You can't protect what you can't see.

KeyCaliber turns the security tools you already own into one clear picture: **every asset you have, every AI tool in use, every gap in your defenses, and what to fix first.**

Everything you own

One trustworthy inventory of every device, server and cloud workload, including the ones nobody registered and no security tool is watching.

Discover Shadow IT proactively, not after it turns into an incident.

Every AI in use

The AI tools your people actually use — web apps, models running locally on laptops, and AI features quietly switched on inside software you approved before AI went mainstream.

Answer your organization's AI questions with automated evidence instead of a manual survey.

What actually matters

Your critical assets (Crown Jewels) empirically identified based on how the systems actually behave. Not from a spreadsheet last updated two years ago.

See business context for every asset, without a tagging project or a workshop series.

Where you're exposed, in a ranked list

One honest number for how protected you actually are, and a ranking ordered by how much risk each fix removes. Patching, missing coverage, and ungoverned AI on one scale.

Work with a defensible figure for the board, and a short list your team can justify and handle.

Your EDR sees endpoints. Your cloud tool sees cloud. Your vulnerability scanner sees vulnerabilities. Your CMDB is out-of-date.
KeyCaliber reads all of them and answers the questions none of them can:
what's important, what's missing, and what AI is running on it

WHY THIS MATTERS NOW

64%
of organizations lack complete visibility into their IT estate

69%
have no accurate view of the AI software they already pay for

40%
of enterprise apps will have AI agents built in by end of 2026

17%
of IT assets are invisible to vulnerability management tooling

WHAT MAKES KEYCALIBER DIFFERENT

01
Ranked by business impact

Every finding arrives attached to what the asset is worth, so “unauthorized AI” becomes “unauthorized AI on the unpatched critical payroll server”.

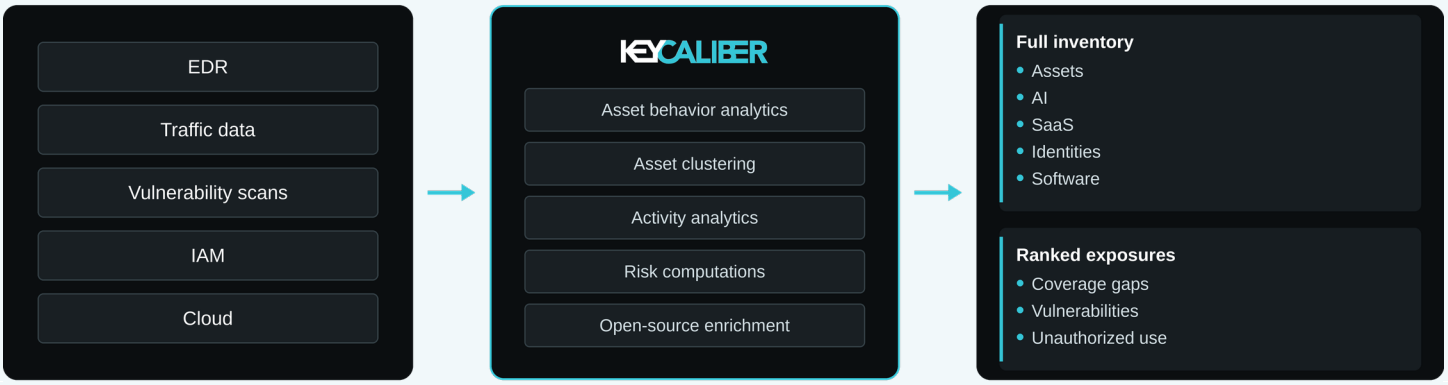
02
Shadow AI uncovered

Discover local AI runtimes on workstations and AI features quietly switched on inside apps you already approved – the places browser, gateway, and SaaS tools all miss.

03
Honest by design

Every attribution carries the signal that produced it and every score breaks down into the factors behind it, so findings can be checked and are defensible.

HOW IT WORKS



QUESTIONS YOU CAN FINALLY ANSWER

- → Which of our critical systems have no endpoint protection?
- → Who is using AI that has not been authorized?
- → Is anyone running AI models locally on a company laptop?
- → Which approved vendors switched on AI without telling us?
- → What's actually on our network that is unmanaged?
- → Which ten things should we fix this week and why?
- → Can we hand an auditor a complete AI inventory today?
- → Did last quarter's security spending change our risk posture?

See your own environment in 30 minutes.

Connect your endpoint tool and traffic or vulnerability scanner data. So far, every trial has surfaced AI and/or unmanaged machines the customer didn't know were there!

keycaliber.com
hello@keycaliber.com