CLOUD SECURITY

WHITEPAPER

Trends, developments, challenges, and the role of CNAPP in public cloud security

YOU CAN'T SECURE WHAT YOU CAN'T SEE

VISIBILITY IS THE FOUNDATION OF CLOUD SECURITY

INHOUDSOPGAVE

INTRODUCTION

More and more organisations are choosing to move to a hybrid cloud infrastructure because of the benefits it offers, such as flexibility, scalability and accessibility. By the end of 2023, 54% of EMEA region-based companies, had implemented cloud technology in all or most parts of their operations and 73% of companies are expected to have all their operations in the cloud within two years.[1] Cloud technology allows organisations to store and manage applications and data without relying on expensive physical infrastructure. This flexibility allows them to scale faster and optimise processes, contributing to increased efficiency and innovation. Moreover, the cloud plays a key role in digital transformation by giving organisations access to advanced technologies such as artificial intelligence and machine learning, which is often difficult to achieve with traditional IT environments.[2]

CLOUD INCREASING THE ATTACK SURFACE

Cloud security has become an essential part of the security stack at a time when more and more businesses are embracing the public cloud. At the same time, the transition to the cloud comes with risks and challenges. These challenges can have major implications for the integrity, confidentiality and availability of corporate data and systems. The rapid adoption of cloud environments significantly increases the attack surface. When companies migrate data and applications to the cloud, they often become accessible via the Internet, exposing them to a wide range of cyber threats.

Cloud technology provides tremendous flexibility and scalability, but securing these dynamic environments presents unique challenges. Traditional security methods are often not designed for the complexity and speed of multi-cloud environments.

INTRODUCING CNAPP

Cloud security is complex, but there is a cloud-agnostic solution: Cloud-Native Application Protection Platforms (CNAPP). This solution offers an integrated approach to reduce and simplify the complexity of modern cloud security. In this white paper, we discuss the trends and developments in cloud security in Chapter 1, the challenges of cloud security in Chapter 2, CNAPP as a solution in Chapter 3, and finally why CNAPP is essential for organisations looking to protect their cloud environments from today's threats in Chapter 4.

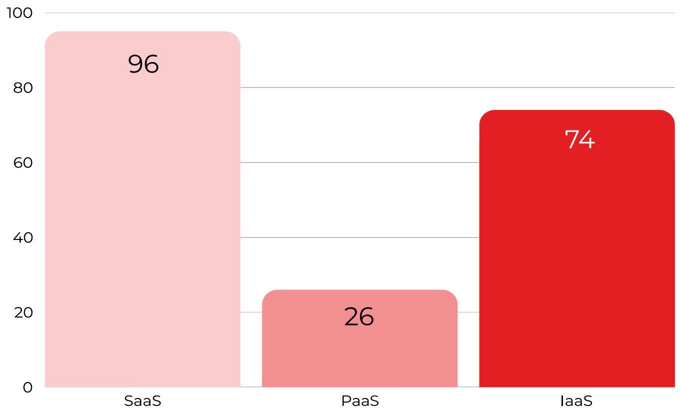
Whether you are an IT professional looking to get a grip on multi-cloud complexity, or a DevOps team looking to improve security without losing speed, this white paper offers essential insights into the future of cloud security and CNAPP's role in it.

[1] PwC, "PwC EMEA Cloud Business Survey 2023: How Businesses Will Unlock the Transformational Power of Cloud."

[2] Giemzo et al., "How CIOs and CTOs Can Accelerate Digital Transformations Through Cloud Platforms."

1 TRENDS AND DEVELOPMENTS

Before we can talk about securing cloud environments, it is first important to identify what cloud environments look like in European organisations. First, we have to to distinguish between three different types of cloud services,namely, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). Each type of cloud service offers different levels of control, flexibility and management.



Percentage of European organisations using the 3 main cloud service types

With SaaS services, a complete product is purchased that is executed and managed by the service provider. With PaaS services, the underlying infrastructure (usually hardware and operating systems) are managed by the service provider. PaaS services are primarily used within DevOps environments in order to efficiently develop applications. IaaS services contain the basic building blocks for cloud IT, offering the highest level of flexibility and management control over IT resources. [3 4 5]

Figures from Eurostat[6] show that SaaS services are used by almost all European organisations as shown in the chart above. Whereas IaaS services are still used by almost three-quarters of European organisations, the use of PaaS services remains outstanding.

1.1 INCREASE IN COMPLEXITY IN MULTI-CLOUD ENVIRONMENTS

Research by Microsoft[7] shows that 86% of organisations are already using a multi-cloud strategy to drive flexibility and innovation. This includes purchasing the aforementioned cloud services from at least two or more cloud providers.

Cloud environments often contain complex configurations consisting of different SaaS, IaaS and PaaS services. When migrating to the cloud, misconfigurations of cloud services are a common pitfall. Simple errors in configurations can lead to breaches, data loss and compliance violations. In addition, these complex environments also create a larger and more distributed attack surface, with traditional security tools struggling to provide full visibility across multiple platforms and systems.

1.2 ADOPTION OF 'SHIFT-LEFT' SECURITY

As organisations adopt the cloud, the number developing applications directly in the cloud is also increasing. The development of cloud-native applications also emphasises the importance of incorporating security practices early in the development process. This creates a clear trend to integrate security earlier in the development cycle, or "shift-left security."

By applying security controls during development (e.g. through Infrastructure-as-Code scans), vulnerabilities can be identified early, reducing costs and risks at later stages.[8] What many encounter at this time is DevOps and security departments operating in silos. This traditional separation leads to systemic problems, with each team limited to its own objectives rather than working toward common goals.[9] However, by making security an integral part of the development lifecycle, they can better manage risk, ensure compliance and maintain a competitive advantage in the marketplace.[10]

[3] "PaaS Vs IaaS Vs SaaS: What's the Difference? | Google Cloud."

[4] "SaaS Vs PaaS Vs IaaS – Types of Cloud Computing – AWS."

[5] "What Is IaaS? Infrastructure as a Service | Microsoft Azure."

[6] Eurostats, "Cloud Computing - Statistics on the Use by Enterprises."

[7] Microsoft, "2024 State of Multicloud Security Report."

[8] Sandler, "How to Modernize Your Cloud Security Posture."

[9] Nahmias, "Better Cloud Security Means Breaking Down Silos Between Dev and SecOps."

[10] Lucanus, "The Role of DevSecOps in Enhancing CNAPP Efficiency - Security Boulevard."

1.3 FOCUS ON RUNTIME SECURITY

Runtime security focuses on protecting applications and systems from threats and vulnerabilities while they are actively running in a production environment. The focus on runtime security in cloud security is growing due to the dynamic nature of modern cloud environments and the increase in advanced cyber attacks. Traditional security methods, such as static code analysis and configuration checks, are often insufficient because threats only manifest themselves at runtime.

Runtime security is therefore essential to detect vulnerabilities and block attacks while applications are actively running (in production). In modern cloud-native environments, such as microservices and container platforms, workloads are constantly changing, posing risks. In addition, zero-day attacks only become visible at runtime. While preventive security remains important, the importance of real-time monitoring and runtime security is growing. Modern solutions must therefore actively detect and respond to threats while applications are running.[11]

1.4 INCREASED USE OF AI AND MACHINE LEARNING

Another trend in cloud security is an increase in the use of AI and Machine Learning (ML), this is a direct result of the increasing complexity of cloud environments. With the increasing volume of threats and data, it is becoming more difficult for teams to manage everything manually. AI and ML are increasingly being used to identify, prioritise and respond to threats. This speeds up attack detection and reduces human error.[12] [13]

In addition, AI-driven cloud management will be increasingly deployed. Through predictive analytics and automation, AI can dynamically allocate resources, anticipate failures and manage workloads more efficiently. As cloud environments become more complex, traditional manual security methods are no longer adequate, making AI's role in managing these systems more indispensable as well.[14]

1.5 COMPLIANCE AS A PRIORITY

Stricter regulations such as GDPR, DORA & NIS-2 are partly causing companies to pay more attention to compliance requirements when setting up and maintaining cloud security. Another reason for the increased focus on compliance is the cost and competitive advantage it can bring. According to PWC [15], companies can exude more trust through compliance, with new and loyal customers as a proven result.

These trends show that traditional security methods are failing, particularly in multi-cloud and hybrid environments. They underscore the need for integrated solutions to automate uniform compliance checks in multi-cloud environments.

[11] Gartner, "Market Guide for Cloud-Native Application Protection Platforms."

[12] Gartner, "Market Guide for Cloud-Native Application Protection Platforms."

[13] Bradley, "Leveraging AI for Better Cloud Runtime Security."

[14] Sfondrini, "Eight Emerging Trends Shaping the Future of Cloud Computing."

[15] PricewaterhouseCoopers, "EMEA Cloud Business Survey 2023."

With the rapid rise of cloud computing, the demand for cloud security has also changed. Where previously organisations mostly had their own data centres and the focus was mainly on properly sealing the environment to the outside, the open nature of the cloud has changed that. With the general acceptance of cloud computing, employees are expected to be able to access their organisation's environment regardless of location or time. As a result, data and applications often become accessible over the Internet, resulting in exposure to a wide range of cyber threats.

Traditional security tools have primarily focused on Endpoint Detection and Response (EDR) and network security through firewalls. While these technologies were fundamental, they do not provide sufficient visibility and control over cloud environments, especially with the shift to containers and microservices. Below, we discuss the key limitations:

2.1 LACK OF FULL VISIBILITY

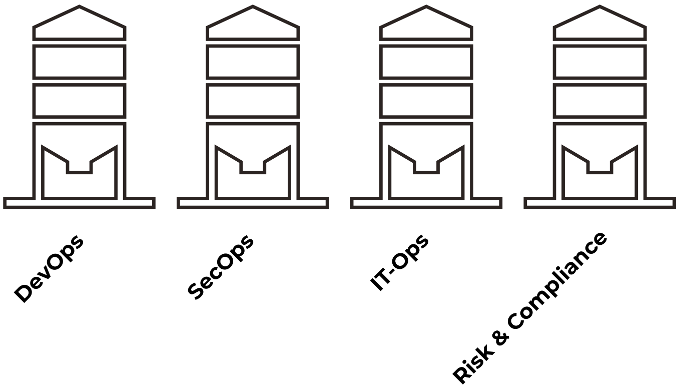
Traditional tools often provide limited visibility across cloud assets, especially in multi-cloud environments. This lack of visibility makes it difficult to identify and address threats or misconfigurations in a timely manner. Without a holistic view, vulnerabilities go undetected. Cloud environments often use microservices, such as containers and serverless architectures that are not readily visible to traditional security tooling. [16]

Moreover, they provide limited support for cloud-native log files and APIs, making correlation and analysis of events in cloud environments laborious. Furthermore, cloud environments also require a deep understanding of Identity and Access Management (IAM), misconfigurations and compliance requirements, something traditional tools often fall short of. Finally, traditional tools are ill-suited to the scalability and speed of modern DevOps practices, such as CI/CD pipelines and Infrastructure as Code (IaC). [10]

2.2 SILO FORMATION BETWEEN TEAMS

In many organisations, development (DevOps), and security (SecOps) teams work in silos. This leads to inefficiencies and a lack of coordination when securing cloud environments. Each team has its own goals, tools and work methodology. For example, DevOps teams focus primarily on speed and innovation, often through CI/CD pipelines. While SecOps teams aim for infrastructure stability and performance, and are often involved late in the process. A lack of collaboration can lead to inefficiencies such as miscommunication, conflicting priorities and fragmentation of responsibilities.

In practice, however, multiple silos exist, particularly within larger organisations. For example, in addition to DevOps and SecOps, there are other separate entities with their own responsibilities and priorities, such as IT-Ops and Risk and Compliance. IT-Ops focuses on the management and maintenance of IT systems, including network management, storage and general infrastructure facilities, and often operates separately from both DevOps and SecOps. Risk and Compliance deals with regulations, audits and risk management, which means they often impose strict frameworks that are not always in line with the agile practices of DevOps teams. This additional layer of complexity increases the challenges around collaboration and alignment, leaving security measures fragmented and reactive rather than proactive and incentivised.



Traditional security tools reinforce this fragmentation by protecting only specific layers or parts of the infrastructure (e.g. network security or endpoint security). In addition, they do not provide integrated visibility to teams, making collaboration and communication difficult. This often causes security teams to lack visibility into how developers configure cloud infrastructures, leading to exposures such as poorly configured IAM rules.
In addition, a potential lack of coordination slows down the identification and resolution of security incidents.

[10] Lucanus, "The Role of DevSecOps in Enhancing CNAPP Efficiency - Security Boulevard."

[16] Berthoty, "Redefining CNAPP: A Complete Guide to the Future of Cloud Security."

2.3 SLOW RESPONSE TIMES DUE TO MANUAL PROCESSES

Many traditional security approaches rely heavily on manual processes, such as regular audits or manual configurations. This is not scalable in dynamic cloud environments where systems are constantly changing, slowing response times and increasing risks.

2.4 VULNERABILITY TO MISCONFIGURATIONS

In the cloud, small configuration errors, such as open S3 buckets or poorly configured firewalls, quickly lead to major security risks. Traditional tools often lack the ability to dynamically identify and correct these errors, leading to data breaches or exposure.

2.5 CONSTRAINTS IN COMPLIANCE AND RISK MANAGEMENT

With increasingly stringent regulations and increasing complexity of cloud environments, ensuring compliance is difficult. Traditional tools often do not provide an integrated way to monitor compliance requirements in real time, leaving organisations at risk of fines or reputational damage.

3 WHAT IS CNAPP AND HOW DOES IT ADDRESS THE CHALLENGES?

One technology development that responds to the aforementioned trends and challenges are Cloud Native Application Protection Platforms (CNAPP). Whereas the Security Framework 'Secure Access Service Edge' (SASE)[17] secures how users access cloud apps and services, CNAPP as a Security Framework secures cloud-native applications and the underlying infrastructure itself. CNAPP is a term first coined by Gartner in 2021 as a comprehensive cloud security platform that consolidates multiple security tools and functions into one integrated solution. The concept evolved from a combination of Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP) and is constantly evolving to address the growing challenges within cloud security.[18] CSPM originally focused on identifying misconfigurations and compliance risks in cloud environments, while CWPP was initially seen as EDR for containers. CWPP has since expanded to include vulnerability scans and network security scans, making it a critical role in cloud security.

CNAPP's core functionalities can be divided into two main areas (1. Posture and vulnerability scanning and 2. Runtime detection and response), each with subcategories.

3.1 POSTURE AND VULNERABILITY SCANNING

- **Cloud Security Posture Management (CSPM):**
  Provides visibility into cloud workload configurations and vulnerabilities, with a focus on misconfiguration detection, asset management and vulnerability scanning.

- **Application Security Posture Management (ASPM):**
  Contains Tools for testing and securing applications, often with different scanners and languages.

- **Cloud Infrastructure Entitlement Management (CIEM) and Non-Human Identities (NHI):**
  Focuses on tracking permissions and activity of both human and non-human entities in the cloud.

- **Data Security Posture Mangement (DSPM):**
  Provides insights into data platforms, such as object and relational storage.

- **Unified Management:**
  works with security tools and developer workflows to provide clear remediation steps for issues identified by scans.

3.2 RUNTIME DETECTION AND RESPONSE

- **Traditionele EDR:**
  Functions like EDR, but in the cloud, with a focus on static servers and file-based detections.

- **eBPF Agent of Sensor:**
  A lightweight eBPF-based sensor that provides runtime visibility and protection, natively integrated with CNAPP. The Extended Berkeley Packet Filter (eBPF) is a Linux kernel technology that allows software engineers to securely run and update programs in the kernel. It provides secure access to operating system operations, allowing developers to address networking, observation and security challenges without impacting the operational system (e.g., server or database workloads).

- **Cloud Detection and Response (CDR):**
  Designed specifically for threat detection and response within cloud environments, where container security is an essential component.

- **Application Detection and Response (ADR):**
  Focuses on monitoring application activity for threats, including user interactions and communication between services.

- **API Security:**
  Focuses on protecting APIs within CNAPP from misconfigurations, unauthorized access and exploits.

[10] "Definition of Secure Access Service Edge (SASE) - Gartner Information Technology Glossary."

[16] Berthoty, "Redefining CNAPP: A Complete Guide to the Future of Cloud Security."

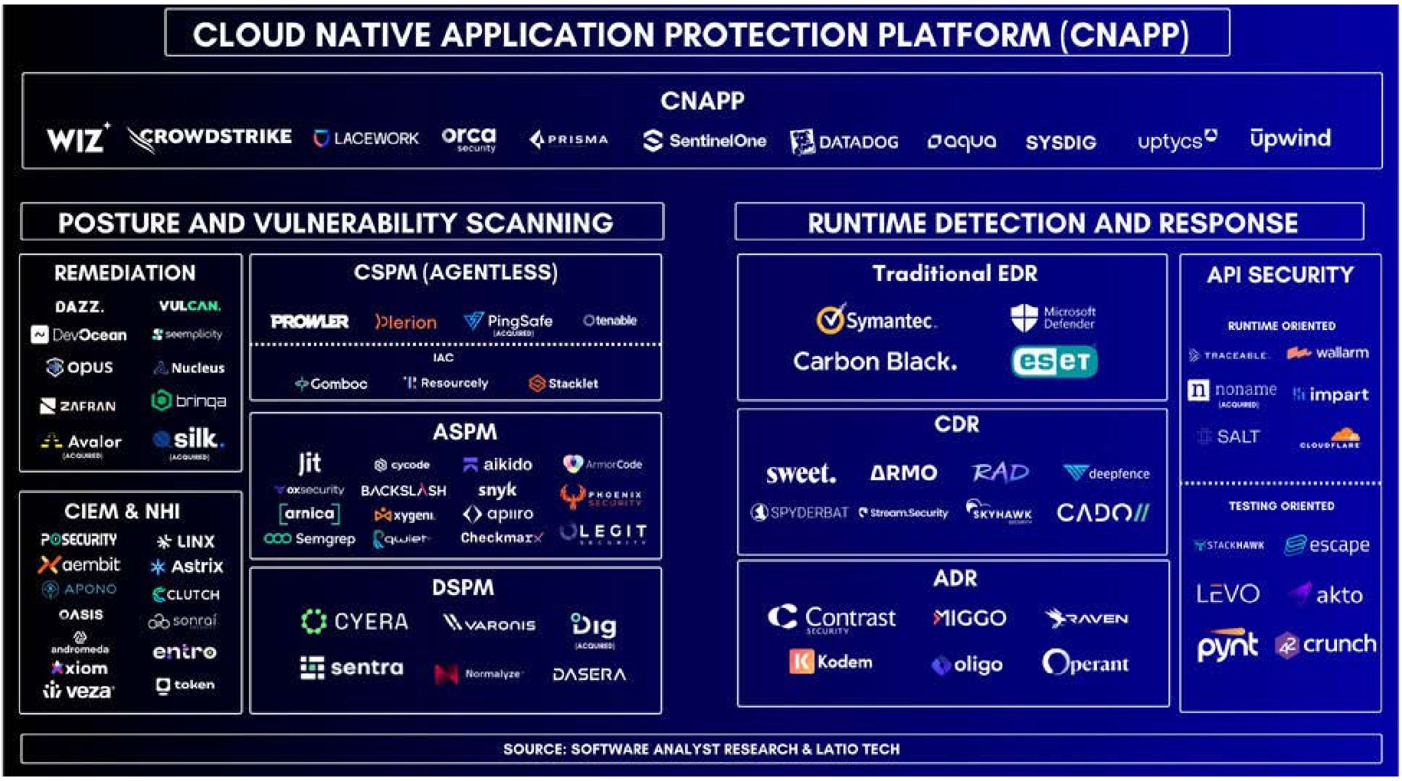
3 WHAT IS CNAPP AND HOW DOES IT ADDRESS THE CHALLENGES?

3.3 WHAT DOES THE CNAPP LANDSCAPE LOOK LIKE?

As shown in the image below, there are several providers within CNAPP as a security framework. On the one hand there are the CNAPP solutions that are overarching, and on the other hand there are point solution providers for the specific functionalities mentioned earlier. These solutions together make up the current cloud security landscape.

3.4 HOW CNAPP ADDRESSES CLOUD SECURITY CHALLENGES

CNAPP (in its best form) can address the challenges of cloud security by providing an integrated and holistic solution based on a Unified Data Model (UDM), as opposed to fragmented point solutions. Fragmented point solutions focus on specific security issues but often operate independently of each other, which can lead to blind spots, higher complexity and inefficient security. CNAPP prevents this by bundling all cloud security functions into one integrated platform, making threats more visible and manageable.



SOURCE: SOFTWARE ANALYST RESEARCH & LATIO TECH

Afbeelding I - Bron: Berthoty, “Redefining CNAPP: A Complete Guide to the Future of Cloud Security.”

3 WHAT IS CNAPP AND HOW DOES IT ADDRESS THE CHALLENGES?

CONSOLIDATION OF SECURITY TOOLS

CNAPP aims to consolidate different security tools into one platform. In the past, security teams used multiple tools for different aspects of cloud security, such as CSPM, CWPP and other tools. CNAPP aims to bring these together to reduce the complexity of managing multiple security tools and reduce the number of tools security teams have to deal with.

VISIBILITY OF CLOUD ENVIRONMENT

In addition, CNAPP provides extensive visibility into cloud environments. Allowing in-depth insights, at the workload level, at all layers (SaaS, PaaS, IaaS) of the cloud estate. Traditional security tools often lack the ability to see end-to-end configurations of resources. CNAPP tools are designed to provide 100% visibility on all cloud assets. To thereby identify any misconfigurations, compliance risks and security gaps, providing an overview of the entire security posture of the cloud environment.

CNAPP combines agent-based and agentless solutions to provide different levels of visibility. Agentless scanning provides lightning-fast visibility into all cloud resources, while a cloud sensor (“light” agent) provides an even more detailed view within the runtime environment of workloads. By working primarily from an agentless approach and deploying light sensors (eBPF agents) only where necessary, a complete picture of the cloud environment is created with minimal impact on the runtime environment.

BRIDGING POSTURE AND RUNTIME

CNAPP bridges the gap between posture management and runtime protection. Posture management focuses on preventing vulnerabilities and misconfigurations before they can be exploited, while runtime protection is designed to detect and respond to threats as they occur. CNAPP provides a unified approach to both of these essential components of cloud security.

WORKLOAD SECURITY

CNAPP secures cloud workloads and focuses specifically on containers. Containers are lightweight, isolated environments that contain all necessary application components, such as code, runtime and dependencies, allowing applications to run consistently across environments. Containers have become popular thanks to technologies such as Docker and Kubernetes, which enable flexibility and scalability in the cloud. Traditional security tools fall short because containers are short-lived and dynamic, making static security measures inadequate. CNAPP tools help by detecting workload-level misconfigurations and provide runtime protection to block active threats.

ADDRESSING SILO FORMATION

Silos between DevOps, ITOps and SecOps can lead to frustrations, inefficiencies and ultimately security gaps. Each team needs different context and prioritisation of risks, and CNAPP can address this. For example, this allows DevOps teams to receive notifications only about real critical problems and SecOps teams to focus on strategic risks instead of endless error messages. CNAPP can also integrate with existing DevOps tools and workflows such as Kubernetes, Terraform, GitHub and CI/CD pipelines, allowing security to be automated without impacting development speed.

RISK AND COMPLIANCE

CNAPP plays a crucial role within Risk and Compliance Management by detecting risks such as misconfigurations, vulnerabilities and threats in cloud environments and linking them to relevant compliance frameworks such as DORA, CIS, NIS-2 and ISO27001.

This component within CNAPP helps organisations with regulatory compliance by performing automated checks, quickly identifying anomalies and prioritising risks based on their impact on business continuity and compliance. In addition, it provides organisations with near-real-time visibility into compliance status, reduces reliance on manual audits and accelerates the detection and resolution of security and compliance issues, allowing them to operate more efficiently and securely within applicable regulations.

4 THE ROLE OF CNAPP IN CONTEMPORARY CLOUD ENVIRONMENTS

4.1 DEVELOPMENTS

CNAPP platforms are increasingly using AI and machine learning to automate securing (multi) cloud environments and proactively manage risk. According to Gartner, advanced detection algorithms and machine learning are among important trends in cloud security. AI can help with:

- Automate threat detection, by recognising patterns in behaviour and anomalies.
- Reduce false positives, allowing security teams to focus on real threats.
- Faster incident response, through automated playbooks and recommendations. This makes security processes less dependent on intervention and allows organisations to address threats more efficiently.

In addition, Gartner[12] expects that by 2029, 60% of organisations that do not implement a unified CNAPP solution within their cloud architecture do not have a comprehensive understanding of the cloud's attack surface and therefore fail to meet their desired zero-trust goals. Furthermore, Gartner expects 35% of all enterprise applications to run in containers by 2029, a 15 percentage point increase over the 2023 prediction. It cannot be ruled out that the predictions will be revised again in the coming years.

Furthermore, Gartner[12] says the CNAPP market has experienced significant growth, accompanied by a trend of acquisitions and consolidations. Although there are many vendors, only a handful offer a comprehensive platform with the required breadth and depth of functionality, with an emphasis on seamless integration into the development and operational process. In addition, there are only a select number of providers with far-reaching cloud native functionality that has not come about through acquisitions alone.

As more and more organisations develop cloud-native applications, the role of CNAPP in DevSecOps strategies will only become more important in the coming years. Collaboration between development and operations is becoming essential, and CNAPP provides the integrated security needed to quickly identify and fix vulnerabilities without slowing the speed of development.

Increasingly organisations are opting for a multi-cloud solution, thus combining multiple cloud providers such as AWS, Azure and Google Cloud Platform (GCP) to increase flexibility and scalability while reducing dependencies. In this development, CNAPP, as a cloud agnostic solution, plays an important role by providing a single platform that supports all cloud environments. This allows security strategies to be applied consistently across clouds, avoiding the risks of vendor lock-in.

[12] Gartner, "Market Guide for Cloud-Native Application Protection Platforms."

4.2 WHAT DOES THIS MEAN FOR YOUR ORGANISATION AND HOW TO PROCEED?

Organisations face the challenge of growing cloud environments not only quickly, but also securely. Often, they already have the necessary security tooling in place to secure public cloud environments. As such, we recommend the following:

- **Evaluate the (cloud) security tooling in use:** Do all components belonging to posture and vulnerability scanning and runtime detection and response (Chapter 3.1 & 3.2) fall within the scope? Is the current security stack set up as efficiently as possible, or is there still a lot of overlap?
- **Evaluate the deployment of AI security:** Is AI already being used to secure the cloud environment?
- **Evaluate the (annual) pentest policy:** Does the cloud fall within the scope of the pen test? Is a cloud assessment performed by a CNAPP partner?

CONTACT

Leon Smit
General Manager
Acora Cyber Security, Acora Netherlands

e: leon.smit@acora.com
t: 0031 (0)651220533

acora