

Sensitive data reaches AI before most policies do.

Ledgerproof places one customer-owned policy boundary before an approved model, then turns every decision into evidence the customer can verify.

01

See

Map workflows, destinations, and sensitive data classes.

02

Control

Apply readable allow, redact, or block rules before forwarding.

03

Prove

Verify the chain and deliver an operating Evidence Pack.

NOT JUST SOCIAL SECURITY NUMBERS

The policy follows the workflow.

Accounting

Names, SSNs, EINs, bank and routing details, contact data, and client-identifying financial figures.

Healthcare pilot

Names, dates, MRNs, NPIs, plan IDs, contact and network data, devices, licences, vehicles, and biometric references.

Banking pilot

Customer and payment data, transaction samples, network and device details, and confidential control evidence.

A VISIBLE RESULT ON DAY ONE

```
raw> patient Elena Marquez | MRN 4471902 | health plan HPN-882-144-90
policy> patient_name=REDACT | mrn=BLOCK | health_plan_id=BLOCK
result> NOTHING FORWARDED | event chained | policy version recorded
```

ONE NARROW PATH TO FIRST PROOF

Start small. Show value. Expand only after proof.

No per-seat SaaS. The customer owns the gateway, policy, log, configuration, and every Evidence Pack.

START HERE - \$2,500

Control Sprint

Exposure map, sector policy draft, synthetic acceptance corpus, before-and-after proof, sample Evidence Pack, and next actions.

15 DAYS - \$6,500

Governed AI Install

One environment, one approved backend, tested policy, three-to-five pilot users, runbook, and first verified pack.

QUARTERLY - \$750

Evidence Assurance

Monthly chain check, quarterly pack, exception summary, guidance bulletin, and one owner review. Keep every artifact.

THE 15-DAY OPERATING SEQUENCE

01

Map

workflow and exposure

02

Decide

policy and owners

03

Test

synthetic acceptance

04

Deploy

small pilot cohort

05

Prove

verify and hand off

THE HONEST BOUNDARY

Ledgerproof governs the approved path. It does not pretend to see every path.

It complements identity, endpoint DLP, browser controls, vendor governance, incident response, and legal analysis. Healthcare masking is not by itself a de-identification determination. Bank-wide deployment requires institutional security and third-party review.

**Bring a sample workflow.
Never bring client, patient, or customer data.**

Request a 15-minute proof walkthrough | bo.umair@gmail.com