HOOP AI ACCELERATION

Scale AI with consistency. Give autonomy with responsibility.

Engineers want to ship with agents. Security needs auditors happy. Data will not hand over a service account that sees more than the user behind it. Hoop is the access plane that resolves all three.

~5 ms	Wire-protocol enforcement overhead per query
3 ×	Layers working as one: identity, governance, agent UX
4 wks	Kickoff to agents querying production with attribution
0	New service accounts. No broader access than the user has.

CHAPTER 01 · IN CUSTOMER WORDS

Four real lines from customer calls in the last two months. Different industries, same worries.

> How do we secure agents so they only see what the user behind them is allowed to see.

SENIOR MANAGER, DATA · FINTECH

> Service accounts have broader access. We are dealing with financial data.

SENIOR MANAGER, DATA · FINTECH

> If two engineers share a session and only one has access, how do you keep the other one out.

LEAD PLATFORM ENGINEER · PAYMENTS

> Alert when someone pulls a thousand PII rows, even if it was an agent.

MANAGER, SECURITY ENGINEERING · PAYMENTS

CHAPTER 02 · THREE ALTITUDES, ONE ACCESS PLANE

The pain shows up in three different rooms. Hoop answers all three from a single substrate. Controls compound instead of fragmenting.

ALTITUDE 01

Operational

Engineers using coding and analytics agents day to day.

> Personal tokens hardcoded into a deployed app.

Identity, federated

OAuth against your IdP. Short-lived JWT carries the named user through every query, approval, and audit log. No personal tokens hardcoded.

> A coworker resumes the agent session and sees data they shouldn't.

Sessions belong to people

When a different user re-prompts, Hoop refuses until they re-authenticate. Their group claims drive what they can see.

ALTITUDE 02

Tactical

Data, Security Engineering, and Platform leads.

Alert when someone pulls a thousand PII rows. Human or agent.

One alarm, two actors

Wire-level masking, output guardrails on sensitive tables, webhooks to your channel. The alert names the human behind the agent.

KPIs leaking through agent prompt instructions.

Guardrails in the gateway

Column-level masking plus AI session analysis. Rules live in Hoop and apply to every agent the org adopts next.

Audit underway. Anything new has to fit the existing model.

AI inherits the trail

Every agent session recorded end to end. The same audit trail your team already accepts for human access.

Approvals kill agent flows. The agent gives up, the user re-prompts.

Agent waits, human approves, query resumes

Approvals return a structured envelope. The reviewer approves in Slack. The agent resumes the original query. Full attribution.

ALTITUDE 03

Strategic

Executive sponsors of AI adoption.

Compliance demand grows with each new use case. Adding controls per use case will not scale.

A substrate, not point fixes

Every new connection, agent, or business team onboards through the same identity, masking, approval, and audit infrastructure. Each new use case lowers per-use-case risk.

Connect what engineers ship in source code with how the business is actually performing.

The post-mortem that writes itself

Agent reads the incident, queries production, pulls revenue impact, hits an approval gate. Writes the post-mortem with masked PII and full audit attached.

CHAPTER 03 · FROM AGENT PROMPT TO GOVERNED QUERY

Four beats. The same path a human takes through Hoop, taken by the agent, with that human's identity carrying every step.

01 · IDENTIFY

Federated sign-in

Agent gets 401 plus discovery. Client runs OAuth 2.1 + PKCE against your IdP. JWT returns with sub, email, group claims.

02 · AUTHORIZE

RBAC by group claim

Hoop validates the JWT and checks group membership. Agent sees only the connections this user can access. JWT never reaches the backend.

03 · ENFORCE

Wire-level controls

Masking redacts PII. Guardrails block dangerous patterns. AI session analysis flags intent. JIT approvals route to Slack.

04 · AUDIT

End-to-end recording

Queries, masks, guardrails, approvals all recorded against the named user. Replayable in Hoop. Exportable for compliance.

CHAPTER 04 · FOUR WORKSTREAMS, ONE PLANE

Same controls carry every agent next.

01 · OPERATIONAL

Incident post-mortems end to end

Reads the incident, queries production, pulls revenue, hits approval, writes the post-mortem with masked PII.

02 · TACTICAL

Coding agents on the warehouse

The connection security has been blocking. Agent reads with the engineer's permissions. Financial KPIs masked.

03 · OPERATIONAL

Internal AI-built apps, governed

Vibe-coded internal tools connect through Hoop. Same masking, approvals, audit. Security stays one story.

04 · STRATEGIC

Business agents, safely

Finance, ops, exec teams on AI assistants. Group claims keep finance away from product. PII masked everywhere.

CHAPTER 05 · PILOT

A working pilot, in four weeks.

One database. One agent platform federated through your IdP. One incident replay. Aligned to your audit timeline.

WK 01	**Federation enabled**	MCP trusts your IdP. Agents pre-registered. JWT and group claim format validated with security.
WK 02	**First connection**	One database onboarded. PII masking. One approval rule. First attributed query on a replica.
WK 03	**End-to-end pilot**	Real workflow reproduced through Hoop. Masking, guardrails, and approvals tuned to what the agent tries.
WK 04	**Expand**	Second connection. Second agent. Second team. Compliance compounds.