tamnoon | upwind

# Connect Tamnoon with Upwind

Combine Upwind's real-time insights with Tamnoon's trusted remediation to close the loop on cloud security.

## The Challenge

Cloud-Native Application Protection Platforms (CNAPPs) like Upwind give teams unmatched visibility across workloads, identities, and runtime environments. They uncover hidden misconfigurations, overprivileged access, and vulnerabilities that traditional tools miss.

But visibility alone doesn't solve the problem. Each discovery adds to an already crowded queue of alerts, many carrying the same level of urgency even when their real-world impact differs. Security teams end up spending valuable time investigating, correlating, and validating findings, often without the context to determine which issues matter most.

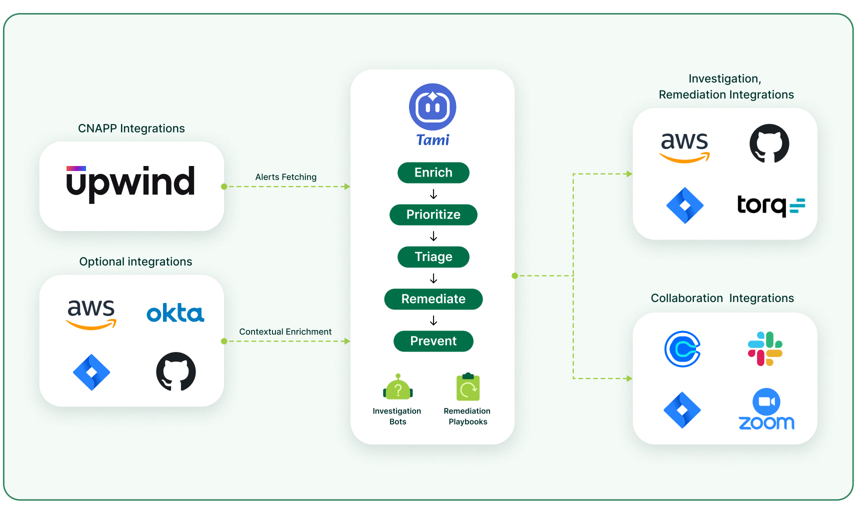
The next phase of cloud security is focusing on acting on those insights with speed and accuracy. Organizations need a way to move from identifying risk to resolving it, safely, consistently, and at scale.

## Our Integrated Solution

Tamnoon integrates seamlessly with Upwind Security to connect runtime visibility with trusted, autonomous remediation, helping teams act on cloud risk faster and with full confidence.

- **Upwind** provides deep, runtime-level visibility across workloads, containers, and cloud infrastructure. Its agentless CNAPP continuously monitors risk in context, mapping vulnerabilities, misconfigurations, and active exposures to their real business impact.
- **Tamnoon** ingests findings from Upwind, enriching them with context, including business insights, crown jewels, ownership, and application analysis, and prioritizing them based on asset value, exploitability, and exposure. Using AI-guided, human-validated playbooks, Tamnoon delivers safe and auditable remediation, treating root causes instead of isolated symptoms.

Together, Upwind and Tamnoon close the gap between detection and resolution. This combined approach turns continuous visibility into continuous action, allowing teams to remediate confidently, reduce MTTR, and maximize the full value of their CNAPP investment.



## Business Impact and Key Benefits

Combining Upwind's real-time visibility with Tamnoon's autonomous, human-validated remediation helps teams reduce noise, resolve risk faster, and finally close the loop between discovery and action.

### Accelerate mean time to remediate (MTTR)

- **Faster Triage:** Upwind's runtime insights feed Tamnoon's prioritization engine to surface only the most actionable risks.
- **Automated Execution:** AI-guided playbooks apply fixes safely without manual intervention.
- **Continuous Validation:** Every remediation step is verified for accuracy and business impact.

### Eliminate alert fatigue and focus on what matters

- **Smart Correlation:** Similar findings across workloads are grouped for faster resolution.
- **Context-driven Prioritization:** Alerts are enriched with context and ranked by asset value, exposure, and exploitability.
- **Reduced Backlog:** Teams spend less time chasing duplicates or low-severity issues and more time on critical exposures.

### Strengthen cloud resilience and compliance

- **Root-cause Remediation:** Fixes address the underlying configuration or permission issue, not just the symptom.
- **Policy Alignment:** Automated checks ensure remediations meet security and compliance baselines.
- **Audit-ready Trails:** Every change is logged, proving continuous improvement and compliance.

### Adopt AI-powered remediation with support from CloudPros

- **Flexible Automation:** Roll out autonomous remediation at your pace with full visibility and control.
- **Safe Remediation:** Tamnoon's CloudPros work closely with our AI agents to validate remediation in dev or production, ensuring all fixes are safe and accurate.
- **Always Supported:** When unique or sensitive cases arise, CloudPros step in to guide, execute, or review fixes, keeping your automation journey on track.

## Better Together

Upwind and Tamnoon deliver a unified approach to cloud security that connects continuous visibility with continuous action. Upwind delivers deep runtime and workload intelligence, while Tamnoon transforms those insights into safe, validated remediation that drives measurable cloud security improvements.

Together, they help teams eliminate manual bottlenecks, shrink risk exposure, and achieve true operational efficiency across every cloud environment. With Upwind identifying what's wrong and Tamnoon fixing it fast, organizations can finally turn detection into proactive protection at scale.

## Use Cases in Action

### Closing Runtime Exposure from Over-Permissive IAM Roles

**SCENARIO**

Upwind detects several IAM roles with broad administrative privileges used across multiple services. While these permissions aren't actively exploited, they present high lateral movement risk.

**SOLUTION**

Upwind provides real-time visibility into which workloads and users are leveraging those roles. Tamnoon takes it further, correlating exposure with asset value, identifying critical dependencies, and generating validated playbooks to tighten permissions without interrupting operations. This enables enforcing least privilege securely and without guesswork.

### Remediating Misconfigured Cloud Storage with Live Context

**SCENARIO**

Upwind flags multiple cloud storage buckets with public access enabled, including several connected to production workloads.

**SOLUTION**

Upwind pinpoints which buckets are actively exposed and what data types they hold. Tamnoon automatically prioritizes those with sensitive or customer data, classifies them by environment, and issues validated fixes to restrict access and enable encryption. Teams know exactly what to fix first and why, as each change aligns with internal security policy.

### Responding to Vulnerable Workloads Detected at Runtime

**SCENARIO**

Upwind identifies running containers in production with outdated base images and unpatched vulnerabilities.

**SOLUTION**

Upwind provides runtime evidence of risk, including active network paths and affected workloads. Tamnoon translates that insight into a step-by-step remediation plan, patching vulnerable containers, validating updated images, and confirming secure redeployment. Teams eliminate runtime risk faster while keeping deployments stable.