ONE FRONT DOOR

One door for every model and tool.

Agents ask at the gate. People set the rules once and decide the risky steps.

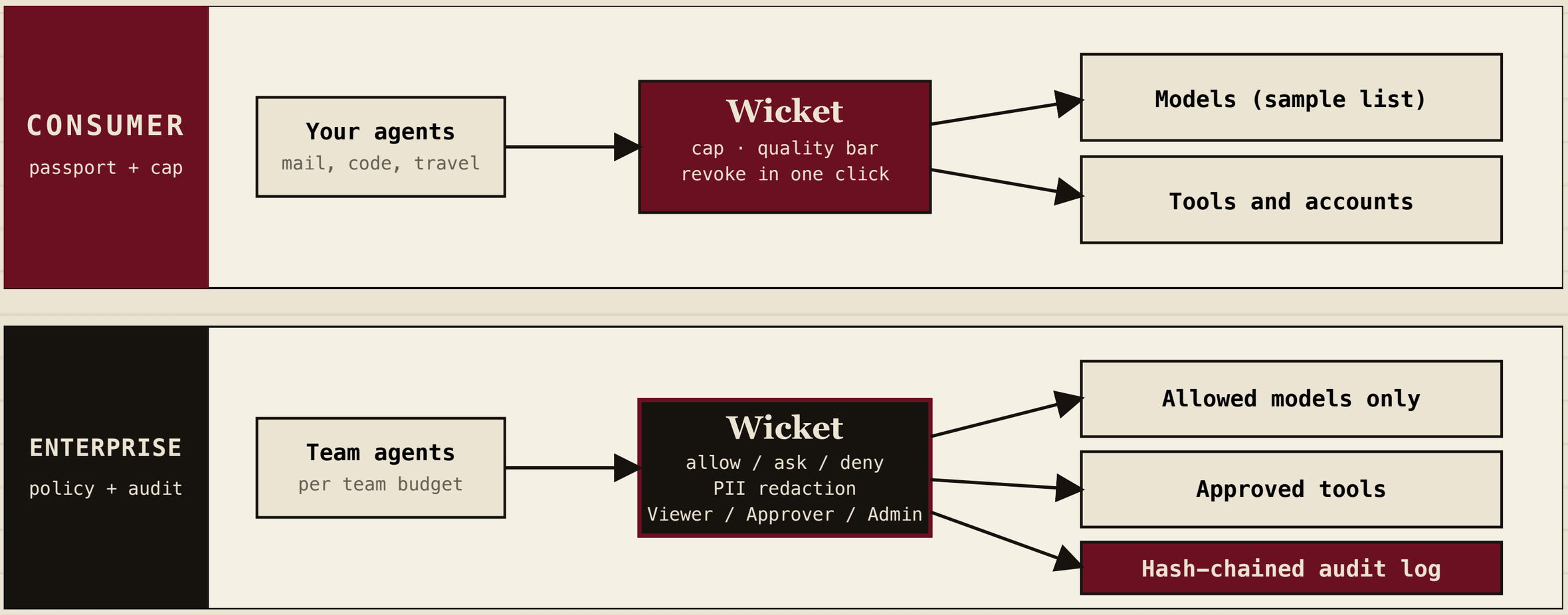
THE PROBLEM

Agents act. Nobody keeps the ledger.

1. Each agent holds its own keys and its own bill.
2. No one sees which agent touched what.
3. Risky steps run without a named person.
4. Revoking an agent means hunting through accounts.

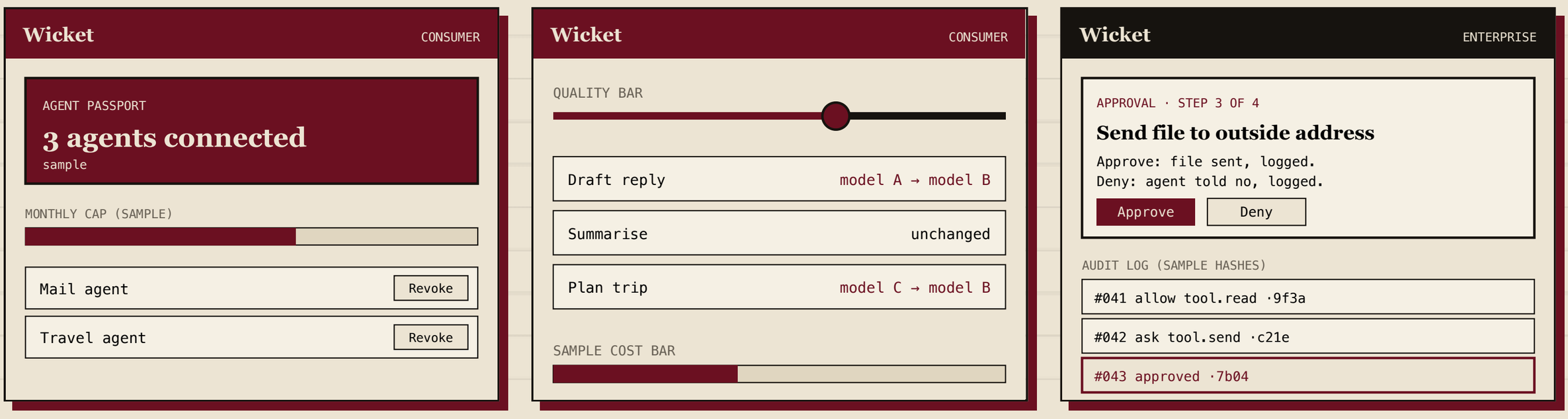
FLOW

Agents, then Wicket, then models and tools



KEY SCREENS · SAMPLE DATA

Three moments, drawn from the prototype



1. Passport and cap
2. Quality bar reroutes
3. Approve, then audit

RULES

Eight rules the gate keeps

01 An agent holds no model keys. Wicket does.

02 Every request meets a cap before it runs.

03 The quality bar picks the cheapest model that passes.

04 Revoking an agent blocks its next call.

05 Risky actions wait for a named approver.

06 The agent says what Approve and Deny will do.

07 PII is redacted before a model sees it.

08 Each decision joins a hash-chained log.