hoop.dev

Audit Readiness Embedded in Everyday Access

Invisible Security for developers.
Command-line Control for Admins.
Built-in Oversight for Security.

Compliance with Full Clarity

GDPR
SOC 2
ISO 27001
HIPAA
PCI DSS
FedRAMP

Make Audits Easy for Any Standard

GDPR

Personal data is masked, tracked, encrypted, and monitored with full auditability and documented risk management

(Article 25)(Article 30)(Article 32)(Article 35)

PCI DSS

Cardholder-data environments are restricted, strongly authenticated, encrypted, logged, and regularly reviewed.

(Req. 7)(Req. 8)(Req. 10)(Req. 3)(Req. 4)(Req. 12)(Req. 1/2)

SOC 2

Access is least-privileged, authenticated, monitored, and auditable with disciplined change control and incident response.

(CC6)(CC7)(CC8)

FedRAMP

Cloud system access follows NIST 800-53 controls with least privilege, strong authentication, logging, and continuous monitoring.

NIST SP 800-53 families: (AC)(IA)(AU)(CM)(SC)(IR)(RA)(CA)

HIPAA

ePHI access is restricted, authenticated, encrypted, and logged, backed by administrative policies and documentation.

(§164.308)(§164.312)(§164.316)

ISO 27001

Access is governed by policy, least privilege, logging, cryptography, and continuous risk management within an ISMS

(Access control)(Operations security)(Communications security)(Cryptography)

Maintain Compliance with Shadow AI or NHIs

Make Sensitive Data Invisible

Masked Data is Invisible to Agents and to Developers who try to Copy and Paste it into LLMs

Block Dangerous Commands

Block risky write actions using customizable guardrails, and fine grained command approvals.

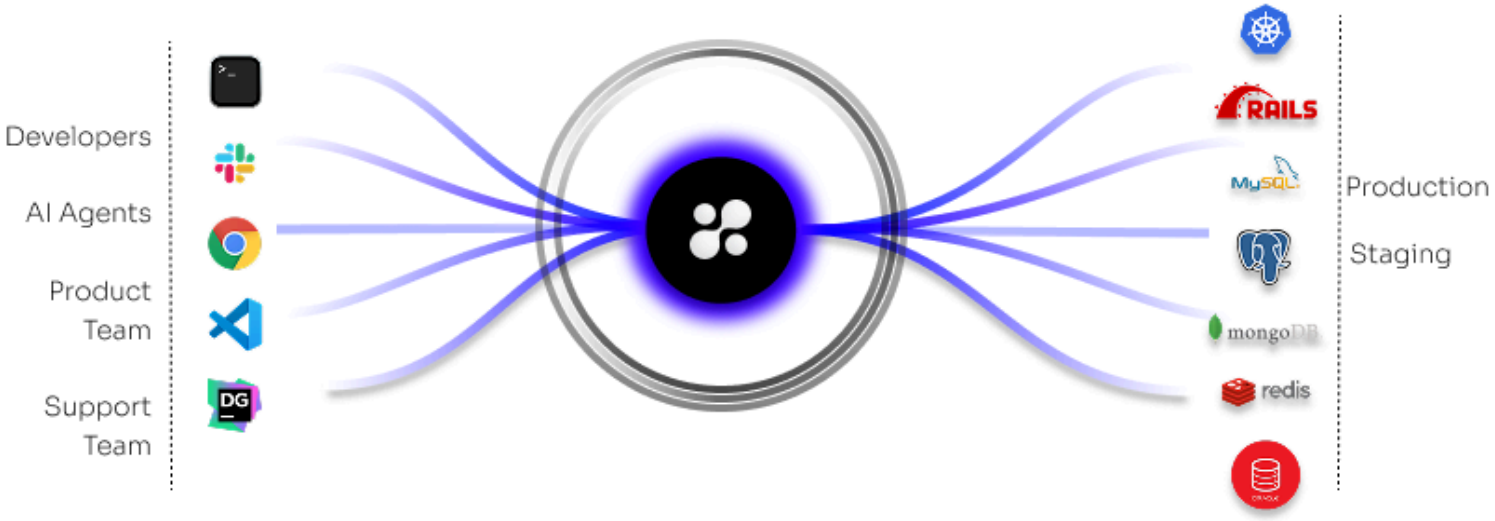
Record Every Action

Every action taken. by an agent is, filtered for quality and danger, routed for approvals and logged and recored.

No Standing Privileges

Every access session is time bound and privileges are revoked immediately after execution

Hoop.Dev Makes You Compliant by Design



1. **Eliminate Data Leaks** with dynamic masking that makes PII/PCI/PHI Invisible to Developers and Agents.
2. **Filter Out Dangerous Actions** with custom guardrails that constantly monitor for and block dangerous actions, risky queries, or suspicious read requests.
3. **Control Every Action** taken after a session begins. Privileges are reduced to their most granular form, a single query, and approved to execute only after they're written, ending the risk of over-permissioned accounts
4. **Record Everything** done by an agent, developer, or admin. As soon as a session begins, hoop.dev begins compiling evidence that is compliance ready
5. **End Standing Privileges** by making every access time bound to a JWT token, mapped to the role of the user.

Databases

Application Runtimes

Infrastructure & Orchestration

Cloud Services

Data Warehouses

Secrets Managers

ChatOps & Ticketing

IdP