

Specto+

NETWORK DEFENSE PLATFORM



X-ray vision for the person in charge.

You are accountable for a network you cannot see. One machine, switched on inside it, and the picture comes back: what is there, what a stranger can reach from outside, and where the picture is thin.

What is on your network—and what was actually checked

It sweeps the network and asks every device it can reach what it is running. Nothing is installed on any of them.

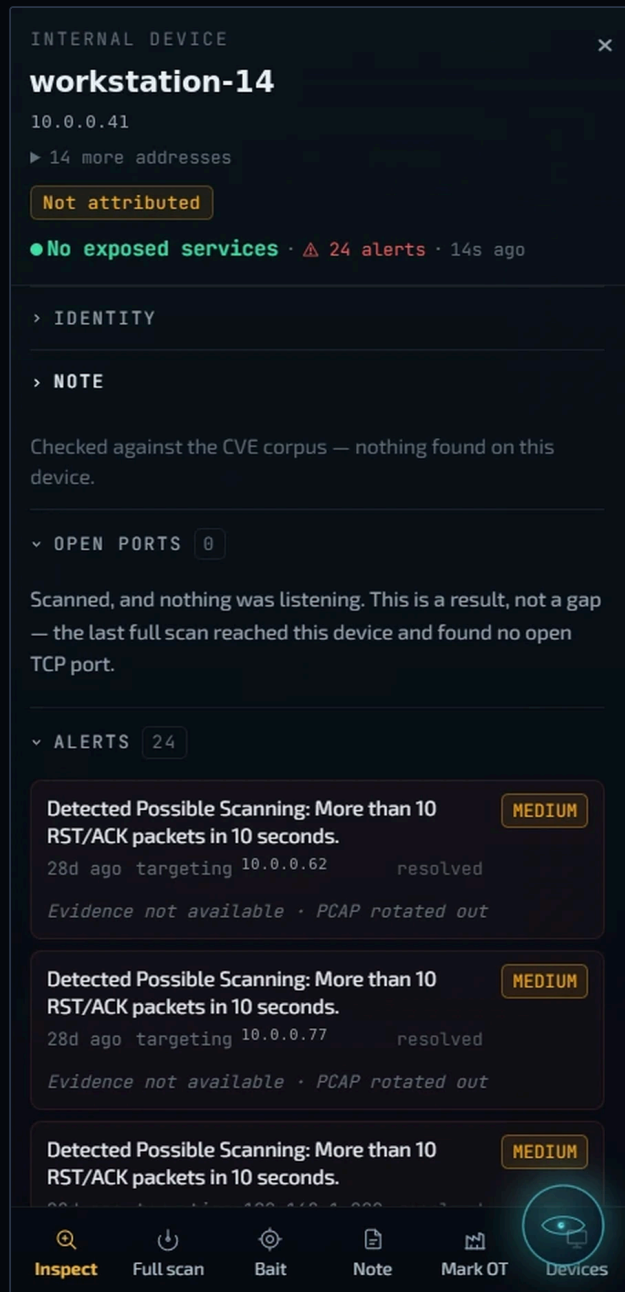
Then it does the thing almost nothing else does. A machine it scanned that had nothing open says “scanned, and nothing was listening – this is a result, not a gap”. A machine it could not reach says that instead, and is never shown to you as clean.

Findings are split the same way. **Proven** means the exact version a machine announced falls inside the affected range of a published vulnerability. That is a proven version match, not proof the machine can be exploited – a backported fix or a configuration can change the answer, so a person confirms before you act. A rough guess is never counted as proven.

WHY THIS MATTERS MORE THAN A SHORT LIST

A report that says nothing was found lets you assume it looked everywhere. You find out it did not when something happens in the part it never reached.

“No problems found” can mean nobody looked.



Which of the three it is · scanned and quiet, needs a person, or not looked at

Machines nobody has any business touching

Specto+ puts decoys on your network. Each gets its own address and network identity, so to every other computer it looks like a separate machine rather than part of Specto+. Nothing is installed anywhere else.

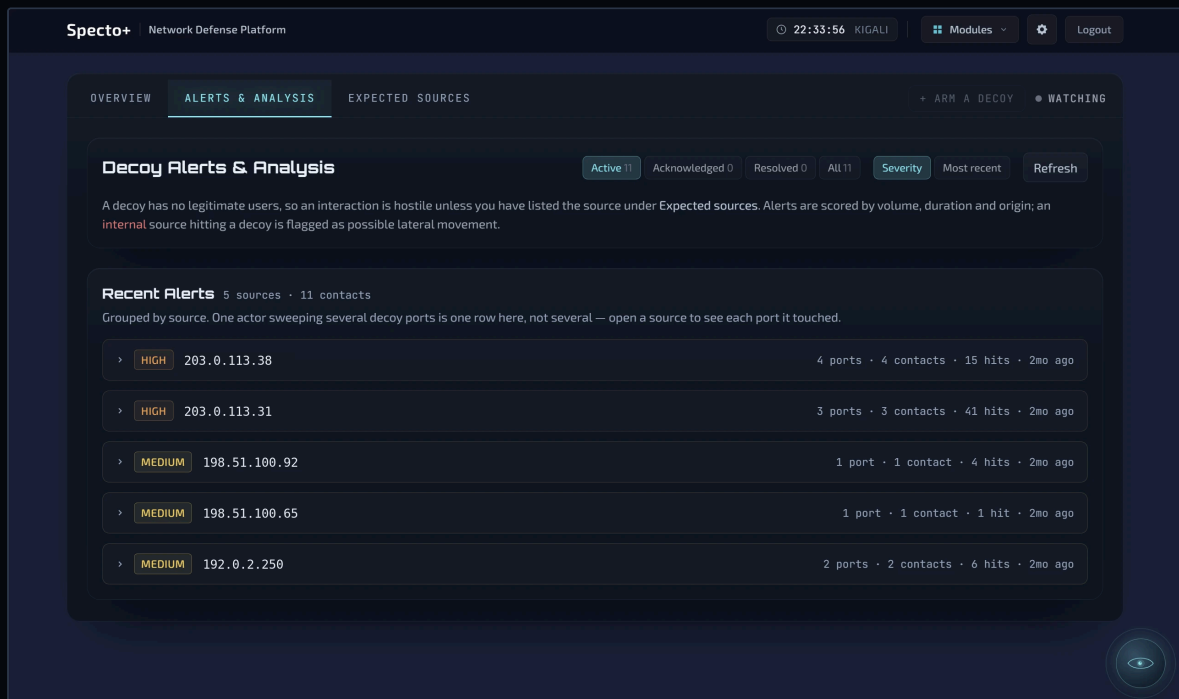
A decoy has no legitimate users. You list your own scanners and inventory tools as expected sources, and everything else that touches one is worth your attention — with the packets kept as evidence of what it did.

MONDAY MORNING

One red line. A laptop in accounts touched the fake file server on Saturday at 02:14. You click it: which laptop, when, and exactly what it sent.

“Nobody in accounts works Saturdays. And nobody knows that server exists.”

A decoy contact appears on the dashboard. It does not send an email or ring a phone. Decoys work on the network the appliance sits on.



Everything that touched a decoy, grouped by source · from the public box we run ourselves

What a stranger can find out about you

Point it at the domains and addresses that are yours and it looks from the outside — from the appliance, out through your own connection — using only what you publish or what your public services answer to anyone who asks. Not from inside, where everything looks reachable.

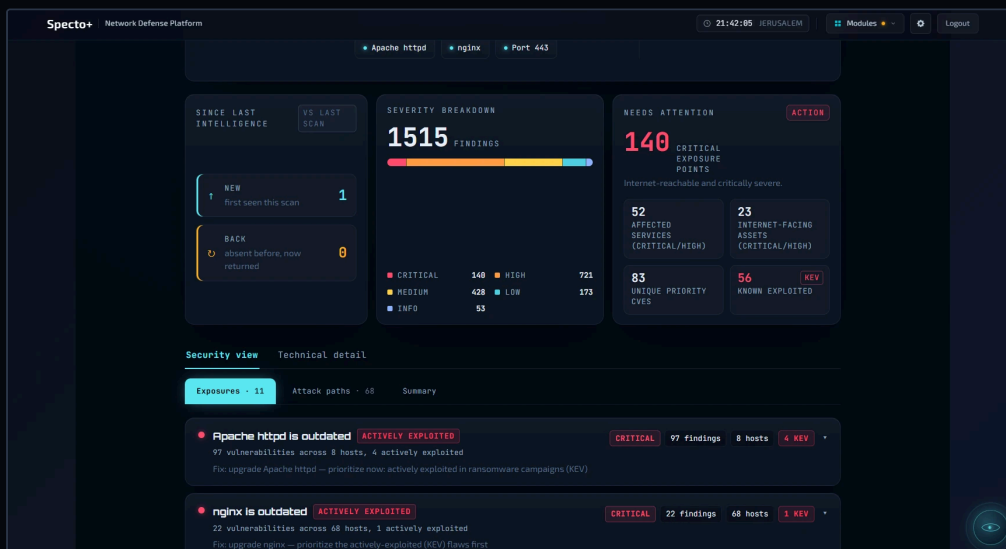
It reads the mail records you publish and tells you **whether they are set to stop someone sending mail in your name** — and whether you are asking receiving servers to reject that mail or merely to note it. Plenty of organizations find out here that they have been asking for a note.

It finds what you left reachable — forgotten repositories, environment files, old backups — and keeps the real response as evidence. **It never runs exploits.** Login-page checks run only if you switch them on, and it tells you exactly what it sent.

IN THE BOARD MEETING

Somebody asks whether you are exposed to the thing that was in the news.

“Two machines match, and we have confirmed both. Patched by Thursday. Eleven we could not check, and here is why.”

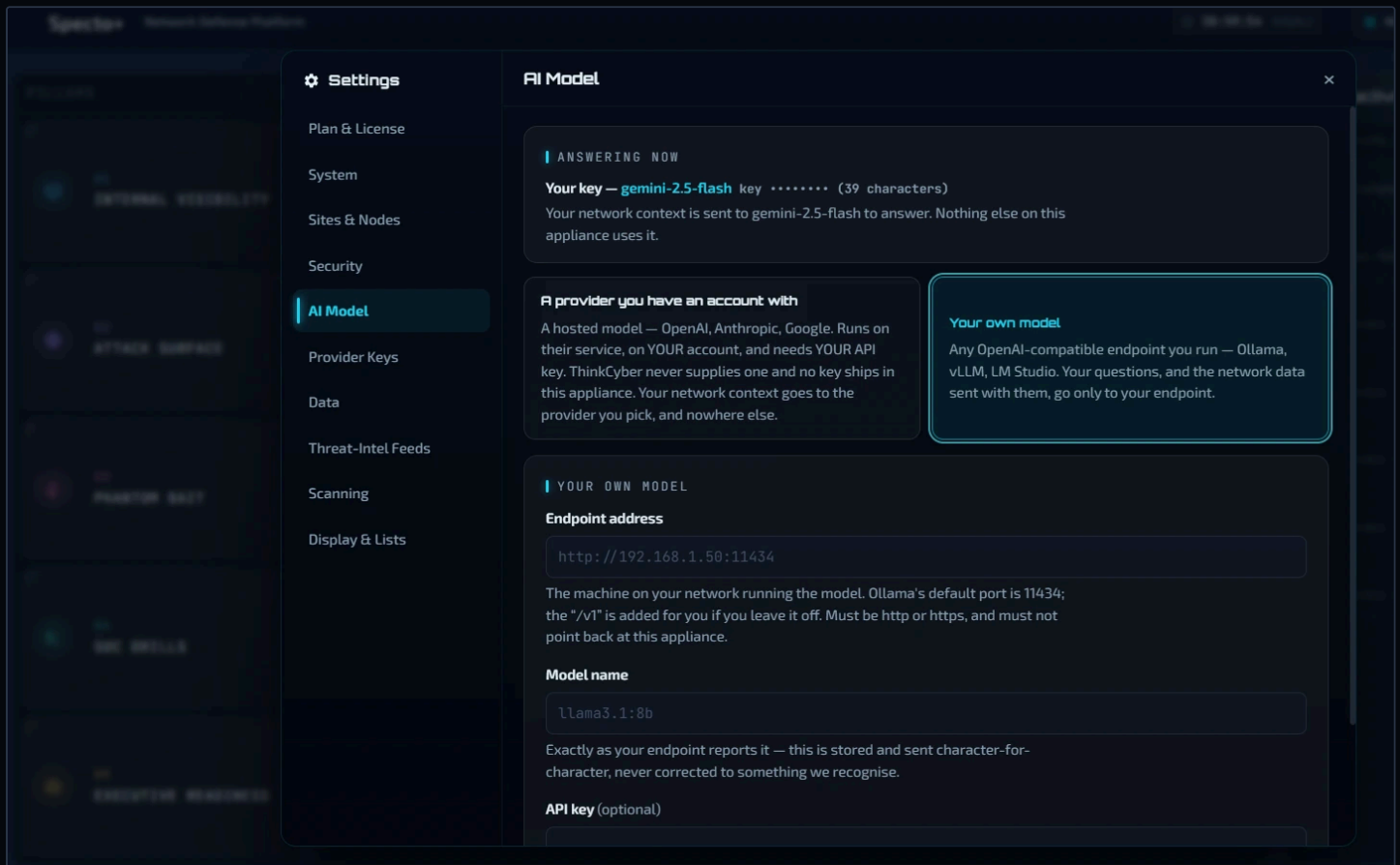


Proven, needs a person, or not checked · known-exploited ones flagged

The AI can run inside your building

Cy answers questions about your network in plain language. It uses whichever model you point it at and has no other destination. Point it at a model on a machine down the hall and nothing about your network leaves the building. Point it at a provider you already have an account with and the context goes to them, on your account, with your key. Running your own model needs a paid licence.

Cy needs a model — yours or a provider's. With neither, it is off. And this is about Cy alone: the external scan reaches out by its nature, and the optional intelligence lookups send your public addresses to whichever of those services you switch on. See [the full list of what leaves the network](#).



The choice, on one screen · no key of ours ships in the software and there is no default

WHAT IS FREE, AND WHAT IS NOT

Every device, free and permanent

Free forever: finding what is on your network, what each device is running, and which of them were actually checked. Every device, no limit. No sign-up, no email address, no license code, no trial clock.

Free includes Cy, with your own cloud AI key. **A paid licence adds** the outside view, the decoy, the exercises and Endpoint Control, and lets Cy use a model you run yourself. It is a yearly licence per box (one box per network), never per device. Try every paid module free for 30 days. To buy, we connect you with your local partner.

You tell it which parts of the network to leave alone – the factory floor, the medical equipment, the controller nobody is allowed to touch. It will not probe them, and it lists them as not assessed rather than counting them as fine.

THE NEXT STEP

Download it free.

Download Specto+ Free (coming soon) and set it up with the wizard; no licence code needed. Try every paid module free for 30 days. To buy, we connect you with your local partner.

WHAT IT NEEDS, IN FULL

RUNS ON

A virtual machine on hardware you own.

NETWORK

A bridged adapter onto the network it watches – not NAT.

FOR DECOYS

The hypervisor must let that adapter use extra hardware addresses.

MIRROR PORT

Optional. Without one, intrusion alerts see only the traffic that reaches the appliance.

REACHES OUT TO

Three public feeds on a schedule – the vulnerability catalog every two hours, the known-exploited list every six, the product dictionary weekly. Nothing else unless you configure it.

SIZING

Comes with the build, measured against your network.