



You bought the tools. Now get everything you paid for.

See a full asset inventory and security coverage analysis for every asset in it.

READ-ONLY API ACCESS • NO AGENT • NO PROXY • NO APPLIANCE • NOTHING INSTALLED ON A SINGLE MACHINE

ANSWERING THE QUESTIONS YOUR INDIVIDUAL DASHBOARDS CAN'T

01

What Shadow IT exists

One asset list from the tools you already run, checked against every control you expect to find: endpoint, vulnerability, device management, cloud, identity, and more.

- **The assets no tool manages at all.** Devices that show up in network, DNS or sign-in activity and in no management console — nobody owns them, which is why they're still there.
- **A list, not a percentage.** The actual machines missing the actual control, ready to assign and export.
- **A denominator you can defend.** Controls that can't run on a device aren't counted against you. And if a feed goes quiet, you'll know before the number does.

02

What you're paying for twice

Stacks accumulate. Two EDRs after an acquisition, a scanner nobody ever retired, a firewall per business unit. See where you can have overlaps that can be removed.

- ☐ **Two products, one job.** Where two tools in the same category are both live — two EDRs, two vulnerability scanners, two firewalls — with the machines each one holds and the ones running both at once.
- ☐ **How far the migration actually got.** "We're moving off that one" is easy to say. This shows how much of the environment each product still holds, and which machines are keeping the old contract alive.
- ☐ **A neutral referee before the renewal.** A product that uniquely covers 400 machines is a different negotiation from one that duplicates another everywhere. The platform reads every tool and sell you none of them.

03

What to fix now

Four thousand uncovered devices isn't a plan. Gaps arrive ranked by what the affected system is worth, so the work starts where the damage would be worst.

- **Impact first, not alphabetical.** Missing endpoint protection on the payroll system is not the same finding as missing it on a spare test box.
- **Priced by risk removed.** Every recommendation carries the risk it actually takes off the board, so the order survives a budget meeting.
- **Evidence when someone asks.** Board, cyber-insurer, auditor, regulator — one number, the same in every room, with the working underneath it.

Example



Three tools averaging **92%** describe an environment that is **84% actually covered** — and 190 machines nobody is watching at all.

Your tools know some of this. They just aren't telling each other.

Connect two or three of the tools you already run, read-only. You get your own gap list — the systems no tool is managing, the controls that never landed, and the fixes that remove the most risk.

Ranked by business impact

Tied to what the system is worth.

One list, every tool

One asset universe, every tool.

Auditable by design

Every score shows its factors.

Nothing to deploy

Read-only. No agent, no proxy.