tamnoon

CNAPP / Cloud Security Platforms

Comparative Overview

Modern cloud environments need more than separate tools for posture or threat detection. CNAPPs unify posture management, runtime visibility, data protection, and workload security in one view. Below is a comparison of four leading platforms, Wiz, Orca Security, Cyera, and Upwind, each addressing different aspects of cloud risk and posture.

WIZ

Core Focus: Cloud Security Posture Management (CSPM) and CNAPP

What Makes It Stand Out:

- Graph-based context: Correlates misconfigurations with identities, data, vulnerabilities, and potential lateral movement paths to reveal how cloud risks connect.
- Real-time visibility: Continuously scans cloud assets and detects issues as they appear, helping teams understand where to focus.
- Market trust: Recognized as a customer-choice leader in CSPM for 2025.

Best For: Teams that want deeper visibility into cloud configurations and relationships between assets, identities, and risks.

Ideal Outcome: Improved visibility and faster identification of misconfigurations and exposures.

orca SECURITY

Core Focus: Multi-cloud Security and Workload Protection

What Makes It Stand Out:

- Agentless SideScanning: Delivers visibility across environments without agents or performance impact.
- Unified coverage: Combines detection of misconfigurations, vulnerabilities, and identity risks with container and data protection.
- Operational simplicity: Unified visibility across AWS, Azure, and GCP.

Best For: Enterprises managing large multi-cloud setups that need consolidated visibility and faster issue identification.

Ideal Outcome: Unified cloud visibility with clearer context and simpler operations.

CYERA

Core Focus: Data Security Posture Management (DSPM)

What Makes It Stand Out:

- ✓ AI-native DSPM: Automatically discovers, classifies, and secures data across SaaS, PaaS, and IaaS systems.
- ✓ Data-centric: Focuses on data exposure and sensitivity instead of only configuration issues.
- ✓ Integrations: Works smoothly with DLP and IAM systems to strengthen broader protection.

Best For: Teams focused on locating and protecting sensitive data, understanding access paths, and preventing misuse.

Ideal Outcome: Strong visibility and control over data exposure across cloud environments.

upwind

Core Focus: Runtime-driven CNAPP

What Makes It Stand Out:

- ✓ Runtime insights: Uses live telemetry such as network flows and process-level data to identify how workloads behave in production.
- ✓ Runtime-aware prioritization: Focuses on risks based on live activity rather than static posture.
- ✓ Full-stack coverage: Combines posture, runtime, API, and container security in one view.

Best For: Teams with dynamic, container-based environments where runtime visibility is essential.

Ideal Outcome: Real-time insight into workloads and critical risk prioritization.

Tamnoon finishes what CNAPPs start. Our platform delivers battle-tested remediation at machine speed, safely resolving vulnerabilities and misconfigurations while dramatically reducing friction between cloud security and development teams.

tamnoon

Cloud SecOps that Feels Like Magic

tamnoon.io