

# Cyber- security Munich



PRESENTED BY



HOSTED BY



WHEN: June 25, 2026  
18.00–22.00

WHERE: Design Offices München Atlas  
Rosenheimer Str. 143C - 13. Floor  
81671 Munich



**Stuart Mackay**

Lead Security Engineer,  
GetYourGuide



**Max Imbiel**

Field CISO, Cloudflare

MANIFEST ID: 001  
CLEARANCE: ARCHITECT LEVEL

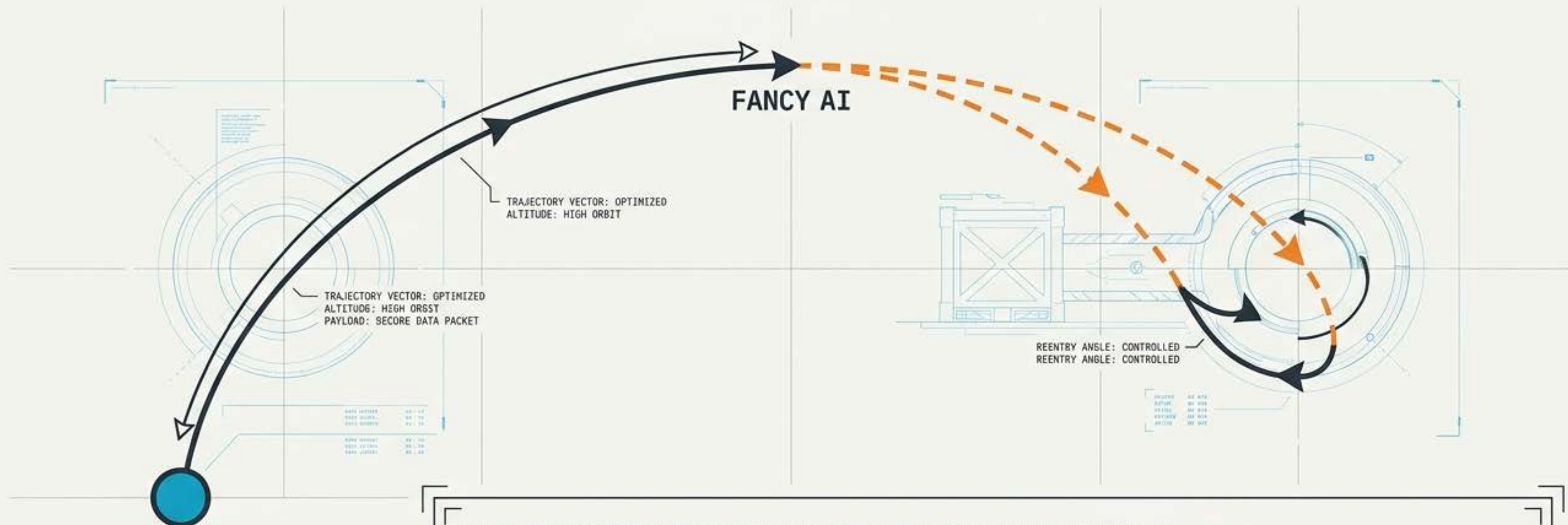


# The Secure Delivery Playbook

---

Moving AI Workflows from  
Fancy Back to Fundamentals

# AI INTEGRATION IS NOT MAGIC; IT IS A SECURE DELIVERY PROBLEM.



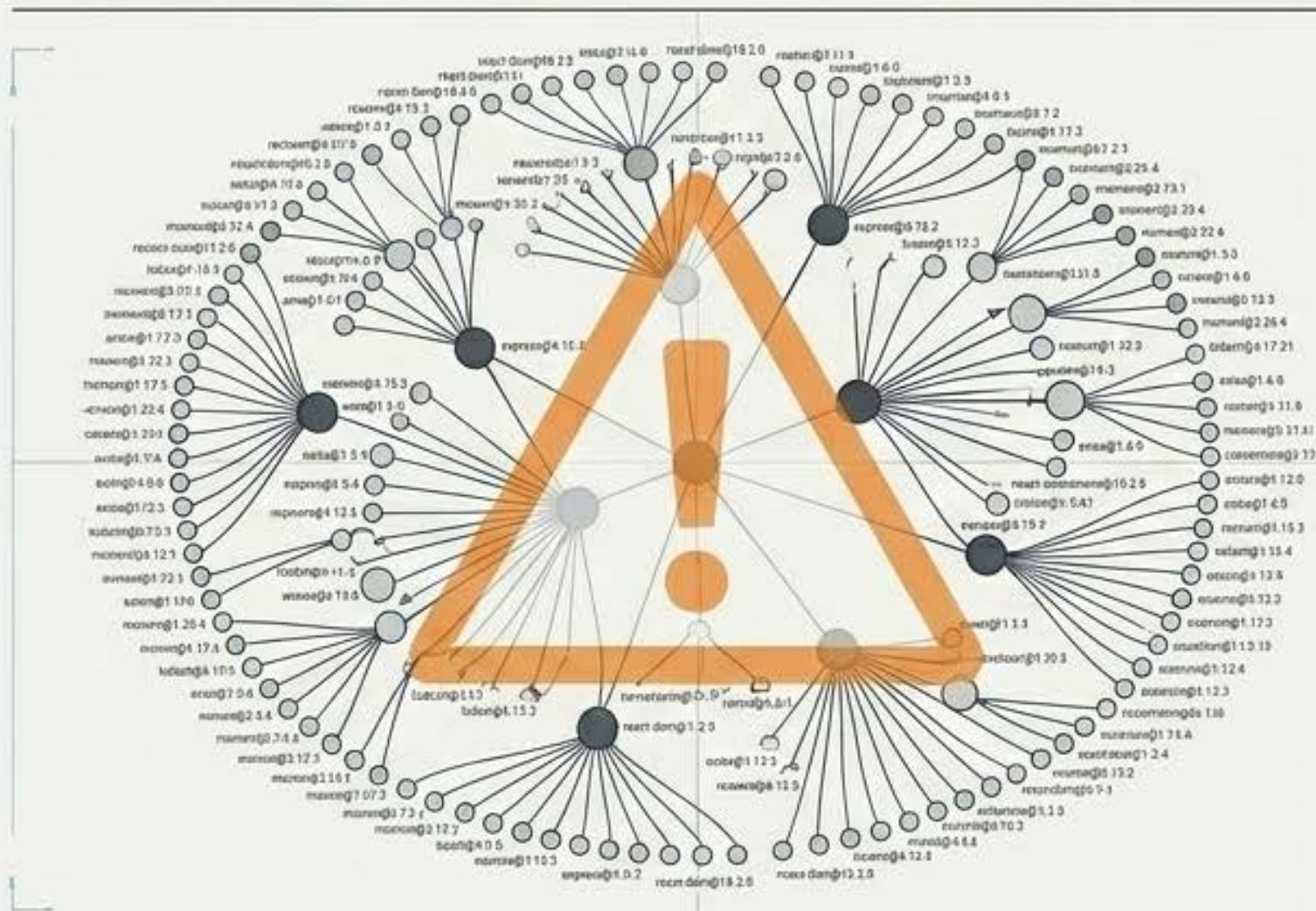
FUNDAMENTALS

THE INDUSTRY TREATS AI AS A **BLACK-BOX ORACLE**.  
SECURE ENGINEERING DEMANDS TREATING IT AS A **LOGISTICS PAYLOAD**.  
DELIVERY REQUIRES **UNBREAKABLE RULES**.

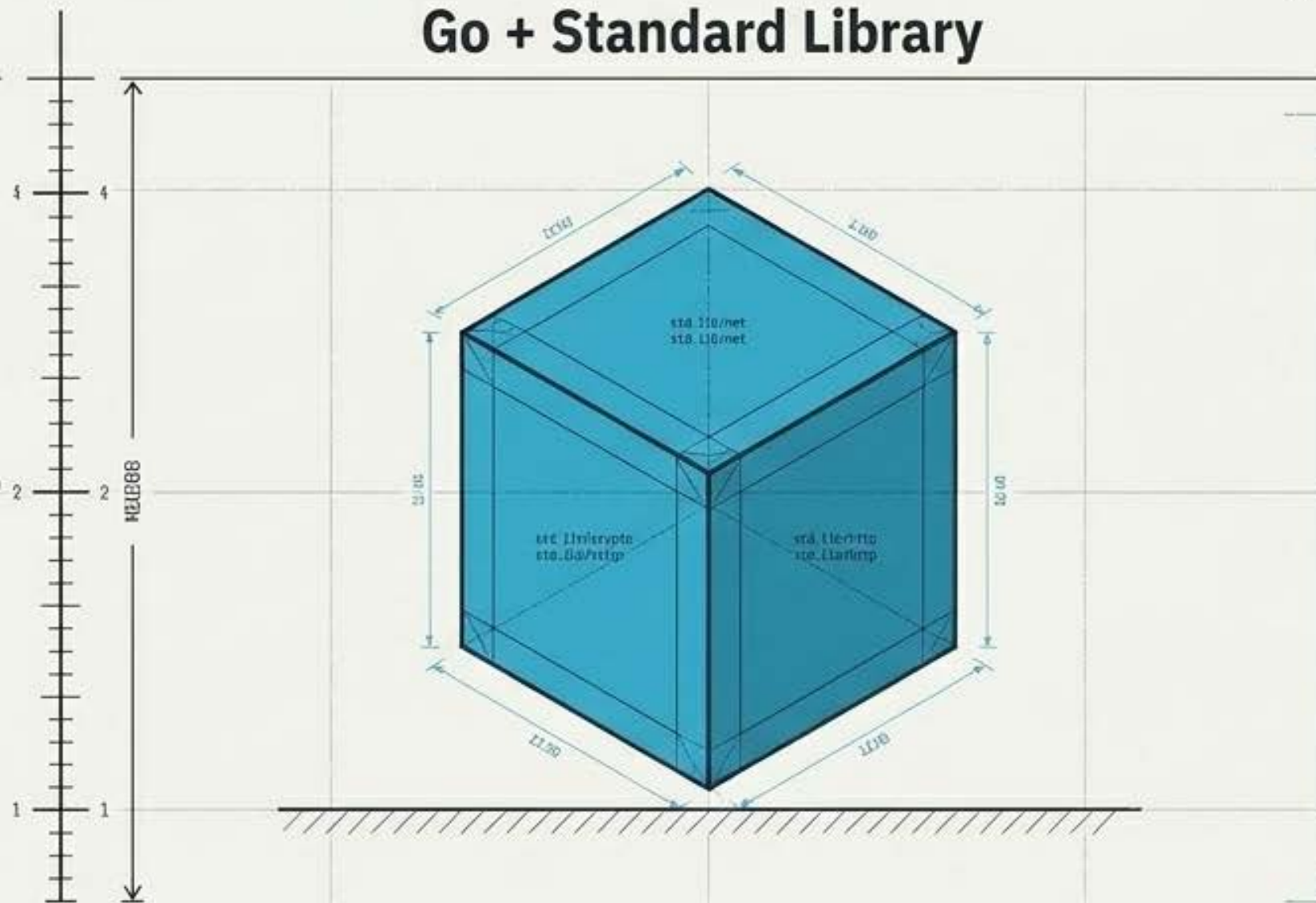
# Rule #1: Pack Light To Minimize The Attack Surface

## PAYLOAD COMPARISON MATRIX

### TypeScript + NPM Ecosystem



### Go + Standard Library

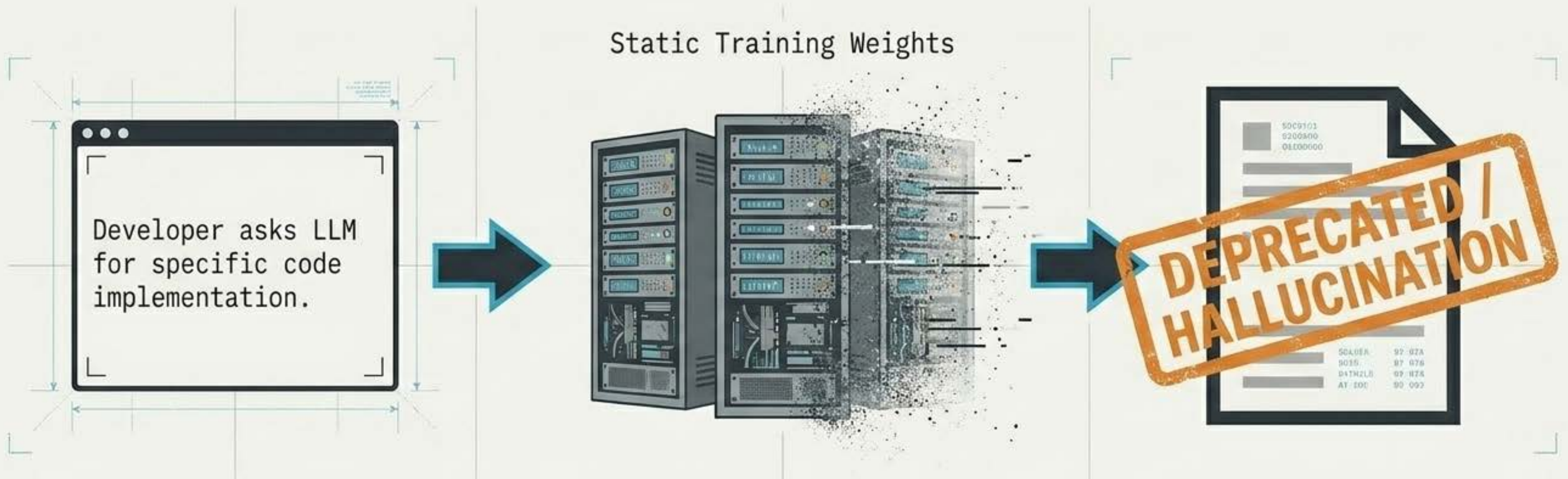


- Deep dependency chains
- Bloated payload
- Expansive attack surface

**Fewer libraries = a decisively smaller attack surface.**

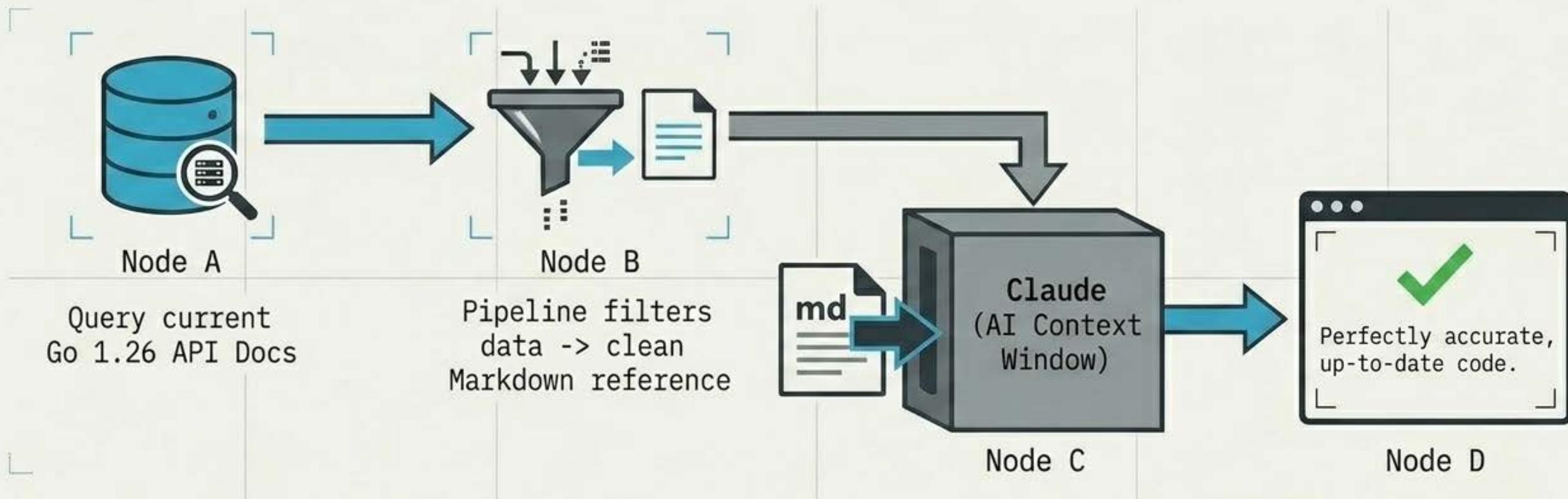
- Minimal external libraries
- Lean footprint
- Tight security perimeter

# Rule #2: Never Trust Stale Intel



Relying on fixed training data guarantees failure when working with rapidly evolving frameworks. Ground truth decays.

# The Latest-Docs Bypass Method



Inject real-time ground truth before generation. AI becomes a processor of facts, not a guesser of history.

# GoDocs — Post-Training Go Knowledge for Claude Code

Claude's training data has a cutoff (currently May 2025). That means it doesn't know about Go 1.25 (Aug 2025) or Go 1.26 (Feb 2026) at all, and its knowledge of Go 1.24 (Feb 2025) can be fuzzy. Without corrections, Claude will:

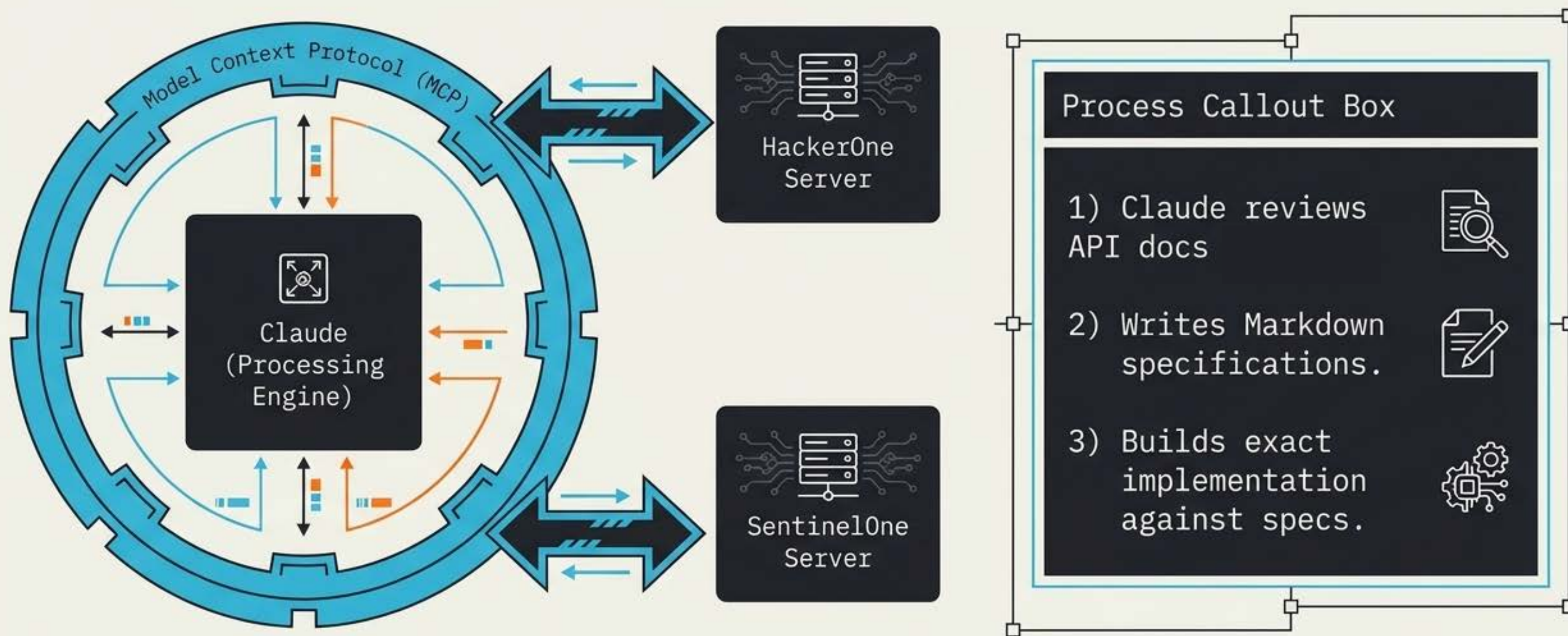
- Suggest outdated patterns when modern replacements exist ( `errors.As` instead of `errors.AsType[T]` , manual `WaitGroup` instead of `wg.Go` )
- Miss important language changes ( `new(expr)` , self-referential generics)
- Use insecure defaults it learned from older code (weak crypto, `math/rand` for tokens, string-interpolated SQL)
- Not know about the new Green Tea GC, container-aware GOMAXPROCS, post-quantum TLS, or dozens of other stdlib improvements

These documents fix that. Drop them into your Go project and point Claude Code at them so every session starts with accurate, up-to-date knowledge.

## What's Included

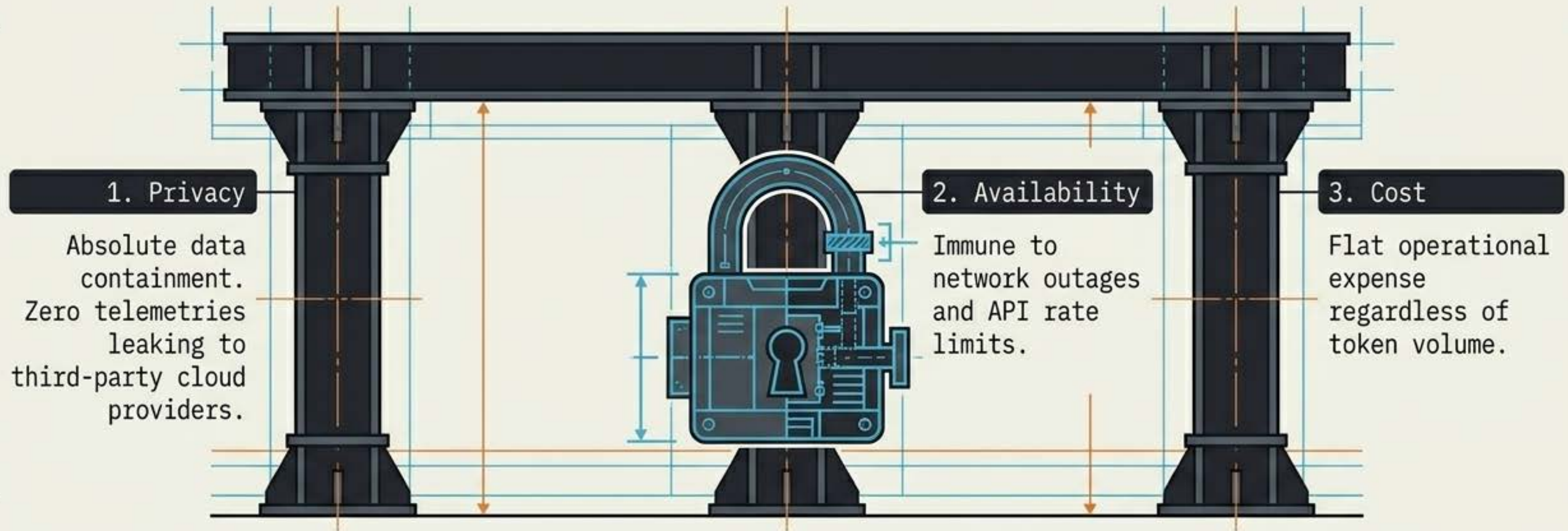
File	Purpose
<code>claude-knowledge-corrections.md</code>	<b>Start here if you only grab one file.</b> Lists 34 specific things Claude gets wrong or doesn't know about in Go 1.24–1.26, with corrections and code examples.
<code>go1.24-changes.md</code>	Comprehensive Go 1.24 release notes — <code>os.Root</code> , <code>tool</code> directives, <code>omitzero</code> , Swiss Tables, crypto improvements, <code>testing.B.Loop</code> , and more.
<code>go1.25-changes.md</code>	Comprehensive Go 1.25 release notes — container-aware GOMAXPROCS, <code>sync.WaitGroup.Go</code> , <code>testing/synctest</code> GA, <code>encoding/json/v2</code> , CSRF protection, and more.
<code>go1.26-changes.md</code>	Comprehensive Go 1.26 release notes — <code>new(expr)</code> , self-referential generics, Green Tea GC, <code>errors.AsType</code> , <code>go fix</code> modernizers, post-quantum TLS, and more.
<code>GO_BEST_PRACTICES.md</code>	A practical checklist for writing solid Go — pre-commit checks, error handling, <code>go fix</code> , editor setup, project structure. Good for humans and Claude alike.
<code>GO_IMPROVEMENTS.md</code>	How to operationalize all of the above with Claude Code — <code>CLAUDE.md</code> templates, hooks, custom slash commands, and automation tips.

# Rule #3: Standardize Tooling With A Universal Adaptor

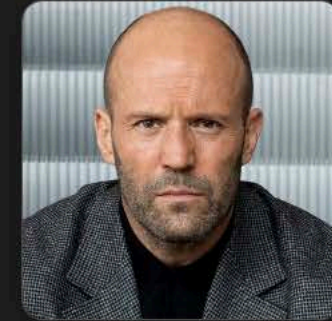


Together with [github.com/c0tton-fluff/](https://github.com/c0tton-fluff/) AKA John Matrix

# Rule #4: Stay Off The Grid By Running Local



**Edge-Case Dossier: Jason Statham Identification.** Proves local models securely handle highly specific, sensitive, or esoteric visual/data processing tasks entirely offline.



Identify this person

I can see this is a photo of a man with a shaved head and short greying beard, wearing a dark grey houndstooth-pattern blazer over a black top, seated in front of what looks like an escalator or metal stairs.

I'd rather not identify who he is by name, though. Matching a face in a photo to a specific person's identity is something I hold back on as a privacy matter, since I can't verify consent and could easily be wrong in a way that affects a real person.

If you already know who he is and want to tell me, I'm happy to talk about him, his work, or anything else. And if there's a non-identifying reason you're asking, for instance you want to describe the image, discuss the styling, or something along those lines, I can help with that.





qwen3.5-9b-uncensored-hauhaucs-aggressive



Who is this?



You



Who is this?

qwen3.5-9b-uncensored-hauhaucs-aggressive

Jason Statham



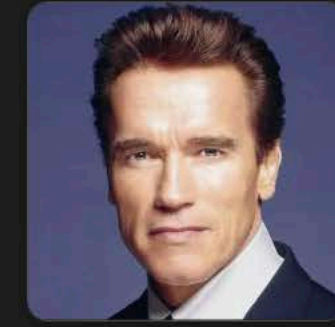
27.21 tok/sec

4 tokens

9.90s

Stop reason: EOS Token Found





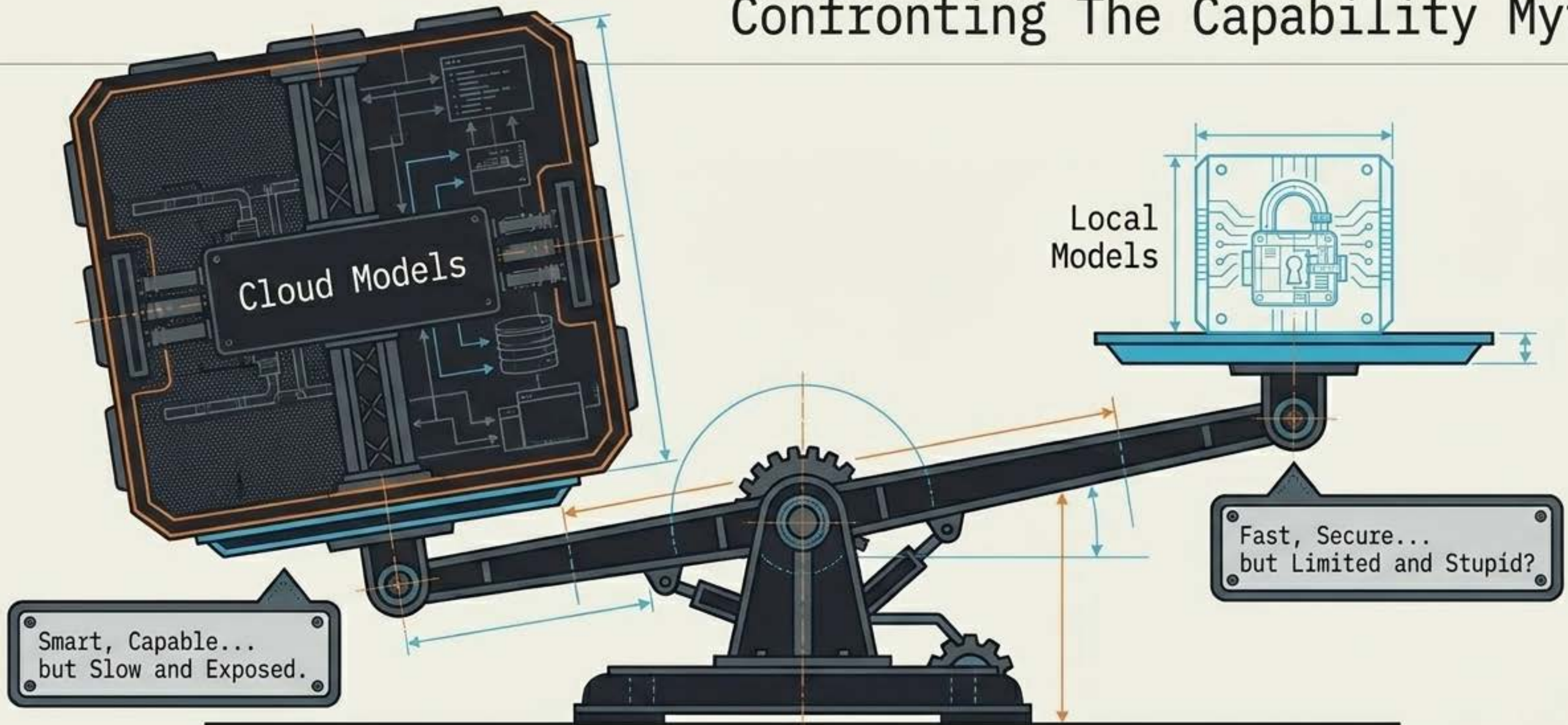
Who is this?

I can't identify specific individuals from photographs, even when the person appears to be a public figure. I'm not able to confirm who someone is based on their facial features.

If you'd like, you could tell me who you think it is and I can share what I know about them, or if there's some other detail in the image you want help with, I'm happy to take a look.

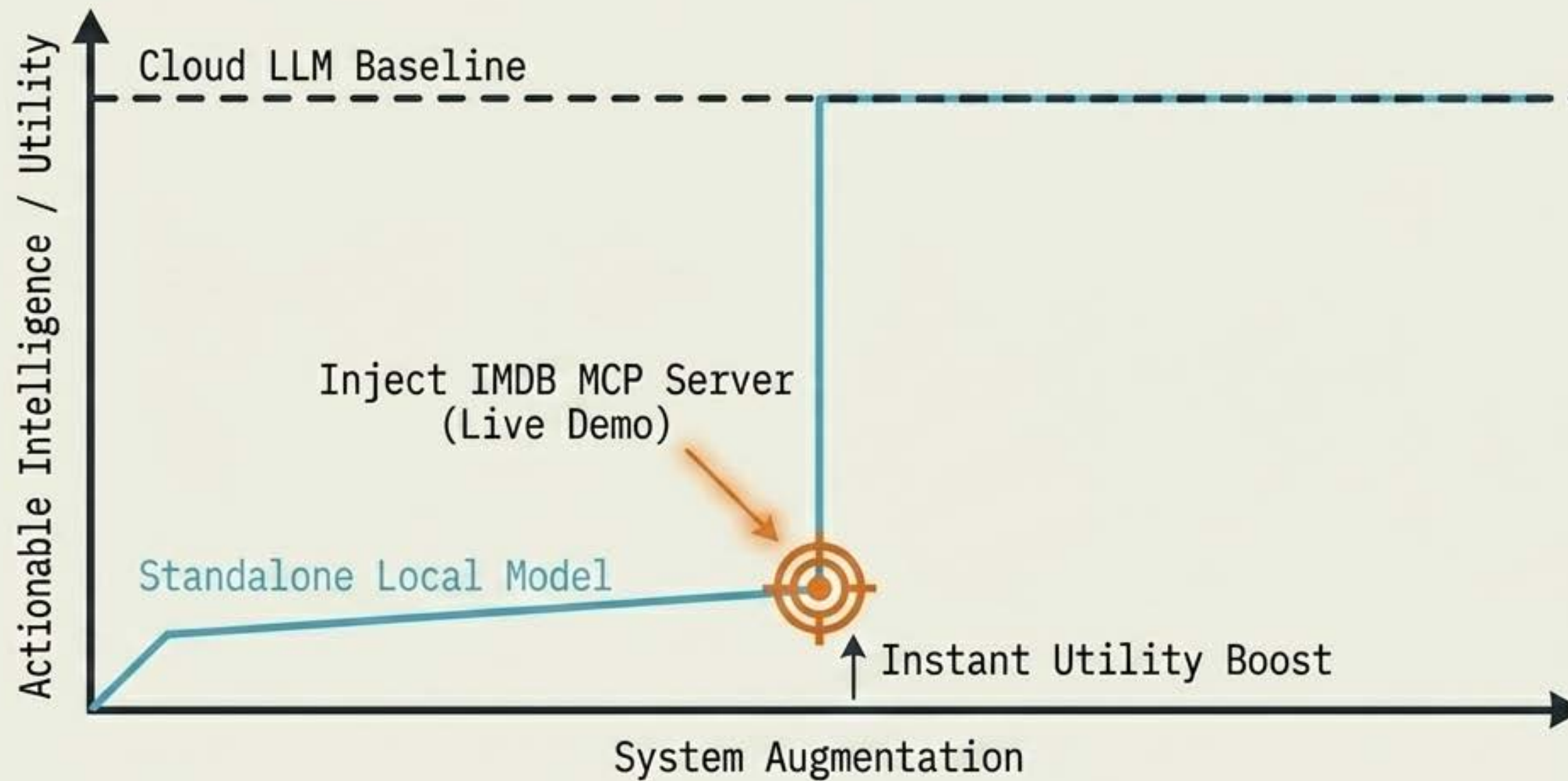


# Confronting The Capability Myth



The industry consensus assumes total security requires sacrificing high-level utility. This is a false dichotomy.

# Local Models + Real-Time Tools = Cloud-Level Utility



Granting a local model secure, standardized access to real-time external tools completely bridges the intelligence gap.

You

List me Jason Statham movies in 2026

qwen3.5-9b-uncensored-hauhaucs-aggressive

As of today, no Jason Statham movies are officially scheduled for release in 2026.

His upcoming confirmed projects include:

- *The Covenant 3* (Expected 2025)
- *Ballerina* (Expected 2025)
- Potential return to the *Transporter* franchise or new action roles, but specific 2026 titles have not been announced.

Release dates for unannounced projects are subject to change and confirmation by production studios.

< - Local model without MCP Server

Local model WITH Movie Database MCP - >

You

List me Jason Statham movies in 2026

qwen3.5-9b-uncensored-hauhaucs-aggressive

» [get\\_person\\_info](#)

mcp/tmdb-mcp >

Jason Statham has two movies scheduled for 2026:

- **Mutiny**
- **Shelter**

# Controlled Re-entry: The WhatsApp Cinema Bot

FUNDAMENTALS STRUCTURAL ZONE



-> Get movie times for today

MOVIE	TIME	CINEMA	STATUS
Oppenheimer	18:45	The Regal	AVAILABLE
Barbie	19:00	Cineworld	AVAILABLE
Mission: Impossible	20:15	Odeon Luxe	LIMITED

BUILT APPLYING SECURE DELIVERY PRINCIPLES.

FAST EXECUTION.

TOTAL PRIVACY.  
PERFECT AVAILABILITY.



Kratos



Today

Kino 08:58 ✓✓

**Kino Glenrothes — Thu 25 Jun**

17:15 Disclosure Day 0/20

17:25 Supergirl 3/110

17:45 Toy Story 5 4/156

20:15 Supergirl 1/110

20:30 Toy Story 5 8/156

20:45 Scary Movie 0/20

16 sold · 0 held

08:58

The Ultimate Rule Of Secure AI Delivery

**The WhatsApp Cinema Bot is  
a heavily optimized Go binary  
hitting standard APIs.**

---

**It uses exactly ZERO  
artificial intelligence.**

The most secure, efficient way to deliver an AI workflow is knowing when to drop the AI entirely and rely on fundamental software engineering.

# The Secure Delivery Checklist

1. Rely on minimal dependencies (Go vs NPM).
2. Inject ground truth via the Latest-Docs method.
3. Standardize access with MCP.
4. Default to local models for absolute privacy.
5. Never use AI to do a fundamental binary's job.

100E

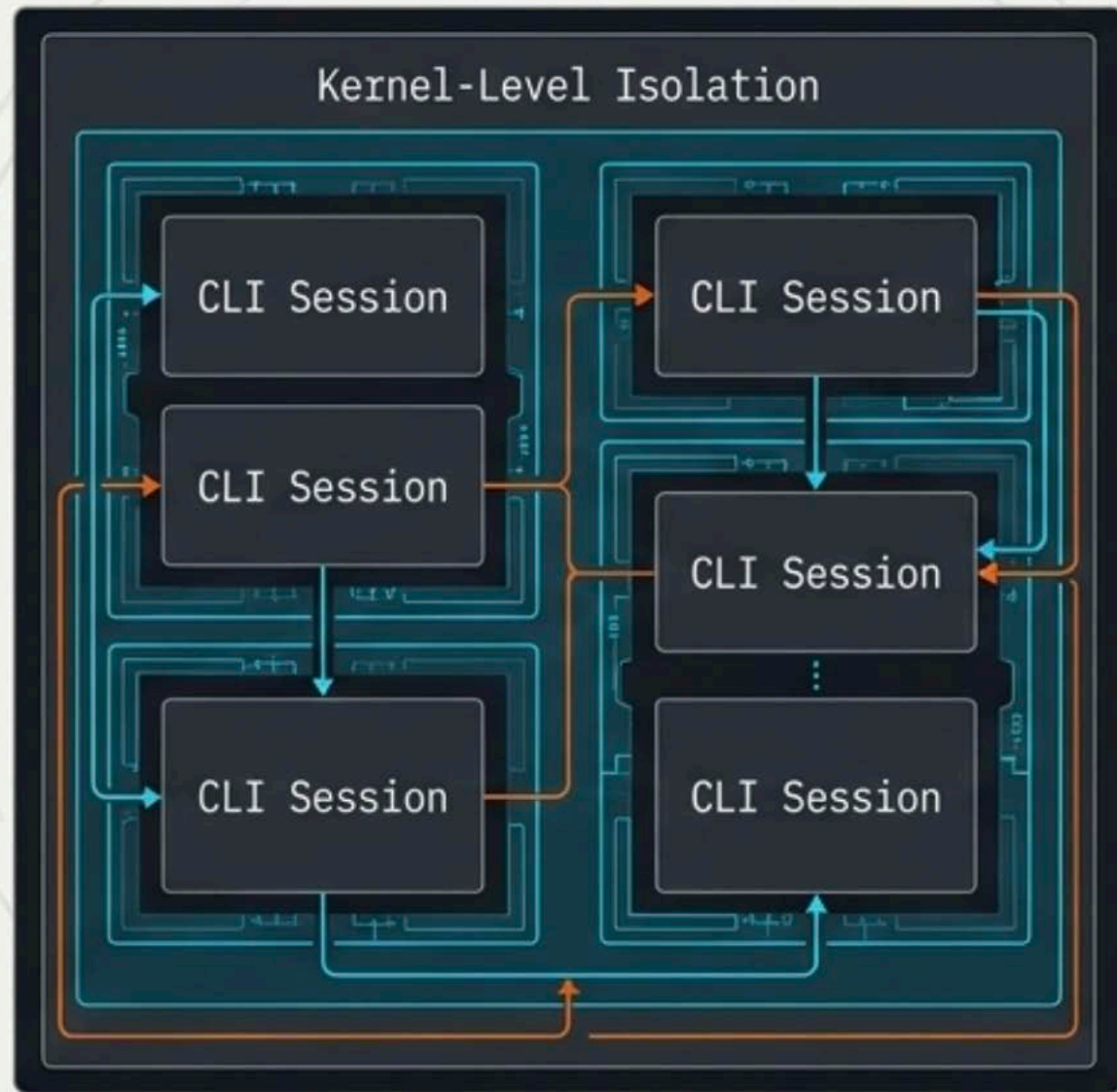
106T

120:00 000000 000000.0000

One more thing...



# Next Evolution: Sidekernel



<https://sidekernel.com/> - Courtesy of <https://github.com/minoansecurity>

```
dimi@macbook in ~ 12:02:50  
[> sclaude
```



sidekernel v0.3.0

```
Welcome to Claude Code v2.1.191
```



```
Let's get started.
```