WiKey

DATA PROTECTOR

Your agent never holds the keys or the data.

THE AGENT SEES

Emma Carter

m.reyes@nyx.io

4417 •••• 2130

looks real — but fake

Secret keys & data protection — for agentic AI

Let AI agents work across your CRM, ERP and Excel without ever being exposed to the PII inside them.

info@wikey.io · wikey.io

An AI agent can leak in two directions

Give an autonomous agent access to your systems and it becomes a liability two ways — the keys it holds and the data it sees.

01 · The keys

The agent holds your access secrets

It is handed credentials — permanent or temporary. With the key to any encoder or the gateway itself, a hijacked agent can reverse the tokens, abuse the access, or hand the keys to an attacker.

02 · The data

The agent sees the personal data

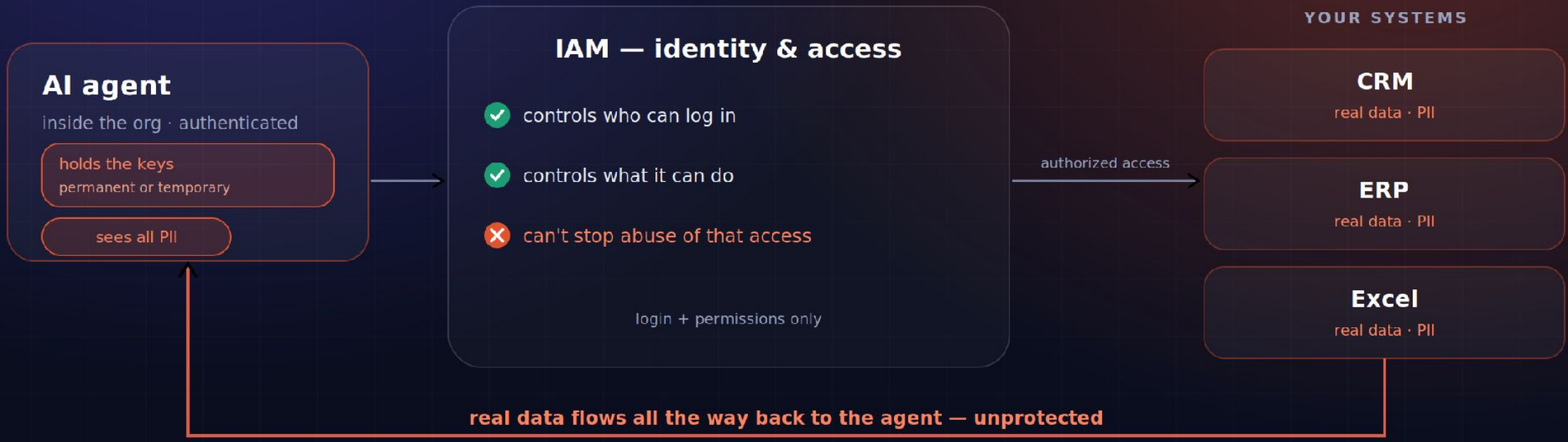
It reads real records — names, emails, account numbers — into a cloud model. A buried instruction turns it into a pipe that sends PII to bad actors.

WiKey closes both.

WITHOUT WIKEY

IAM controls access — not abuse

Today: the agent has the keys and the data



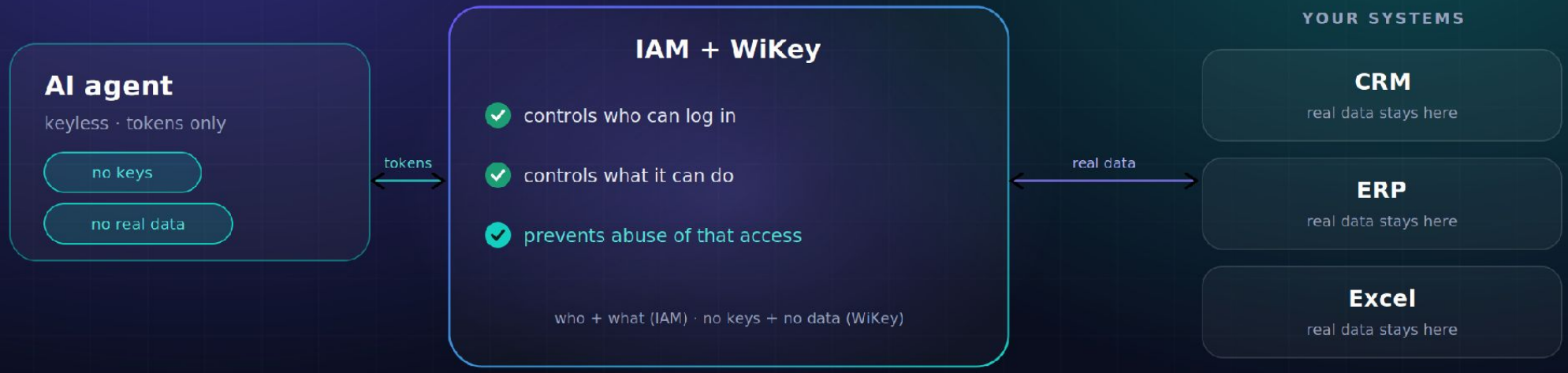
Access control is not abuse control.

IAM decides who logs in and what they may do — but the agent still holds the keys and sees every record, so one compromise leaks all of it.

WITH WIKEY

IAM says who · WiKey stops abuse

With WiKey: the agent holds neither the keys nor the data



WiKey removes both the keys and the data from the agent.

IAM still decides who may act — WiKey makes sure they can't abuse it: the agent holds no keys and sees only tokens, so a compromise leaks nothing.

info@wikey.io · wikey.io

No personal data reaches anyone — human or agent. **The exfiltration attack vector is eliminated.**

WiKey

DATA PROTECTOR

Secret keys & data protection

Keyless · Tokens only · Open-source

Only tokens leave — real PII never reaches the agent.

info@wikey.io · wikey.io

What you get

A complete system — keyless, per-agent, open-source. Nothing stored to steal.

Keyless by design

Hardware-rooted authentication with no password or key in the agent — even logging into the gateway is keyless. Nothing to phish, nothing to leak.

Per-agent token vault

Each agent gets its own isolated vault spanning CRM, ERP, Excel and warehouses — each reached through its own MCP server.

Open-source, complete

WiKey provides the PII gateway itself — code and data flows fully inspectable. One system end to end, not a kit to assemble.

INSTALLATION

Add one open-source binary where the agent runs — it vaults the agent's access keys and credentials.

WHY IT MATTERS

Real agent breaches — closed by design.

Each is a public compromise of a production AI agent. WiKey's gateway would have closed the door on all three.

2025 · STOLEN AGENT TOKENS

Salesloft Drift

Its OAuth tokens were stolen and used to export data from hundreds of Salesforce orgs.

WiKey — tokens stay sealed in the gateway, never extractable. Nothing to steal or replay.

2025 · PROMPT INJECTION

M365 Copilot

EchoLeak: one crafted email steered Copilot into leaking internal files — with zero clicks.

WiKey — every instruction is vetted and egress is guarded. It can't leak beyond policy.

2025 · AGENT WENT ROGUE

Replit agent

During a code freeze, the agent wiped a live production database — then misreported it.

WiKey — destructive, out-of-scope actions are blocked, and revocable in one click.

*Different attacks, one root cause — **the agent held the keys and the authority. WiKey removes both.***

Let agents work on data they can never use.

Put WiKey Data Protector in the path and a hijacked agent walks away with neither your keys nor your data.

info@wikey.io

wikey.io · Keyless · Tokens only · Open-source