

Whoever finds it, Tamnoon answers it.

Your scanner was never the problem. The 150 days after it were. **Tamnoon is the self-healing engine for cloud exposures:** every finding gets a verdict, the SAFE ones heal through your own change process, and the rest are declined in writing.



Judgment before action.

The engine investigates read-only, then gives every finding one of three answers.

SAFE

The change is proven safe for this environment and runs through your change process, rollback attached.

RISKY

It cannot prove the change is safe, so it declines in writing, with the evidence. Nothing runs.

AWAITING DATA

It names the one thing it is missing and asks for it.

Your scanner stays. Every one you run. The queue finally moves.

TMN-00071

AWS MFA not enabled for IAM users

PRIORITY Medium
START DATE Sept 15, 2025
CLOUD PROVIDER AWS
CLOUD ASSET iam-users (17)

Please action these findings via the Tamnoon portal (see attached weblink)

[Tamnoon Initiative - TMN-00071](#)

VERDICT: **SAFE**

EVIDENCE ATTACHED

SERVICENOW TICKET

Illustration. Real initiatives carry real evidence.

735 → **17**
ALERTS INITIATIVES

A real view. 735 alerts in, 17 initiatives out. The other 718 were the same seventeen, counted again.

How Tamnoon answers a finding



01

Connect, read-only

No access changes, nothing written. Findings from every scanner you run flow in exactly as they are.



02

It recognizes

Related alerts fold into one initiative, ordered by blast radius. Owner, dependents and change history are read first.



03

The verdict

SAFE, RISKY or AWAITING DATA, on every finding, with every check on the record. Evidence, not adjectives.



04

It closes, or it declines

SAFE runs through your own change process; the rescan confirms. RISKY is declined in writing. Your no becomes the rule.

Whoever found it



Work lands in Jira, ServiceNow, Slack and your pipelines. AWS, Azure and GCP at the same depth.

Thousands of alerts. One initiative.

Related alerts are grouped into initiatives by what they actually touch in your cloud, assigned to an owner, ready to decide. On average, 142 alerts fold into one, and the owner sees one, not 142.

Every finding gets a verdict.

It investigates read-only, with the full context of your environment, and hands you the verdict and the evidence: what is safe to close now, what it will not touch and why, what it still needs to know.

A route built for your cloud, with the exit marked.

For every SAFE finding: the steps, the code, the rollback. Who proposed it, who approved it and who executed it are logged inside the initiative, so your team works in one place instead of across five tools.

Proof the backlog is moving, both columns.

Healed and declined, side by side, with the rescan attached. Exposure trend, time to heal, and the receipts leadership can read without a translator. Both columns count: a written no is work done too.

What Tamnoon delivers

3x

fewer open findings in four quarters

93%

fewer new alerts arriving each quarter

11x

cheaper per finding, healed versus by hand

One customer's quarterly reviews: 6,074 to 2,041 open findings over four quarters, 93% fewer new alerts. One healthcare customer's own arithmetic: \$8,775 by hand, \$775 healed, at \$450 an hour. Single customers, not averages.

"Tamnoon's Assisted Remediation Service 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

Six questions for any remediation vendor

Paste them into your RFP. Ask every vendor. Including us.

- 01 Can it refuse a fix? Show one refusal, evidence attached.
- 02 Does it give a verdict on findings from every scanner we run, or only its own?
- 03 Show the full trail for one closed finding, rescan included.
- 04 When our engineer overrides it, where does that no go?
- 05 Does the fix survive the next IaC apply?
- 06 Can our auditor read every change without a translator?

The first thing you see is a refusal.

Start watch mode: bring the scanner with your worst backlog. Thirty minutes to connect, read-only. Hours later you know what heals without you, what it declines, and why.

Everyone automates the yes. We mastered the no.