

53%

**is not your number.
It never was.**

Once a quarter you present the only chart in the deck that goes up and to the right. Nobody claps.

Across 800 cloud accounts, 53% of everything scanners ever detected is still open. Not because teams got slower: what is left waits until someone can prove the change is safe. **It is not waiting for a patch. It is waiting for a meeting.**

The one the board needs is smaller, and every line of it has a date.

Open findings on crown-jewel assets, by age. A short list, since 6.3% of alerts touch a crown jewel. Illustration.

UNDER 30 DAYS

Core API

Payments

30 TO 90 DAYS

Core API

Identity

Data platform

90 TO 180 DAYS

Identity

Payments

Edge

OVER 180 DAYS

Payments

Data platform

Every line has an owner.

**Report the crown jewels.
Decide the rest.**

Everyone automates the yes. We mastered the no.

Start watch mode. Tamnoon is the self-healing engine for cloud exposures. Connect it read-only in thirty minutes, nothing written.

One day someone will ask why a finding was still open.

Not how you missed it: the finding existed, and your scanner did its job.

A written no is a decision you can sign.

“Why was it still open?”

ILLUSTRATION

NOT AN ANSWER		It was in the backlog.
		Open eleven months. No decision on file.
AN ANSWER		
FINDING		Metadata service v2 not enforced
VERDICT		RISKY declined 14 March
EVIDENCE		A service still calls v1 from an old SDK
MANUAL PATH		Owned by the platform team

Three answers, each with evidence.

It reads first: who uses it, what depends on it, who owns it, what changed last week.

SAFE

Proven safe for this environment.
Heals through your own change process, rollback attached.

RISKY

Cannot be proven safe. Declined in writing, with the evidence and a manual path for the owner.

AWAITING DATA

One thing is missing, so it asks for it by name. It does not guess, and nothing runs.

Same scanners. Same team. A number that goes down.

fewer open findings in four quarters		3x
fewer new alerts arriving each quarter		93%
cheaper per finding, healed versus by hand		11x

“Tamnoon’s Automated Remediation Platform has enabled us to quickly and seamlessly resolve misconfigurations, while minimizing the impact on our environment.”

John Remo, Senior Vice President, Global Infrastructure & Cybersecurity, Warner Music Group

One customer’s quarterly reviews: 6,074 to 2,041 open findings, 93% fewer new alerts. One healthcare customer’s worked case: \$8,775 by hand, \$775 healed, at \$450 an hour. Single customers, never averages.

Automation you can put your name to.

You carry the AI mandate in one hand and the AI risk register in the other. The only automation both hands can hold is one that declines what it cannot prove safe.

Read-only first.

Write is earned. The exact permissions are published, per cloud and per scanner.

Your process, your keys.

Nothing runs outside your change process and your IAM. Rollback attached.

Every change, on record.

Who proposed, approved and executed it, with the rescan attached.

A no, in writing.

What it cannot prove safe, it declines, with the evidence. So you can leave it on.

“Our engineers won’t let a bot touch prod.”

Neither will we.

Market figures: State of Cloud Remediation 2026, Tamnoon. 14.86M CNAPP detections, 800 cloud accounts, 10 CNAPPs, through May 2026. The record and the slide are illustrations. Permissions: github.com/tamnoon-io/Tamnoon-Public-Permissions