WIZ + tamnoon

Securing the cloud effectively requires organizations to build new processes and learn new skill sets. The cloud introduces an environment with new risks and shared responsibility models that require existing security processes to change. Wiz and Tamnoon combine to help secure the cloud by providing visibility, detection, and prioritization for issues across the cloud with cybersecurity experts on-hand to help triage and remediate issues quickly.

Market challenge

The cloud continues to be the infrastructure choice for organizations running business-critical applications. Teams aiming to secure the cloud effectively are facing a few challenges:

- **Gaps in cloud visibility** - Traditional security tools require agents to gain visibility across cloud infrastructure. Ensuring every workload has agents installed and teams have security visibility cloud services that you can't install agents into creates gaps and missed security issues.
- **Alert fatigue** - Teams receive hundreds or thousands of alerts that don't provide the context to understand the issue's business impact and how the security team should prioritize it.
- **Time spent fixing cloud alerts** - Whether it's business-critical issues or ones that can be in the backlog, the cloud security, development, and SOC teams all work together to fix cloud issues. Some issues can be resolved through automated remediation, but others may take hours or days of investigation. Fixing these issues takes away teams' time and focus from other critical business initiatives.

Benefits of the integration

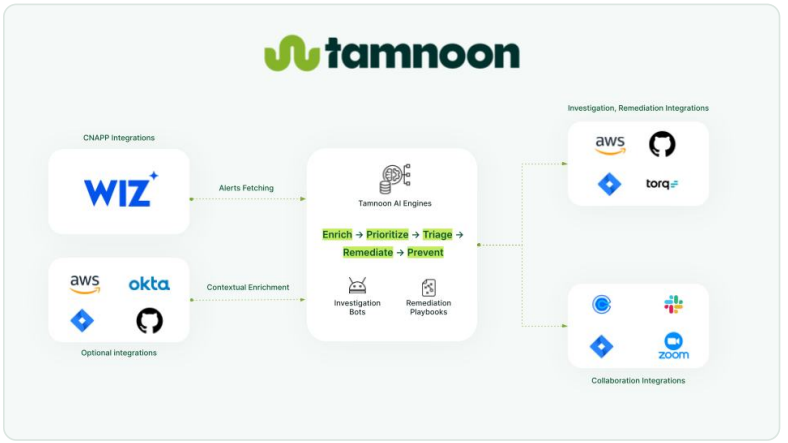
The Wiz and Tamnoon integration streamlines cloud visibility, detection, and remediation by delivering benefits such as:

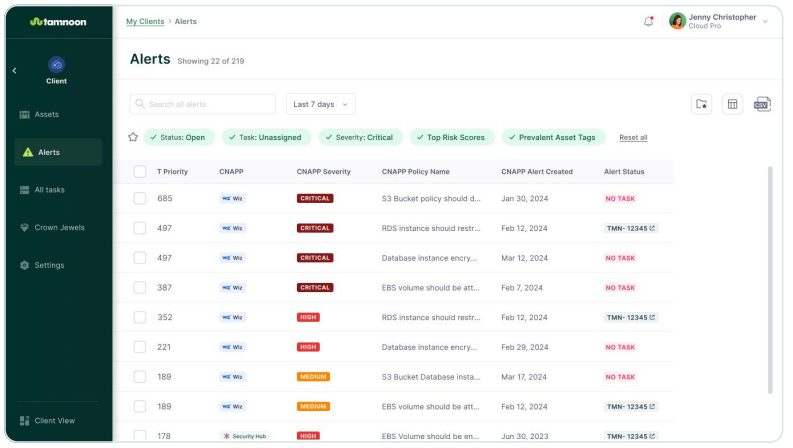
- **Enhanced Cloud Visibility:** Wiz's agentless scanning provides teams immediate visibility into all workloads and cloud services in their environment.
- **Reduced Alert Fatigue:** Wiz Issues combine toxic risk combinations that lead to open attack paths helping teams see what issues to prioritize and fix. Tamnoon takes any alerts from Wiz and enriches further based on information about critical assets, ownership, and past alerts that were similar. Having this context ensures that when Tamnoon's cybersecurity experts receive a cloud alert, they have the context to prioritize and fix the most business-critical issue.
- **Visibility to remediation:** The integration automates sending context-rich Wiz Issues to Tamnoon's cybersecurity experts to start the incident response.

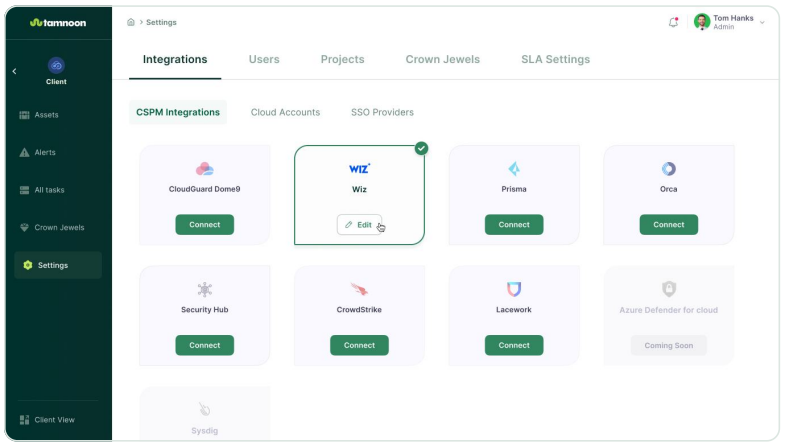
Better Together

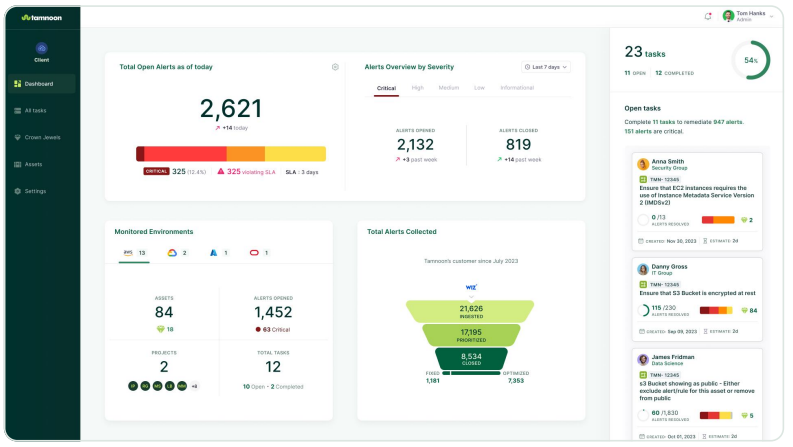
Combining Wiz's advanced CNAPP capabilities with Tamnoon's expert-curated prioritization and remediation playbooks, organizations can effectively tackle cloud misconfigurations and enhance their security posture. With Tamnoon's SLA management features, organizations can set clear expectations and track remediation progress, ensuring timely resolution of security issues.

Together, Wiz and Tamnoon empower organizations to confidently protect their cloud environments and foster collaboration between security and DevOps teams. Tamnoon provides prioritization and robust impact analysis of all alerts, ensuring the resolution of misconfigurations doesn't damage working production environments. DevOps teams can feel confident – before any remediation action is taken – that the proposed fixes take into account the context of their environment. Tamnoon also provides a clear remediation plan at the outset, giving DevOps teams visibility into the security flows.









About Tamnoon

Tamnoon is the Managed Cloud Detection and Response platform that helps you turn CNAPP and CSPM alerts into action and fortify your cloud security posture – fast. Tamnoon's pioneering blend of purpose-built technology, AI, and cloud expertise helps security and dev teams streamline cloud security from prioritization through remediation and prevention. Companies rely on Tamnoon to reduce critical and high alerts, accelerate MTTR, and get the full value of their cloud security stack.

About Wiz

Wiz is on a mission to transform cloud security for customers – which include 35% of the Fortune 100 – by empowering them to embrace a new cloud operating model. Its Cloud Native Application Protection Platform (CNAPP) delivers full-stack visibility, accurate risk prioritization, and enhanced business agility. The result? More context with less noise, so that security teams can focus their time on what matters most.