WIKEY

Protect your data and assets in the agentic world.

The universal identity & security layer for autonomous agents.

3	Live	Any
active pilots	production identities	system the agent touches

THE GAP

Your data is only as safe as the agent's keys.

Agents now reach across every system you run — and the keys they carry can be stolen, and can't be traced.

WHERE AGENTS REACH TODAY

Everywhere your data lives.

- Internal systems — Salesforce, Microsoft, AWS
- Third-party SaaS tools and APIs
- The open web, which no vendor controls
- Databases, funds, logins and identity

WHAT TRAVELS WITH THEM

A key — held as a secret.

- **Client secrets and bearer tokens**
- **OAuth and long-lived refresh tokens**
- **Vault entries and wallet seeds**
- **One shared, non-human identity**

*The gap isn't capability — **it's the key.** The work where most breaches happen rests on a credential the agent carries from system to system.*

THE THREAT SURFACE

Two structural failures — and a recovery back door.

These follow from how keys and logs work today, not from any vendor's mistake.

KEYS CAN BE STOLEN

What the agent holds.

A stored secret is an extractable secret — prompt injection, exfiltration or a rogue dependency lifts it. It's copied into backups too, so it's stealable from there. Whoever holds it inherits the access.

THE AGENT CAN BE TURNED

No key theft required.

Phishing and prompt injection can circumvent the agent into releasing data or authorizing an action — even without ever giving away the key. The key stays put; the data still leaks.

RECOVERY IS THE SOFT TARGET

The way back in.

Help-desk and reset workflows bypass even phishing-resistant MFA. AI voice and video impersonation now defeat the human verification these resets rely on.

Drift / Salesforce: stolen agent tokens exposed data across 700+ organizations. **MGM · Caesars · M&S · Co-op**: breached at the recovery desk, not the login.

The cryptography held. The keys — and the path used to recover them — did not.

TODAY'S TOOLS

Platform trust layers secure the platform — not the key.

Each is strong inside its own estate. None covers an agent that doesn't stay in one.

Tool	What it secures	Where it stops
Salesforce Einstein Trust Layer	Prompt defense & zero-retention for Agentforce data	Anything outside Salesforce
Microsoft Entra Agent ID	Agent identity & access inside the Microsoft estate	Tenant-bound; the rest via Microsoft's own gateway
AWS Bedrock AgentCore Identity	Agent credentials, token vault & MCP gateway auth	Workloads and data outside AWS
Okta / Auth0 (identity providers)	Authenticate users; issue agent tokens (OAuth/OIDC)	Stored secrets & bearer tokens remain stealable
Astrix / Oasis (non-human identity)	Discover, govern & rotate machine credentials	Existing credentials, governed after the fact
Silverfort & inline gateways	Evaluate or block tool calls at one choke point	The authority the agent carries everywhere else

*Guard one source at a time and you always miss the level below — **the keys the agent carries from source to source.***

OUR ANSWER

Protect the key. Protect the data.

Hold the key where it can't be read or copied — and protect the data with an engine the agent can't switch off.

UNREADABLE KEYS

Held, never stored.

Keys live in a post-quantum virtual HSM — the secure enclave or TPM — separated from the agent and the app. Never backed up, so there is no copy to steal or restore.

SCOPED & TRACEABLE

Every action to a person.

The agent acts under a scoped, time-bound, revocable sub-identity that descends from a human owner. Credentials are short-lived and refreshed often — a stolen one expires fast.

THE DATA STAYS PROTECTED

Guarded by the compliance engine.

An external engine supervises every login, read, write and transfer — without ever seeing the data. Even a circumvented agent can't move data or funds outside policy.

Filters reduce the attacks. Scope, supervision and revocation limit the damage.

WIKEY

HOW IT WORKS

Two independent layers. One identity that travels.

Human client

Device-bound credential on the phone.

AI agent

Requests a signature. Never holds the key.

WIKEY PROTOCOL

Virtual HSM · PQC

A per-identity secure store in the enclave / TPM. Keys are never reconstructed anywhere, and never backed up.

Compliance engine

External and distributed. Signs and checks every login (MCP, OIDC); supervises every read, write and transfer — never the content.

Distributed guardians

Recovery by cryptographic attestation. Human and non-human, hardware-attested and deepfake-immune.

Presents as an external OIDC / OAuth identity provider — ***Salesforce, Entra and AWS AgentCore accept it at the door. No rip-and-replace.***

payments · funds · logins · identity · data — protected

BULLETPROOF UNDER ATTACK

Compromise the agent. No damage gets through.

Whoever is compromised, the compliance engine evaluates independently — no single party moves what policy hasn't approved.

Compromised agent

Prompt-injected, jailbroken or running poisoned code. Asks for a transaction or a login.

Compliance engine

Independent, distributed and outside the agent's reach. Evaluates every request before a signature exists.

BLOCKED out-of-policy — never reaches the system.

DELEGATED routed to a quorum for approval.

HOW WIKEY CLOSES EVERY DOOR

- **Prompt injection** → The agent has no key to leak — it requests signatures, it doesn't produce them.
- **Jailbroken reasoning** → Scope and limits are enforced outside the model, where reasoning can't reach.
- **Stolen tokens & seeds** → Nothing standing for a thief to hold — credentials are short-lived, scoped, revocable.
- **Compromised dependency** → Recovery is by guardian attestation — the same flow for one agent or ten thousand.

ACCOUNT RECOVERY

The breaches start at recovery. We close that door.

Most attacks don't break authentication — they talk a help desk into resetting it.

THE PLAYBOOK

- Pass verification with breached personal data
- Claim a lost or broken phone
- Enroll an attacker-controlled MFA device
- AI voice and video now defeat the human check

MGM & Caesars (2023) · M&S & Co-op (2025) · insurers & airlines (2025).
Mandiant: a help-desk call to domain-admin in under an hour.

THE WIKEY MODEL

- Recovery by cryptographic attestation
- Trusted parties — installer, prior counterparty — sign with their own keys
- No password, no phone number, no help-desk reset
- A signature can't be social-engineered

*Keys held in the virtual HSM and never backed up — **no copy to restore, and no reset path to exploit.***

FLAGSHIP

Settlement at agent speed.

$2.8B+ lost to bridges built on multisig and human signers; 82% of breaches involve the human element — we take the human off the hot signing path.

ALWAYS RUN

3 deterministic algorithms

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

+

ABOVE THRESHOLD

N independent humans

- A quorum of independent reviewers
- Distinct parties, no shared trust
- Invoked only when value warrants human judgment

→

ORCHESTRATOR

Decentralized policy engine

All checks agree → **release**

Hard fail → **reject**

Disagreement → **dispute-safe**

Treasury agent moves $5M Ethereum → Solana. Deterministic checks clear policy, sanctions and anomaly in ~200ms. Above $1M, N independent humans review counterparty and on-chain provenance. All signals agree → **the vHSM signs.** *No human ever held a key or produced a signature — the quorum approves, the protocol signs.*

WHERE WE SIT

Everyone concentrates trust. We distribute all three.

A vendor share, a hardware enclave, or an off-chain policy server — each is a single point to compromise.

Dimension	Platform-native trust layers	Universal layer (WiKey)
Keys / credentials	Stored in tokens, vaults & backups — stealable	Post-quantum virtual HSM; keys never backed up
Account recovery	Help-desk / reset bypasses phishing-resistant MFA	Attestation by trusted parties — no passwords or help desk
Traceability	Often a service account; logs siloed per vendor	Every action traces to the agent's owner
Coverage	No single vendor reaches every source	Consistent across systems that accept it, incl. external MCP
Identity across hops	Re-issued and re-translated at each boundary	One inherited identity across systems
Neutrality	A platform won't be neutral toward rivals	Vendor-neutral by design

Salesforce won't secure your AWS agents; Microsoft won't be neutral toward Google. ***Universality isn't a feature they're behind on — their business model precludes it.***

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 — no per-agent key management for the studio.

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

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

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.

info@wikey.io · **wikey.io**