PART OF THE KAI AUTONOMOUS DEFENSE PLATFORM

External Attack Surface Management

See your environment as an attacker would.

Type your company name. Kai finds what you expose, attributes it with evidence, and puts every exposure in one queue with your internal findings.

1	company name is all it takes to discover exposures
0	packets sent to your assets during passive discovery
1	queue for internal and external exposures, prioritized together

01 · THE PROBLEM

The outside view lives in a silo

Most organizations watch the external surface with a separate EASM tool, its own list and scores, matched by hand to internal data. Discovery happens. The fix often doesn't.

Meanwhile the surface keeps moving: old subdomains, acquired sites, unreviewed APIs and forgotten AI services. Attackers start from the outside and work in.

02 · THE SOLUTION

Your external surface, in the same record

From a company name, Kai finds what you expose, and every exposure lands in the same queue, owner and workflow as everything else.

03 · USE CASES

Start from a company name
Kai lists the entity and its subsidiaries, each with source, evidence and confidence.
Nothing is in scope until you tick it.

Scanning that stays in scope
Passive sends no packets. Active scanning needs a signed authorization.
Every request passes one scope gate.

APIs and exposed AI
API specs, LLM endpoints, MCP servers and leaked keys, found from outside.
See what you expose online.

Exposures into Kai
Each exposure lands in Kai with its rule and evidence, matched to known assets.
Prioritized, owned and tracked to SLA.

04 · HOW KAI DOES IT

From discovery outside to the fix inside Kai.

FROM THE OUTSIDE

1 **Discover**
From a company name, passively, each asset attributed with evidence.

2 **Assess**
Technology, APIs and exposed AI checked against rules, with evidence.

3 **Validate**
Safe, non destructive proof an exposure is real.

IN KAI

4 **Consolidate**
External exposures join Kai's record with your internal findings.

5 **Score**
Prioritized with the owner and business context Kai already holds.

6 **Remediate**
Routed to the owner through the remediation workflow you run.

05 · OUTCOMES

0 packets

sent to your systems in passive discovery, with every source recorded per run

6 views

of one attack surface map, from tiers and domains to paths and orbit

1 record

external exposures in Kai's finding model, prioritized with internal findings

What you can trust, and what you can hand your legal team

Scope is signed and enforced
Every scanner and adapter passes one scope gate before anything reaches a target.

Egress is pinned
Targets are re-resolved and IP-pinned, blocked ranges refused, requests rate-limited.

The record can't be rewritten
Findings and the audit log are append-only; evidence is stored by content hash and can be verified later.

Single-tenant
Your surface data stays apart from every other customer's. Nothing to install on your network.

06 · WHAT KAI DOES

Six things you can see from the outside

01 Attribution you can audit.
Each asset linked to you with a confidence score and evidence. Weak matches are held back.

02 API contracts, not just hosts.
OpenAPI, Swagger and GraphQL specs parsed into the individual endpoints they expose.

03 Exposed AI infrastructure.
LLM endpoints, MCP servers, vector databases and leaked AI keys, with secrets redacted.

04 Services read, never probed.
Ports, banners and versions from internet scan data. Zero packets reach your estate to find them.

05 Exposures with receipts.
TLS, email, takeover, CVE and end of life rules. Each exposure names its rule and data.

06 One map, six views.
Six layouts, from tiers and domains to orbit, show the same assets in every view.

> Attackers don't need an asset inventory. They start from the outside and work in. Kai now starts there too, and hands what it finds to the workflow that fixes everything else.
>
> KAI EXTERNAL ATTACK SURFACE MANAGEMENT

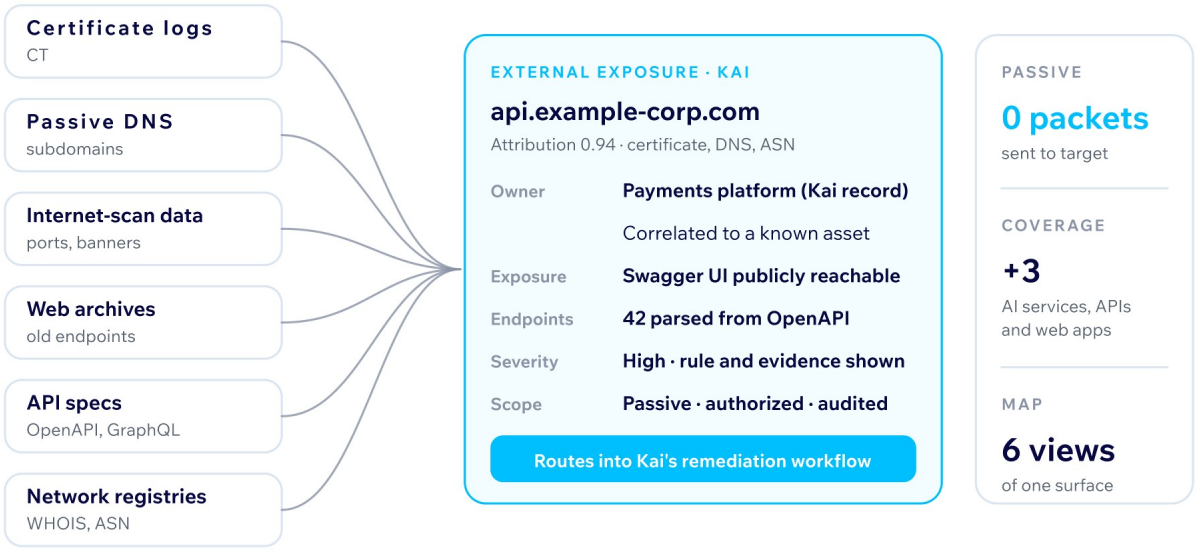
07 · IN PRACTICE

From the internet to the fix, in one platform

A standalone EASM stops at a list. Kai discovers and attributes your internet-facing assets, ranks what attackers use, and hands every external exposure to the workflow that prioritizes and fixes everything else.

External Attack Surface Management

From internet entry point to fix



Attribution uses certificate transparency, passive DNS and internet-scan data, with the reasoning shown. Example data is illustrative.

See your attack surface the way attackers do.

Give us your company name. We will map your internet-facing assets and show you the exposures and blind spots your current tools miss, in the same place you fix everything else.

Passive by default. Scope authorized before anything is scanned. kai.security

Get a demo