Securing every identity in an agentic stack.

How a Layer 7 proxy changes the risk profile of AI-driven infrastructure — and why it matters for compliance, governance, and engineering velocity.

01 **Data masking**

02 **Guardrails**

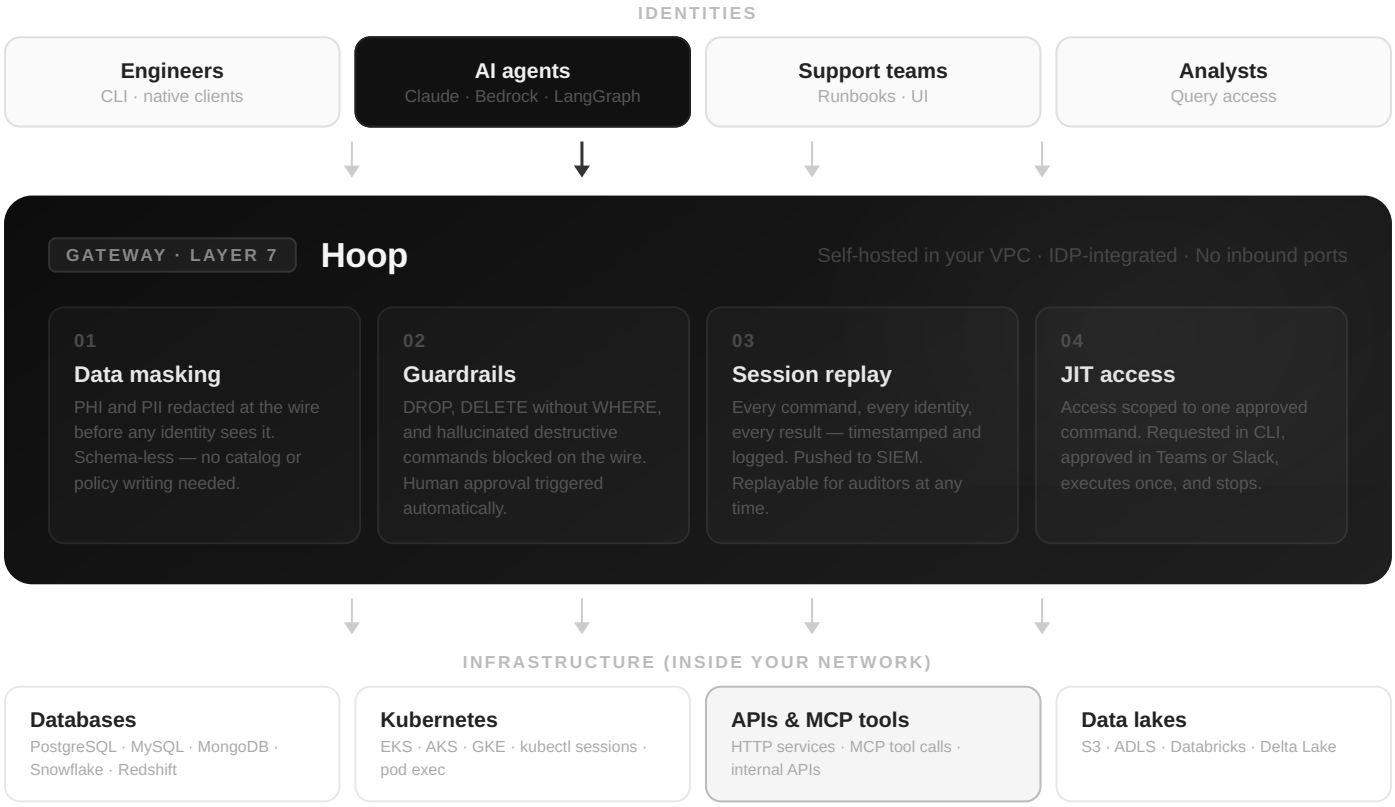
03 **Session replay**

04 **JIT access**

ARCHITECTURE

Where Hoop sits in the stack

Every identity — engineer, AI agent, support team, or analyst — passes through Hoop before reaching any resource. Because the proxy operates at Layer 7, it sees inside every connection and acts on it in real time.



No data leaves your VPC · Engineers use existing CLI and native clients · No agent install required

SIEM push supported · SOC 2 Type II

CAPABILITIES

Four capabilities, one control plane

Because every connection passes through the gateway at the wire level, the same enforcement applies to every identity — human and machine — without changing how engineers work or how agents connect.

01

Live data masking — schema-less

PHI, PII, and sensitive fields are redacted in the query result before they reach any terminal, notebook, or model context. Hoop operates at the wire, so it requires no advance knowledge of your schema. It inspects the output in transit and redacts matching patterns regardless of how the query was written or what the database permissions say. Engineers and agents get the information they need — they never see what they should not see.

02

Guardrails — commands blocked before execution

DROP TABLE, DELETE without WHERE, and mass updates are intercepted and blocked before they reach the target system. If an AI agent hallucinates a destructive operation, it is stopped at the gateway and a human approval request is generated automatically. The agent does not stall waiting for manual intervention — it surfaces the request, the human approves or rejects in one click, and execution continues or stops.

03

Session replay — full command-level audit trail

Every action through the gateway is recorded at the wire level: the exact command or query, the identity that ran it, the resource it targeted, the result returned, and the timestamp. This is not an application log — it is a recording of what actually happened inside the session. When an auditor asks what engineers or agents did in production last quarter, the answer is a search query, not a reconstruction effort. Events push to your SIEM automatically.

04

Just-in-time access — least privilege at command level

Instead of broad time-bound access to production systems, Hoop scopes access to a single approved command. The engineer or agent requests what they need from their existing CLI. The request surfaces in Teams or Slack with a one-click approve or reject. Once approved, that specific action executes once, and nothing else runs. No standing permissions, no forgotten credentials, no shared accounts appearing in an audit months later.

One policy engine for humans and agents

AI agents inherit the identity of the human who authenticated them. If Maria starts an agent session, the agent can only access what Maria is permitted to access, and every action is logged against her identity. You do not write new IAM policies per agent — which becomes unmanageable at scale for a fleet of dozens or hundreds of services.

IDENTITY FEDERATION

OAuth 2.0 · SPIFFE

Standards-based agent identity. Supports agent-to-agent communication with scoped credentials and no shared secrets.

MCP GATEWAY

Tool calls governed

Every MCP tool call passes through Hoop. Same masking, guardrails, and session replay as any database connection.

PERMISSION INHERITANCE

No new IAM policies

Agents inherit human permissions automatically. RBAC roles from your IDP carry over with no duplication or per-agent setup.

DEPLOYMENT

Self-hosted in your VPC. Running in under an hour.

Hoop runs entirely within your own infrastructure. Your data never leaves your network. The gateway deploys as a container in your existing Kubernetes cluster and requires no inbound firewall rules.

STEP 01

Deploy the gateway

The gateway runs as a pod in your Kubernetes cluster. One command to deploy via Helm or Docker Compose. PostgreSQL stores sessions and audit data — you bring your own managed instance.

STEP 02

Connect your IDP

Hoop integrates with Okta, Azure Entra ID, Google, Auth0, and any OIDC-compliant provider. Existing RBAC roles and group memberships carry over automatically.

STEP 03

Register resources

Point Hoop at your databases, Kubernetes clusters, SSH hosts, and internal APIs. A lightweight agent establishes outbound connections only — no inbound ports required on any resource.

No agent install. No VPN. No new UI.

Engineers connect through their existing CLI — psql, mysql, kubectl, or any native client. The connection string points at Hoop instead of the resource directly. From the engineer's perspective, nothing changes. From the security team's perspective, every session is governed, logged, and auditable.

COMPLIANCE

Evidence generated continuously

Hoop generates audit evidence automatically from every session. No manual assembly before audits.

Framework	Controls	What Hoop generates
HIPAA	164.312(b) 164.312(d) PHI masking	Session-level audit trail with PHI redacted. Cross-border access logs for distributed teams.
PCI DSS 4.0	Req 3 Req 7 Req 8 Req 10	Command-level session logs. Least-privilege access enforcement. Cardholder data masked in transit.
SOC 2	CC6 CC7 CC8	Continuous immutable access log. JIT approval records. Anomalous activity pushed to SIEM.
GDPR	Art. 25 Art. 30 Art. 32	PII redaction by default. Processing activity records. Cross-border data access audit trail.
NIST 800-53	AC-2 AC-17 AU-2 AU-12	Account management controls. Remote access audit logs. Auditable events at the command level.

Request a technical walkthrough hoop.dev / hoop.dev/meet