

You were right not to trust auto-remediation.

Tamnoon is the self-healing engine for cloud exposures.
It closes what it can prove is safe.
What it cannot prove, it declines in writing.



What it costs you, in a normal week

One bucket, three tickets.

Three scanners flag the same public bucket, so one problem is three tickets. Merging them is nobody's job.

Nobody knows what it does.

Who owns this instance? What depends on it? Five consoles and a Slack thread with forty-one replies. No answer.

Undone by the next apply.

You tighten a security group in the console. The 02:00 terraform apply puts it back, and the finding reopens.

Why it persists

There is a button in your CNAPP that says Remediate. You have never pressed it. The last person who did closed a "public" bucket at 4:40 on a Friday. It was the origin behind the company website. He is a legend now.

53%

A button that can only act has two settings: dangerous, or off. Most teams pick off and call it caution.

of everything ever detected is still open.

The problem was never automation. It was automation that cannot say no.

What you get instead

An engine you can leave on.

Whatever it can prove safe, it heals on its own, through your change process. Nobody presses anything at 4:40.

Only the no's reach you.

Whatever it cannot prove, it declines in writing, with the evidence. Your morning is the short list, not the queue.

What heals once stays healed.

Changes are written back to IaC, so the next apply keeps them. Say no once, and every finding of that type stays a no.

The five steps, in plain words

- 01

Connect read-only
A guest badge,
not a master key.

Reads your scanners and your cloud. Nothing installed, nothing written.

IN YOUR WORDS
CNAPP integrations · agentless
- 02

It recognizes
142 alerts are
usually one problem.

So it groups them. Then it reads who uses it, what depends on it, who owns it.

IN YOUR WORDS
deduplication · blast radius
- 03

The verdict

SAFE

RISKY

AWAITING DATA

Proven safe, declined in writing, or asked for the one missing thing.

IN YOUR WORDS
evidence on record
- 04

It closes
Your systems,
your keys.

SAFE runs through your change process, rollback attached, written back to IaC.

IN YOUR WORDS
PR to IaC
- 05

It remembers
That kind of
door stays shut.

The rescan confirms. Your override becomes the rule for that finding type.

IN YOUR WORDS
rescan · guardrails

11x One healthcare customer priced a single finding at \$450 an hour of engineer time. By hand: \$8,775. Through Tamnoon: \$775. Their numbers.

The next thirty days

- WEEK ONE

Read-only. Verdicts on your real findings within hours. Nothing is written.
- WEEK TWO

One finding type you pick heals on its own, through your change process. You read the log.
- DAY THIRTY

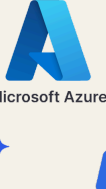
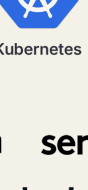
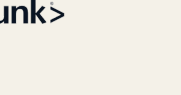
Every finding type you have approved heals on its own. You only see the declines.

"Our engineers won't let a bot touch prod."

Neither will we. Read-only first. Write is earned.
Then it takes the night shift.

Built for your toolchain

No new console to live in.

READS	Every scanner you already run. One finding, one verdict, whichever scanner found it.	  
WRITES	Jira, ServiceNow and Slack for the work. Terraform and Jenkins for the change. Datadog and Splunk for the trail.	 
RUNS ON	AWS, Azure and GCP, and Kubernetes on any of them. Same depth on each.	    

Start watch mode on your worst backlog.

Thirty minutes to connect. Hours later you know what heals without you, what it declines, and why.

Everyone automates the yes.
We mastered the no.