Check Point CloudGuard x Tamnoon

Transforming CNAPP Alerts into Actionable Insights for Critical Prioritization, Faster Remediation, and Resilient Defense.

The Challenge

While Check Point's CloudGuard delivers industry-leading cloud security and detection capabilities, organizations often find themselves overwhelmed by the sheer volume of alerts. Security teams struggle to determine which alerts require immediate attention, spending valuable time assessing actual unique criticality levels based on operational and risk context for misconfigurations across cloud workloads to guide prioritization.

This lack of context makes it challenging for security teams to identify and focus on the most critical vulnerabilities, leaving sensitive data and high-value resources at risk. Organizations require solutions that provide tailored prioritization based on their specific architecture and critical business priorities to address vulnerabilities effectively.

Our Integrated Solution

The collaboration between **Check Point CloudGuard** and **Tamnoon** bridges the gap between detection and remediation, delivering a seamless end-to-end cloud security solution.

- **Check Point's Cloudguard** Comprehensive scanning and security management across cloud workloads, configurations, and identities, ensuring continuous compliance and threat detection.
- **Tamnoon prioritizes** Check Point Cloudguard alerts using contextual insights such as the type of the resource, its environment, the criticality of the vulnerability, whether it is exposed to the public, who the owner is, and more. By incorporating this context, Tamnoon ensures critical misconfigurations and risks are addressed first, delivering actionable, expert-verified remediation workflows to resolve issues effectively.

This hybrid approach empowers organizations to resolve vulnerabilities while maintaining operational stability and security. Tamnoon's managed service adapts to each customer's unique environment, regardless of its complexity or simplicity, leveraging deep knowledge of their architecture and critical infrastructure to deliver contextulized and effective remediation.

Business Impact and Key Benefits

Enrich Alerts with Deep Context

- Automatically identify and tag critical infrastructure by evaluating their type, environment, sensitivity, and public exposure. Use enriched insights to ensure high-priority risks are addressed first, thanks to Tamnoon's AI-powered prioritization engine and managed service.

Focus Resources Where They Matter Most

- Provide security and development teams with a unified view of alert criticality. This enables collaboration and reduces time spent on less impactful issues and communication gaps between the two teams, which often take up most of the time.

Resolve Issues Swiftly and Securely

- Use Tamnoon's expert-guided remediation playbooks to reduce resolution times while ensuring changes are safe for production environments.
- Tamnoon's impact analysis ensures remediation plans are aligned with operational priorities, reducing the time to resolve critical issues by half while maintaining production safety.

Proactively Defend Your Organization

- Continuously assess and adjust asset prioritization as cloud environments evolve. Implement proactive measures to protect high-value resources from emerging threats and minimize future risks.

Use Cases in Action

Narrowing Network Access and Encrypting Cloud SQL Databases

Scenario:

Check Point CloudGuard flags a publicly exposed and unencrypted Cloud SQL database in GCP, with traffic from malicious IPs and misconfigured firewall rules.

Solution:

Tamnoon builds on the comprehensive detection capabilities of Check Point CloudGuard, which identifies the publicly exposed and unencrypted database, along with traffic from malicious IPs and misconfigured firewall rules. Using this foundation, Tamnoon conducts a deep investigation to refine prioritization, updating VPC firewall rules to block unauthorized access with tag-based controls, enabling encryption for the database with minimal disruption, and ensuring seamless integration by updating configuration files. A tailored operational impact analysis ensures all changes are safe and effective, leveraging the partnership to protect critical resources without disrupting functionality.

Optimizing Unattached Block Volumes

Scenario:

Check Point CloudGuard identifies over 270 unattached block volumes in an Oracle Cloud Infrastructure (OCI) environment, consuming resources and incurring unnecessary costs.

Solution:

Building on Check Point CloudGuard's detection of unattached block volumes, Tamnoon refines the findings and assigns tasks to owners, developers, or the security team to determine which volumes to retain or delete. Tamnoon provides detailed playbooks to guide the team through cleanup, ensuring resources are optimized without disrupting workloads. It also recommends OCI best practices to improve volume management and reduce costs moving forward.

Better Together

Integrating Check Point's robust cloud security capabilities with Tamnoon's expertise in contextual prioritization and remediation offers a powerful solution for securing cloud environments. This partnership ensures that organizations can confidently address their most critical risks while maintaining operational efficiency and compliance by streamlining detection, prioritization, and remediation.