Attackers don't read your CMDB.
They find what's actually there.

Stay ahead of adversaries with one complete asset inventory, **built from the security tools you already run**, mapping what's reachable from the internet and from inside.

ANSWERING WHAT NO SINGLE CONSOLE CAN

01 RECONCILE

What the CMDB never knew about

Your CMDB isn't wrong because your team is careless. It's wrong because it waits on people, and reality doesn't wait for a change ticket.

- **The records that were never created.** Devices your tools see daily that skip every process, because nothing exists to trigger one.
- **The records that outlived the hardware.** Nothing has seen them in months, so they age out on a threshold you set.
- **Disagreements shown, not settled in silence.** Two sources, two owners, both attributed — nothing overwritten by whichever system synced last.
- **It stays true on its own.** Refreshed from live tool data rather than from anyone's discipline.

02 ATTACK SURFACE

Shadow IT, and what else is reachable

An inventory is only useful if it tells you what can be touched. KeyCaliber covers both directions and lands them on the same assets.

- **Your internet-facing footprint, found from the outside in** — including the hosts nobody mentioned standing up.
- **Exposed services as ranked findings** on named assets, so the list arrives already sorted by what's worth doing.
- **Shadow IT with a name attached.** Devices visible in traffic or sign-in activity that have no security tool coverage at all.
- **What one machine can reach.** Who signed in, what it talked to, and what an intruder could pivot to from that seat.

03 EVIDENCE

How do you know it's right?

Producing a list is the easy half. Whether the data is current and accurate is what creates the operational value.

- **Provenance on every line** — the source behind each fact and how confident it is. The difference between a record and evidence.
- **Owner, location, classification and criticality** on each asset, plus your own tags for whatever else is in scope.
- **"How is it kept current?" answered by design.** Refreshed on a schedule, stale records aged out on your policy.
- **Slice it and hand it over.** Filter and export by scope, business unit, environment or location, the day it's asked for.

Why individual tools can't provide the full picture

Ask three teams how many assets you have and you'll get three numbers. **Each is right about its own question.** None of them is answering yours.

THE QUESTION	CMDB	ENDPOINT AGENT	VULNERABILITY SCANNER	KEYCALIBER
What was previously documented?	•	—	—	•
What is the agent installed on?	—	•	•	•
What is exposed to the internet?	—	—	•	•
Where is the Shadow IT that no tool manages?	—	—	—	•
Which records are stale?	—	—	—	•
Where did each answer came from?	—	—	—	•

Why the asset question came back

Examiners and underwriters stopped taking your word
NYDFS now expects a documented inventory of all assets with a stated validation cadence. Insurance carriers verify what applicants attest to, and partial counts as none.

AI landed on assets you have to name
Models, runtimes and copilots run somewhere. Governing them starts with an inventory that includes the machines nobody tracks.

Observed, not declared
Built from what your tools see, not what someone entered.

One list, every tool
One asset universe. Sources never silently overwrite each other.

Auditable by design
Every fact shows the source behind it.

Nothing to deploy
Read-only. No agent, no proxy, no appliance.