KPMG

A cloud-native application protection platform – a solution for cloud security or just marketing?

February 2025

As a security expert, you are likely facing the growing challenge of safeguarding your cloud-native applications. With your organization adopting multiple cloud technologies, you are required to protect your applications and data from advanced cyber threats, while meeting compliance requirements and maintaining the trust and confidence of your customers. However, managing multiple tools and staying ahead of threats can become an overwhelming task.

A Cloud-Native Application Protection Platform (CNAPP) promises to help you address these challenges, by providing a comprehensive security solution specifically tailored for your organization's cloud-based operations. Multiple vendors have joined the race of developing these platforms, including Microsoft (Defender for Cloud), CrowdStrike (Falcon Cloud Security), SentinelOne (Singularity Cloud Security), Palo Alto (Prisma Cloud), and Trend Micro (Trend Vision One – Cloud Security). While these platforms are stepping up to help, are they really an efficient solution for cloud security? Industry trends suggest that the value of CNAPP in cloud defense is increasingly being acknowledged, compared to other available solutions. A recent study[1] of 500 CISOs reveals that a larger part of their investments for 2025 are focused on these platforms. The primary reason for this choice is the platforms' integrated approach for protection across the cloud, reducing the need for multiple security solutions coming from different vendors. Therefore, a CNAPP appears to be a great candidate to solve your cloud security challenges.

Considering its capabilities, investing in a CNAPP seems the easiest and cost-effective option. The platform should be able to protect your cloud environment, by offering **visibility** (discover shadow IT and create an asset inventory), **alerting** (notifying about suspicious events), **remediation points** for a better security posture, but also **automated actions**, which can aid in a faster response in the case something might be going on. Furthermore, the solution does not only cover cloud workloads, but also cloud identities, software development process, network architecture, data, cloud applications, and containers. Hence, a CNAPP stands as an effective solution which can make the management of security tools less overwhelming.

While CNAPP may appear promising in theory as a solution to protect your entire cloud environment, it does require a well-tailored and personalized configuration in practice. Out of the box, CNAPP will likely not perform as expected. Most of these solutions advertise a powerful AI as part of their offering, and while it can provide some time-saving assistance in configuration, internal knowledge of your organization will always be needed when setting up the solution and when identifying anomalies. Moreover, the platform will probably not be able to cover your entire infrastructure (which is likely a hybrid one) due to its cloud focus, and therefore integration with other security (monitoring) solutions becomes an imperative part in the configuration process. Thus, the effectiveness of a CNAPP will unfold through environment-specific customization and integration with your security stack.

Before acquiring a CNAPP, it is advised to research its capabilities, and ensure its compatibility with your cloud environments and your current stack. An ideal solution integrates well with your existing infrastructure, and bridges the gap in your security stack. Obviously, you should not just select the solution that offers the best marketing; a thorough analysis of the available solutions is required to enable you to make such a decision. Product reviews and market guides are a great start for your research, followed by direct contact with selected vendors who can provide live demonstrations of their products. Consider also how the new solution will fit into your current stack, and determine how it can be integrated to provide the most security value. You may also come to the conclusion that other security solutions might be a better fit for your environment, and that a CNAPP is not required. Taking all aspects into consideration before making a decision will ensure you will get the solution that provides the most value in the context of your organization.

Once you've chosen a CNAPP, it is important to tailor it to meet your organizational requirements. Therefore, **below are aspects to consider after acquiring a license for a CNAPP solution and commencing its deployment.**

Aspects to consider

Enable the solution to discover and protect all the cloud components it is able to cover.
This usually incurs additional costs, however unless the components are covered by other solutions, it is recommended to allow the CNAPP to monitor those to limit gaps in your visibility. Examples of these components include cloud-hosted servers, containers, databases, data storage, and code (DevOps).

Integrate the solution with your cloud, DevOps, and on-premise environment(s).
Leverage the ability of CNAPP to cover cloud environments from multiple vendors (Azure, AWS, GCP, etc.), and if possible, DevOps environments (GitHub, Azure DevOps, GitLab, etc.) and on-premise environments. This will ensure that you will get the best value from your solution, with the platform protecting and monitoring your environments from a single pane of glass.

Integrate the platform with your already existing security stack (firewalls, endpoint protection, intrusion detection and prevention systems, SIEM, etc.). The CNAPP is highly focused on the cloud, and hence it is not able to protect your entire digital environment. Because of this, most of the CNAPPs offer integrations with multiple platforms, to include the data from other security solutions, or simply the logs from different endpoints, appliances, and applications.

Finetune alerting provided by the solution.
CNAPP usually comes with predefined alerting rules that target compliance, security posture, and various types of anomalies of resource use. Beside these, for each component, additional rules may be enabled for more granularity. Evaluate the existing rules and how they match your organizational context. Remove or tune rules that are likely to produce noise, and create new rules that monitor activities which match your organizational context.

Configure your platform to prioritize your crown jewels.
Determine the assets which should be prioritized in consultation with your risk management department. If required, manually assign risk levels, and ensure these assets are thoroughly monitored and protected by the platform.

Evaluate all the other configuration and customization options the platform offers and ensure you integrate your organizational context with the platform.

CNAPP is a powerful tool which can help you protect your cloud infrastructure, by providing a comprehensive and integrated approach. However, bear in mind that it may not cover all aspects and that other specialized solutions might be necessary to achieve robust protection, especially outside the cloud. Moreover, it is not an easy out-of-the-box solution, and it requires time for configuration. Opting for this solution might seem an easy upgrade to your security stack, offering protection through a single pane of glass, but it might not provide all that is required immediately. Hence, the key is finding a combination of technologies that together offer a comprehensive security platform to cover your entire infrastructure. A CNAPP should be part of this combination, helping you gain a powerful, all-in-one solution to safeguard your cloud.

Contact us

Henrik Smit
Director Defense & Response
KPMG Netherlands
+31 (0)20 656 7247
smit.henrik@kpmg.nl

Cristina Olteanu
Tech Specialist
KPMG Netherlands
+31 (0)20 656 2940
olteanu.cristina@kpmg.nl

© 2025 KPMG Advisory N.V.. All rights reserved.