tamnoon | CYERA

From Data Risk to Actionable Security

Correlating CNAPP misconfigurations with DSPM findings for business-driven prioritization

The Challenge

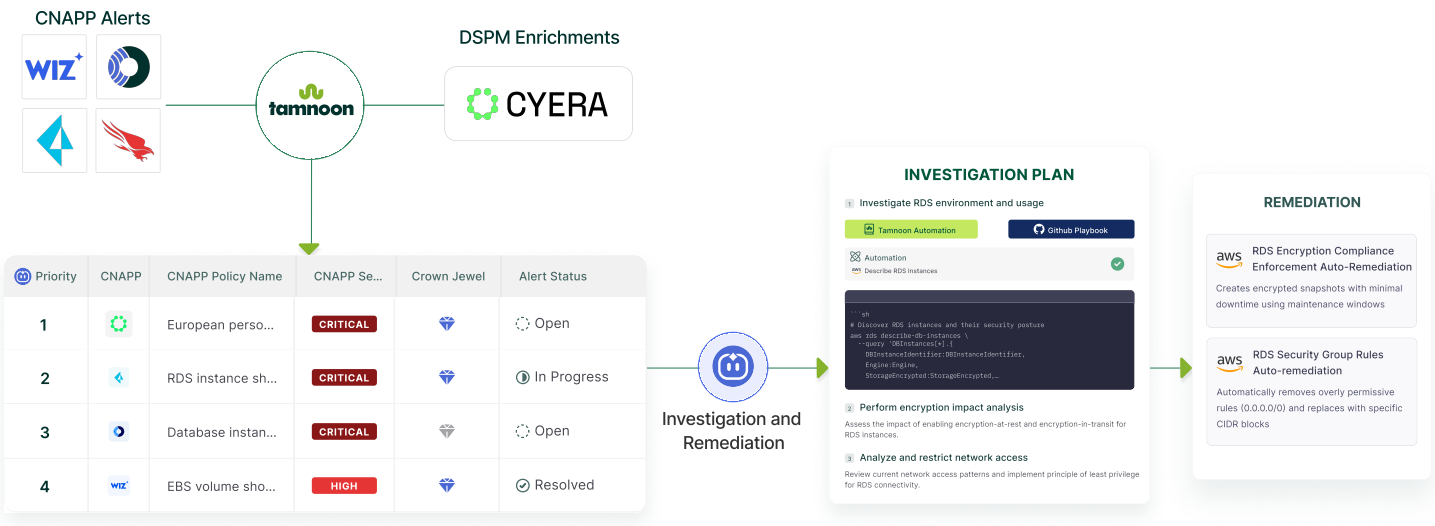
Cloud security teams must manage both infrastructure misconfigurations flagged by security tools and sensitive data exposures identified by DSPMs. However, these risks rarely intersect. Security tools may generate hundreds of alerts on exposed assets without showing where sensitive data resides, leaving teams unsure which risks truly threaten regulated or business-critical data.

This means analysts or engineers must manually investigate across tools, reconcile which alerts matter most, and design remediation plans on their own. Toggling between dashboards, comparing findings, and designing fixes without a unified context is time-consuming, prone to issues and errors, and, despite in-house expertise, challenging to scale.

Our Integrated Solution

Cyera provides deep visibility into sensitive data, classifying information, uncovering risks, and highlighting exposures with compliance or business impact. Tamnoon ingests Cyera's findings, correlates them with CNAPP and CSPM alerts, and turns them into prioritized, AI-investigated plans with expert oversight and engineering-friendly playbooks.

Tamnoon's Cloud SecOps Agent, Tami, takes over the alert backlog, investigates alerts, plans remediation, and consults in-house experts (CloudPros) to validate plans safely. Together, the two platforms create a single workflow where risks are not only detected but prioritized, contextualized, and turned into actionable outcomes that reduce exposure and restore compliance.



Business Impact and Key Benefits

Correlation and Prioritization

- **End-to-End Correlation:** Cloud security tools show misconfigurations, while DSPMs show data exposures. Correlating the two reveals which misconfigurations directly compromise sensitive data.
- **Contextual Prioritization:** A misconfigured asset without sensitive data can be handled at a lower priority, but one exposing regulated data must be prioritized and this partnership ensures it happens automatically.

From Alerts to Action

- **From Alerts to Action:** Other integrations enrich alerts for visibility, but Tamnoon goes further by creating detailed remediation plans and coordinating execution with engineering teams.
- **Compliance Confidence:** Issues are remediated in line with frameworks like PCI DSS, HIPAA, and GDPR. By combining Cyera's investigation with Tamnoon's remediation, every fix ties directly to sensitive data, keeping organizations audit-ready and aligned with regulatory demands.

Strengthening Security Posture

- **Strengthen Posture:** Continuously reduce exposure by eliminating risky permissions and misconfigurations with AI-powered, expert-validated remediation.
- **Control Data Sprawl:** Detect, prioritize, and remediate redundant or overexposed sensitive data.

Use Cases in Action

Prioritizing alerts based on business impact

CNAPP

CNAPP flags infrastructure misconfigurations on the compute instance holding data

CYERA

Cyera provides data context by mapping sensitive and regulated data to assets

tamnoon

Tamnoon correlates findings DSPM + CNAPP alerts to surface the issues with highest business risk

Avoiding a compliance violation

CNAPP

CNAPP Highlights EC2 instance with public IPv4

CYERA

Cyera flags EU personal data stored abroad, revealing a potential GDPR violation

tamnoon

Tamnoon ranks the violation to top priority and turns fragmented alerts into a custom remediation plan