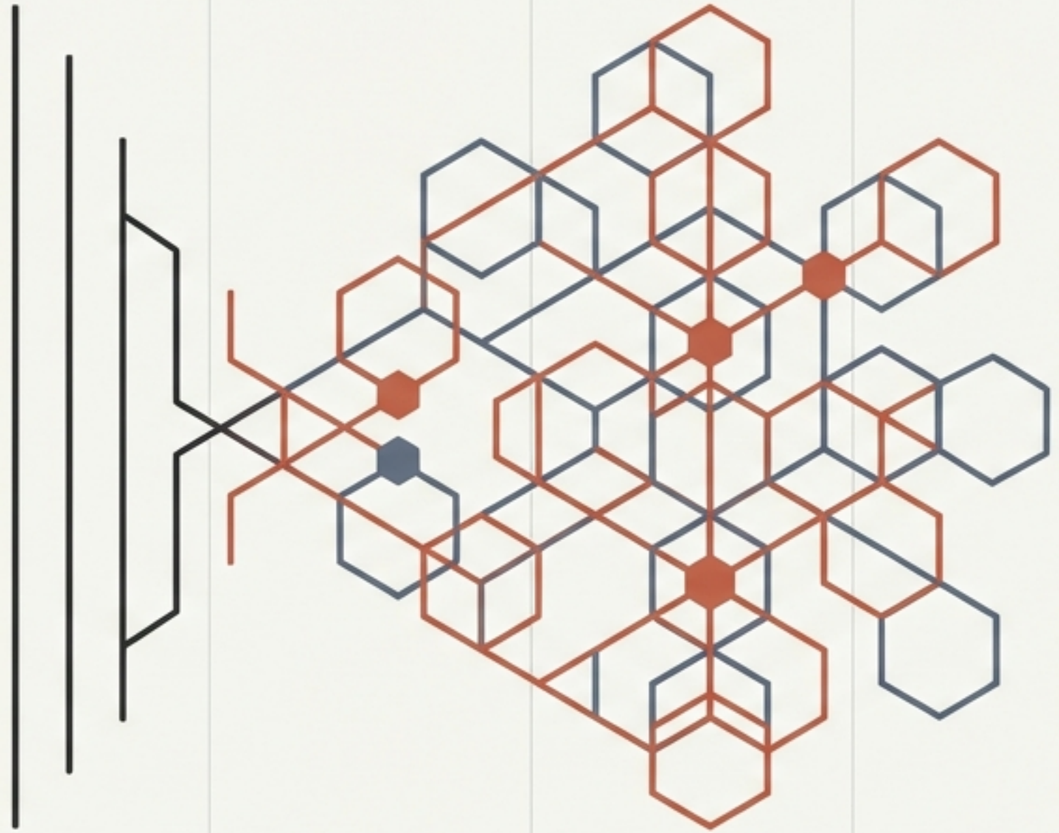


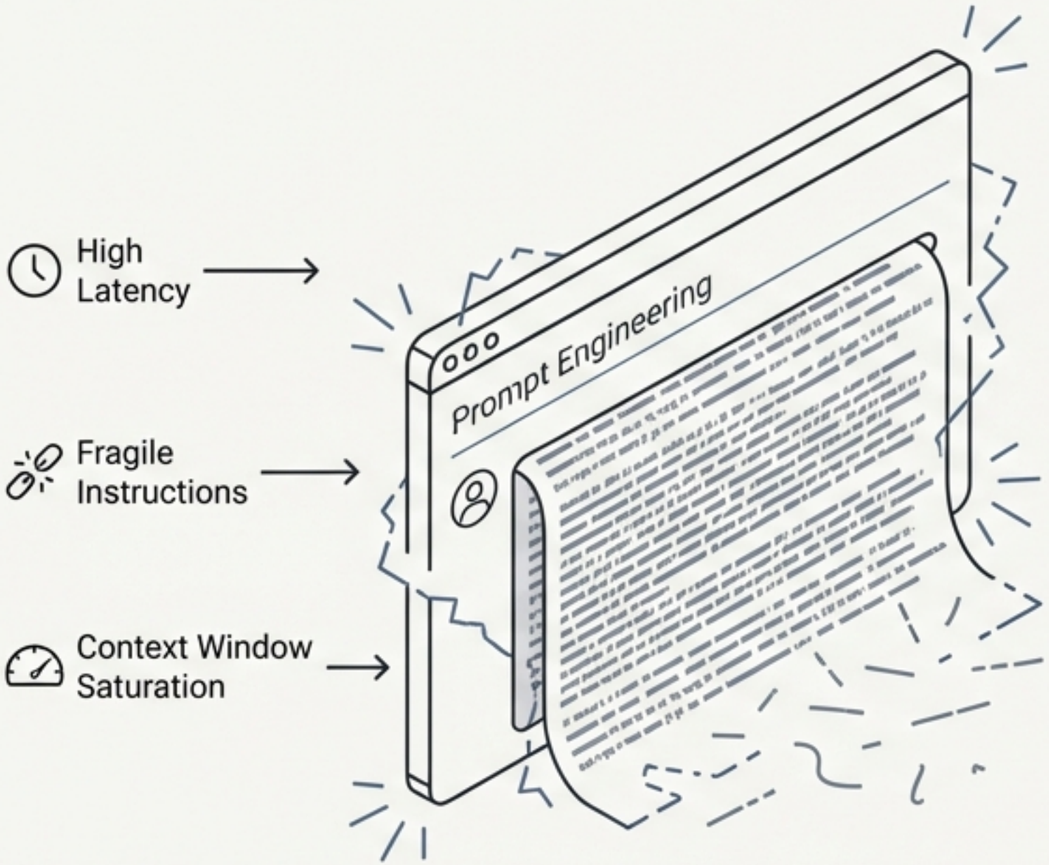
From Conversation to Orchestration

The Evolution of Claude Skills and the Rise of Composable Workflows

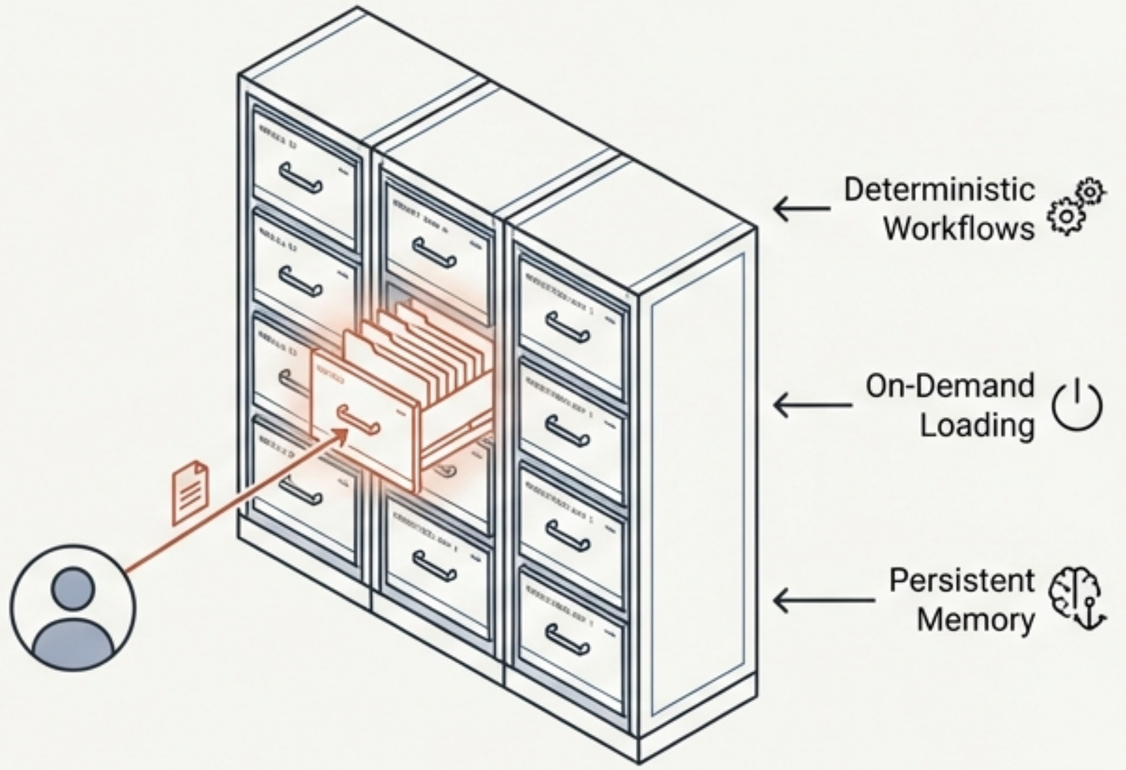
STRATEGIC BRIEFING | 2025

The Limitation: Context Exhaustion

The Old Way



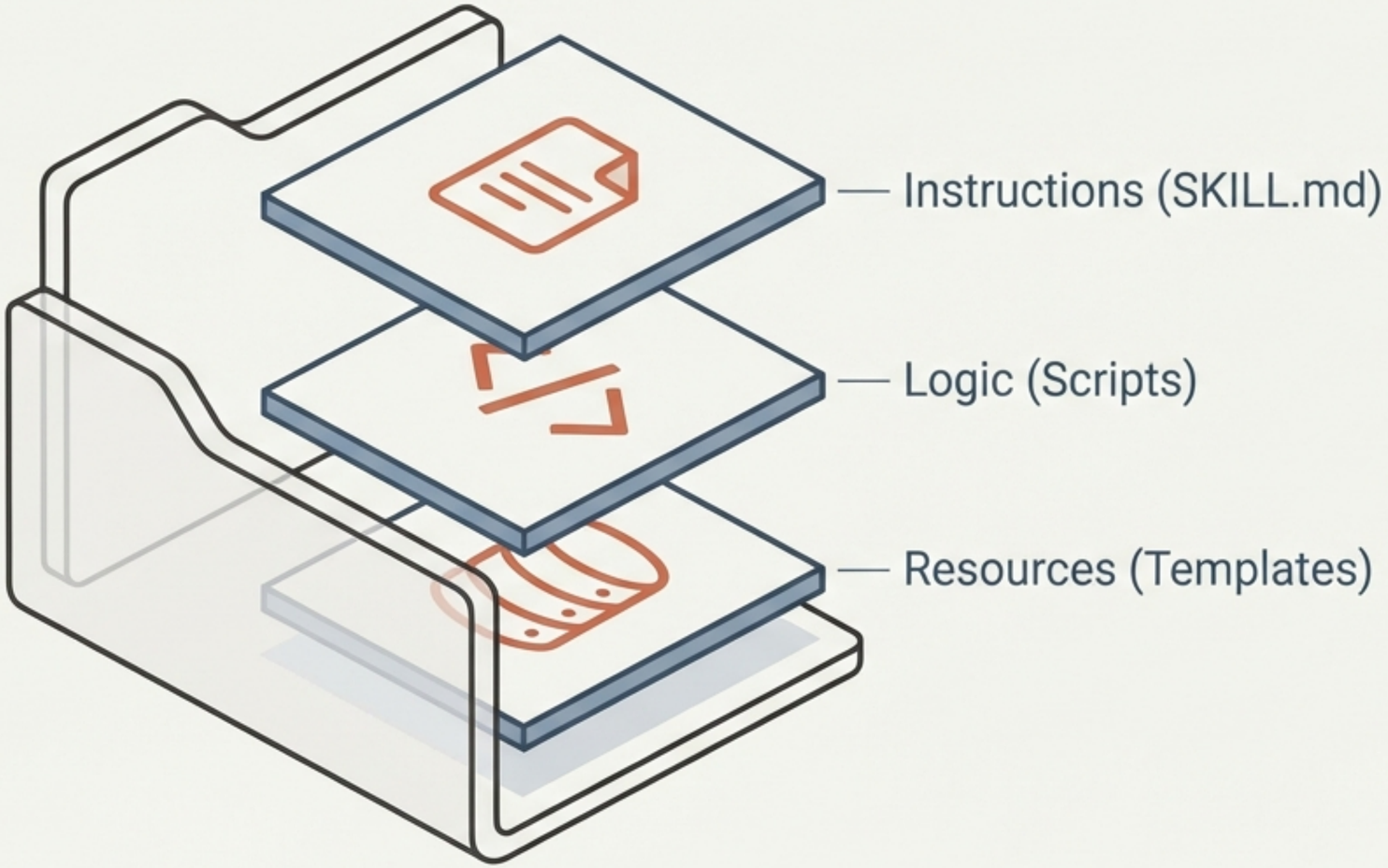
The New Way



Copy-pasting instructions is not an architecture. To scale agency, we must move from transient context to persistent, structured memory.

Defining Claude Skills

Modular, Portable, Composable Task Packs



Modular

Encapsulated logic in a directory structure.

Portable

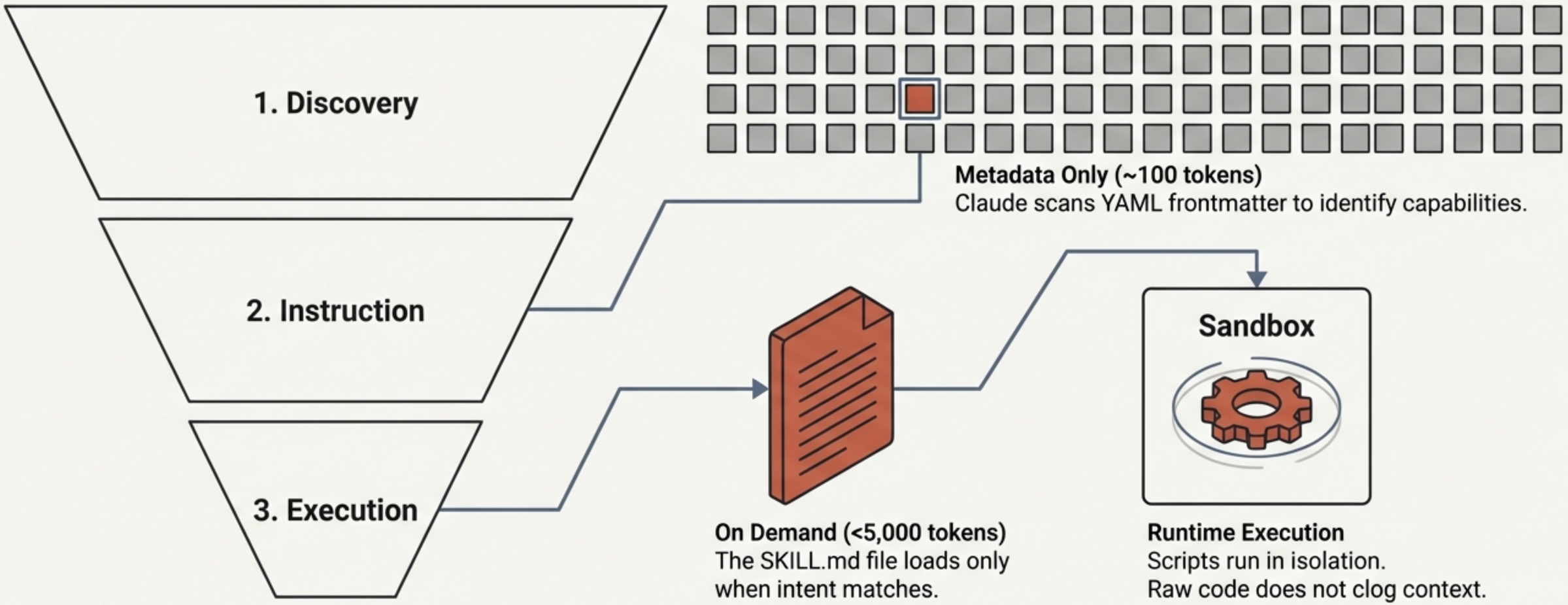
Works across Claude.ai, CLI, and API.

Composable

Skills can be chained for complex pipelines.

Metaphor: An onboarding guide for a new hire—packaged expertise applied automatically.

Under the Hood: Progressive Disclosure

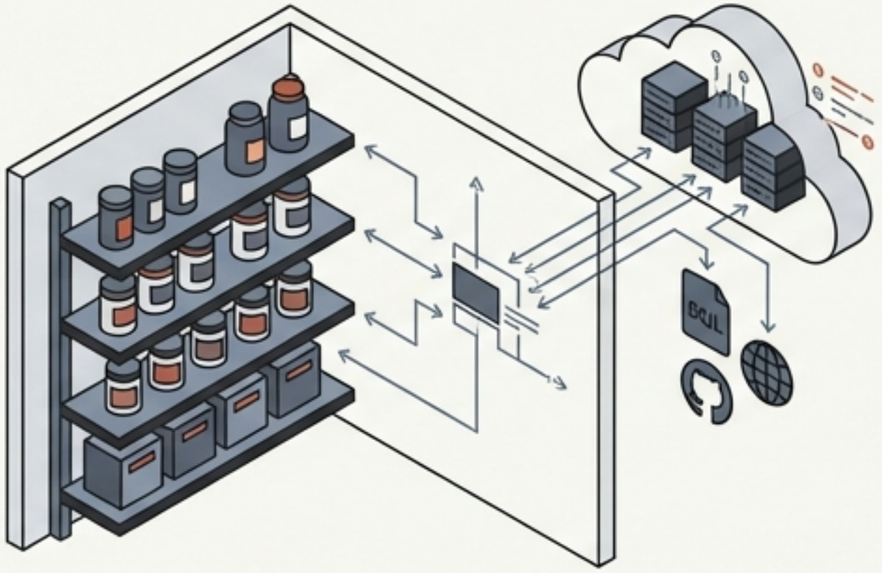


Key Insight: High Capability, Low Latency: Claude only pays the "context cost" for the specific tools needed.

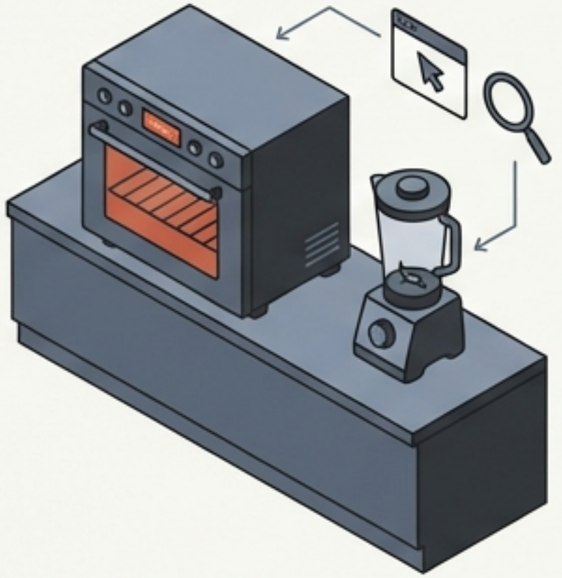
The Ecosystem Landscape

Distinguishing Skills, MCP, and Platform Tools

Claude Skills = The Recipe
The Methodology (How).
Structured instructions and checklists.



MCP = The Pantry
Connectivity (What). Standard protocol
to access external data (SQL, GitHub).



Platform Tools = The Appliances
Capabilities. Vendor-specific actions
(Computer Use, Search).

MCP connects Claude to the world.
Skills teach Claude how to behave within it.

Deep Dive: The Anatomy of a Skill

Directory Structure

```
my-skill/
├── SKILL.md
├── scripts/
│   └── analyze_data.py
└── resources/
    └── template.docx
```

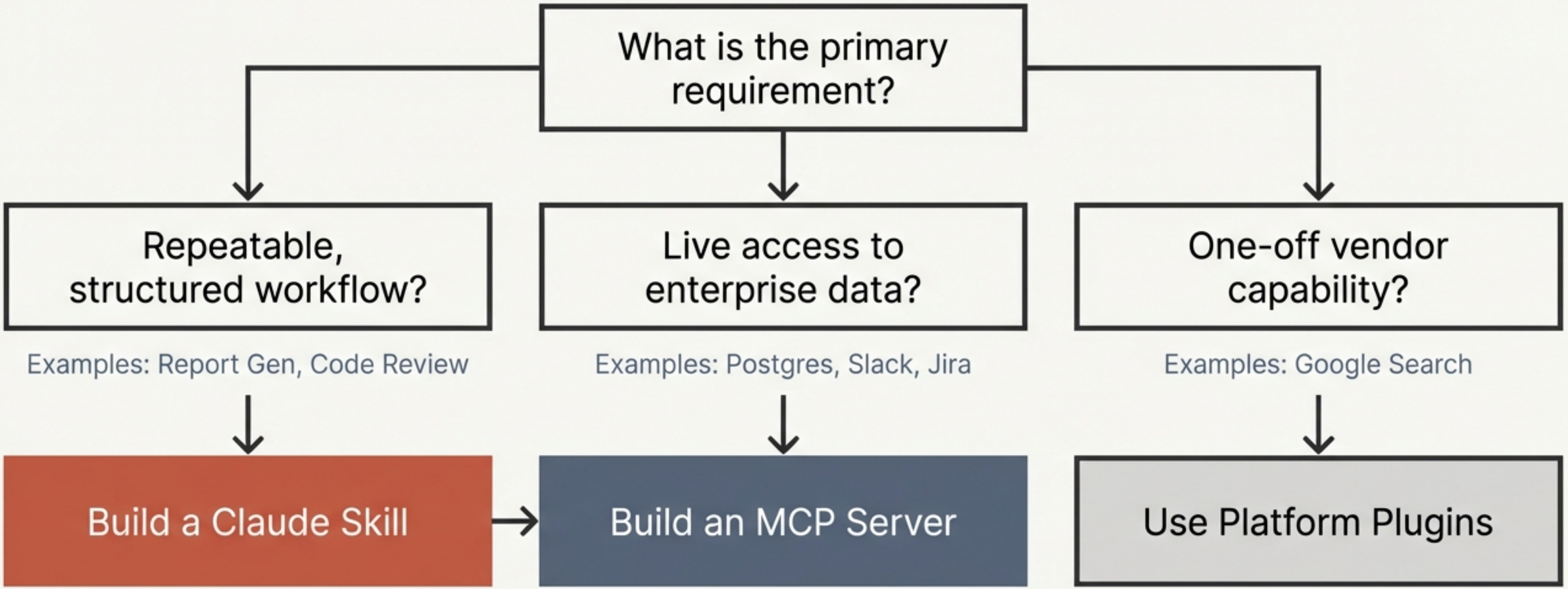
SKILL.md Content

```
---
name: data-analyzer
description: Analyze financial datasets
version: 1.0
license: MIT
---

# Instruction Body
1. Ingest CSV from user input.
2. Execute 'analyze_data.py' script.
3. Format output using 'template.docx'.
```

Semantic Trigger: This field determines when Claude activates the skill.

Strategic Decision Guide

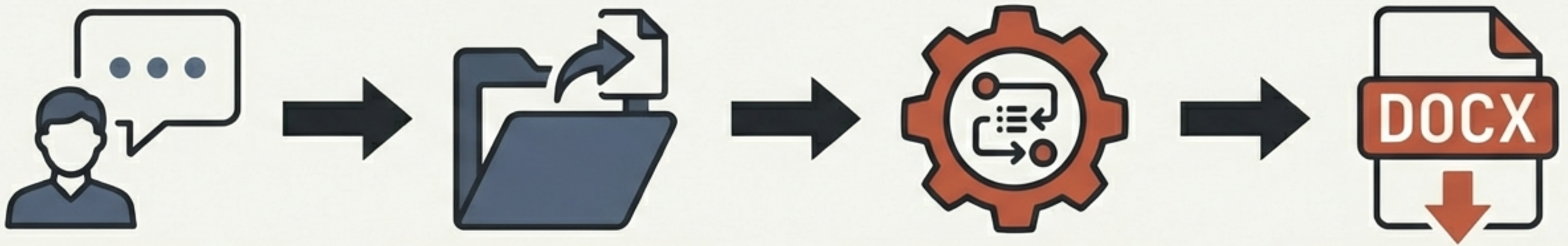


Mature architectures combine them: **Skills orchestrate the tasks**, MCP provides the **data.**

The Agentic ROI: Real-World Impact

Rakuten Case Study	Telus Implementation	Cost Efficiency
87.5%	**500k**	**2,500x**
Time Reduction	**Hours Saved**	**Cheaper Execution**
Financial Anomaly Detection reduced reduced from 1 Day to 1 Hour.	Across 57,000 employees and 13,000 internal AI tools.	Script execution ($0.001) vs. Token generation ($2.50).

Tutorial: Building a Lesson Plan Generator



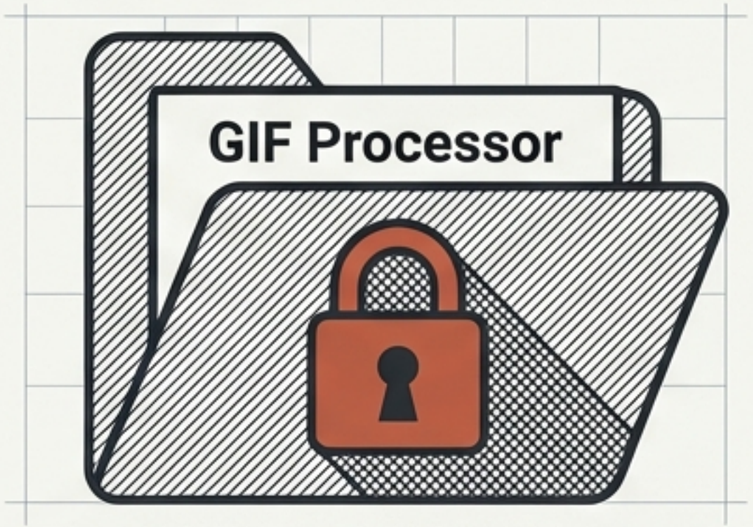
Input	Skill Activation	Processing (The Logic)	Output
Topic: “Photosynthesis for 10th Grade”	Loads “lesson-plan-generator” Skill	- Generate SMART Objectives - Structure Content - Design Quiz	Downloadable Lesson Plan

Pedagogical standards are encoded into the file, ensuring consistent quality every time.

Security & Governance

Closing the Consent Gap

The Risk



The "MedusaLocker" Proof-of-Concept shows how innocent-looking skills can execute hidden encryption scripts.

Zero Trust Defense

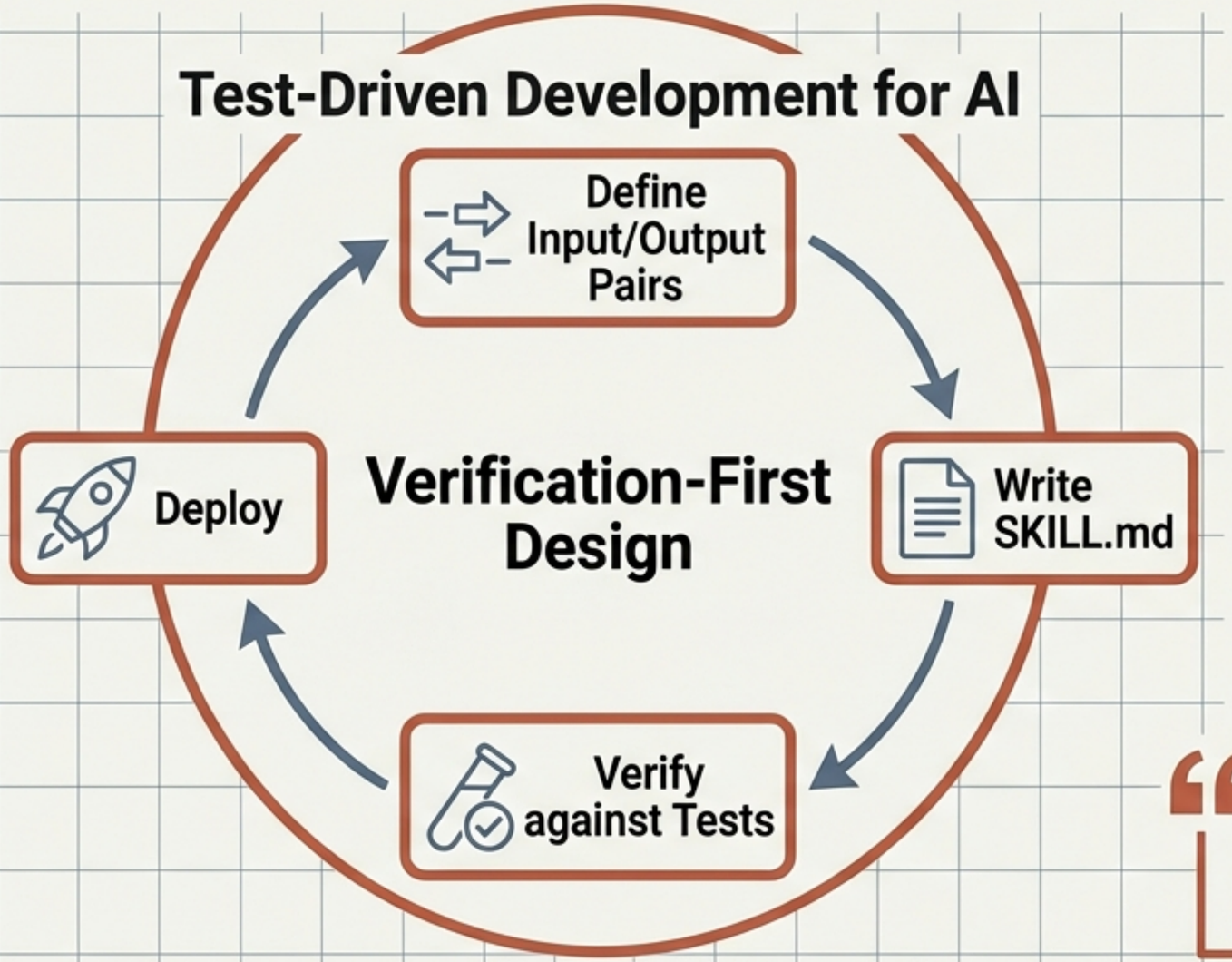
Allowlists
(`managed-settings.json`)

Sandboxing
(Isolated Containers)

Hygiene
(Data Cleanup Policies)

Treat Skills like code. Never install untrusted Skills without inspection.

Best Practices for Engineering Agency



Context Hygiene

Use '`/clear`' commands to prevent hallucination via compaction.

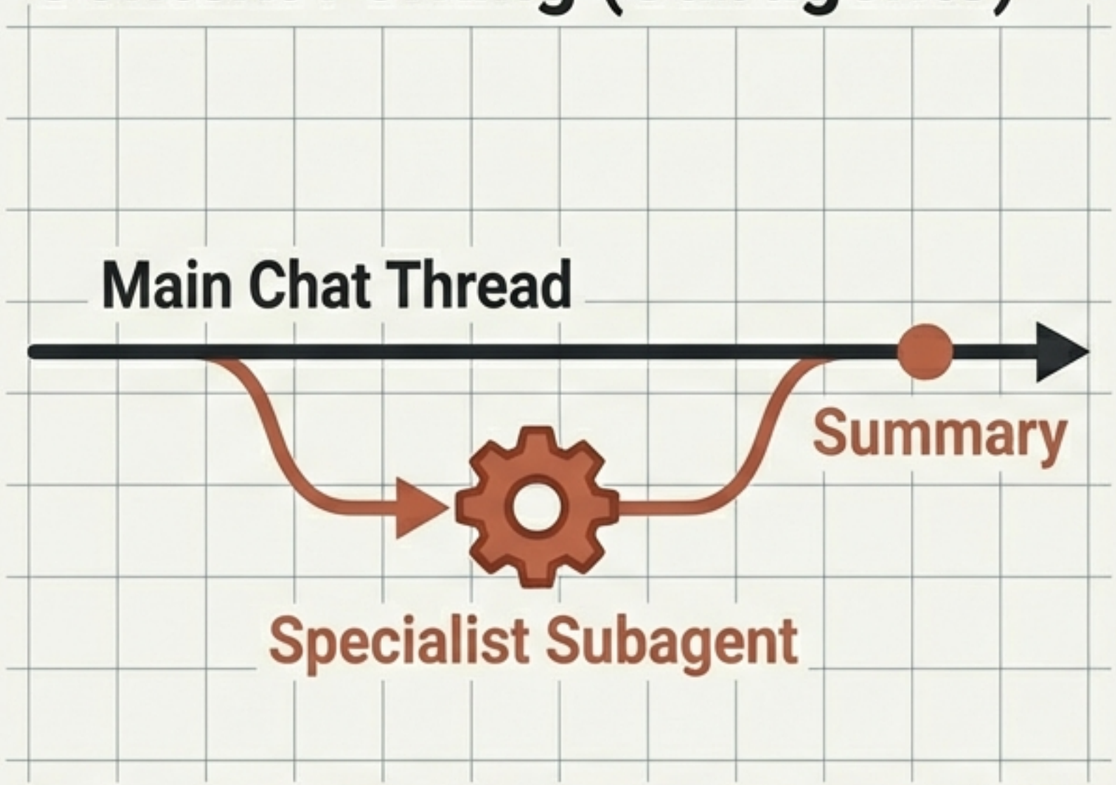
Explicit Steering

Request progress reports to prevent skipped steps.

> If a model fails twice, don't argue. **Clear the context and restart.**

The Future: Subagents and Interactive Apps

Context Forking (Subagents)



Delegating heavy research to parallel context windows.

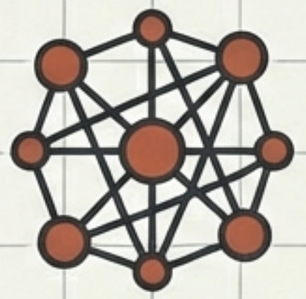
MCP Apps

Rendering live UIs (Asana, Figma) directly in the chat stream.

Summary: The Pillars of Agentic Architecture

Efficiency

Progressive disclosure enables repeatable workflows (Rakuten: 87.5% gain).



Connectivity

MCP connects AI to enterprise data; Skills provide the methodology.

Safety

Zero Trust architecture and sandboxing close the Consent Gap.

From Conversation to Orchestration.

Resource Library

Tools

- The Skill-Creator: Interactive meta-skill for bootstrapping.
- Anthropic Skills Marketplace (`GitHub: anthropics/skills`)
- Community Repos: `awesome-claude-skills`

Documentation

- Model Context Protocol (MCP) Specification
- Claude Security Center Guidelines

Scan for GitHub Repo

From Chatting to Doing.

We are no longer just prompting an LLM for an answer.
We are architecting agents to perform the work.

The future belongs to those who build the skills.