tamnoon

How zinnia® Resolves 65% Of High-Severity Misconfigurations

An insurtech leader used Tamnoon's managed cloud detection and response platform to gain control of its complex cloud attack surface and enhance its security posture

> Tamnoon has been critical to us gaining control over our cloud security. With Tamnoon, we've been able to turn alerts into action – so that the team spends less time chasing down misconfigurations, and more time on strategic priorities for the business.

– **Information Security Manager**, Zinnia

1900+

Misconfigurations

Directly remediated by Tamnoon

72%

MTTR reduction

For critical alerts remediated by Tamnoon

65%

High Severity

Misconfigurations remediated by Tamnoon

The Challenge

Rapidly-growing insurtech company Zinnia simplifies the process of buying, selling, and administering insurance through its technology offerings, marketplace, and third-party administrator (TPA) offerings.

The company was created through the merger of multiple industry-leading platforms, including SE2 and Life.io.

As Zinnia has grown, so has its cloud complexity – along with vulnerabilities. The merger led to a web of cloud infrastructure and services, further increasing the challenge of securing its attack surface.

Zinnia used Check Point CloudGuard as its CNAPP, but the lean team lacked resources to effectively triage and remediate issues. Critical exposures persisted, making it hard to meet the company's internal service-level agreements (SLAs) around resolution of high-severity issues.

> Our customers rely on us for the absolute highest level of cloud security, so we knew we needed a new approach to prioritizing and fixing alerts.
>
> – **Information Security Manager**, Zinnia

The Solution

Zinnia partnered with Tamnoon, the pioneer of cloud detection and response, to take control of its cloud security end-to-end.

Tamnoon began by ingesting 40,000+ raw alerts from Check Point CloudGuard. Zinnia then worked with Tamnoon's AI-powered platform – and its team of cloud experts (CloudPros) – on a four-step process for strengthening its security posture:

AI-Assisted Triage and Prioritization

Tamnoon's platform used AI to mine through CloudGuard alerts and enrich them with context – eliminating duplicates, identifying crown jewels, and attributing issues to the right owners.

Remediation

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

Impact Analysis

For issues identified, Tamnoon simulated different remediation approaches to determine the most effective resolution for each issue without disrupting crucial services.

Prevention

Tamnoon worked with the Zinnia team to implement policies and guardrails to prevent similar misconfigurations in the future.

One of the security risks Zinnia identified with Tamnoon, for example, was unencrypted Amazon EBS volumes. Remediating unencrypted EBS volumes is complex – and risks downtime or production impact if the volume is in use by a running EC2 instance.

Tamnoon implemented an end-to-end playbook that involved identifying and implementing the optimal resolution path – by identifying for each volume if:

- The EBS volume is attached to any EC2 instances.
- The EBS volume is not referenced or in-use by any critical services or applications (looking at tags, volume name, and other identifiers)
- The EBS volume is part of an Auto Scaling group or referenced in a launch configuration/template. Deleting volumes that are part of Auto Scaling groups can cause issues.

By applying rich context to alerts and mapping the impact of potential fixes, Zinnia was able to select the optimal remediation path and minimize production impact.

The Results

Through its partnership with Tamnoon, Zinnia has significantly enhanced its cloud security posture.

The Zinnia team was able to remediate 65% of high severity cloud misconfigurations – and reduce time to resolution for these by 72%. Remediation and preventative policies have enabled Zinnia to make significant progress on strategic security priorities including:

- Enforcing EBS, S3, and ECS encryption
- Hardening security groups
- Tightening role permissions
- Hardening password requirements
- Enabling logging and backups

Want to see Tamnoon in Action? **Request a demo @ tamnoon.io**