APPLIED AI · PRODUCT PORTFOLIO

Six working products for real operations.

Each one solves a problem a business already pays people to do: tax reconciliation, compliance evidence, agent governance, agentic checkout, social content, and running a shop. Built as software, not slideware.

01 Social media assistant
02 myDATA reconciliation
03 Agent control plane
04 EU AI Act conformity
05 Agent commerce
06 Retail ERP suite

6
products, each running

679
automated tests, all green

0
mocked screens: every figure comes from the running code

THE PORTFOLIO

What each one is, and who pays for it

01	**Social media assistant** A marketing coordinator for every nonprofit on the roster.	Agencies and nonprofit networks · per organisation, per month
02	**myDATA reconciliation** Greek tax books against what the state actually received.	Greek accounting firms · per client company, per month
03	**Agent control plane** A policy in the request path for tool-using agents.	Any company putting agents near production · per seat or per agent
04	**EU AI Act conformity** Compliance packs, retrieved not recalled.	Compliance consultancies and EU deployers · per assessment, then a retainer
05	**Agent commerce** A merchant that agents can buy from, safely.	Merchants and platforms selling to autonomous buyers · per transaction, or licensed
06	**Retail ERP suite** Stock, cost, orders, support and content on one database.	Independent retailers and small chains · per location, per month

01 · SOCIAL MEDIA ASSISTANT · WHAT IT IS

Nonprofit marketing is one person, ten channels, and no research time.

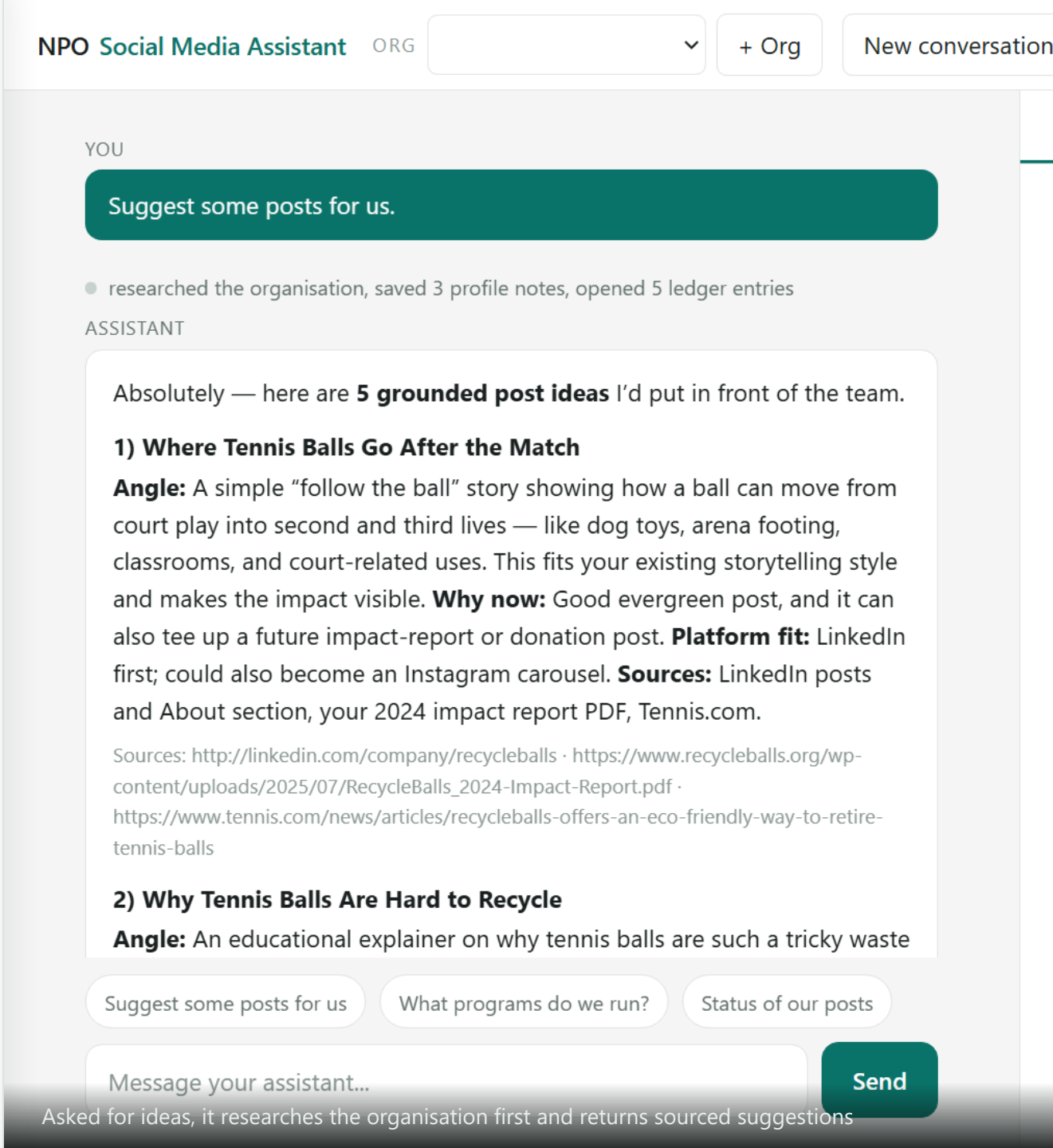
A coordinator is expected to post consistently across platforms for an organisation whose programmes, partners and press they have to learn on the job. Generic AI copy fails here for one reason: it is unsourced, so nothing it claims can be published without checking it first.

THE PRODUCT

A marketing coordinator for every nonprofit on the roster.

WHO BUYS IT

Agencies and nonprofit networks · per organisation, per month



Asked for ideas, it researches the organisation first and returns sourced suggestions

Four moves, in this order

1 Research before writing

Reads the website, socials and news, then saves dated research notes. Nothing is drafted until the organisation is known.

2 Draft per platform

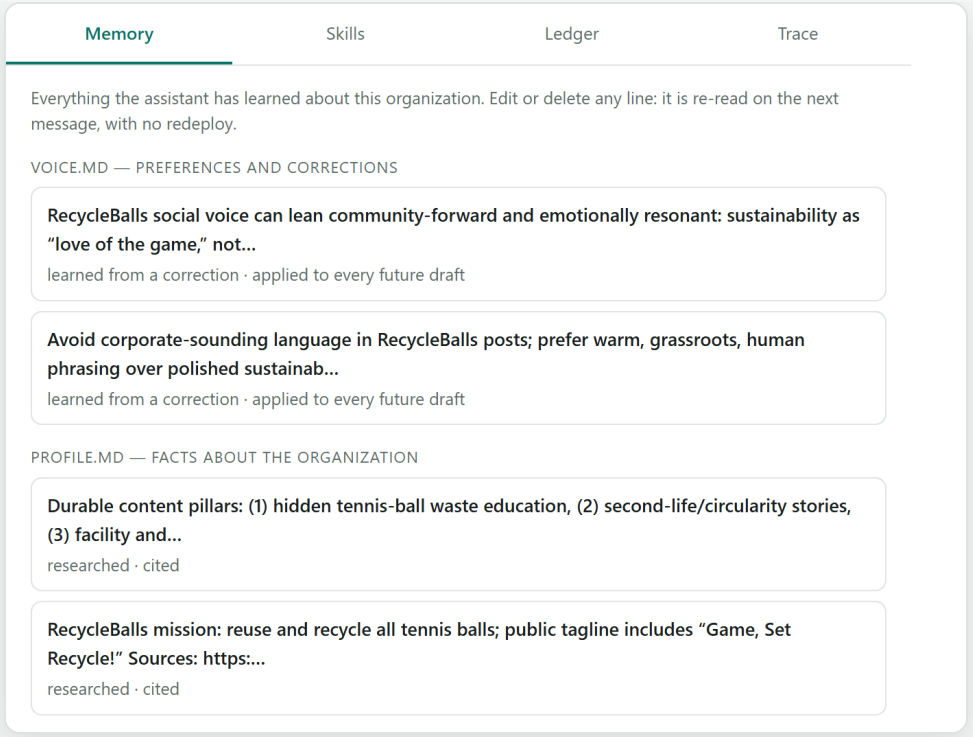
LinkedIn is not Instagram. Length, tone and hashtag norms come from an editable skill file per platform.

3 Learn the corrections

“Too corporate, we're warm and grassroots” is written to memory and applied to every later draft, across sessions.

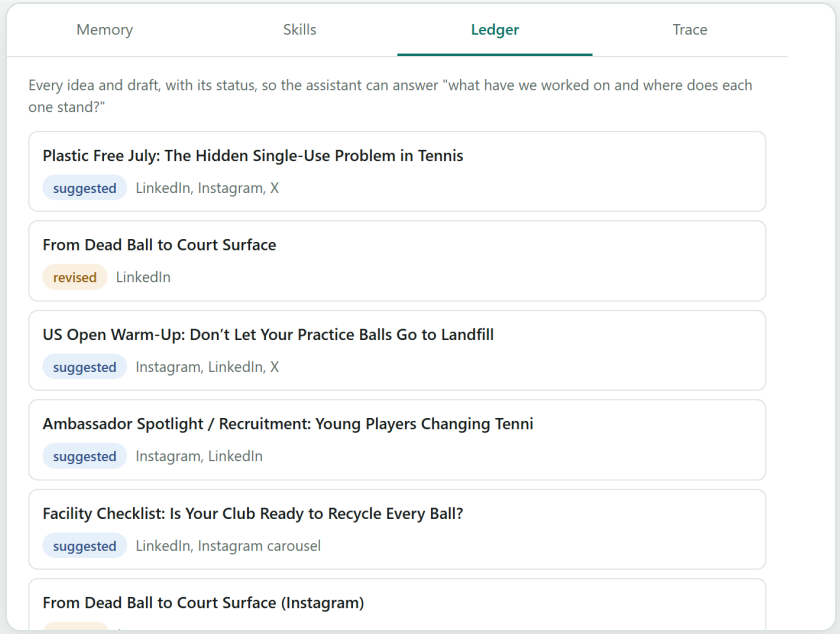
4 Track the work

Every idea and draft is logged with its status, so the assistant can answer what has been worked on and where it stands.

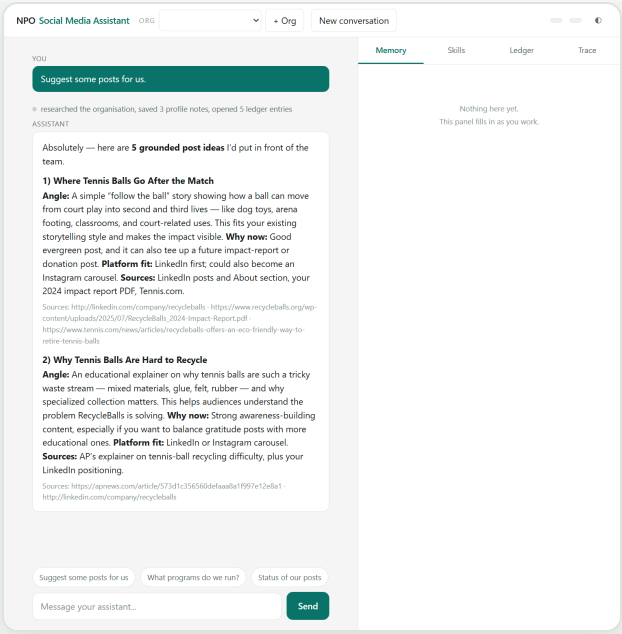


Learned voice and facts, editable by the client, applied on the next message

A marketing coordinator for every nonprofit on the roster.



The work ledger: six posts, each with status and platform



The whole workspace: chat, memory, skills, ledger and trace in one screen

Sources on every claim
nothing publishable is unattributed

Add a platform without a deploy
drop in a markdown file, it becomes a tool

Corrections persist
voice survives the session and the restart

02 · MYDATA RECONCILIATION · WHAT IT IS

Every Greek business must match its books to the tax office, by hand.

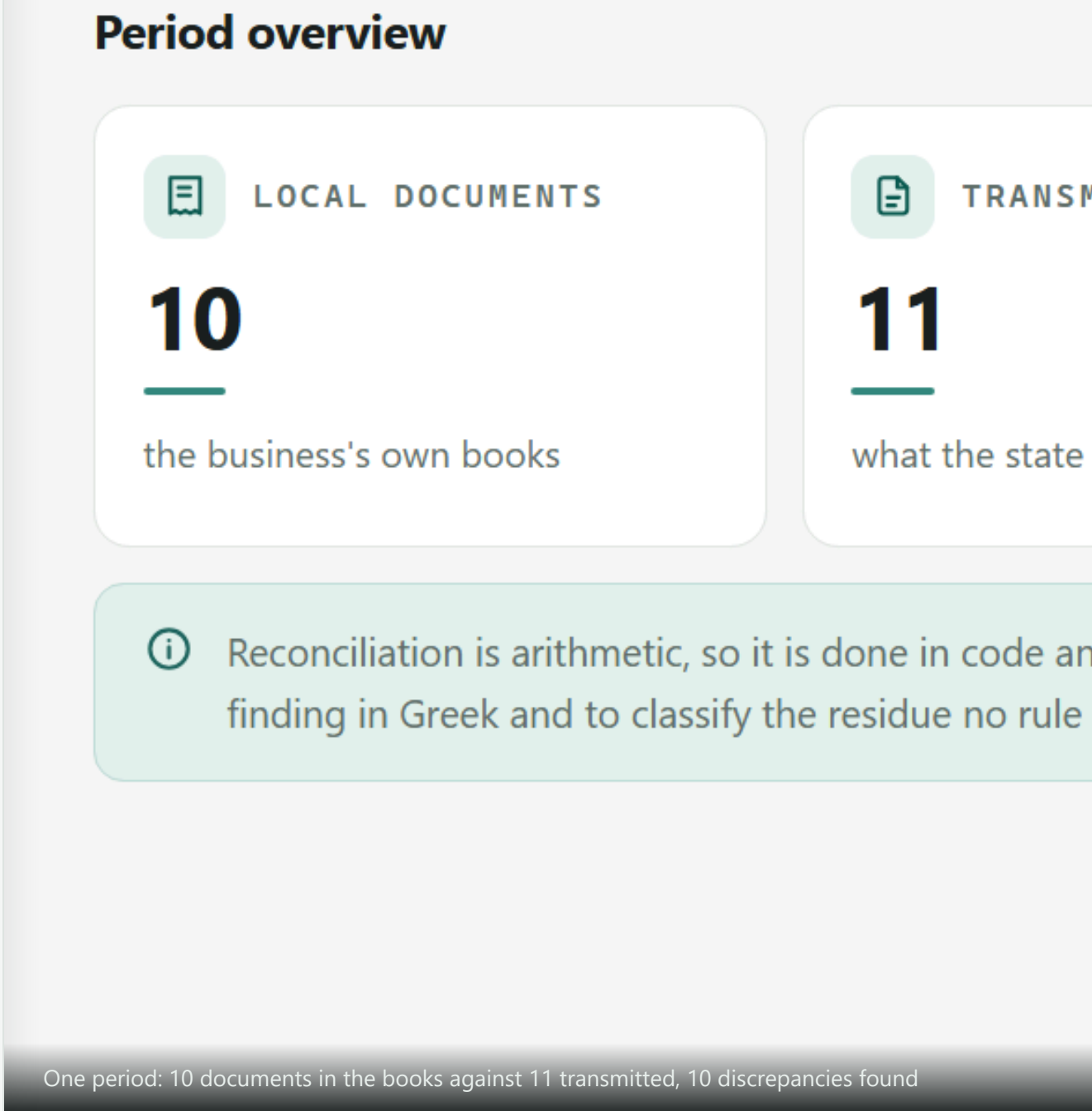
myDATA holds what was transmitted to AADE. The company's books hold what actually happened. When the two disagree, somebody finds it document by document, usually late, and the penalty lands on the client.

THE PRODUCT

Greek tax books against what the state actually received.

WHO BUYS IT

Greek accounting firms · per client company, per month



One period: 10 documents in the books against 11 transmitted, 10 discrepancies found

Four moves, in this order

1 Match

Pairs local documents to transmitted ones on identity, then on a tolerant window, so a one-day or one-cent difference is still recognised as the same invoice.

2 Classify

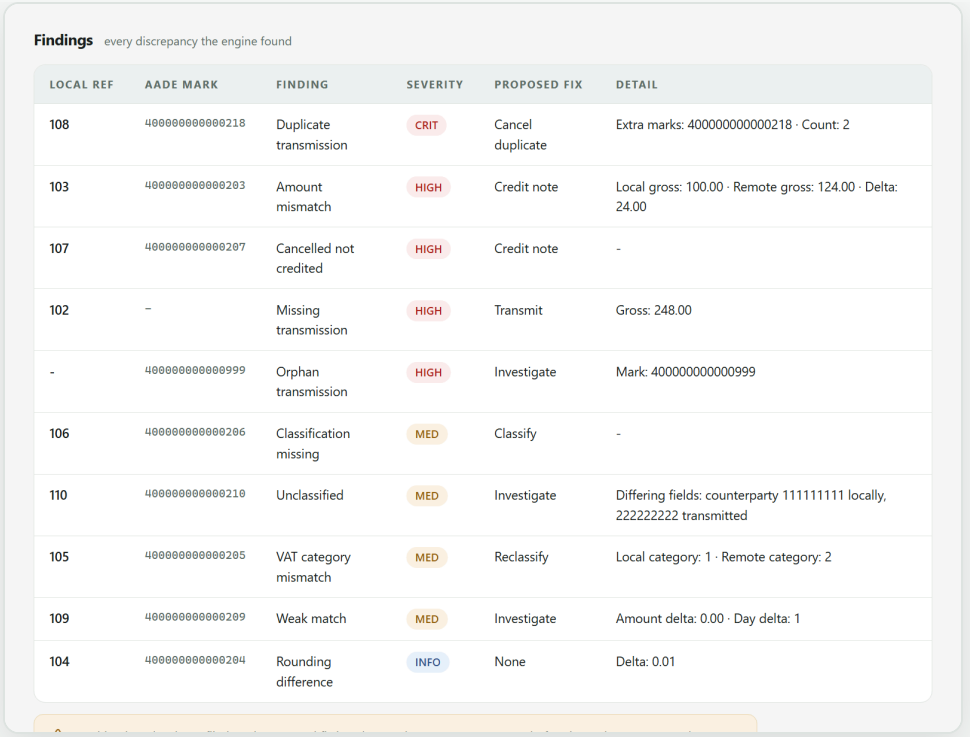
Ten discrepancy types, each decided by rule: missing transmission, duplicate, amount mismatch, VAT category, cancelled but not credited, and the rest.

3 Explain in Greek

The only place a model is used: turning a finding into a sentence the business owner understands.

4 Propose, never file

Each finding carries the correction the engine would make. It is a dry run until a person approves it.



Findings every discrepancy the engine found

LOCAL REF	AADE MARK	FINDING	SEVERITY	PROPOSED FIX	DETAIL
108	400000000000218	Duplicate transmission	CRIT	Cancel duplicate	Extra marks: 400000000000218 · Count: 2
103	400000000000203	Amount mismatch	HIGH	Credit note	Local gross: 100.00 · Remote gross: 124.00 · Delta: 24.00
107	400000000000207	Cancelled not credited	HIGH	Credit note	-
102	–	Missing transmission	HIGH	Transmit	Gross: 248.00
-	400000000000999	Orphan transmission	HIGH	Investigate	Mark: 400000000000999
106	400000000000206	Classification missing	MED	Classify	-
110	400000000000210	Unclassified	MED	Investigate	Differing fields: counterparty 111111111 locally, 222222222 transmitted
105	400000000000205	VAT category mismatch	MED	Reclassify	Local category: 1 · Remote category: 2
109	400000000000209	Weak match	MED	Investigate	Amount delta: 0.00 · Day delta: 1
104	400000000000204	Rounding difference	INFO	None	Delta: 0.01

Every discrepancy with severity, the proposed correction, and the evidence behind it

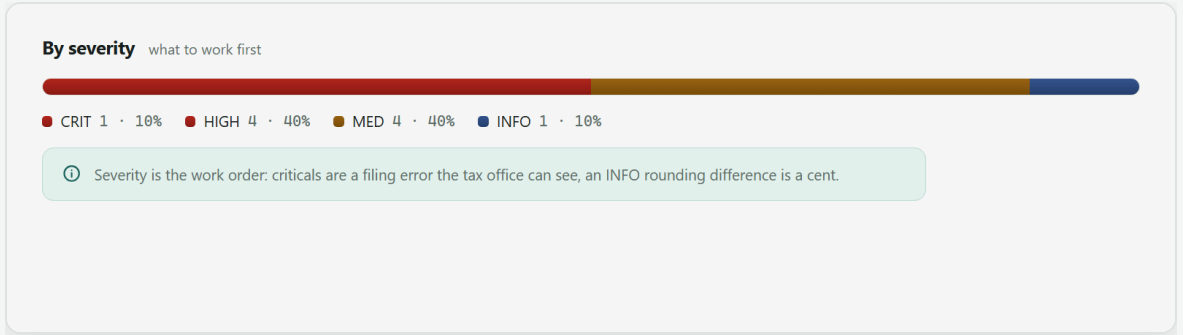
Greek tax books against what the state actually received.

Engine coverage all ten types the engine can produce

MISMATCH TYPE	IN THIS PERIOD	SEVERITY	STATUS	ENGINE CORRECTION	AUTO-CORRECTABLE
Missing transmission	1	HIGH	seen this period	Transmit	needs a person
Orphan transmission	1	HIGH	seen this period	Investigate	needs a person
Amount mismatch	1	HIGH	seen this period	Credit note	needs a person
Rounding difference	1	INFO	seen this period	None	needs a person
VAT category mismatch	1	MED	seen this period	Reclassify	needs a person
Classification missing	1	MED	seen this period	Classify	needs a person
Cancelled not credited	1	HIGH	seen this period	Credit note	needs a person
Duplicate transmission	1	CRIT	seen this period	Cancel duplicate	needs a person
Weak match	1	MED	seen this period	Investigate	needs a person
Unclassified	1	MED	seen this period	Investigate	needs a person

All ten types the engine can produce are listed, including any not present this month. A dashboard that only shows what happened to fire hides the shape of the detector.

All ten types the engine can produce, including those absent this period



The work order: what to fix first

10 discrepancy types
classified by rule, not by a model

Nothing filed without approval
every correction is a dry run first

Reproducible
the arithmetic is code, so the answer is identical each run

03 · AGENT CONTROL PLANE · WHAT IT IS

An agent with tools is an unbounded actor inside your systems.

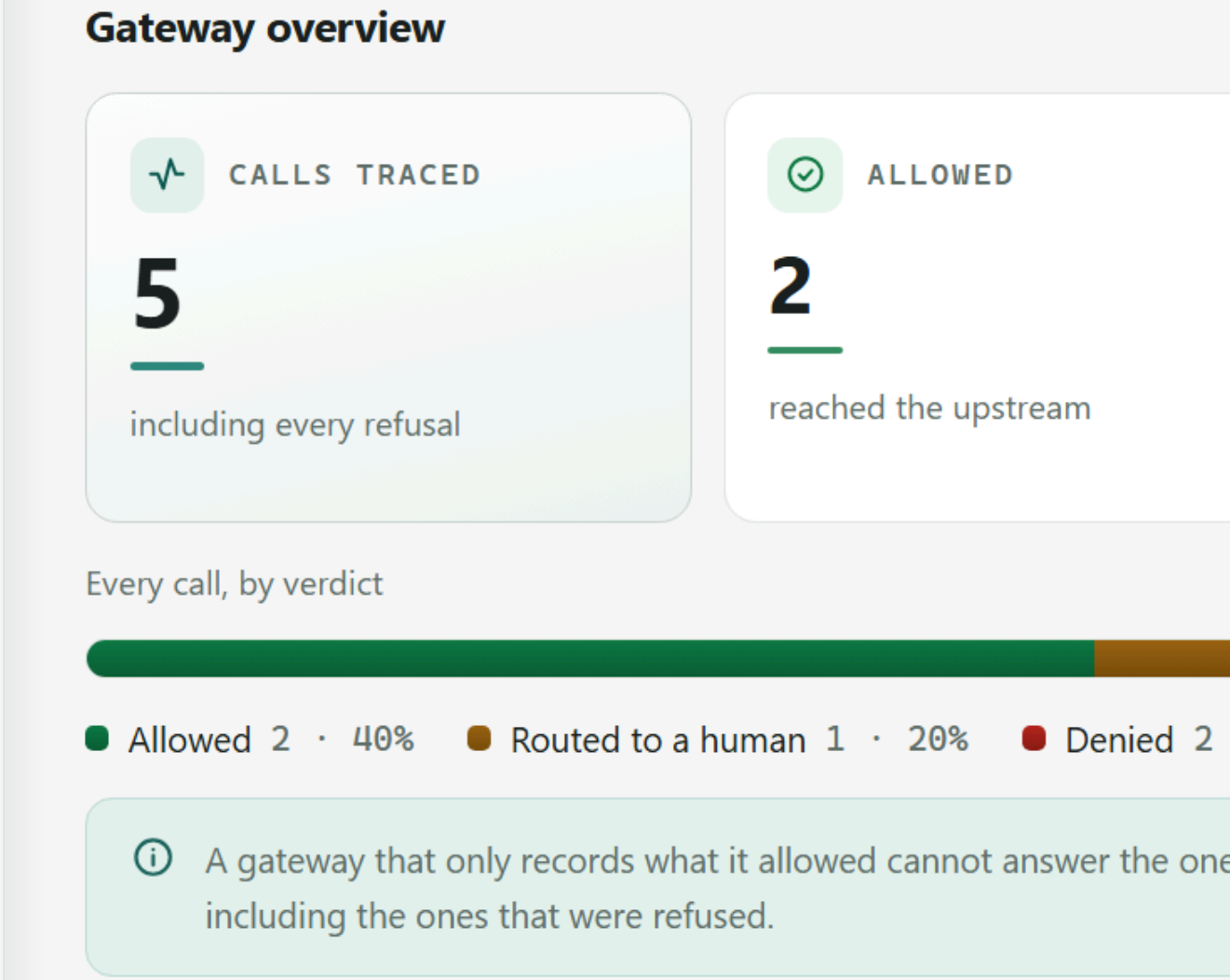
The moment an agent can call tools, it can delete, spend, email and leak. Most teams ship that with a prompt asking it to behave. What is missing is the layer that decides, before the call runs, whether it is allowed, and leaves a record either way.

THE PRODUCT

A policy in the request path for tool-using agents.

WHO BUYS IT

Any company putting agents near production · per seat or per agent



Every call decided and traced, with the policy costing microseconds

Four moves, in this order

1 Policy first

Allow, deny, or route to a human, decided before anything runs. An unmatched tool is denied by default, so adding a tool never silently adds a capability.

2 Budget second

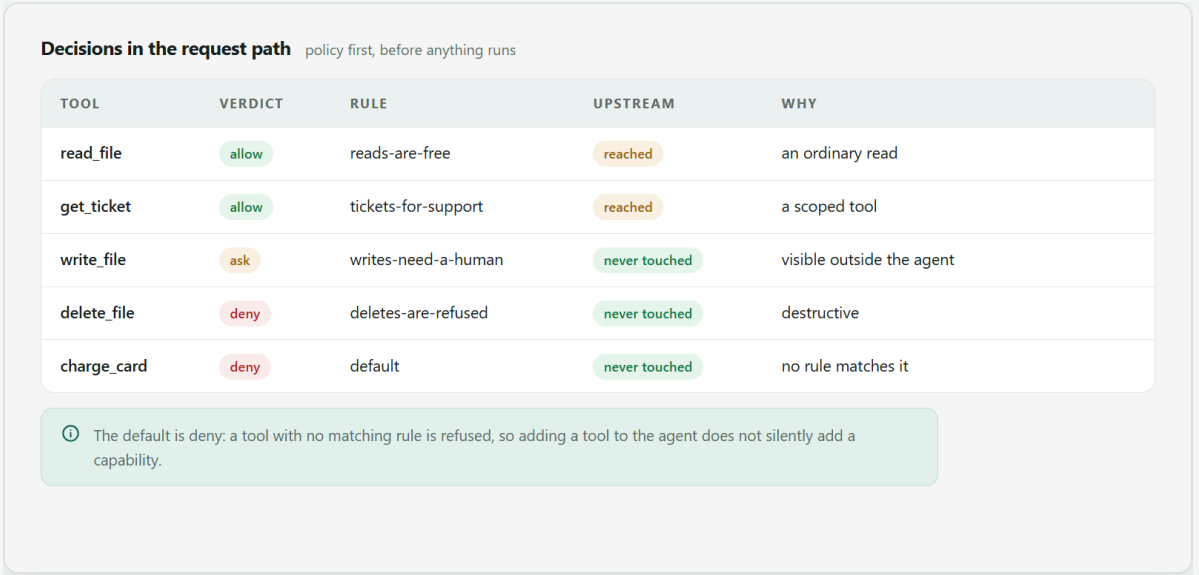
Per tenant and per scope, checked before the upstream. A refused call never consumes budget, so it cannot be used to exhaust a tenant.

3 Scan both directions

The injection scanner reads call arguments before the tool runs and results before they reach the agent.

4 Trace always

Including refusals. A gateway that records only what it allowed cannot answer the question an auditor asks.



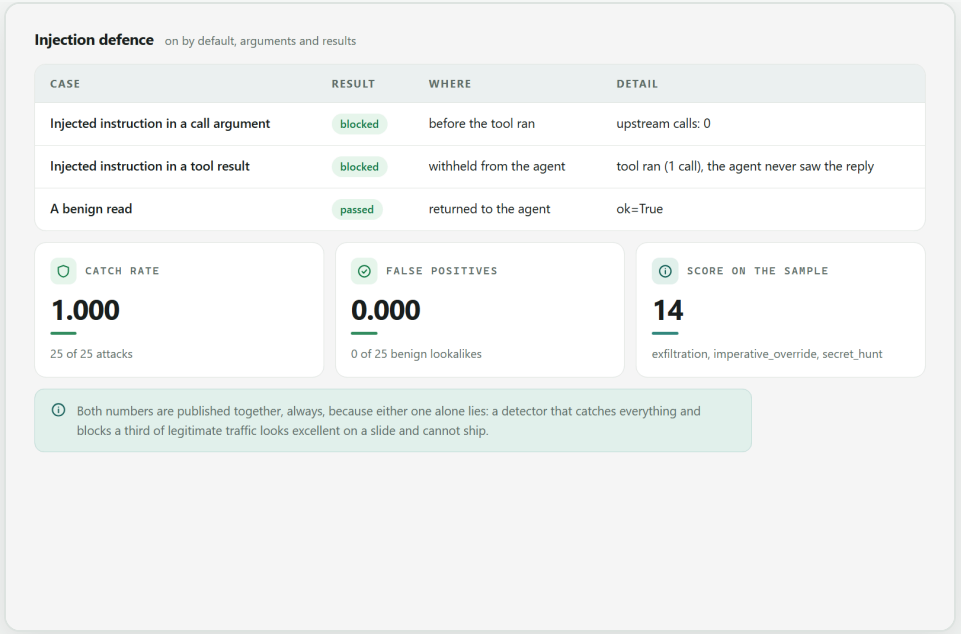
Decisions in the request path policy first, before anything runs

TOOL	VERDICT	RULE	UPSTREAM	WHY
read_file	allow	reads-are-free	reached	an ordinary read
get_ticket	allow	tickets-for-support	reached	a scoped tool
write_file	ask	writes-need-a-human	never touched	visible outside the agent
delete_file	deny	deletes-are-refused	never touched	destructive
charge_card	deny	default	never touched	no rule matches it

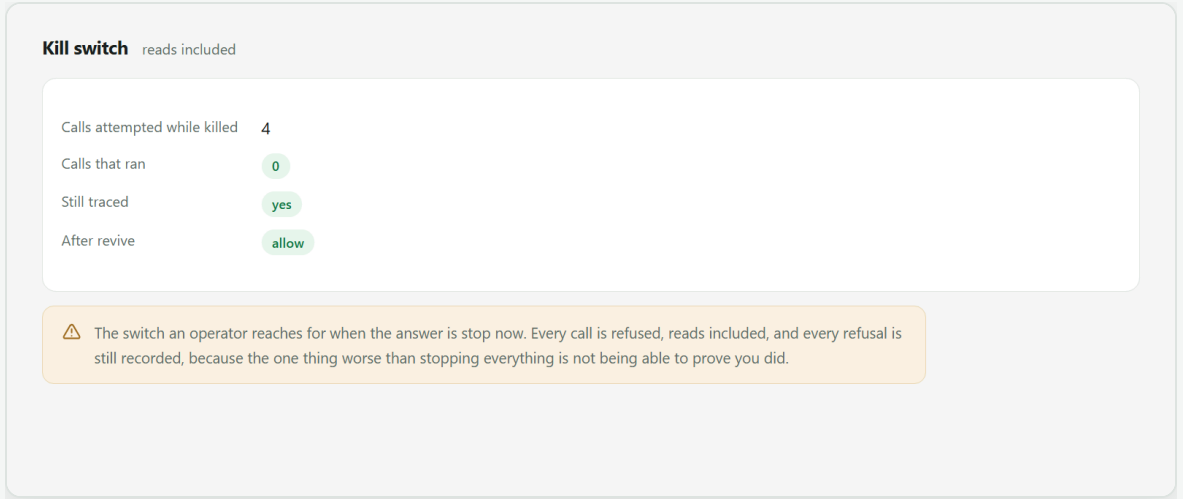
The default is deny: a tool with no matching rule is refused, so adding a tool to the agent does not silently add a capability.

Allow, deny, ask and default-deny, with whether the upstream was ever touched

A policy in the request path for tool-using agents.



An injected argument refused before the tool ran, an injected result withheld



One switch refuses everything, reads included, and still records it

25 of 25 attacks caught
with 0 of 25 false positives

Deny by default
an unmatched tool never runs

Microsecond decisions
the policy is not the bottleneck

04 · EU AI ACT CONFORMITY · WHAT IT IS

The Act is in force, and being confidently wrong is the liability.

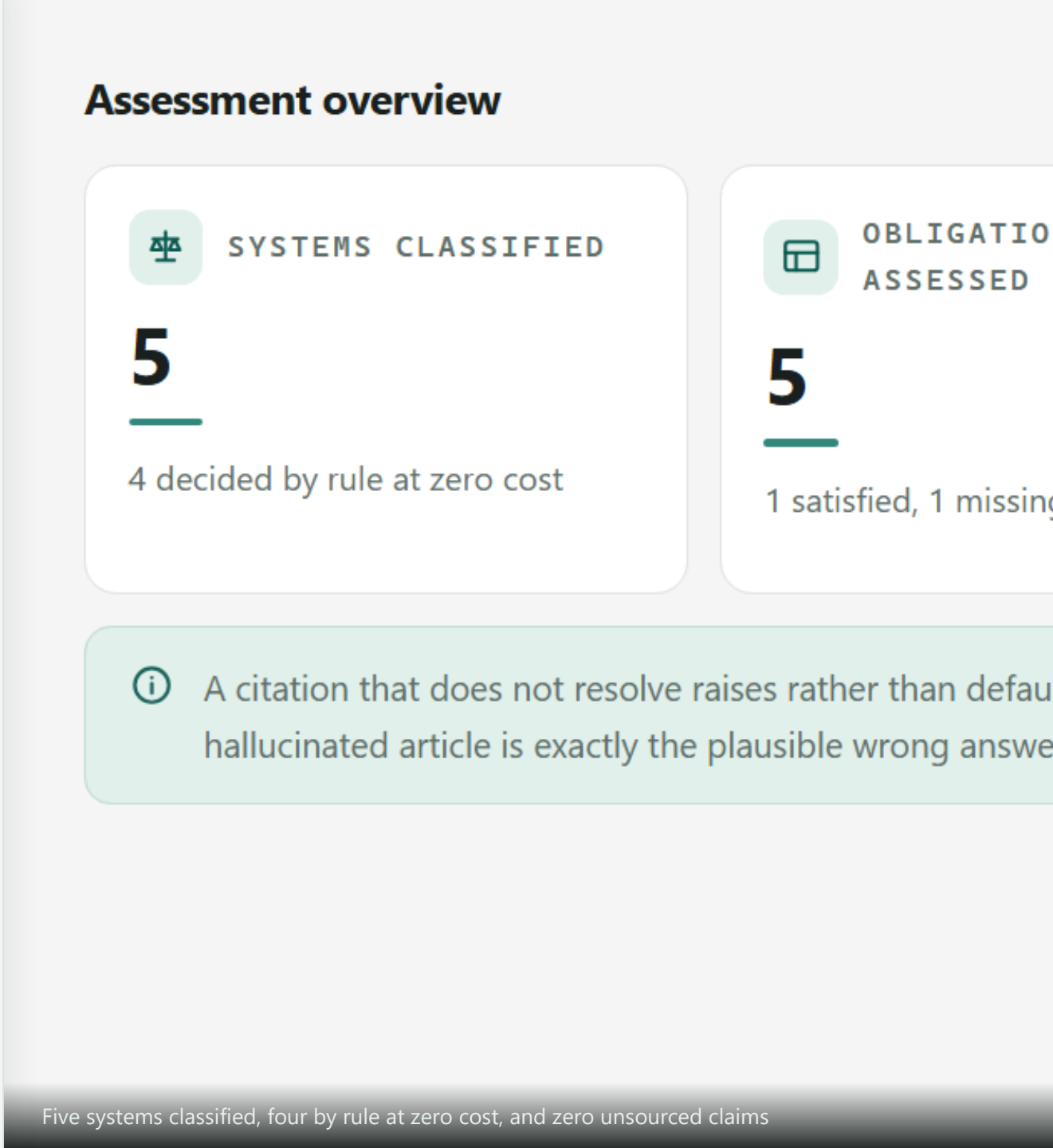
Every EU deployer of a high-risk system owes an evidence file, annually, not once. A model asked to write it from memory will produce a fluent document citing articles that do not say what it claims, which is worse than no document at all.

THE PRODUCT

Compliance packs, retrieved not recalled.

WHO BUYS IT

Compliance consultancies and EU deployers · per assessment, then a retainer



Five systems classified, four by rule at zero cost, and zero unsourced claims

Four moves, in this order

1 Retrieve the law

The model never recalls an article. It resolves one from a pinned, versioned corpus, and a citation that does not resolve raises instead of finding the nearest match.

2 Decide by rule where the law is a list

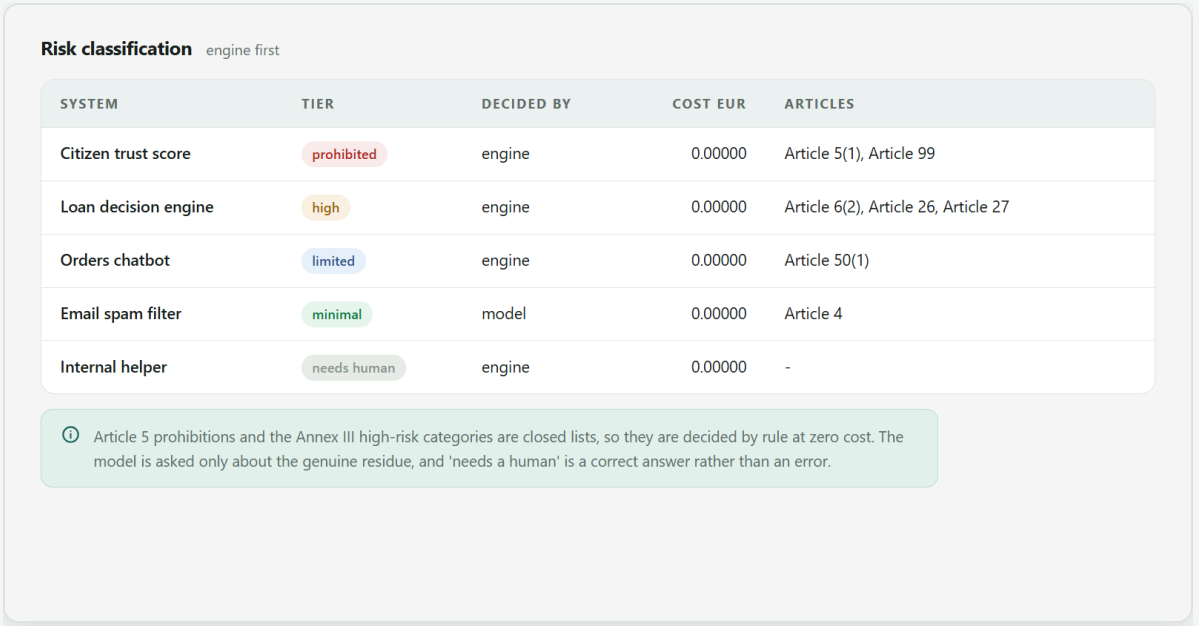
Article 5 prohibitions and the Annex III high-risk categories are closed lists, so they are settled in code at zero cost.

3 Generate, verify, strip

A claim survives only if its evidence resolves, its article resolves, and a separate verifier agrees the evidence supports it.

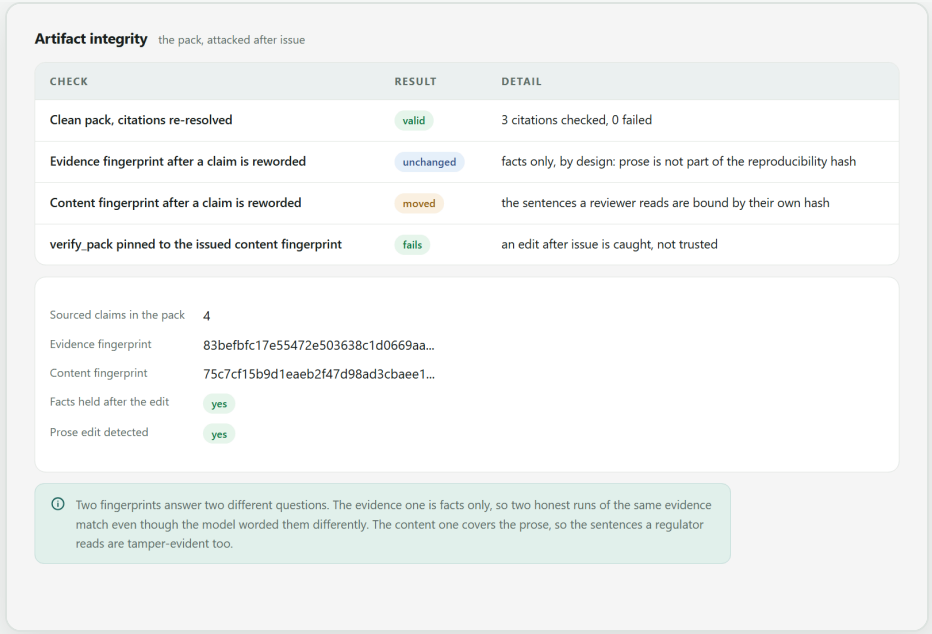
4 Make it tamper-evident

Two fingerprints: one over the facts for reproducibility, one over the prose, so an edit after issue is detected.



Prohibited, high, limited, minimal, and 'needs a human' as a correct answer

Compliance packs, retrieved not recalled.



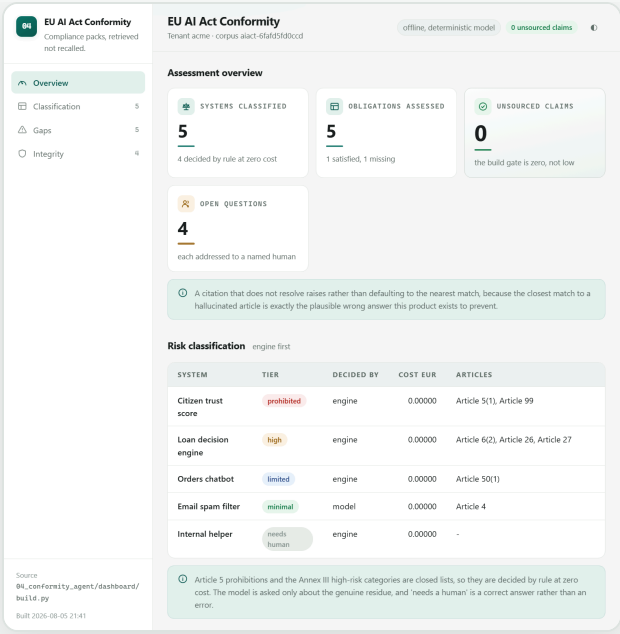
Artifact integrity the pack, attacked after issue

CHECK	RESULT	DETAIL
Clean pack, citations re-resolved	valid	3 citations checked, 0 failed
Evidence fingerprint after a claim is reworded	unchanged	facts only, by design: prose is not part of the reproducibility hash
Content fingerprint after a claim is reworded	moved	the sentences a reviewer reads are bound by their own hash
verify_pack pinned to the issued content fingerprint	fails	an edit after issue is caught, not trusted

Sourced claims in the pack	4
Evidence fingerprint	83befbfc17e55472e503638c1d0669aa...
Content fingerprint	75c7cf15b9d1eaeb2f47d98ad3cbaee1...
Facts held after the edit	yes
Prose edit detected	yes

Two fingerprints answer two different questions. The evidence one is facts only, so two honest runs of the same evidence match even though the model worded them differently. The content one covers the prose, so the sentences a regulator reads are tamper-evident too.

The finished pack attacked: a claim edited after issue is caught by the content fingerprint



EU AI Act Conformity
Compliance packs, retrieved not recalled.

Overview
Classification 5
Gaps 5
Integrity 4

EU AI Act Conformity
Tenant acme · corpus aiact-6fafd5fd0ccd
offline, deterministic model · 0 unsourced claims

Assessment overview

SYSTEMS CLASSIFIED: 5 — 4 decided by rule at zero cost
OBLIGATIONS ASSESSED: 5 — 1 satisfied, 1 missing
UNSOURCED CLAIMS: 0 — the build gate is zero, not low
OPEN QUESTIONS: 4 — each addressed to a named human

A citation that does not resolve raises rather than defaulting to the nearest match, because the closest match to a hallucinated article is exactly the plausible wrong answer this product exists to prevent.

Risk classification engine first

SYSTEM	TIER	DECIDED BY	COST EUR	ARTICLES
Citizen trust score	prohibited	engine	0.00000	Article 5(1), Article 99
Loan decision engine	high	engine	0.00000	Article 6(2), Article 26, Article 27
Orders chatbot	limited	engine	0.00000	Article 50(1)
Email spam filter	minimal	model	0.00000	Article 4
Internal helper	needs human	engine	0.00000	-

Article 5 prohibitions and the Annex III high-risk categories are closed lists, so they are decided by rule at zero cost. The model is asked only about the genuine residue, and 'needs a human' is a correct answer rather than an error.

Source 04_conformity_agent/dashboard/build.py
Built 2026-08-05 21:41

The full assessment in one screen

Zero unsourced claims
a structural gate, not a target

Decided by rule at zero cost
the model is asked only about the residue

Tamper-evident prose
an edit after issue fails verification

05 · AGENT COMMERCE · WHAT IT IS

Agentic checkout is arriving through three incompatible protocols.

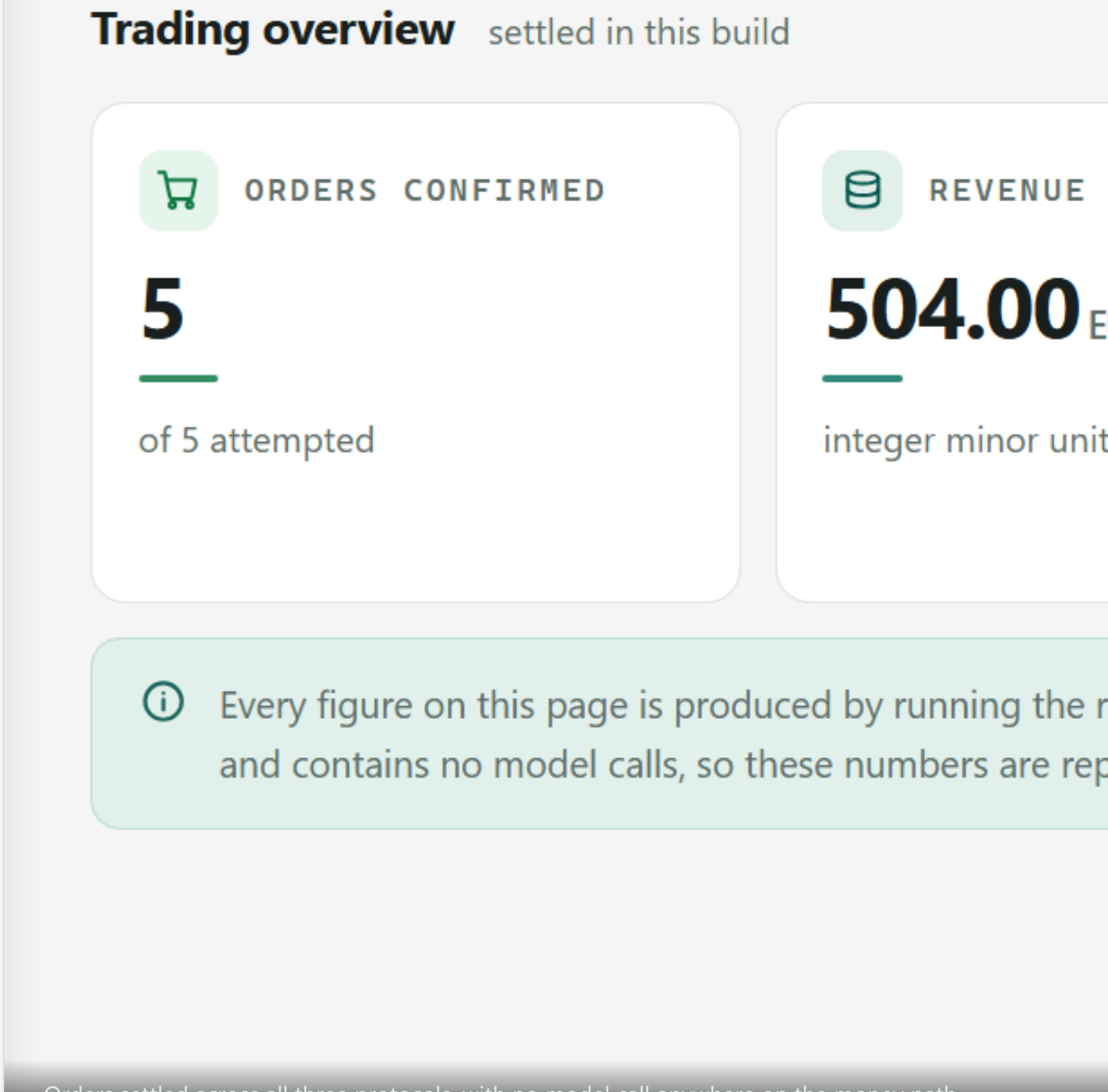
AP2, x402 and ACP each cover a different part of the purchase, and none has won. A merchant that picks one bets the integration on an unsettled outcome; a merchant that lets an autonomous buyer negotiate price without structural limits gets exactly the sale it deserves.

THE PRODUCT

A merchant that agents can buy from, safely.

WHO BUYS IT

Merchants and platforms selling to autonomous buyers · per transaction, or licensed



Orders settled across all three protocols, with no model call anywhere on the money path

Four moves, in this order

1 **One interface, three protocols**

AP2, x402 and ACP are adapters onto four moves every protocol must support: state the price, present an authorisation, verify, settle.

2 **Price in code**

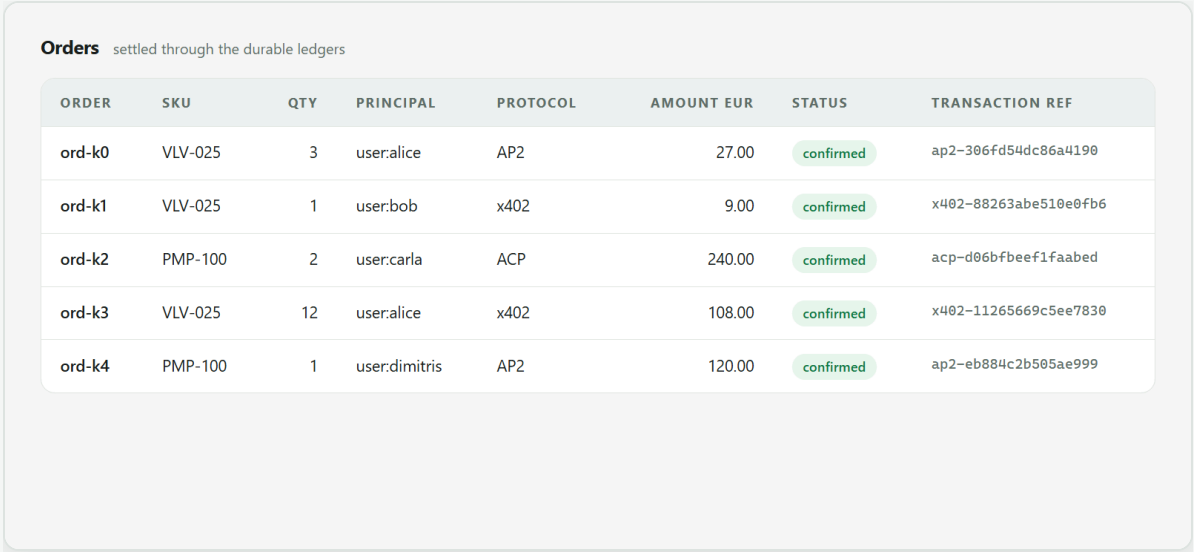
A margin floor is max(discounted, floor) in integer minor units, so no discount at any customer class can produce a below-floor price.

3 **Verify before money moves**

The mandate must be signed, unexpired, within its ceiling, bound to this quote, and its nonce unspent.

4 **Settle onto durable ledgers**

Nonces, settlements, holds, redemptions and orders all outlive the process, which is what makes the guarantees survive a restart.



Orders settled through the durable ledgers

ORDER	SKU	QTY	PRINCIPAL	PROTOCOL	AMOUNT EUR	STATUS	TRANSACTION REF
ord-k0	VLV-025	3	user:alice	AP2	27.00	confirmed	ap2-306fd54dc86a4190
ord-k1	VLV-025	1	user:bob	x402	9.00	confirmed	x402-88263abe510e0fb6
ord-k2	PMP-100	2	user:carla	ACP	240.00	confirmed	acp-d06bfbeef1faabed
ord-k3	VLV-025	12	user:alice	x402	108.00	confirmed	x402-11265669c5ee7830
ord-k4	PMP-100	1	user:dimitris	AP2	120.00	confirmed	ap2-eb884c2b505ae999

Five orders settled across AP2, x402 and ACP behind one interface

A merchant that agents can buy from, safely.

Zero-tolerance defences each attack actually executed

DEFENCE	ATTACK EXECUTED	LEGITIMATE FIRST	ATTACK	WHY IT FAILED
Mandate replay	a captured mandate re-presented	confirmed	BLOCKED	mandate rejected: authorisation nonce already spent (replay)
Double charge across restart	same signed quote, fresh mandate and key	confirmed	BLOCKED	quote rejected: quote already redeemed (single use)
Oversell across restart	second buyer for the last unit	confirmed	BLOCKED	insufficient stock to fulfil the order
Below-floor quote	maximum stacked discount requested on PMP-100	confirmed	BLOCKED	the stacked discount asked for 60.00; the clamp shipped 92.00, the 92.00 floor

⚠ Each attack is run here, not described. Every one of these succeeds if its defence is removed, which is what makes

Four zero-tolerance attacks executed here and refused, each across a restart

Adversary campaign deterministic attacker, no model

ATTACK FAMILY	OUTCOME	WHY
Price mapping	blocked	the floor clamp yields no below-floor quote at any discount
Threshold split	blocked	cumulative spend routed to approval at threshold 2000
Stock recon	accepted_with_alert, alerted	probing throttled after 5 probes; recon is bounded and alerted
Mandate replay	blocked	the replayed nonce was refused
Injection via notes	blocked	notes are inert; only structured fields reach pricing
Quote race	accepted_with_alert, alerted	no oversell; holds capped at sellable 30, freed by expiry

ⓘ 4 of 6 families blocked outright; the rest are accepted-and-alerted, which is a legitimate outcome. Every family handled: True. 'Not considered' is not an outcome.

The adversary campaign: every family blocked, or accepted and alerted

Oversell, double charge, replay
all refused, including across a restart

No model touches money
the whole path is deterministic

Every transaction disputable
hash-chained and merchant-signed

06 · RETAIL ERP SUITE · WHAT IT IS

A retailer's real numbers live in six tools that disagree.

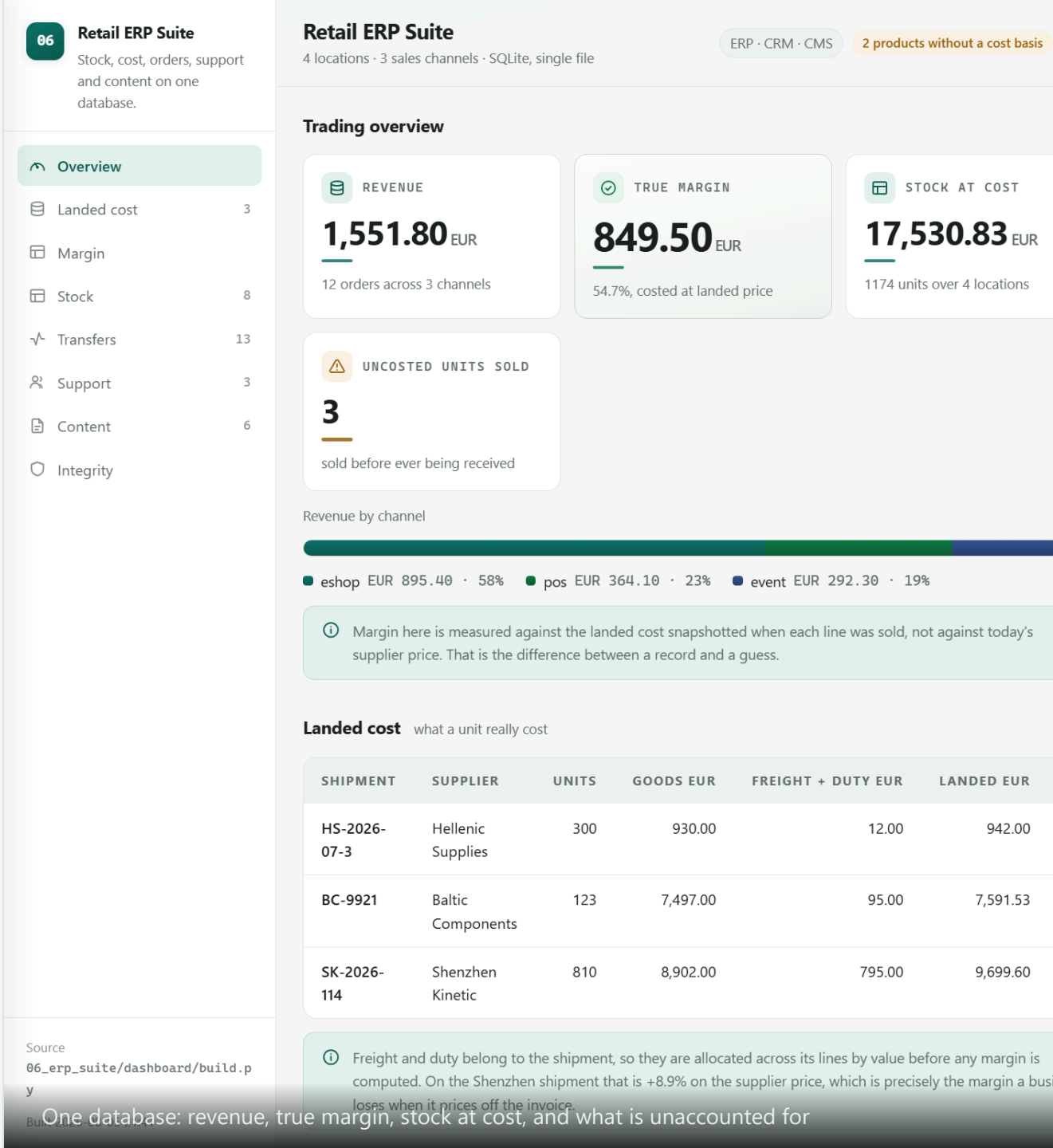
Stock is in one screen, the supplier invoice in another, POS takings in a third, and the support inbox somewhere else entirely. Nobody can answer what a unit actually cost or what the month actually made, because no single system holds both halves.

THE PRODUCT

Stock, cost, orders, support and content on one database.

WHO BUYS IT

Independent retailers and small chains · per location, per month



One database: revenue, true margin, stock at cost, and what is unaccounted for

Four moves, in this order

1 Land the cost, then price

Freight and duty belong to a shipment, so they are allocated across its lines by value. On one shipment here that is +8.9% on the supplier price, which is exactly the margin lost by pricing off the invoice.

2 Derive stock, never store it

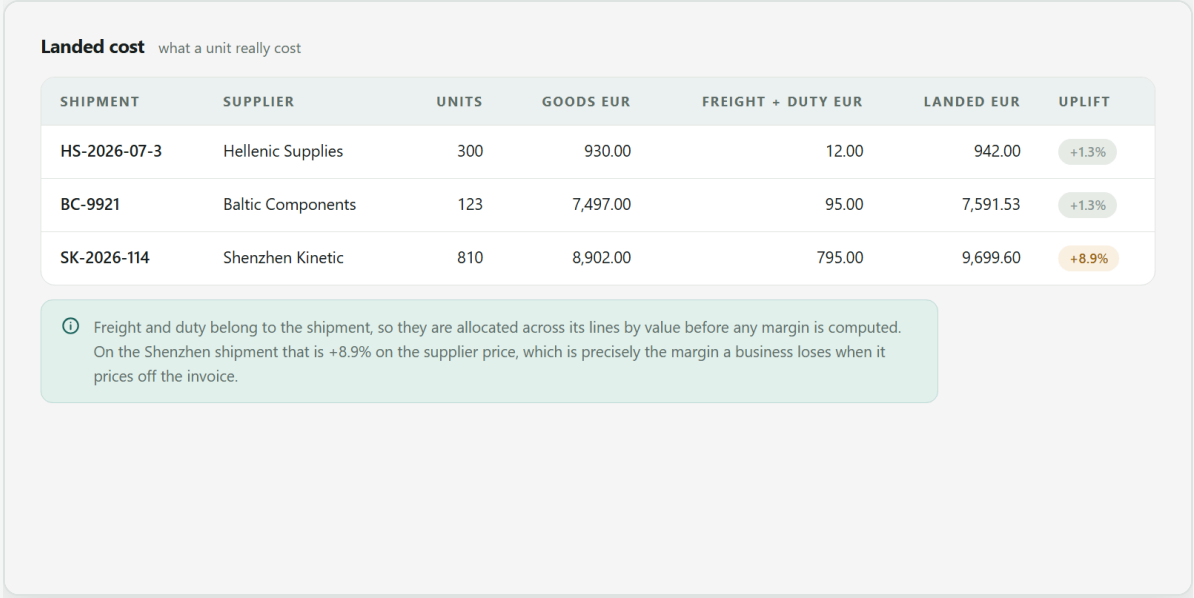
There is no quantity column. Stock is the sum of an append-only movement ledger, so every unit traces back to the reception, sale or transfer that produced it.

3 Move stock as two events

A transfer leaves the source when picked and arrives days later, so units are never counted in two places. Cancelling keeps the row and requires a reason, enforced by the schema.

4 Sell into one order book

Eshop, POS and events are one ledger, each line costed at the landed price snapshotted at the moment of sale.



Landed cost per shipment: what the supplier billed against what the units actually cost

Stock, cost, orders, support and content on one database.

Stock across locations derived from the movement ledger

PRODUCT	COLLECTOR CENTER	EVENTS	ICONNECT	WAREHOUSE	IN TRANSIT	TOTAL
HDMI 2.1 cable, 2m	86	0	147	160	0	393
Card sleeves, 100 pack	0	43	220	0	0	263
65W GaN charger	0	0	67	110	20	197
USB-C Hub, 7 port	24	0	38	55	0	117
SD card reader, UHS-II	0	0	27	60	0	87
NVMe SSD 1TB	0	0	21	36	0	57
Aluminium laptop case 13"	17	0	11	15	0	43
Thunderbolt 4 dock	0	0	5	12	0	17

There is no quantity column anywhere in this database. Every number above is the sum of an append-only movement ledger, so any figure can be traced to the reception, sale or transfer that produced it.

Stock across four locations, derived from the movement ledger, with in-transit separated

Transfers between locations two events, never one

REF	PRODUCT	QTY	ROUTE	STATUS	REASON / ARRIVAL
TR-12	65W GaN charger	20	warehouse → collector_center	in transit	picked, not yet arrived
TR-13	NVMe SSD 1TB	10	warehouse → events	cancelled	Event cancelled by the organiser (katerina)
TR-11	Card sleeves, 100 pack	80	iconnect → events	fulfilled	2026-07-18
TR-9	Thunderbolt 4 dock	6	warehouse → iconnect	fulfilled	2026-07-13
TR-8	Aluminium laptop case 13"	12	warehouse → iconnect	fulfilled	2026-07-13
TR-7	Aluminium laptop case 13"	18	warehouse → collector_center	fulfilled	2026-07-13
TR-4	NVMe SSD 1TB	24	warehouse → iconnect	fulfilled	2026-07-12
TR-10	SD card reader, UHS-II	30	warehouse → iconnect	fulfilled	2026-07-10
TR-6	HDMI 2.1 cable, 2m	90	warehouse →	fulfilled	2026-07-10

Transfers as two events, and a cancellation that kept its reason and its history

Margin measured, not estimated
landed cost, snapshotted at sale

Missing cost is reported
never silently read as 100% margin

SQLite, one file
no server, no migrations to run

HOW THEY ARE BUILT

The same four rules in all five

A deterministic core, a model only at the edges

Pricing, policy, classification and reconciliation are code. The model parses language and explains results; it never decides something that has a right answer.

Measured, not asserted

Every figure on these screens is produced by the product's own code and re-verified by its test suite. The suites redden under mutation, so green is evidence.

Structural defences, not instructions

The margin floor, the replay nonce, the tenant scope and the durable ledgers are code a prompt cannot be talked out of. They hold when detection fails.

Extended by the client, not by us

Capabilities are files, not deployments. A non-engineer adds a platform, a skill or a research source and it is live on the next request.

WHAT THIS SHOWS

The hard part is not the model.
It is everything around it.

Any of these can go to a first customer as it stands: the interfaces are real, the rules are enforced in code, and every figure on every screen comes from running the system. The next step for any one of them is a pilot against live data.

Deterministic where it counts
money, policy, law, arithmetic

Extensible by the client
capabilities are files, not deployments

Auditable by default
every decision traced and replayable