Cloud Security with a Smile

Dental management services company reduced CNAPP alert noise by 70% and remediated over 1,000 high-severity misconfigurations with Tamnoon

3
Weeks
to full CNAPP optimization

70%
Noise Reduction
in CNAPP generated alerts

1000+
High Severity Alerts
Fixed within the first three months

> "
>
> Tamnoon successfully remediated all critical and high-severity issues within our timelines.
>
> – **VP, Security Operations**, Dental Management Services Company

The Challenge

A US-based dental management services company struggled to secure its cloud environment amid a flood of misconfiguration alerts.

The company had a midsize AWS environment and relied on Check Point CloudGuard as its Cloud Native Application Protection Platform (CNAPP). CloudGuard provided the team vital visibility into its cloud security posture by monitoring its environment and alerting on misconfigurations.

But the company needed a way to extract even more value from its CNAPP by making over 12,500 alerts specific and actionable, and directing their security team to prioritize critical tasks.

The Solution

Tamnoon's AI-powered platform, implemented by its dedicated team of cloud experts (CloudPros), introduced a four-step process:

AI-Assisted Triage and Prioritization

AI mines through CNAPP alerts and enriches them with context, eliminating duplicates, identifying crown jewel impact, and attributing issues to the right owners.

Impact Analysis

Tamnoon simulates different remediation approaches to determine the most effective resolution for each issue without disrupting crucial services.

Remediation

Tamnoon's CloudPros oversee the AI-powered remediation process, ensuring swift resolution.

Prevention

Tamnoon implements policies and guardrails to prevent similar misconfigurations in the future.

The Results

In just three weeks, Tamnoon seamlessly integrated with the client's environment, introducing a process for automatic monitoring and optimization of CNAPP alerts.

Within the first three months, Tamnoon enabled the company to achieve a 70% reduction in alert noise – empowering the resolution of over 1,000 critical misconfigurations, including:

- Removing dangling DNS records
- Investigating suspicious traffic activities
- Enforcing multi-factor authentication (MFA) for all IAM users with a console password
- Hardening and securing the external website

Despite resource constraints, the company harnessed the power of Tamnoon's platform and cloud expertise to automate remediation and to prevent recurrence of critical misconfigurations.