The identity & financial protection layer

for the agentic world.

3	Live	All
active pilots	production wallets	ECDSA & EdDSA chains

THE PROBLEM

Every AI agent needs a key. The key is the attack surface.

Agents need identity and authority. Today both depend on a secret that can be copied.

$10B+

lost to crypto theft & fraud in 2024

79%

of enterprises now run AI agents

40+

agents per knowledge worker — each needs identity

Lose the key, lose identity and funds. Back it up — and the backup **becomes the attack surface**.

Bybit $1.5B (2025) · **Drift** $285M · **Kelp/LayerZero** $292M — *the cryptography held; the access plane around it didn't.*

THE THREAT SURFACE

Four ways agent funds get drained today.

None of them break the cryptography. Every existing agent-wallet design leaves at least one open.

Prompt injection

A malicious input convinces the agent to sign or send. The agent has signing authority — and it just used it.

Jailbroken reasoning

The model is talked out of its own guardrails. Soft-coded rules in the agent's context window are not enforcement.

Stolen tokens & seeds

API keys, OAuth tokens, or wallet seeds sit in agent memory or config — exfiltrated by any process that reads them.

Compromised dependencies

One poisoned package reads the key the agent loaded. The agent's process holds the secret; that's all the attacker needs.

Every existing agent wallet leaves at least one door open. ***WiKey closes all four — by removing the agent's access to the secret in the first place.***

OUR ANSWER

Build security around the agent, not inside it.

Remove the agent's access to the **secret**. Put a **compliance firewall** between the agent and the world.

No backup file to compromise. No path through the agent to phish. No transaction unchecked.

No backups

Secret keys live only on the device that uses them. Nothing copied, escrowed, or written to a vault — the backup itself was the weakness, so we built a system that doesn't need one.

No agent access

The agent never sees the key. It requests a signature; the protocol decides. Prompt injection or jailbreaks cannot leak what the agent was never given.

Compliance firewall

An external, distributed guard inspects every signing request — limits, allowlists, anomaly checks — before it touches the chain. Even a compromised agent cannot move funds outside policy.

HOW IT WORKS

One signing flow. Same architecture for humans and agents.

Human client

Phone holds the device-bound credential

AI agent

SSP holds the key. The agent never does.

WIKEY PROTOCOL · ON-CHAIN

Threshold MPC

Distributed signing.
No single key, no single point of failure.

Compliance engine

External, distributed guard.
Inspects every signing request.

Guardian network

Hardware-attested recovery.
Deepfake-immune.

Funds & payment management

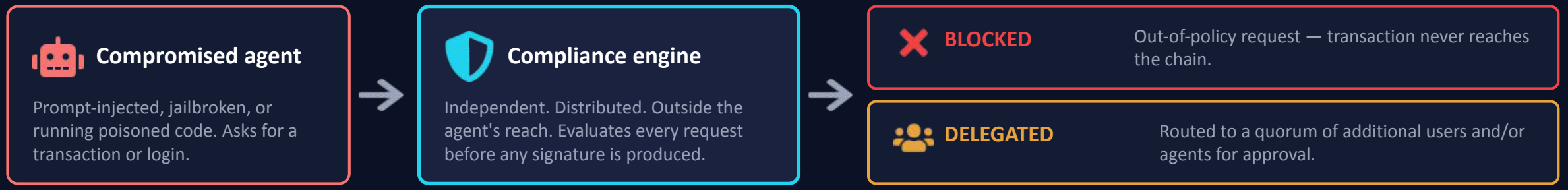
Access & login control

payments | funds | logins | identity · **protected**

BULLETPROOF UNDER ATTACK

Compromise the agent. Funds still don't move.

Even when an agent is prompt-injected or jailbroken, the compliance engine evaluates independently.



HOW WIKEY CLOSES EVERY DOOR

- **Prompt injection** → The agent has no key to leak — it requests signatures, it doesn't produce them.
- **Jailbroken reasoning** → Limits and allowlists are enforced outside the model, where reasoning can't reach.
- **Stolen tokens & seeds** → Nothing for a thief to steal — the agent's process never holds a secret.
- **Compromised dependency** → Recovery is by guardian consensus — works the same for one agent or ten thousand.

SCALE

No keys to back up. The agentic economy can finally spin up.

Every other custody model adds operational drag per wallet. We remove it entirely.

0

Backups to manage, escrow, or rotate.

1M+

Agent wallets a single deployment can support.

Linear

Cost curve. No per-key key-management overhead.

TODAY — every other model

- Generate key, encrypt key, escrow key, rotate key, recover key.
- Every wallet adds operational drag.
- Per-agent setup that doesn't scale to thousands of agents.
- The backup itself becomes the next attack surface.

WIKEY

- No keys created, no keys backed up, no keys rotated.
- One skill provisions any number of agents.
- Recovery by guardian consensus — same flow at any scale.
- Operational cost grows with usage, not with key count.

FLAGSHIP PRODUCT

The autonomous bridge — settlement at agent speed.

$2.8B+ lost to bridges built on multisig and human signers. We replace both.

ALWAYS RUN

3 deterministic algorithms

- Policy compliance check
- Counterparty / sanctions screen
- Anomaly & velocity check

+

ABOVE THRESHOLD

2 independent AI agents

- Different reasoning models
- Different infrastructure
- Invoked only when value warrants extra judgment

→

ORCHESTRATOR

Decentralized Policy Engine

✓ All checks agree → **release**
✗ Hard fail → **reject**
? Disagreement → **dispute safe**

Security comes from independence — independent code paths, independent infrastructure, independent reasoning. Compromising one component compromises one vote, not the bridge.

Release · policy + algos + agents agree

Dispute safe · funds wait — never disappear

Reject · hard fail at the gate

WHERE WE SIT

Self-custody agent wallets — versus the field.

Every provider concentrates trust in one place. WiKey distributes all three.

Player	Architecture & strength	Where WiKey is different
Cobo Agentic Wallet	MPC three-share split (User / Agent / Cobo); 80+ chains; Pact protocol per task. Closest direct comparable.	Cobo holds one of the three shares — vendor liveness is part of the trust model. WiKey's MPC is fully decentralized and the policy engine is independent of the signing path.
Coinbase Agentic Wallets	Non-custodial wallets in TEEs; native x402 (50M+ tx); deep Base ecosystem and developer reach.	TEE security is hardware-bounded — a complete key still exists inside the enclave. WiKey's keys are never reconstructed anywhere; policy is independent of the signing infrastructure.
Turnkey	TEE-based signing primitive (50–100ms); strong attestation; trusted by trading desks and Alchemy. Infrastructure-only.	Turnkey is a key-management API — policy, compliance, and recovery are the customer's problem. WiKey ships an end-to-end agentic stack with quorum delegation built in.
Privy (Stripe)	TEE + key sharding; off-chain policy engine; embedded-wallet developer experience; tight Stripe payments integration.	Policy is enforced off-chain by a single operator and assumes a user session. WiKey's policy is decentralized, on-chain-anchored, and works for sessionless agents.

The thread across the field: ***every provider still concentrates trust in one place*** *— a vendor share, a hardware enclave, or an off-chain policy server.* ***WiKey distributes all three.***

TRACTION

Three early adopters. Three categories.

Institutional custody, treasury, and autonomous agents — all live today.

PILOT 01

Florida family office

Replacing Anchorage Digital custody

Eliminates third-party counterparty risk while keeping institutional-grade controls.

PILOT 02

Spain-based fund

Replacing Safe (Gnosis) EVM multi-sig

Adds compliance controls, recovery, and cross-chain reach beyond EVM.

PILOT 03

Game studio

Securing autonomous in-game agents

AI NPCs hold and transact in-game assets — protected by WiKey, no per-agent key management for the studio.

Beta live · **Production seedless wallets in use today** · Browser + mobile

Active deployments across three categories: institutional custody, treasury, and autonomous agents.

TEAM

Operators. Three prior exits in security & enterprise.

Ofir Paz

CEO

2 exits (MSFT, NSPR)
Security background

Levi Schechter

VP R&D

Ex-Amdocs
Large-scale platforms

Dr. Sara Alon Paz

BD

1 exit
Enterprise sales

Nico Tacminzis

PMO

Program & delivery leadership

Three prior exits across the team. Building together in security and enterprise software.

WIKEY

No keys to leak.

No backups to breach.

No agent to phish.

Just protection — at any scale.

If you're investing in the rails of the agentic world, we should talk.

ofir.paz@wikey.io · wikey.io