aqua

# 6 Common CNAPP Pitfalls and How to Avoid Them

# Introduction

Cloud native application protection platforms (CNAPPs) have become an essential tool for ensuring the security and compliance of applications and infrastructure across multiple cloud environments. However, choosing and implementing a CNAPP solution can come with its own set of challenges.

This guide outlines common pitfalls that organizations encounter with CNAPP solutions and provides guidance on how to avoid them, thus ensuring a smooth implementation into your cybersecurity framework that drives the right value for your organization.

aqua

# Which pitfall do you want to solve today?



# 1 Deployment complexity, limitations, and delays

One of the first hurdles that many organizations face with CNAPP solutions is the complexity of deployment. Many solutions require custom scripting, deep configuration, and the installation and maintenance of agents on each asset. A CNAPP that's difficult to deploy can significantly delay the benefits it offers in terms of security and may require substantial in-house training or external consultancy fees.  Additionally, not all solutions work in the environments where you work or plan to work - i.e., on-premises, in the cloud, across the relevant public cloud providers - nor do they scale to your organization's breadth and depth of needs.

## Pro tip:

Look for an enterprise-grade solution that enables you to secure your cloud environment with a simple and highly scalable deployment. A solution that you can configure once and deploy anywhere quickly helps you prioritize incidents across all your environments. It also delivers rapid time-to-value, with the ability to support thousands of cloud workloads.

The solution should have out-of-the-box security policies that protect against advanced threats, eliminating the need for specialized security expertise.

# 2 Runtime protection that slows you down

The runtime agents that your CNAPP deploys and uses on your cloud assets should have minimal impact on system performance - i.e., a CNAPP should give you real-time protection while keeping overhead low. You don't want your runtime agent to block the CPU while it's responding or force you to restart the container every time you change a policy. Slow agents can lead to delayed data processing, which in turn affects the responsiveness and operational efficiency of your security operations.

## Pro tip:

During the trial phase, monitor the impact that the CNAPP's agents have on performance. Check reviews or ask for references to learn from other customers' experiences regarding the agents' performance impact on large-scale environments.

# 3 Duplicate alerts or “flapping”

“Flapping,” or the frequent toggling of alert status between safe and unsafe, can create a high volume of duplicate alerts, leading to alert fatigue and resource drain. It also can make it harder for security teams to track the progression of threats. This reduces efficiency and increases the risk of missing genuine threats.

## Pro tip:

Look for a fully integrated CNAPP platform that’s sophisticated enough to correlate and contextualize alerts across the entire platform and provide a single, clean view of prioritized alerts, eliminating any duplicates and reducing noise.

# 4 Disappearing assets

**A CNAPP must consistently track and manage all cloud assets. Assets that disappear from the inventory or dashboard can lead to unprotected entry points, gaps in vulnerability monitoring, and failure to meet compliance requirements. Any blind spots leave unmonitored assets susceptible to attacks or breaches, potentially compromising sensitive data.**

## Pro tip:

Test the reliability of the CNAPP's asset discovery and management features. Ensure that the platform can handle dynamic cloud environments where assets are frequently created and decomposed, and that assets don't randomly appear and disappear.

# 5 Lack of true integration

**A CNAPP that claims integration but fails to work seamlessly with existing security tools and workflows can lead to fragmented security postures. Lack of true integration complicates security management and reduces overall threat visibility with a siloed approach to processing and stopping attacks.**

## Pro tip:

Stay away from solutions that have a pretty graphical user interface but are still siloed in the back end. These solutions are typically built from many acquisitions with different architectures and poor integration, resulting in poor data correlation and connection. Look under the hood and confirm whether the CNAPP truly has a unified data model and can connect issues found in the cloud back to the exact line of code.

# 6 Poor support and hidden fees

Effective support and communication are crucial to resolving potential issues that arise in the deployment and operation of any CNAPP. Poor customer support significantly affects the resolution time and can cause minor issues to escalate to major disruptions.
As a customer, you don't want to be contacted only at the time of renewal, be surprised with unexpected fees, have your account manager change every few weeks, or get bounced around multiple support teams to get help, which often happens when a platform is not fully integrated behind the scenes.

## Pro tip:

Dig deep. Ask questions and observe the vendor's commitment to building a relationship with you, not just during the selling process but during implementation and after you're up and running on the platform. Look for truth in pricing.
Opt for vendors that understand your organization at a strategic level and are interested in developing a long-term partnership. Tactically speaking, ask the vendor about its support team structures and service level agreements, how often they meet with their customers, how they seek your input and feedback, and how they handle urgent issues. Compare this with your experience during the trial.

# Conclusion

Selecting the right CNAPP vendor involves thorough research and planning. By being aware of these common pitfalls and actively seeking vendors that not only avoid them but also align with your organization's specific needs, you can significantly enhance your cloud security posture and ensure robust protection across your cloud environments, while maintaining a high return on investment. By addressing these issues upfront, you'll be better equipped to choose a CNAPP solution that provides effective security without compromising on performance or usability. It also provides stronger outcomes without wasting time, money and resources and getting your CNAPP to work optimally.

# Aqua CNAPP

## Enterprise-grade protection powered by real-world threat intelligence

Aqua's unified platform is purpose-built to keep up with the dynamic and ephemeral nature of cloud native applications. The solution is built for unmatched enterprise-grade scale, proven in some of the world's largest container-based and serverless deployments.

Many of the world's largest financial institutions in highly regulated environments and 41 of the Fortune 100 trust Aqua to secure their cloud native applications.

Aqua's cutting-edge threat research team, Nautilus, powers our CNAPP with innovative, research-driven insights specific to cloud native environments, empowering you to truly understand your security posture, make better security decisions, and confidently report compliance to auditors and management.

aqua

Aqua Security sees and stops attacks across the entire cloud native application lifecycle in a single, integrated Cloud Native Application Protection Platform (CNAPP).
From software supply chain security for developers to cloud security and runtime protection for security teams, Aqua helps customers reduce risk while building the future of their businesses.
Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL protecting over 500 of the world's largest enterprises. For more information, visit https://www.aquasec.com

Schedule demo ›