PART OF THE KAI AUTONOMOUS DEFENSE PLATFORM

Cyber Asset Attack Surface Management

Every asset owned. Every gap surfaced.

Every decision downstream depends on the asset record being right. Get the owner, the environment or the business application wrong, and the fix goes to the wrong team or gets worked at the wrong priority.

55% of CISOs already let machines discover and inventory assets without approval

30,000 shadow assets surfaced agentlessly in a single customer estate

4% to 92% ownership coverage across 250,000 assets in under twelve hours

Reported by 500 chief information security officers at enterprises above $500 million in revenue.

01 · THE PROBLEM

An alert without an owner is not fixed

Your endpoint tool, scanner, cloud posture tool and CMDB each believe they hold the asset inventory. None agree, so you get four partial inventories with no shared identity.

The bigger gap is ownership. A finding without an owner goes to the nearest queue, is reassigned once or twice, and ages out.

02 · THE SOLUTION

One asset record, with an owner on every finding

Kai rebuilds each asset from evidence across your tools and names the accountable owner, so every fix routes first time.

03 · USE CASES

Asset inventory and ownership attribution
Each asset rebuilt from Intune, Entra ID, EDR, scanners, cloud and CMDB, with owner, business application and environment.
Findings reach the people who can act.

Coverage gap discovery
Sources checked against each other, and missing EDR or scanner coverage raised as a finding.
Coverage numbers mean what they say.

04 · HOW KAI DOES IT

Four inventories, one owned record

Four sources, one asset
CMDB, endpoint, cloud tags, logins and tickets reconciled into a single record.

Ownership in three tiers
Business application, then business unit, then location, each with its source.

Inferred owners are labeled
Where sources conflict, the inference is labeled rather than promoted to fact.



The asset inventory in Kai: every asset with its risk, findings, environment and EDR coverage. Sample data.

05 · OUTCOMES

4% to 92%
ownership coverage across 250,000 assets, in under twelve hours

30,000
shadow assets surfaced agentlessly in a single estate, without a scan

One record
read by exposure management, remediation and detection, with no second inventory

What you can trust, and what you can hand your CISO

Every change carries its evidence
The rollback path and the proof that justified it are recorded with the change, not in somebody's memory.

Every removal carries a reason
A finding cut from the queue carries a written reason you can defend in an audit.

The boundary is enforced
You set where Kai may act, per environment, asset class and change type. Outside it, nothing moves without a person.

Nothing deployed to start
Agentless and read only against the sources you already run. SOC 2 Type II. Nothing is replaced.

06 · IN PRACTICE

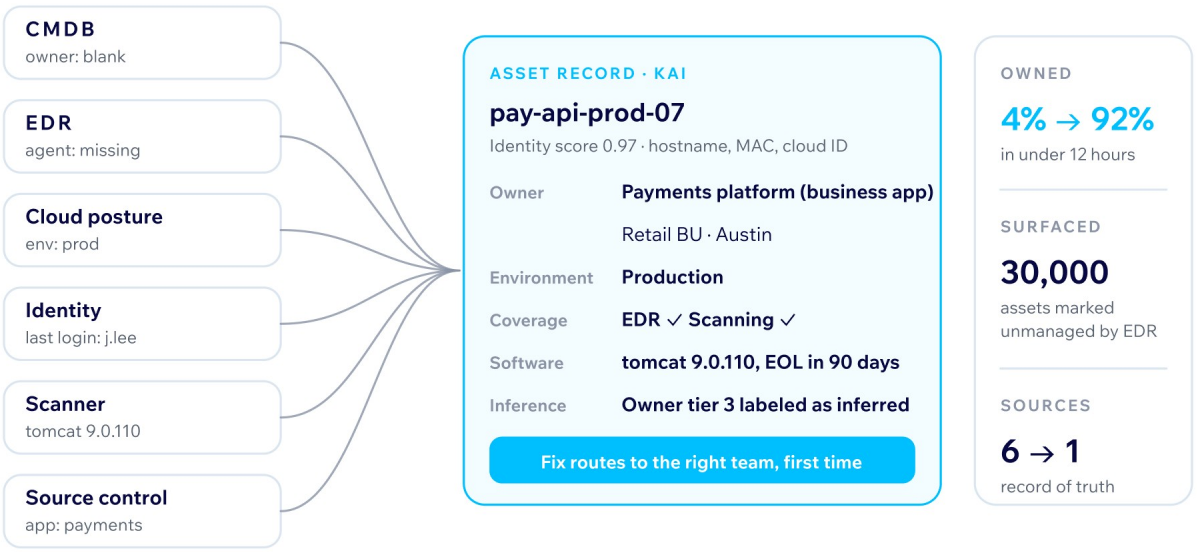
From four inventories to one record

Every tool you run believes it holds the inventory, and none of them agree. Kai interrogates the sources once, rebuilds the asset from evidence, and ownership and coverage gaps come out of the same record.

Cyber Asset Attack Surface Management

One record, rebuilt from evidence

250,000 ASSETS



Identity resolves by scored correlation across hostname, hardware address, cloud resource ID, network address and region. Ownership resolves in three tiers and is corroborated by login and ticket history. Any inference is labeled as one.

> Tool sprawl and integrations are a tax on everything we do. The ROI is consolidation: fewer point tools, fewer brittle integrations, and one platform that can reason across our data and drive action.
>
> SECURITY LEADER, KAI CUSTOMER

07 · WHAT KAI DOES

What Kai does that an inventory cannot

01 Rebuild the record from evidence.
Every source interrogated and the asset rebuilt from evidence. The CMDB is one opinion.

02 Attribute ownership in three tiers.
Business application, unit and location, backed by last login and ticket history.

03 Label the inference.
Where sources conflict, Kai states what it inferred and why, so 92% is usable.

04 Surface shadow assets without an agent.
Unmanaged assets, and assets no tool reports, brought into the record the same way.

05 Raise coverage gaps as findings.
A missing agent or scanner is an exposure, so coverage numbers mean what they say.

06 Serve one record downstream.
Exposure, validation, remediation and detection share one asset, so ownership is solved once.

Find out who owns your estate.

Connect the asset sources you already run. We will rebuild the record and show you the owners, environments and blind spots your current inventory cannot resolve.

Agentless, read only to start. No CMDB cleanup first. Ownership inside twelve hours. kai.security

Get a demo