CYCOGNITO

CHEAT SHEET

Five Common Gaps in CNAPP Coverage

How to Spot – and Fix – Blind Spots in Your Cloud Security Stack

Cloud-Native Application Protection Platforms (CNAPPs) provide full-stack cloud protection but can have blind spots that attackers can exploit.

This cheat sheet highlights five high-impact coverage gaps and offers practical, actionable guidance to help security teams close them effectively.

GAP 1

Incomplete Asset Discovery and Visibility

The Gap: CNAPPs depend on cloud provider APIs or agent-based methods, which can overlook shadow assets, ephemeral resources, or misconfigured third-party services.

Why It Matters: 67% of organizations struggle with limited visibility into their cloud infrastructure, making it harder for CNAPPs to deliver full coverage and risk assessment.

What to Look For: Solutions that integrate with external attack surface management (EASM) to discover unknown assets and services.

What to Do About It: Augment CNAPPs with seedless EASM technology to baseline asset inventories. Monitor drift carefully, especially in the first 6 months.

GAP 2

Absence of Active Testing in Production

The Gap: CNAPPs lack active testing on externally exposed production systems, focusing instead on pre-production environments for static and active tests.

Why It Matters: The delta between development and production environments can leave exposed issues. 82% of cloud security breaches are attributed to a lack of visibility.

What to Look For: CNAPPs that integrate with black box active security testing technologies to validate security measures in production.

What to Do About It: Integrate autonomous security testing and validation tools with your CNAPP or deploy autonomous testing as a standalone technology.

GAP 3

Siloed Risk Views Across Cloud Layers

The Gap: CNAPPs may assess risks in silos—code, infrastructure, workload, and identity—without correlating them into unified attack paths.

Why It Matters: Real-world attacks exploit combinations of weaknesses. Misconfigurations remain the number one cause of cloud breaches.

What to Look For: CNAPPs that map multistage attack paths, link misconfigurations, vulnerabilities, and identity flaws, and prioritize risks based on real exploitability.

What to Do About It: CNAPPs without unified risk correlation can be supplemented with tools like attack path analyzers or identity graph engines. You can also export findings via API or SIEM and correlate risks through a SOAR or XDR platform.

GAP 4

Incomplete Identity and Access Risk Analysis

The Gap: Most CNAPPs analyze identity and access management (IAM) configurations in isolation, missing combinations like excessive privileges combined with public exposure.

Why It Matters: IAM is often a weak link in security. Attackers exploit overly permissive roles or forgotten access paths to escalate privileges or move laterally. 68% of organizations say that cloud account takeovers are one of the biggest security risks.

What to Look For: CNAPPs that analyze effective permissions and privilege paths, provide contextual identity risk scoring, and integrate cloud IAM and Kubernetes RBAC.

What to Do About It: Regularly review and simulate access paths using IAM graph analysis tools. Remediate risky combinations.

GAP 5

Weak Integration with DevSecOps Workflows

The Gap: CNAPPs may bolt on security rather than integrate into CI/CD pipelines, ticketing systems, or Infrastructure as Code (IaC) scanning tools.

Why It Matters: If security isn't embedded in the development workflow, risks are addressed late or not at all. 82% of organizations report that human error is the cause behind most cloud security breaches.

What to Look For: Solutions that integrate into build pipelines and IaC templates, offer APIs and webhook support, and push findings into JIRA, Slack, etc., for remediation.

What to Do About It: Shift security left with IaC scanning and ensure security alerts reach developers in their daily tools.

How Can CyCognito Help Your Organization?

CyCognito automatically discovers exposed assets across cloud and internet-facing environments without seeds or credentials. It performs black box unauthenticated testing and integrates with CNAPPs for enriched test findings and better issue prioritization.

Check out our website and explore our platform with a self-guided, interactive dashboard product tour. To learn more about how CyCognito can help you identify and remediate emerging threats to your attack surface, request a customized demo.