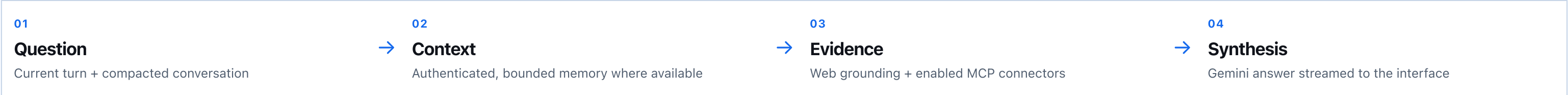


A grounded answer is a trace.

The answer is not the system. The answer is the final synthesis of bounded evidence, explicit tools, and a streaming execution path.



CONTROL SURFACES

A

Tool schemas are adapted per provider

Connector schemas are sanitized for the active Gemini provider before declaration.

B

Read and action tools are split

Read/search tools can be model-callable; action tools remain marked as requiring consent.

C

Execution is observable

Thought, route, connector, and result events are streamed as SSE for the client experience.

FAILURE MODES DESIGNED FOR

• Tool output is bounded; malformed schemas do not silently become usable tools.

• Workspace reads are containment-checked; hidden files, binaries, and secrets are blocked or redacted.

• Connector failures use timeouts, circuit breaking, and a graceful agentic-to-legacy fallback.

• Optional live tool discovery is deliberately off by default.

GROUNDING
RULE

Attach only relevant, bounded context. A large private memory dump is neither better retrieval nor a privacy win.

