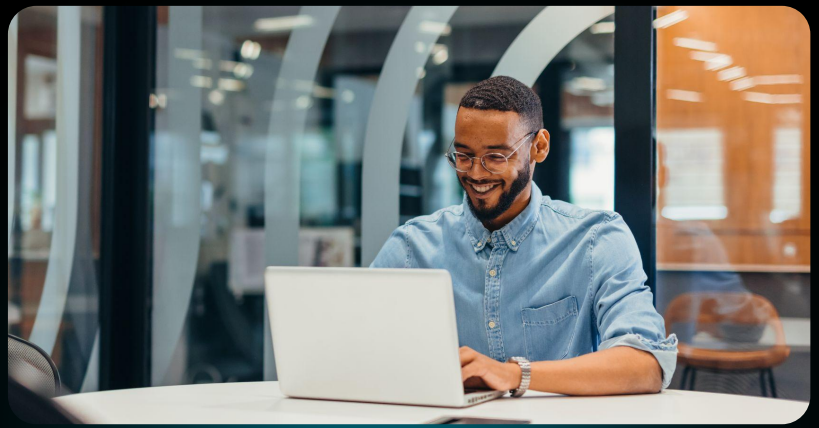
We'd love to help you get started.Get in touch with us at **info@safe.com**

Experience the FME Accelerator

A world where data is not just a commodity but a catalyst for real change.

fme.safe.com/accelerator






The Peak of Data and AI • 2027
London, UK
Registration Now Open!
Get Tickets

Safe Software

FME Community

Claim Your Community Badge & Dive into the new Community!

- Get community badges for watching webinars
- community.safe.com
- Today's code... **56B29A**

Join the Community today!



8
Q&A

Safe Software

Thank You

Safe Software

Recap of Next Steps

1. Follow us on LinkedIn!
2. Contact us
3. Experience the FME Accelerator

Please fill out our webinar survey