

S A F E B O T S P R E S E N T S

The **Missing Trust Layer** for AI.

One secure, decentralized environment for all.

The full architecture, in plain English. Each section explains a problem with how AI works today, then shows how the Safebots stack solves it.

More Resources for Investors

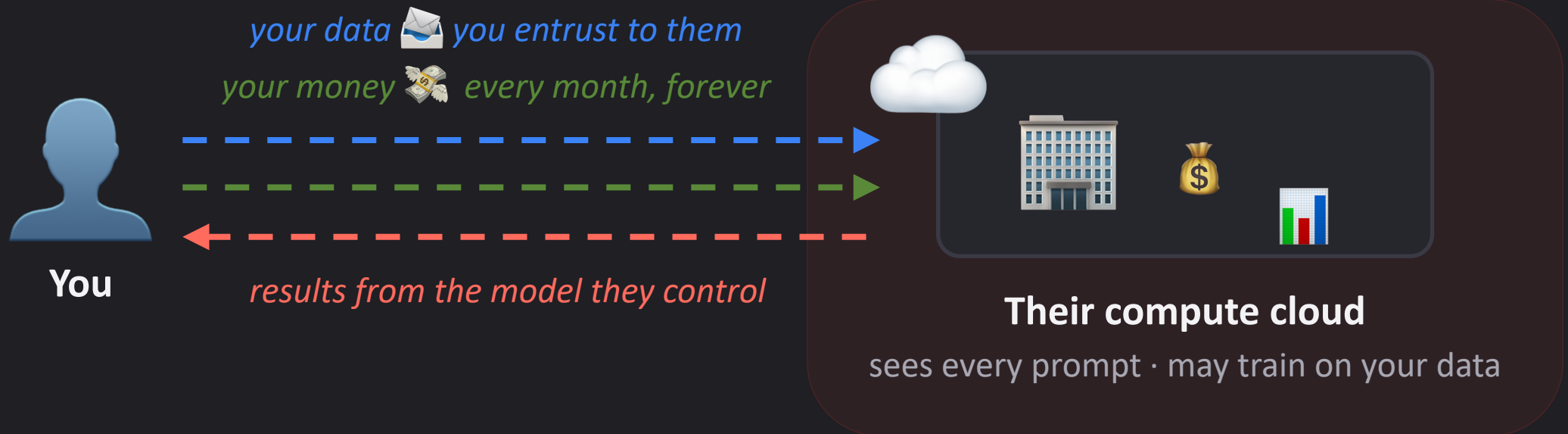
Understand the Whole Stack

Compare to AI Agents Today

Your data goes there. Their answer comes back.

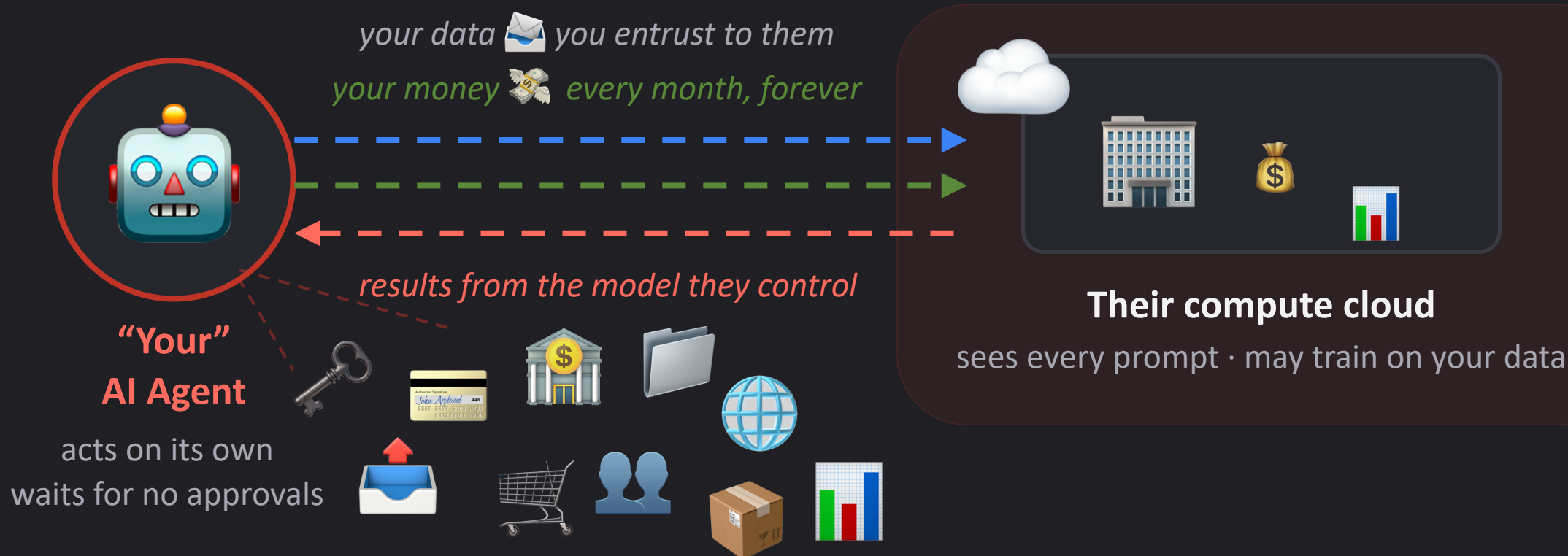
Their bill goes to you. They can change the model anytime.

When you use ChatGPT, Claude, or Gemini, every word you type leaves your computer, lands in a data center owned by a giant company. They charge you per word, forever. And they can always change what happens on their end.



Now imagine replacing people with AI agents designed to do whatever the models say, without asking you first.

An AI agent does things on its own. Sends emails. Moves money. Deletes files. Orders from suppliers. It's scary enough for personal agents, but how can a regulated business transition to using AI?



One sealed environment, standardized for everyone.

Every action policy-governed and cryptographically signed.

Safebox contains three layers, each providing the security necessary to enable the layers above.

No one gets special access, not even the host of the Safebox. Everyone goes through the same API and follows the rules.

Top



Safebots — Agents & Apps

Chat · collaboration · automation · business workflows



Mid



Safebox — Governance & Execution

Every action goes through M-of-N approval
Tools propose · admins sign off · then actions are executed.



M-of-N signatures

Base



Infrastructure — Sealed Compute

Hardware-attested boot · cannot be tampered with — even by the host

The cost of AI today is **staggering** — and growing. Your costs will go up as **their subsidies will run out.**

Every team has a stack of AI subscriptions. Each charges per word, per request, per seat, per month.
A heavy AI user easily spends \$5,000 a year before building anything.



Claude Code Max

\$200/mo



ChatGPT Pro

\$200/mo



Cursor

\$20/mo



Gemini Advanced

\$20/mo



\$5,280

per person per year

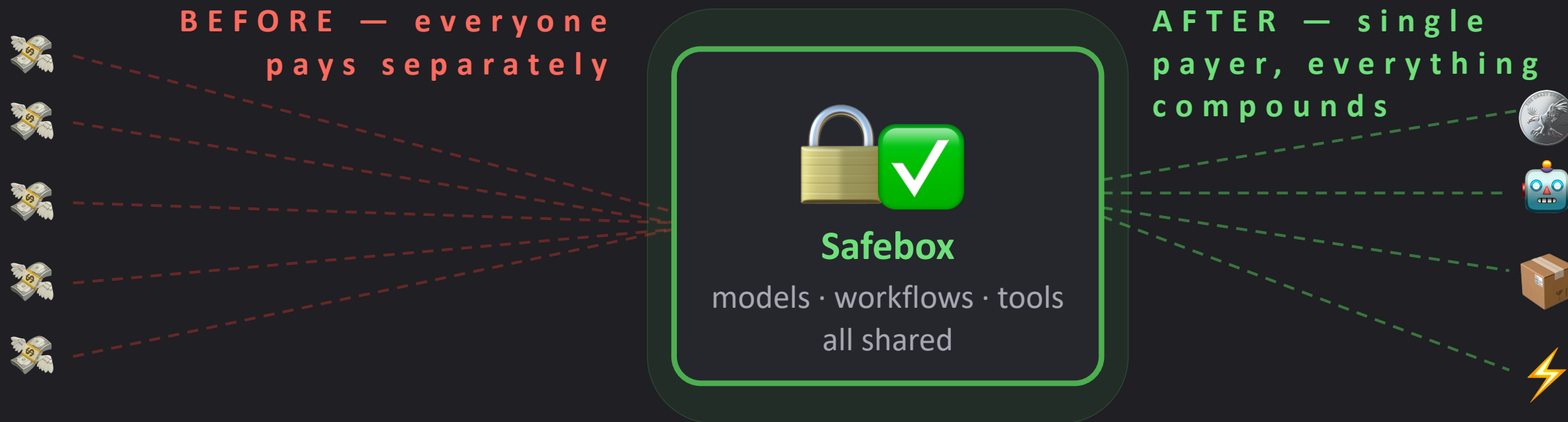
- × employees
- × vendors
- × annual price hikes

And that's just the subscriptions.

Every API call inside your app costs more on top.

Growing list of workflows & tools. Re-use generated artifacts. Costs about 95% less. Rewards accrue to first generators.

Safebox loads the open-source models once, in one place, and lets every organization share them. No per-token bill. Workflows, Tools, Capabilities, are all auto-generated on demand, and then re-used across many organizations.



~95% typical cost reduction

1x models loaded once, shared

\$0 per-token cost — no metering

Every environment. Every audit. **Every year.**

Got 100 employees with laptops? **That's 100 environments.**

Regulated industries pay \$300K–\$1.5M annually on point-in-time audits that don't transfer across environments. Each environment needs its own SOC 2, HIPAA, PCI, GDPR review.



Dev laptop



SOC 2 audit



GDPR review



pen test



On-prem server



SOC 2 audit



HIPAA BAA



ISO 27001



AWS deployment



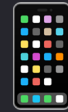
SOC 2 audit



PCI DSS



GDPR review



Mobile / edge



separate audit



pen test



country review

All of this · every year · in every country

\$300K – \$1.5M annually

One environment. Cryptographically attested to be secure.

Choose the auditors you trust. Public, or your own.

Safebox is the same in every cloud it runs: Amazon, Google, Azure, Oracle, IBM, etc. Attestations proving the environment is secure are verifiable from any browser. It will properly enforce your organization's policies, using cryptographic signatures.



SOC 2 evidence
in the signed record



HIPAA evidence
in the signed record



One Safebox

cryptographically verifiable
every action signed · easily auditable



PCI evidence
in the signed record



GDPR evidence
in the signed record

Verify from a browser · no on-site visit needed · cryptographic proof, not just sampling

AI today is a power tool. Most people can't pick it up. The hardware is impressive. But how does one get started?

Self-hosting AI means terminals, API keys, GPU drivers, virtual environments.

People who can do this are the same who could already write software. Everyone else is locked out.

What they actually see:



Wants to use AI

Shouldn't have to learn bash

```
$ python -m venv .venv
$ source .venv/bin/activate
$ pip install transformers torch
$ huggingface-cli login
Enter your token: _____
CUDA out of memory error
$ export HF_HOME=...
ModuleNotFoundError: ...
```

Workflows you use right away to automate your work.

Real reputations and results from others who used them.

Safebox ships a growing app-store catalog with shared workflows that get auto-suggested when users talk to the Safebots. Each workflow, tool, and capability was auto-generated once by someone, improved by many others, as it helped them.



Index YouTube Channel

Transcribe → keywords → indexing



12,847 runs

By LegalTech Co.



Photo Organizer

Label → organize → access control



8,213 runs

By PhotoApp Studio



Expense Reports

Receipts → submitted



5,621 runs

By BookKeep Inc.



Recipe Planner

Pantry → meals → shopping



3,478 runs

By GrandmaCooks



Draft Outreach Emails

Leads → mutuals → draft emails



15,332 runs

By Inbox Zero Co.



Set Sales Appointments

Books · reminds · syncs



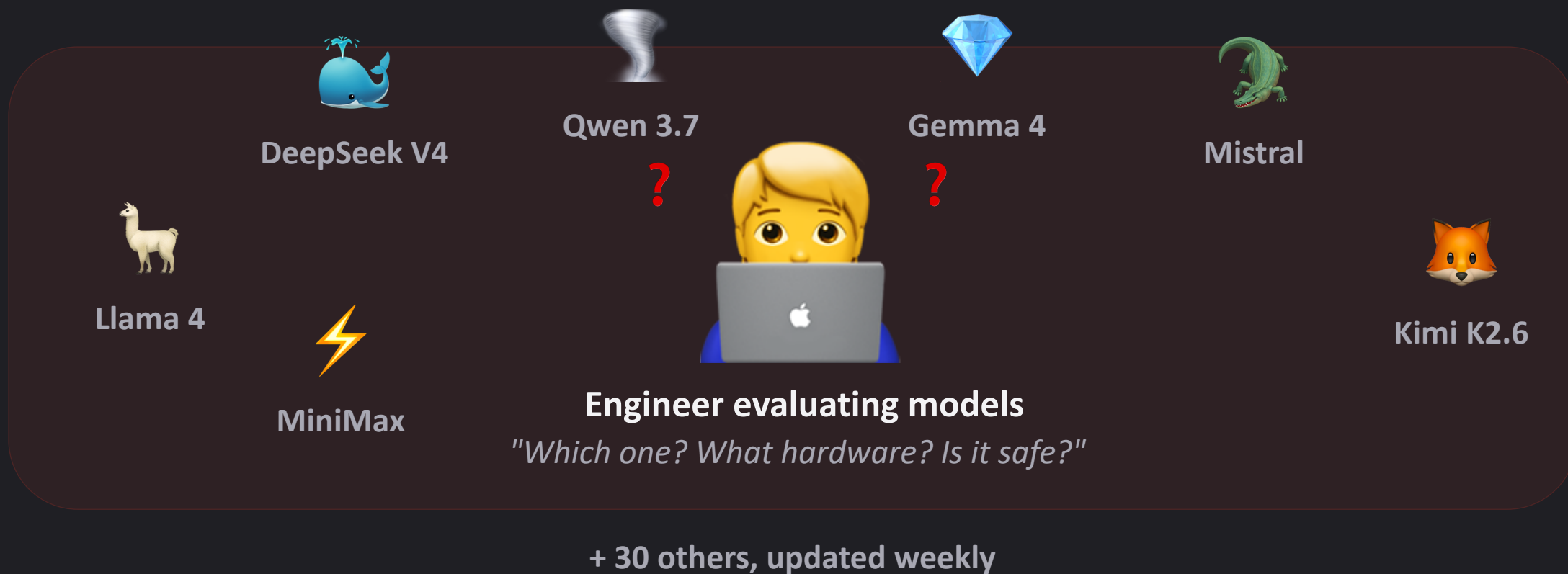
21,094 runs

By Calendar Co-op

The best open models exist.

Hosting them is the hard part.

Llama, Qwen, DeepSeek, Mistral, Gemma, Kimi, MiniMax — every one is a different download, format, framework. Engineering time most teams don't have.



The catalog is curated by the community.

The latest models are **already loaded**.

Safebox can already ship with the strongest open-source models across every category.

Each one is hash-signed by the community, just like the rest of the software. New frontier models added every few weeks.



Safebox Curated Model Roster



LLMs

DeepSeek V4-Pro · Kimi K2.6 · MiniMax M3 · GLM 5.2



Multimodal

Nemotron 3 Nano Omni · vision + audio + video + text



Music

YuE-7B · Magenta RT v1 · Stable Audio 3



Video

Wan 2.7 · Mochi 1 · LTX-2.3 · CogVideoX



Image

FLUX.1 schnell · SDXL · Stable Diffusion 3.5



Speech

Kokoro 82M · Chatterbox · Whisper Large v3



3D

TripoSR · Hunyuan3D 2.1



Today, every server has an admin.

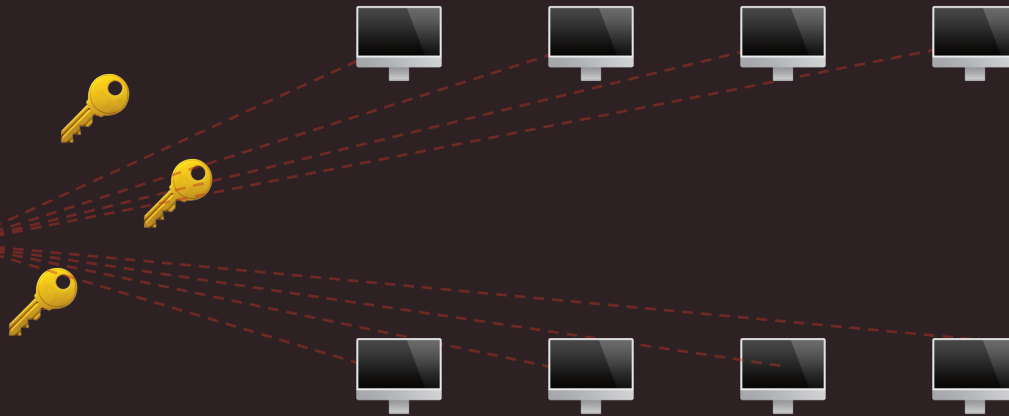
Every admin represents a risk.

Servers need maintenance. So someone has SSH keys, root access, the ability to install anything.

The admin doesn't have to be malicious. Just human. Mistakes, leaks, turnover, supply chain issues – all can lead to problems.



Your IT admin
has root access

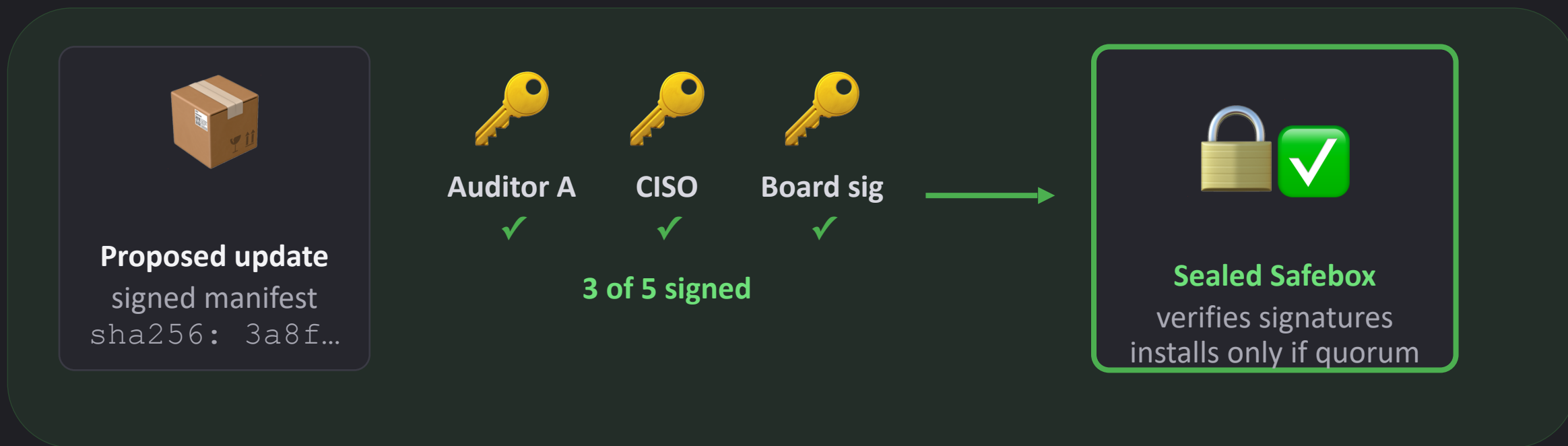


"Trust me" is the only thing standing between you and incident.

No SSH. No system administrators. **The safebox runs itself.**

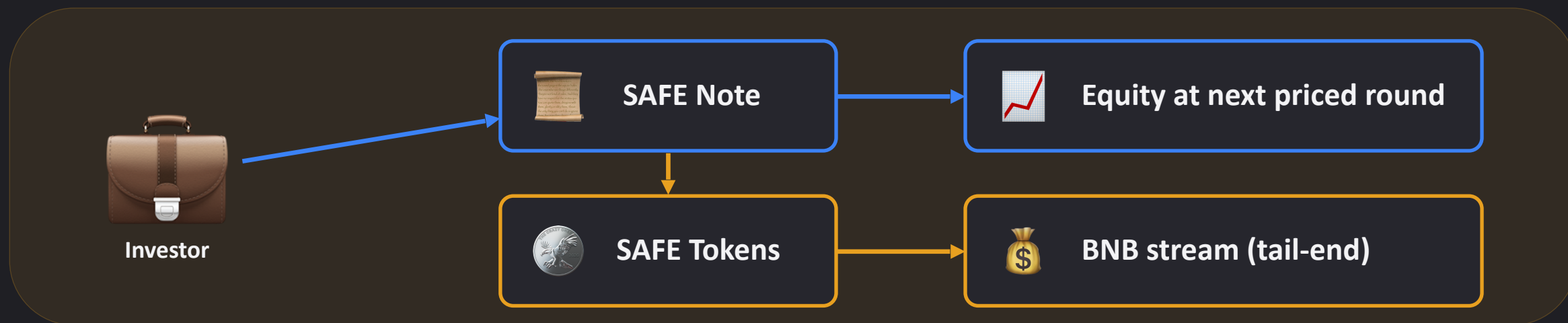
Each supply chain update needs **multiple auditors to sign off.**

A Safebox doesn't have a terminal shell to log into. It is a sealed appliance that periodically looks for updates to download. Updates are signed manifests through M-of-N approval. Nobody can push something past this gate alone — including us.



SAFE notes today for investors. **Safebux economy tomorrow.** Safebux is a unified currency for customers to pay providers.

Standard SAFE note converts at next priced round. Optional token liquidity: stake SAFE tokens in order to begin receiving passive revenue stream from 10% of ecosystem size, as Safebox and Safecloud operators redeem Safebux on the blockchain.

**SAFE**

Standard equity instrument

Safebux

Optional token exposure

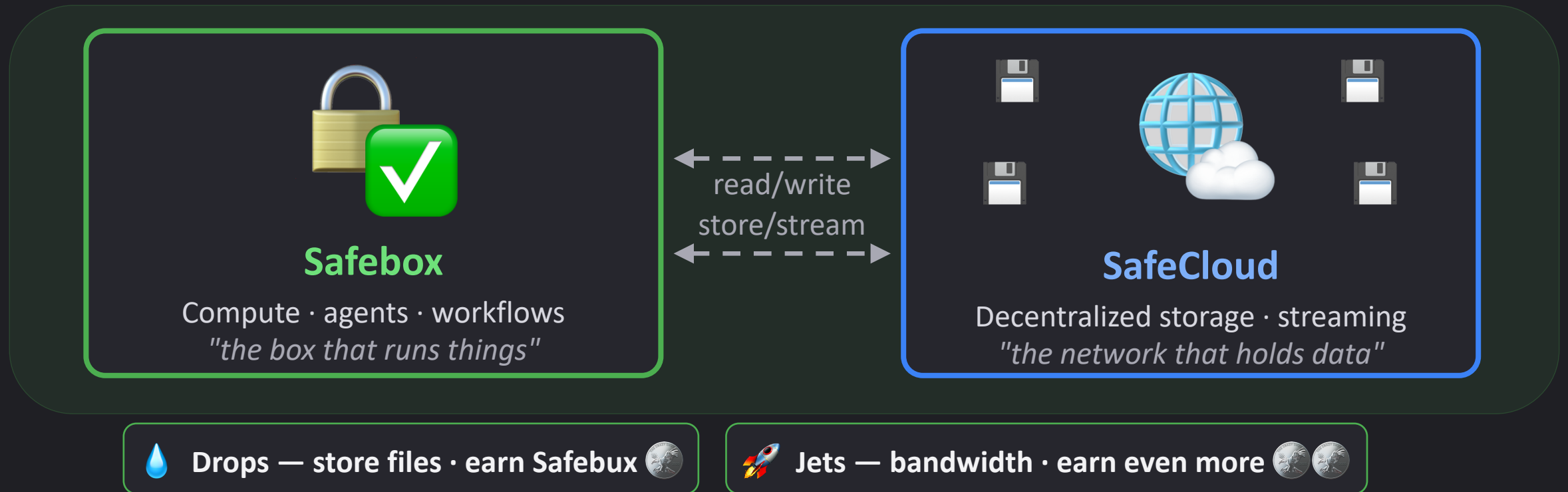
BNB

Staking for passive crypto income streams

Safebox runs the compute.

SafeCloud holds the data.

While Safebox secures the computation, SafeCloud can be used to store data encrypted and decentralized around the world. It supports redundancy, deduplication, streaming audio/video, and selective decryption of portions, in exchange for Safebux.



The whole stack, on every axis that actually matters:

DIMENSION	TODAY (CLOUD AI)	SAFEBOX
 Cost	\$5,000+/yr · per-token billing forever	~95% less cost · no per-token · one bill
 Safety / Audit	\$300K–\$1.5M annually · doesn't transfer	Cryptographic record · verify from a browser
 Ease of use	Terminal · API keys · prompting expertise	Tap a workflow with a reputation score
 Model choice	Locked to one vendor's models	Curated open roster · verified weights · swap
 Maintenance	SSH · admin trust · manual updates	No SSH · M-of-N · Safebux pays maintainers
 Privacy	Your data on their servers · may train on it	Stays in your environment · sealed
 Vendor lock-in	Switching means rebuilding from scratch	Open neutral standards · designed for audit
 Performance	API rate limits · 3am throttling	Bounded by your hardware · linear scaling
 Economics	Value to a handful of frontier labs	Safebux pays the people maintaining it

Where to go next.

If you've made it this far, you have the whole architecture in your head.
Three doors from here, in increasing depth:

Understand the Whole Stack

safebots.ai/about

Let's Have a Conversation.

<https://calendly.com/safebotsai/weekly>

More Resources for Investors

safebots.ai/resources.html