Market Guide for Cloud-Native Application Protection Platforms

22 July 2024 - ID G00790337 - 35 min read

By Dale Koeppen, Charlie Winckless, **and 2 more**

CNAPPs address the full life cycle protection requirements of cloud-native applications and infrastructure from development to production. Security and risk management leaders responsible for cloud security strategies should use this research to analyze and evaluate emerging CNAPP offerings.

Overview

Key Findings

- The attack surface of cloud-native applications and infrastructure is expanding, with attackers focusing on the runtime environment, including network, compute, storage, identities and permissions, and the misconfiguration of cloud management and control features. Additionally, APIs and the software supply chain itself have become targets for potential attacks.
- The cloud-native application protection platform (CNAPP) market has witnessed substantial growth, accompanied by a trend of acquisitions and consolidations. While numerous providers exist, only a handful offer a comprehensive platform with the required breadth and depth of functionality, particularly emphasizing seamless integration through the development and operations processes.
- With operational responsibilities shifting toward developers and cloud architects, the need for advanced tools to address vulnerabilities, deploy infrastructure as code and manage production implementations has grown to accommodate this expanded scope. Proactively identifying and prioritizing risks during development, while providing developers with adequate context, is essential due to developers perceiving security as an obstacle.

Recommendations

Security leaders responsible for cloud security strategies should:

- Safeguard cloud-native applications and counter the growing attack surface by adopting CNAPP offerings. These solutions protect against threats in the runtime environment, mitigate misconfigurations in cloud infrastructure, and streamline security integration and collaboration throughout the overall development experience.
- Leverage CNAPP to strengthen defenses against attacks on network, compute, storage, identities, permissions, APIs and the software supply chain, thereby mitigating potential risks and safeguarding critical assets.
- Prioritize comprehensive and unified CNAPPs that offer a wide range of capabilities with the necessary breadth and depth of functionality to seamlessly integrate across the entire development ecosystem and cloud platform environment.
- Select shorter-term contracts to be flexible and adapt to the market's changing dynamics. This ensures the organization stays aligned with the most suitable CNAPP solution for their requirements. No single vendor offers best-of-breed capabilities across all domains.
- Form a cross-functional team comprising experts from security operations, cloud security architecture, application security and development operations to evaluate and choose CNAPP offerings.
- Prioritize solutions that cater to the increasing operational responsibilities of developers and cloud architects. Emphasize the need for advanced tools that effectively address cloud and application security risks, efficiently manage production implementations, and provide developers with sufficient context to overcome security obstacles, while fostering a collaborative approach toward secure application development.

Strategic Planning Assumptions

- By 2029, 60% of enterprises that do not deploy a unified CNAPP solution within their cloud architecture will lack extensive visibility into the cloud attack surface and consequently fail to achieve their desired zero-trust goals.
- By 2029, more than 80% of enterprises will adopt a centralized platform engineering and operations approach to facilitate DevOps self-service and scaling, from less than 30% in 2023.
- By 2029, 35% of all enterprise applications will run in containers, an increase from less than 15% in 2023.

Market Definition

Cloud-native application protection platforms (CNAPPs) are a unified and tightly integrated set of security and compliance capabilities, designed to protect cloud-native infrastructure and applications. CNAPPs incorporate an integrated set of proactive and reactive security capabilities,

including artifact scanning, security guardrails, configuration and compliance management, risk detection and prioritization, and behavioral analytics, providing visibility, governance and control from code creation to production runtime. CNAPP solutions use a combination of API integrations with leading cloud platform providers, continuous integration/continuous development (CI/CD) pipeline integrations, and agent and agentless workload integration to offer combined development and runtime security coverage.

CNAPPs emerged to offer enhanced visibility, configuration and compliance monitoring, and remediation for modern cloud-native applications across a DevOps-style framework. These offerings consolidate a set of distributed capabilities under a single integrated platform, irrespective of the underlying hyperscale cloud providers. They help identify, prioritize and remediate risks that result from the dynamic and complex processes of cloud architectural deployment, application development and cloud security operations.

CNAPPs are primarily sold and delivered through a cloud provided, as-a-service solution, designed to protect infrastructure as a service (IaaS) and platform as a service (PaaS) public cloud environments and the associated running workloads and applications.

CNAPPs' combined features offer a collaborative platform for development teams, cloud architecture teams, infrastructure security and security operation teams to identify and prioritize cloud risks. It enables these teams to communicate effectively in a single cohesive platform during cloud-native application development. This results in a robust, mature and secure cloud-native application development, while minimizing the business risk associated with coding and modern application deployment.

Mandatory Features

The mandatory features of this market include:

- Integration via API with hyperscale cloud platforms (including, at a minimum, Amazon Web Services [AWS], Microsoft Azure, and Google Cloud Platform [GCP]) and Kubernetes, to review and audit configuration and identity permissions for common misconfigurations that lead to security exposures.
- Development operation workflows that provide risk analysis and prioritization of risk through the development life cycle of modern applications. At a minimum, the platform should provide infrastructure as code scanning and container registry scanning.
- Visibility into runtime states of workloads, either in real time or via point-in-time analysis, to discover security vulnerabilities and the presence of secrets and anomalous behavior in cloud workloads (virtual machines, containers and serverless), and use this to add context to cloud configuration findings.

- Solution is provided through a cloud-delivered “as-a-service” platform, rather than a loosely coupled portfolio of products.

Common Features

The common features of this market include:

- Generation of comprehensive reports, dashboards and visualizations to communicate security posture and remediation progress to relevant stakeholders.
- Predefined templates for benchmarking against common compliance standards. Specific examples are standards from the Center for Internet Security (CIS), National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Payment Card Industry (PCI) and the U.S. Health Insurance Portability and Accountability Act (HIPAA).
- Options for integration with lesser-common common cloud and Kubernetes platforms like OCI, IBM, OpenStack, and OpenShift.
- Integration into web-based CI/CD pipelines and/or directly with developer integrated development environments (IDEs).
- Integration with other common tools, such as server endpoint protection tools and on-premises cloud and orchestration platforms, as well as integration with SIEM/SOAR/TDIR/SOC platforms.
- Ability to integrate with third-party application security posture management (ASPM) and application security testing (AST) tools for context, or offer these natively built into the platform.
- Deliver structured developer workflows and provide security guardrails that scale with the application development, which can adapt to the dynamic nature of multicloud adoption.
- Software compositional analysis, software bills of materials and pipeline hardening.
- Workload architectural graphing and attack path analysis, including attack vector mapping on known vulnerabilities and abnormal behavior.
- Management of workload vulnerabilities in runtime. Capabilities include virtual patching and workload isolation/segmentation, as well as management of running services/processes.
- Ability to offer API discovery, scanning and protection services, or provide methods of integration with third-party API protection solutions.
- Expanded cloud detection and response (CDR) beyond basic workload monitoring, for advanced correlation and remediation.

- Integrated or self-delivered ASPM, including but not limited to application security testing, application vulnerability management, API security testing and remediation workflow management.

- Support for AI/ML integration for policy enrichment, recommendations or common language interpretation.

Market Description

Securing cloud-native applications often required multiple tools from different vendors, which lacked cross-integration and were primarily designed for security professionals, neglecting collaboration with developers. Consequently, this lack of integration results in fragmented views of risk with limited context, making it difficult to effectively prioritize overall business risk. The use of fragmented tools also leads to excessive alerts, wasting developers' time, complicating remediation efforts and causing confusion for targeted roles.

In a modern DevSecOps environment, a key challenge is meeting the expectations of all stakeholders involved in developing and securing cloud-native applications. Traditionally, development teams, cloud architecture teams and security operations teams have operated independently from one another, leading to a lack of cross-team communication. This gap is further exacerbated by each team using disconnected tools during the complex process of developing cloud-native applicatio

A cloud-native application typically has the following characteristics:

- Constructed using discrete code functions inside containers that operate as loosely coupled microservices, often interacting via application programming interfaces

- Developed within a DevOps-style continuous integration (CI)/continuous delivery (CD) pipeline supporting frequent updates and making the workloads and their microservices more ephemeral

- Use a combination of custom code and open-source code as well as libraries from open source or privately sourced repositories

- Deployed onto programmatic cloud infrastructure with applications abstracted away from the infrastructure dependencies and take advantage of cloud shared infrastructure in an elastic manner to scale up and down as the business requires

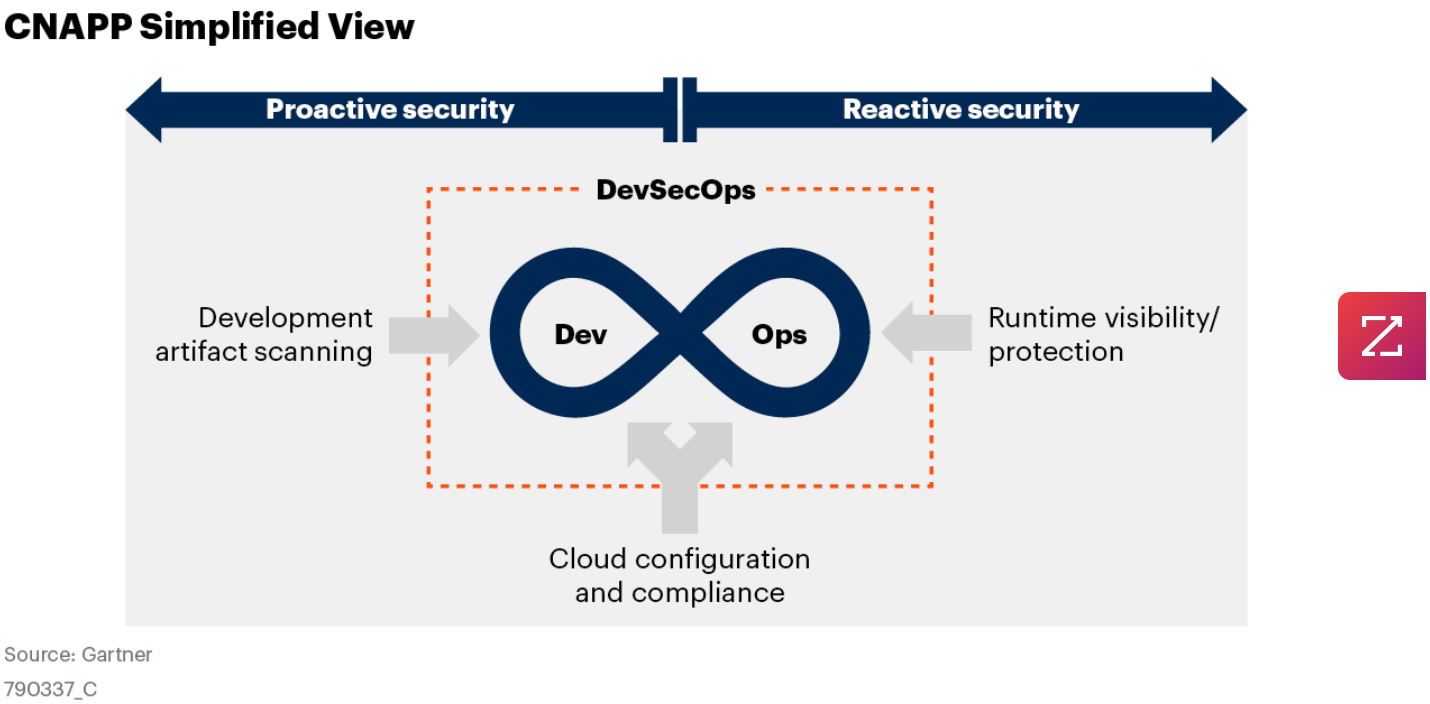
- Managed with a bias toward immutability so few or no changes to production workloads are allowed (All changes in production are driven through the development pipeline.)

CNAPPs offer a consolidated and tightly integrated set of proactive and reactive security capabilities designed to ensure visibility, configuration compliance, code analysis and risk assessment throughout the development and operations stages of cloud-native applications. Ideally these capabilities should be seamlessly integrated within a modern DevOps-style framework, regardless of

the underlying hyperscale cloud platform. CNAPP solutions complement your security posture by proactively addressing risks that arise from known, unknown and unexpected exposures that in turn arise from the dynamic and complex nature of developing and deploying cloud-native applications.

CNAPPs aim to deliver a comprehensive analysis of various elements and characteristics of the application and cloud environment with a strong emphasis on empowering developers to take responsibility for application risk (see Figure 1). The consolidation of these capabilities into a unified engine provides organizations with a centralized and cohesive platform to proactively identify and mitigate excessive risk within the intricate logical boundaries of modern cloud-native applications.

Figure 1: CNAPP Simplified View



Source: Gartner
790337_C

Gartner

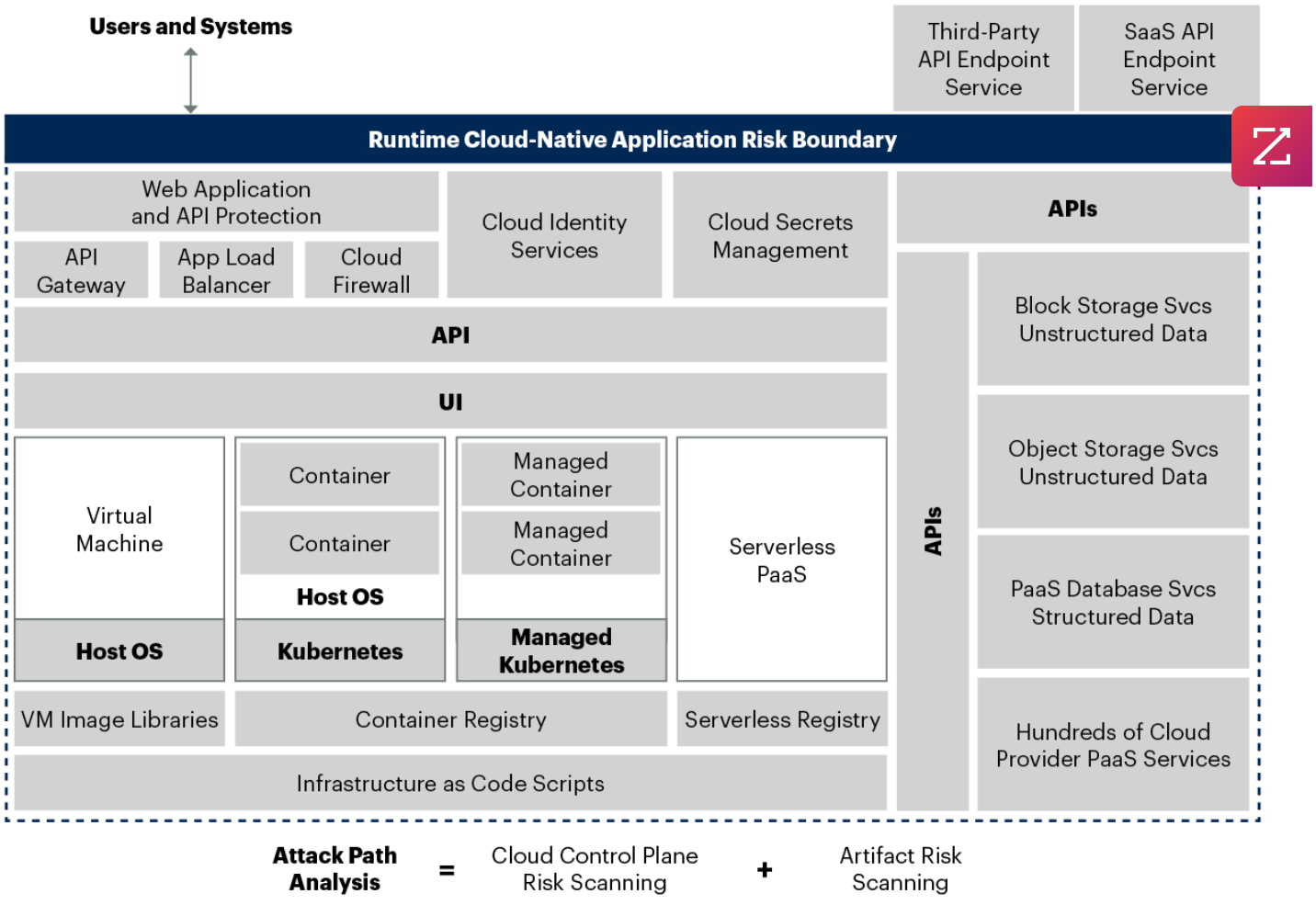
CNAPP platforms are primarily sold and delivered as a single integrated solution through a cloud-provided, as-a-service offering that aims to secure and protect infrastructure as a service (IaaS) and platform as a service (PaaS) platforms and the running workloads within these environments. CNAPP solutions are integrated into public cloud environments through the following methods:

- Into the cloud service provider (CSP) via API and as a CSP-native functionality for configuration, compliance, identity and risk analysis, typically provided by cloud security posture management (CSPM), Kubernetes security posture management (KSPM) and cloud infrastructure entitlement management (CIEM)
- Into the cloud workload runtime environments via API or through an agent-based deployment for runtime monitoring and risk analysis, typically provided by cloud workload protection (CWP)

- Into the development pipeline tools to provide workflows and compliance guardrails for coding development teams and cloud architecture teams
- To provide support for integration with supplementary tooling required by development teams for code and application testing

CNAPP solutions address risks across both single cloud or multicloud environments (see Figure 2). This integration fosters improved communication and collaboration between developers, architecture teams and security operation teams, which drives robust and secure application development processes, as well as the assurance of secure workloads in the runtime environment (see Figure 3).

Figure 2: Explosion in the Risk Surface Area of a Cloud-Native Application



Source: Gartner
785751_C

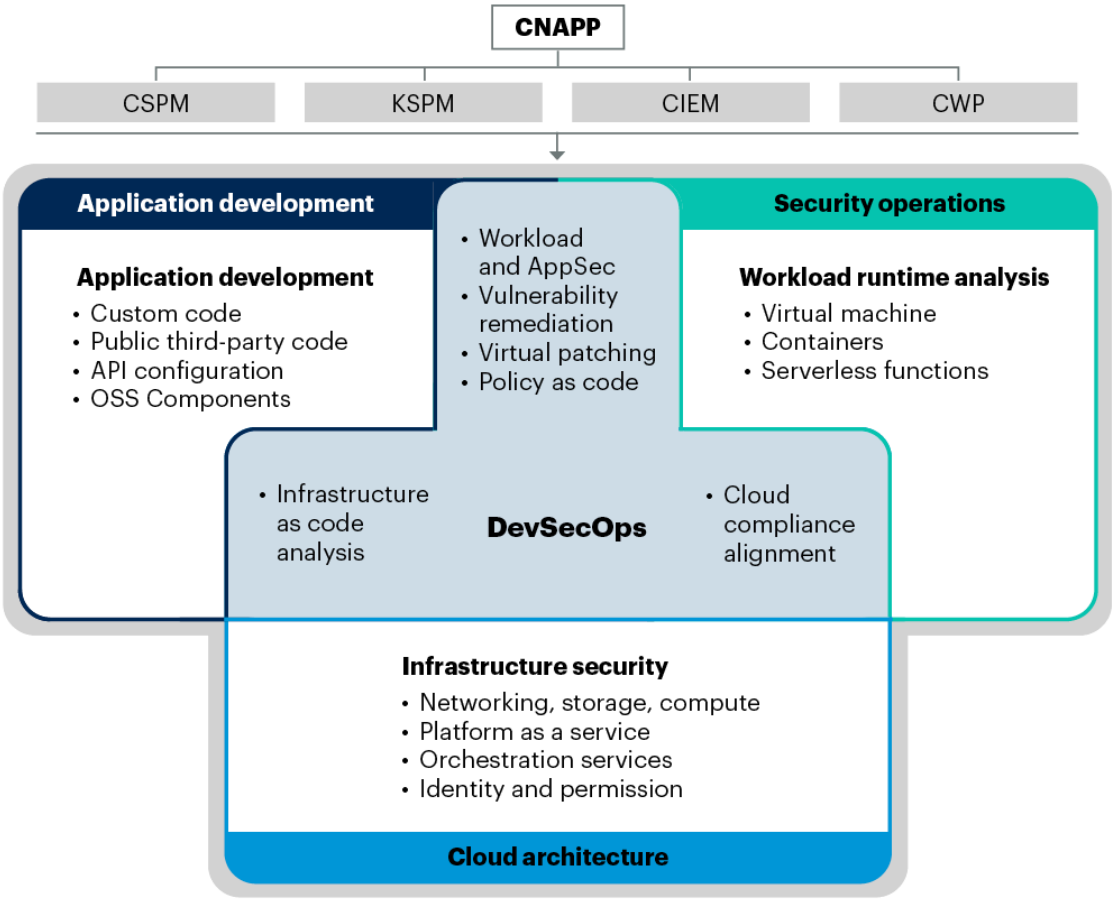
Gartner

Runtime risk visibility is only a part of the risk equation. Developers and cloud architects are increasingly responsible for building more of the cloud infrastructure shown in Figure 2, including the containers and cloud infrastructure setup using infrastructure as code scripts (see Figure 3). In addition, security operations teams find it challenging to manage runtime vulnerabilities discovered within published workloads.

Security operations teams are not responsible for code changes, but in certain cases, they are accountable for remediation efforts. Therefore, better collaboration between SecOps and the responsible developer(s) is required to prioritize the remediation efforts. CNAPP offerings are essentially bringing three previously siloed groups closer together by consolidating the application development teams, cloud architectural and configuration teams, and security operations teams shown in Figure 3.

Figure 3: Developers' and Architects' Expanded Scope of Responsibility for Cloud-Native Applications

Developers' and Architects' Expanded Scope of Responsibility for Cloud-Native Applications



Source: Gartner

CIEM = Cloud infrastructure entitlement management; CNAPP = Cloud-native application protection platforms; CSPM = Cloud security posture management; CWP = Cloud workload protection; KSPM = Kubernetes security posture management; OSS = Open-source software

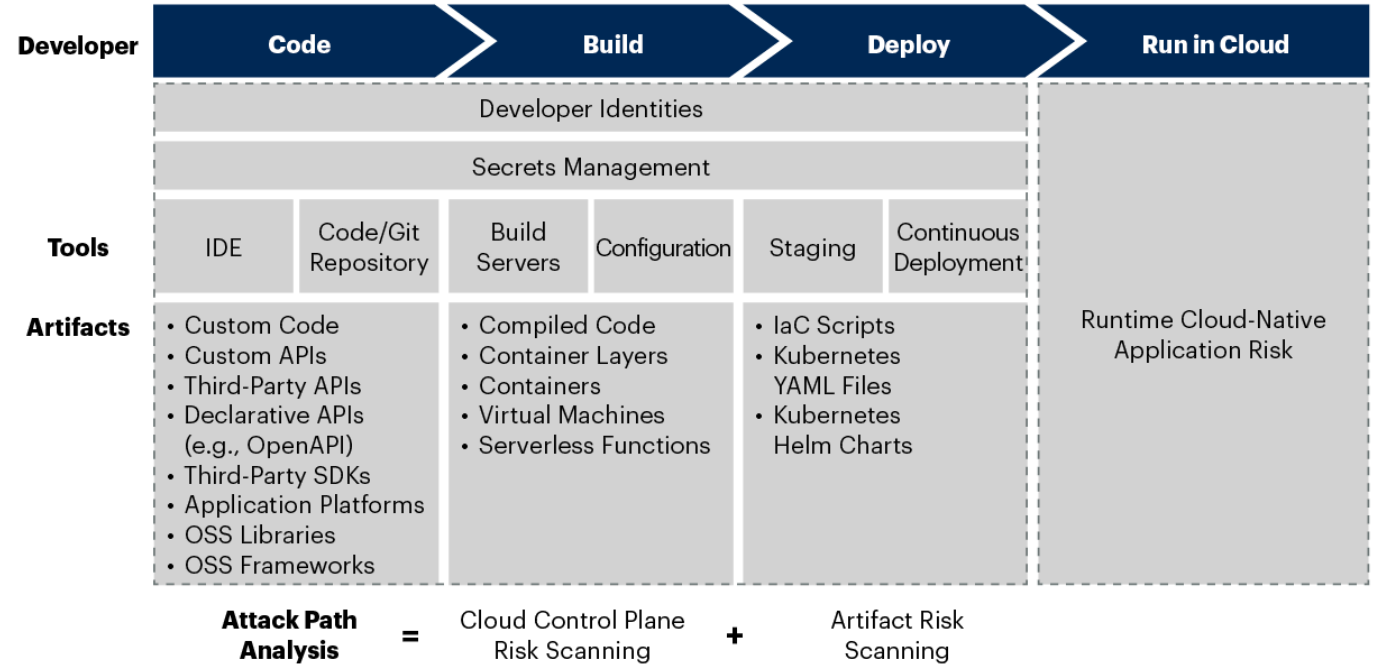
790337_C

Gartner

Because developers are creating containers, serverless functions and cloud infrastructure, CNAPP tooling has since shifted into the development phase — in addition to the comprehensive runtime visibility shown in Figure 5. Shifting risk visibility to development requires a deep understanding of the development pipeline and artifacts and extending vulnerability scanning earlier as these artifacts are being created (see Figure 4 and Note 2).

Figure 4: Code-to-Cloud Risk Visibility, Prioritization and Remediation

Code-to-Cloud Risk Visibility, Prioritization and Remediation



IDE = integrated development environment; OSS = open-source software

Source: Gartner

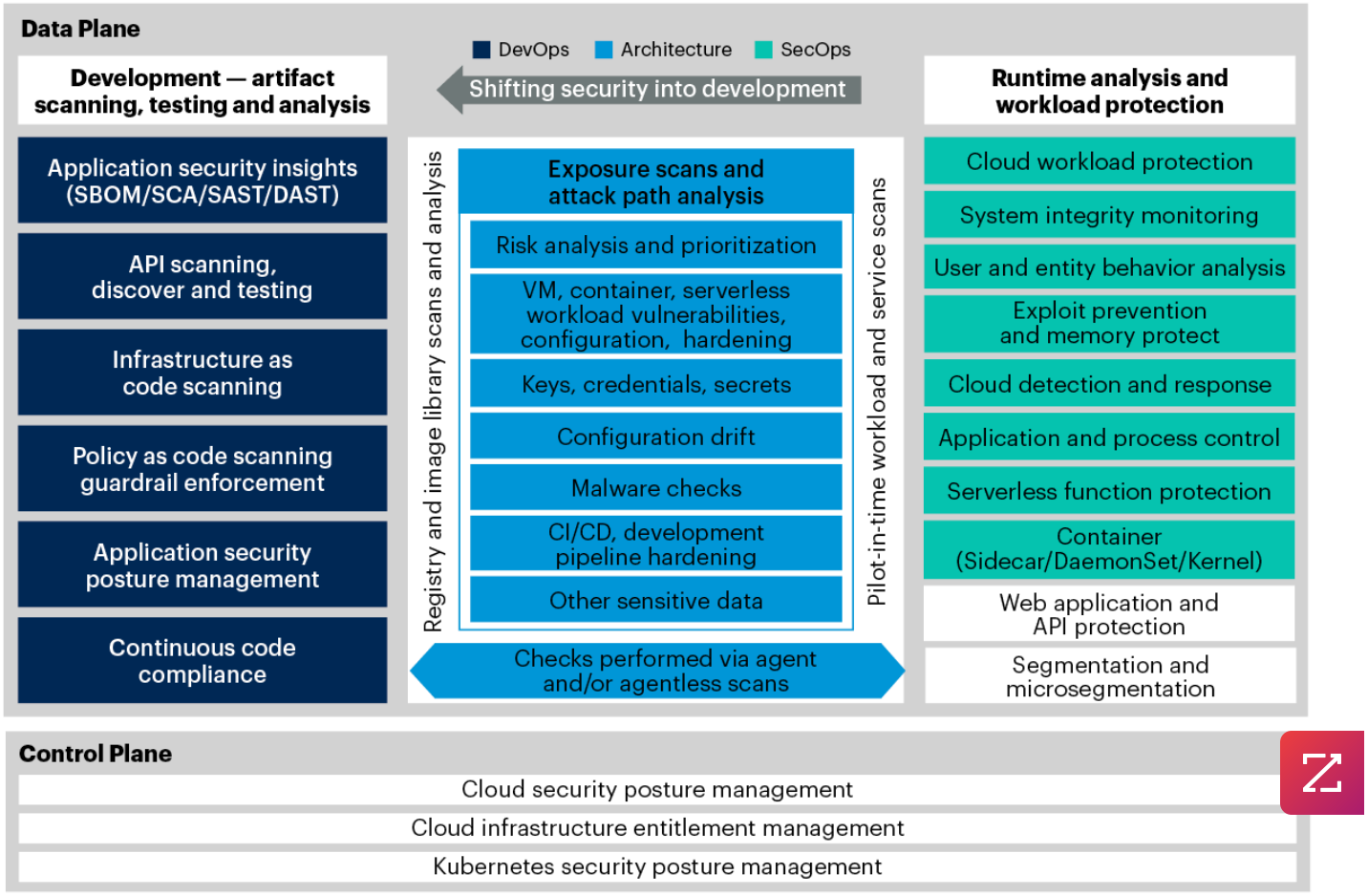
785751_C

Combining the need for runtime risk visibility, cloud risk visibility and development artifact risk visibility results in a robust integrated set of capabilities needed for a complete CNAPP platform (see Figure 5).

Today, no single vendor delivers all of the capabilities shown in Table 2 today.

Figure 5: CNAPP Detail View

CNAPP Detail View



API = Application programming interface; CNAPP = Cloud-native application protection platform; DAST = Dynamic application security testing; SAST = Static application security testing; SBOM = Software bill of materials; SCA = Software composition analysis; VM = Virtual machine

Source: Gartner

790337_C

Gartner

Market Direction

Since identifying the convergence between CSPM, KSPM, CIEM, CWP and other cloud security technologies in mid-2022, client interest — as indicated by Gartner inquiry volume growth — has grown significantly. [1] End-user calls on CNAPPs rose 29% from 2023 to 2024, with an emphasis on CSPM driven by compliance and easy API deployment, with expectations of runtime visibility and control.

The budget for a CNAPP typically comes from the chief information security officer organization, with specific buying centers of cloud security operations, cloud security architects, development/product teams, DevSecOps architects, cloud-native application architects and application security. Gartner has observed a notable shift in the primary buyer landscape, with the security/AppSec team playing a more influential role. This trend is accompanied by the emergence of platform engineering team leaders and cloud and application architects, as well as a greater emphasis on security collaboration. These stakeholders are not only influential in purchasing decisions but also show a keen interest in

the capabilities offered by CNAPP solutions (see **Adopt Platform Engineering to Improve the Developer Experience**).

A few factors drive client interest in CNAPPs.

- The most significant is the need to unify risk visibility across cloud environments and the entire application development life cycle. This simply cannot be achieved using separate and siloed security and legacy application testing offerings. CNAPP offerings operationalize cloud-native application risk analysis by "connecting the dots" to help understand the effective risk throughout the multiple layers of a modern cloud-native application. Prioritizing the risk findings is critical, as developers and security professionals are overloaded with the alerts and findings of siloed tools.

- Another driver is the desire to reduce the complexity and blind spots that come from using multiple cybersecurity vendors and tools by consolidating multiple overlapping security capabilities from a variety of vendors into a single unified platform (see **Simplify Cybersecurity With a Platform Consolidation Framework**). This process not only reduces the total cost of ownership and minimizes technical debt but also requires fewer staff to operate, improves operational management and requires less effort to analyze risk throughout the ecosystem.

- Clients also desire to integrate security and compliance testing seamlessly and transparently in modern DevOps (referred to as DevSecOps) in a manner that balances security and speed and doesn't unnecessarily slow down digital innovation. Information security's role shifts to one of providing the guardrails throughout the entire development pipeline and avoiding gating developers throughout the development process. For example, consider a racetrack where the guardrails are encountered by the driver only for serious issues. Likewise, developers are allowed to innovate at their desired speed with little or no friction from security, unless a critical risk issue is identified. CNAPP offerings enable the construction of guardrails for a modern cloud-native application development pipeline.

The presence of these drivers is exerting a strong influence on the decision-making process of buyers, compelling CNAPP vendors to adapt their capabilities and make substantial platform changes. This adaptation involves introducing natively developed features or acquiring and integrating complementary platforms to meet buyers' evolving demands.

CNAPP offerings primarily concentrate on scanning efforts that target known vulnerabilities, misconfigurations and hard-coded secrets in development artifacts. This is achieved by using a combination of static and dynamic techniques. On the other hand, traditional static and dynamic analysis application security testing tools focus on discovering unknown vulnerabilities in custom code using similar techniques. As a result, CNAPP offerings and application security offerings complement each other, but their functionalities are increasingly overlapping.

To obtain the most comprehensive understanding of risk, use both CNAPP and application security tools. For this reason, more CNAPP vendors are either developing their own capabilities or providing third-party integrations with these specific functions. By doing so, they aim to offer a comprehensive solution that covers all aspects of cloud and application risk management. Over the next several years, Gartner expects several CNAPP offerings to expand into the following areas:

- Application security testing (AST) such as traditional static AST and dynamic AST (SAST/DAST) use cases
- Application security posture management (ASPM)
- API discovery and testing tools and API posture management
- Distributed web application firewall (WAF) for application protection
- Cloud detection and response (CDR)
- Data security posture management (DSPM) for very specific data management use cases

All of this is expected to lead to significant growth in the CNAPP market over the next several years. While Gartner has not yet sized the CNAPP market, it overlaps capabilities and will pull revenue fr several stand-alone markets that make up the core of CNAPP functionality (see Table 1 and **Forecast: Information Security, Worldwide, 2022-2028, 2Q24 Update** and **Market Share: All Software Markets, Worldwide, 2023**). [2]

Table 1: Spending on CNAPPs Will Pull From These Market Segments

Gartner Market Forecast	Estimated Market Size at Year-End 2023, Billions of U.S. Dollars in Constant Currency	Estimated Market Percentage Growth in 2024 in Constant Currency
Cloud Security Posture Management (CSPM) [2] (also see Note 3)	1.4	26.3
Application Security Testing Software [2,3]	1.8	27
Cloud Workload Protection Platforms (CWPP) [4]	3.9	27.9

Vulnerability Assessment	2.2	14.8
Web Application and API Protection	1.7	16.2

Source: Gartner (May 2024)

Benefits of CNAPP Offerings

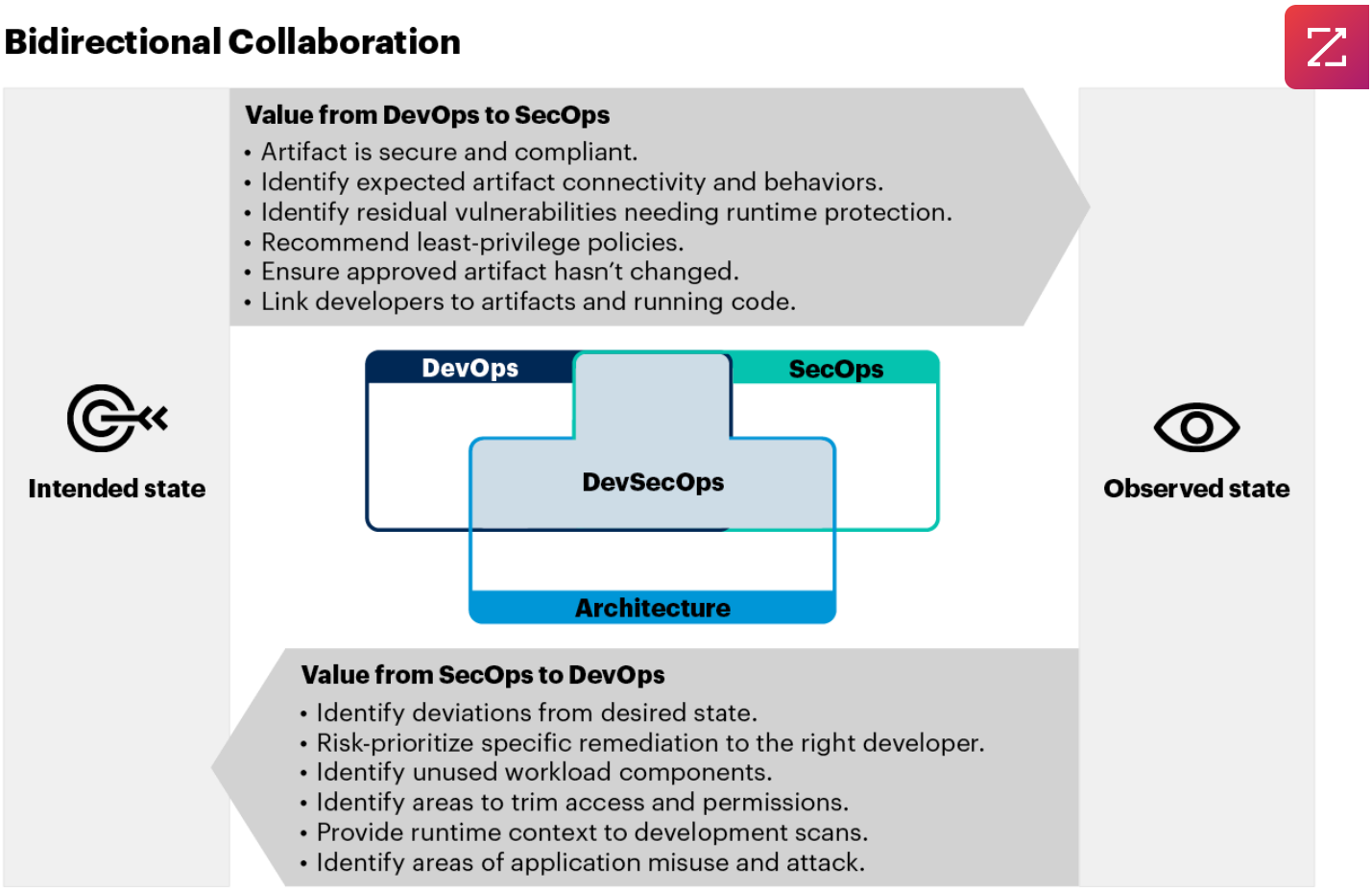
An organization could implement 10 or more tools to deliver fully against the capabilities shown in Table 2. However, organizations have reasons to move toward consolidation in a CNAPP offering:

- It provides better identification, prioritization and remediation of cloud-native application risk through a centralized and unified platform providing actionable insight in a multiteam structure.
- CNAPP reduces operational complexity through consolidation of vendors, consoles, policies and contracts, thereby reducing chances of misconfiguration or mistakes. This enables:
  - A single collaborative platform to define consistent security policies throughout development and operations
  - Consistent enforcement of security policy across all application artifacts — code, containers, virtual machines (VMs) and serverless functions irrespective of the hyperscale cloud environment
  - Elimination of overlapping policies of disparate products and standardization of application policies and policy objects across all development artifacts
- A CNAPP vendor should implement a single data lake, data model and unified graph database for all event logging, reporting, alerting and relationship mappings. This enables the vendor to deliver effective risk analysis — finding the root cause of the risk, identifying the person/team responsible for fixing it and risk-prioritizing the remediation efforts. This reduces the attack surface and shortens remediation times.
- By having consistently enforced policies and by risk-prioritizing remediation efforts, a unified CNAPP offering should reduce developer friction and improve developer experience. By integrating security testing throughout the life cycle and directly into the developer's toolset versus one large test prior to production, CNAPP offerings proactively enable:
  - Proactively fixing problems earlier

- Shortening application deployment time
- Minimizing runtime vulnerabilities identified through reactive toolsets that monitor runtime environments

- CNAPP eliminates redundant capabilities (for example, most cloud providers offer container vulnerability scanning).
- These offerings greatly increase runtime visibility so it can be used as context to feed back into development teams. Likewise, a single platform more easily enables visibility from development used to strengthen runtime protection (see Figure 6).
- CNAPP bridges the communication gap of previously siloed development teams, security architecture teams and security operations teams with a consistent view of risk across the entire cloud environment(s).

Figure 6: Bidirectional Collaboration



Source: Gartner
790337_C

Gartner

Challenges to CNAPP Adoption

- **Security organizational buying personas:** Multiple teams are partly responsible for cloud-native application security as it's considered a shared responsibility. These teams are distributed across various areas such as data center security, application security and cloud architecture and information security. Each of these teams has tools that solve a part of the cloud risk puzzle, but rarely do these teams cooperate in product evaluation and selection. Some teams will prefer specific tools that address their immediate need and will avoid change.

- **Adversarial relationship between developers and security:** Developers perceive security teams as impeding the speed of modern DevOps processes. Security controls weren't designed for the speed and scale of cloud-native applications and weren't designed with the developer as the central customer. Historically, the result has been poorly integrated testing that required the developer to leave their development environment, slow development and waste their time with false positives or asking them to remediate low-risk vulnerabilities.

- **Existing investments:** Many organizations have existing technical debt from a variety of niche vendors to cover code to cloud security and compliance. Most organizations already have some form of runtime CWP in their virtual machines such as existing traditional endpoint detection and response (EDR) solutions. Many public cloud adopters selected scanning tools for containers i development and also introduced a stand-alone solution for CSPM. Most organizations have several vendors for different (or sometimes similar overlapping) functions, creating silos of users and findings and making it difficult to create a unified picture of risk. As organizations shift to a CNAPP-based approach, the synergy of an integrated platform will provide more benefits than a best-of-breed strategy that is difficult to scale.

- **Mindset changes:** Security teams must understand and acknowledge that a perfect, risk-free application is not possible. Perfect is the enemy of good enough. Instead, security teams should focus on an approach that identifies the highest severity, highest confidence risk and risk-prioritizes remediation efforts to the responsible developer. Similarly from the developers' side, cloud-native security becomes a risk-prioritized set of guardrails (replacing the former model of security "gates" in the development process), thus placing more accountability on the developer, which may hinder adoption.

- **Architecture:** Some CNAPP offerings are built to be provided as a SaaS-only offering. Others were designed to be run entirely with the customer environment. The best offerings will use a distributed cloud architecture with a cloud-managed control plane and decentralized inspection under the customer's control (for example, scanning containers or snapshots locally without requiring them to be uploaded to a SaaS service). Some CNAPP solutions do not provide options for where data is scanned but rather force the end user to scan within the public cloud environment, which only increases compute costs and inhibits the adoption of CNAPP.

- **Maturity:** For the next several years, CNAPP capabilities will continue to vary widely, and some vendors are immature in multiple areas. For example, sensitive-data visibility and control is often a priority capability for clients but is difficult for many CNAPP vendors to address. Understanding of data context in unstructured and structured storage repositories is necessary to fully understand and address the context and prioritization of risks, but many CNAPP vendors don't yet offer this. Also, CNAPP vendors that don't offer both agent and agentless integration limit their solution's adoption.

- **Legacy applications:** Older applications that aren't fully cloud-native may require specialized tooling and rely more heavily on traditional approaches, such as SAST and WAFs.

- **Immature single vendor offerings:** Certain vendors make claims about their ability to encompass all the elements and capabilities of CNAPP. However, upon closer examination, while these vendors offer a wider range of capabilities, they often lack the necessary feature maturity and specialization in specific capabilities.

- **Stand-alone tools Integration:** Some CNAPP solutions lack robust technology partnerships and comprehensive integration options with other vendors and stand-alone tools. This limitation can result in fragmented views of risk and potentially impact the application development pipeline. However, many CNAPP vendors are actively addressing this challenge by investing in research development. They are working toward mitigating these limitations by offering options to integ with supplementary services.

Market Analysis

CNAPP vendors have emerged from diverse origins, with some initially focusing on supporting development and cloud architecture through stand-alone CSPM functions. These vendors expanded their offerings to include more reactive observability by introducing workload runtime capabilities and incorporating agent and/or agentless workload monitoring for enhanced reactive security controls. On the other hand, other vendors originated in the workload runtime space and introduced complementary capabilities, shifting further left toward providing proactive security visibility and control.

The convergence of markets formed the foundation of the CNAPP market. Recognizing the need for improved orchestration compliance and identity and entitlement management, vendors in both submarkets developed or acquired additional functionality to cover Kubernetes and identity permissions management. The net result was the establishment of the comprehensive CNAPPs we see in today's market.

CNAPP offerings can be broken down and categorized into several baseline origins:

- Vendors that initially focused on runtime workload visibility and protection derived from the EDR market or were purpose-built from the ground up for container security and were previously established as CWPPs

- Vendors that initially focused on a shifting security into the development space, providing CSPM with a focus on cloud configuration scanning, infrastructure as code script scanning and orchestration visibility and control
- Vendors that initially focused on artifact scanning early in the development life cycle, such as software composition analysis and API security testing
- Vendors who initially offer mature CIEM services alongside their CSPM capabilities that provided consumers with better guardrails for identity access management, entitlement and permissions management within cloud infrastructure environments for human and workload entities

As with any emerging technology category, and especially as CNAPP progresses through the Trough of Disillusionment in multiple Gartner Hype Cycles (see **Hype Cycle for Application Security, 2023** and **Hype Cycle for Workload and Network Security, 2023**), CNAPPs have been subject to an immense amount of marketing hype and media abuse over the past two years. CNAPP offerings bring together multiple disparate security and protection capabilities into a single platform focused on identifying and prioritizing excessive risk of the entire cloud-native application and its associated infrastructure.

However, we frequently see vendors that market CNAPP but don't meet Gartner's minimum requirements. Since the complete listing of CNAPP capabilities is quite broad, we have broken the capabilities into three categories: core, recommended and optional (see Table 2).

Table 2: CNAPP Core, Recommended and Optional Capabilities

Core Functions	Recommended Capabilities	Optional Capabilities

- CSPM, including integration with leading hyperscale providers
- KSPM providing security risk analysis of Kubernetes orchestration platforms
- Infrastructure as code (IaC) scanning, including support for major IaC scripting languages and YAML/Helm for Kubernetes
- CIEM providing identity, entitlement and permissions visibility and control
- Scanning of containers and container registries for risk [a]
- Cloud workload protection providing:
- Agentless runtime visibility into VMs, containers and serverless functions
- Point-in-time analysis of workloads
- Attack path analysis

- Advanced cloud workload protection providing:
  - Agent-based runtime visibility into VMs, containers and serverless functions
  - Real-time, runtime analysis of workloads
- API discovery and monitoring
- Scanning of unstructured IaaS data repositories for risk [a]
- Traffic monitoring capabilities and connectivity mapping
- WDR
- CDR capabilities beyond just workload monitoring (for example, looking at event logs, network logs and DNS look-ups)
- Workload drift detection from expected state
- Support for other common clouds — Oracle, IBM, Alibaba Cloud
- Scanning of application artifacts for risk
- Serverless code scanning
- Software composition analysis, including software bill of materials creation
- Application layer observability
- Scanning of code repos

- Runtime application self-protection (RASP)
- API scanning for unknown vulnerabilities
- Support for on-premises deployments
- Support for other container environments such as Red Hat OpenShift
- Support for policy as code scanning including support for Open Policy Agent
- AI security posture management
- API protection and distributed WAF at runtime
- CI/CD development pipeline hardening
- AST elements (DAST/SAST)
- ASPM and application observability
- Integration with software supply chain security solutions
- Scanning of IaaS structured data repositories for risk (combined with unstructured data scanning, delivers a DSPM capability [b])
- Support for AI/ML integration for policy enrichment, recommendations or common language interpretation
- Digital forensics and incident response

	• Support for Extended Berkeley Packet Filter (eBPF)	
[a] Risk scanning includes • Configuration scanning • Vulnerability scanning for known vulnerabilities • Secrets scanning • Attack path analysis		[b] DSPM in relation to CNAPP specifically refers to the scanning and assessment of unstructured data stores in an IaaS/PaaS environment.

Source: Gartner (July 2024)

The capabilities in Table 2 should be cohesive. A well-architected, single-vendor CNAPP offering should have the following characteristics:

- All core services should be fully integrated, not loosely coupled independent modules (typically resulting from a vendor's internal silos, poorly integrated OEM components or those added from an acquisition). Integration should include the front-end console, unified policy across multiple points of inspection and a unified back-end data model
- A deep understanding of the relationships between an application's elements (VMs, containers, service functions and storage), security posture, permissions and connectivity, typically enabled by underlying graph database technology.
- An understanding of the relationship between development artifacts (custom code, libraries, container images, VMs and IaC scripts) as well as who created them and when they were created, who deployed them and when they were deployed, and who changed them and when they were changed.
- Integrated advanced analytics that are combined with the graph relationships to risk-prioritize findings in development and at runtime.
- A single unified management plan reduces switching between multiple consoles, not disparate management systems loosely integrated via API.
- Primary management console is cloud delivered through an as-a-service offering. Optionally, support for customer-hosted management consoles is provided to address security and risk-

sensitive environments, such as air-gapped environments or regulatory domains.

- Inspection across all artifacts: containers, VMs, serverless functions and data storage.
- Simple consumption-based pricing model based on major cloud-native application assets, such as VMs, container hosts, serverless functions and unstructured/structured storage repositories.
- The customer should have the flexibility to decide where the inspection of artifacts takes place, whether it is within the cloud environment or under their own control. This includes the option for on-premises inspection, which is suitable for security-sensitive use cases, as well as the choice to leverage cloud compute resources for cost-reduction purposes.
- The option for single tenancy even if delivery is cloud-based (for security-sensitive use cases).
- Integration with key management systems to allow scanning of encrypted storage objects for risk.
- Integration into CI/CD common development toolsets including code repositories, build servers and container registries and their audit/logging telemetry.
- Predefined templates for reporting against common compliance standards — for example, CIS, NIST, PCI, GDPR and HIPAA.
- Support for all three major hyperscale providers: Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP). Some organizations may require integration with additional clouds, such as Oracle, IBM, Alibaba Cloud, VMware and others.

Even in this early phase of the market, multiple CNAPP offerings in the market meet these core requirements. Vendors of these offerings are listed in Table 3.

Due to the diverse origins of vendors in the CNAPP market, capabilities are fragmented, and the maturity levels of the offered stack of capabilities vary based on each vendor's foundations. Therefore, when assessing CNAPP offerings, businesses must establish a collaborative team consisting of members from development, cloud security architecture, and security operations. This team should prioritize and rank their requirements for mandatory, recommended and optional functionality during the evaluation of different CNAPP offerings. By involving all relevant stakeholders and aligning their needs, organizations can make informed decisions and select the most suitable CNAPP solution for their specific requirements.

These collaborative teams more deeply understand the relationship between a cloud-native application's different elements (see Figure 2), and each team's priorities for success. A collaborative team is a critical step to delivering risk mitigation vision across the cloud ecosystem. In other words, to make risk identification and remediation operational, CNAPP tools must be able to build a model of the application code, libraries, containers, scripts, configuration and vulnerabilities to identify where the effective risk resides.

Since risk-free applications are impossible, information security must prioritize risk findings according to business context, identifying the root cause and enabling developers to focus first on the highest risk findings with the highest confidence of potential business impact. Likewise, the business requires a deep understanding of the relationship between developers/development teams throughout an application's life cycle (see Figure 3 and 4) is critical to identifying the right developer/development team or engineering team to rectify the risks identified and to provide these teams with sufficient context to understand and remediate the risks quickly and effectively.

With cloud-native applications, IT or information security is rarely responsible for remediating the issues identified. The developer who codes it owns it!

With modern cloud-native applications, it can be difficult if not impossible to use a traditional host-OS-based agent approach. In some cases, the DevOps product teams won't accept them, and in other cases, the value of runtime visibility into ephemeral workloads is not offset by the operational overhead of deploying and managing agents. To address this, leading CNAPP offerings provide a variety of agent and agentless alternatives for runtime visibility into workloads, including:

- Snapshots of running workloads and analysis of the snapshot created
- Privileged containers
- DaemonSets
- Kubernetes sidecars
- Libraries for inclusion in the development pipeline
- eBPF-based instrumentation for Linux
- LD_PRELOAD Linux system call interception [5]
- Envoy or F5 NGINX proxy integration
- Service mesh integration
- Cloud control plane, API-based integration to inspect configuration and activity logs
- Kubernetes API controller integration to inspect configuration and activity logs
- Copies of workloads that are mounted and dynamically observed in an isolated environment (application sandboxing)
- Language-specific runtime instrumentation (sometimes referred to as RASP)

- Serverless function instrumentation layering techniques (e.g., AWS Lambda layers)

Hyperscale providers are investing in generative AI (GenAI) technology aggressively and offer cloud AI developer services (see **Magic Quadrant for Cloud AI Developer Services**). A few CNAPP offerings extended their coverage to some of these GenAI-related services.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

Cloud security leaders looking to secure the rapid development needs of cloud-native applications should consider CNAPP offerings as an integrated, developer-centric solution. CNAPPs can improve the developer experience by integrating into their native development toolset as seamlessly and transparently as possible. CNAPPs do this by reducing false positives and noise, by risk-prioritizing their remediation efforts and by providing specific remediation guidance to resolve the identified risk. CNAPP offerings can also help organizations adopt a stronger security posture in their development pipeline throughout the entire development life cycle (code to cloud).

Table 3 lists representative CNAPP vendors. To develop the list of representative vendors, we used the core and recommended capabilities and characteristics described in the Market Analysis section of this research. Some vendors sell multiple modules to build out the full set of CNAPP capabilities. In this early stage of the market, no single vendor has all capabilities.

Table 3: Representative CNAPP Vendors

Vendor	Offering
Aqua Security Software	Aqua Cloud Security Platform
Caveonix	Caveonix Cloud-Native Application Protection Platform
CrowdStrike	CrowdStrike Falcon Cloud Security
Cyscale	Cyscale CNAPP

Datadog	Datadog CNAPP
Data Theorem	Cloud Secure
Google Cloud	Google Security Command Center
Lacework [6]	CNAPP Security
Microsoft	Microsoft Defender for Cloud
Orca Security	Orca Cloud Native Application Protection Platform
Palo Alto Networks	Prisma Cloud
Qualys	Qualys TotalCloud
Rapid7	InsightCloudSec
SentinelOne	Singularity Cloud Security
Sophos	Sophos Cloud Native Security
Sysdig	Sysdig Secure
Tenable	Tenable Cloud Security
Trend Micro	Trend Vision One – Cloud Security

Uptycs	Uptycs CNAPP
Wiz	Wiz CNAPP

Source: Gartner (July 2024)

Market Recommendations

Strategy and Planning

- Whether a CNAPP is adopted or not, establish a vision for DevSecOps that puts developer experience as the primary goal. Aim for reduced developer friction, better risk identification and reducing false positives through improved security collaboration. Don't force development teams to leave their native tools, and provide specific context and recommendations for remediation.
- Create a unified CNAPP strategy and evaluation team spanning cloud security, container security and application security, cloud architecture, and security operations. Cloud security is now a shared responsibility, but the developer is the ultimate persona who will remediate the identifie risk and the SecOps team should include representatives from DevSecOps/development. Inventory the organization's CI/CD pipeline tools as this will be a critical input into the evaluation process.
- Use adoption of a CNAPP offering to consolidate vendors to cut complexity, simplify security policy enforcement, provide better context and prioritization, and improve the developer experience. There is also the potential to reduce duplicative costs of point solutions as contracts renew for CWP, CSPM, SCA, CIEM and container security offerings.

Evaluation

- Have the joint development/security team identify and rank the enterprise functionality requirements into required, preferred and optional before sending out requests for information/purchase, as no single vendor is best-of-breed in all CNAPP capabilities.
- Prioritize CNAPP offerings with deep relationship graph analytics expertise. The ability to identify cloud risk and deliver against risk prioritization and mitigation requires the ability to understand the relationships between a cloud-native application's different elements and to understand each element's risk. This requires an understanding of cloud control plane risk and artifact risk and then combining these together to understand, prioritize and remediate the resultant risk of the entire system.

- Evaluate the organization's existing security DevSecOps tools portfolio from development through to runtime SecOps. Build a matrix of what is essential to each of your teams and find where the overlaps are within CNAPP. Work with your teams to determine if tools consolidation is possible into CNAPP without causing major operational gaps or security holes.

- Run a functional pilot with real developers and applications before selecting a single-vendor CNAPP offering to ensure that functionality and developer experience meet your requirements.

Deployment

- Focus the CNAPP rollout on cloud-native applications being developed first versus applications being migrated as-is to cloud — where development speed is paramount and risk identification is imperative. Even if a full CNAPP deployment is not possible, deploy CSPM and CIEM capabilities if you haven't already, as most cloud-native application risk is caused by misconfiguration, mismanagement or excessive permissions.

- Make software composition analysis and scanning containers, OSS libraries and dependencies for known risks (common vulnerabilities and exposures [CVEs], hard-coded secrets, passwords, API keys, etc.) a high priority as this is another common source of risk in cloud-native applications.

- Be pragmatic, not dogmatic in the CNAPP deployment. Agents may provide the best visibility b aren't always possible. Use inside-out workload runtime visibility where you can and agentless snapshots where you can't because some visibility into risk is better than nothing.

Evidence

[1] Hundreds of Gartner inquiries on the topic of CNAPPs with end-user organizations were analyzed for the 12 months between 2022 and 2023 and compared to the 12 months between 2023 and 2024 with a year-over-year increase of 29%.

[2] The estimated market size for CSPM was taken from **Forecast Analysis: Cloud Security Posture Management, Worldwide** and **Market Share: All Software Markets, Worldwide, 2023**.

[3] The estimated market size for application security spending was taken from **Magic Quadrant for Application Security Testing** and **Market Share: All Software Markets, Worldwide, 2023**.

[4] The estimated market size for CWPPs is pulled from a major category called Cloud Security, which is a combination of CASB and CWPP markets. Gartner sees the CASB market as a separate market. See Note 3.

[5] **What Is the LD_PRELOAD Trick?**, Baeldung.

[6] **Fortinet to Acquire Lacework, Enhancing the Industry's Most Comprehensive Cybersecurity Platform**, Fortinet. Fortinet announced on 10 June 2024 its intent to acquire Lacework. As of writing this Market Guide, the two vendors and their associated CNAPP products were still operating

independently. Fortinet's current CNAPP offering has some capability gaps in their coverage which the Lacework acquisition will close out.

Note 1: Gartner's Initial Market Coverage

This Market Guide provides Gartner's coverage of the market and focuses on the market definition, rationale for the market and market dynamics.

Note 2: Development Artifacts That Should Be Scanned for Vulnerabilities, Misconfiguration, Malware and Secrets

The following artifacts should be scanned to ensure they are secure, configured correctly and free from malware, vulnerabilities or inappropriately exposed sensitive information:

- OSS modules, libraries and frameworks
- Third-party software development kits
- Container layers and containers
- Serverless functions
- APIs and declarative API schemas
- Custom application code
- Compiled code/binaries
- Infrastructure as code scripts
- YAML Ain't Markup Language (YAML) and other cloud configuration files, such as Kubernetes Helm charts
- Virtual machine images

Note 3: SSE, CASB and CNAPP Overlap

Most stand-alone CASB revenue will migrate to the security service edge market (SSE). Several SSE vendors also have included limited CSPM capabilities (and some of these also have limited CWP capabilities) that will overlap with CNAPP and be sold to buyers targeting the CNAPP use case. Gartner sees a distinct separation in the SSE market and the CNAPP market based on buyer requirements and capabilities consolidation toward each respective market type.

Note 4: Application and Software Supply Chain Security Tools Adjacent to CNAPP

Several vendors focus only on identifying the relationship between development tools, developers and the artifacts they create. These vendors aren't full CNAPP providers but do add value to a CNAPP deployment in several ways. Most importantly, by having a deep understanding of the provenance of artifacts created in development by multiple developer/development teams, the offerings help to identify the person or team responsible for remediating the identified risk and speeding the time to remediate.

Some of these offerings will also identify the tools used in the code pipeline and the security posture of the code pipeline. Some offer a more intelligent, risk-based approach to software composition analysis or application security posture management. Others deduplicate risk findings of multiple security and risk scanners to help prioritize remediation efforts. Example vendors here include Apiiro, BoostSecurity, Cycode, Dazz, Deepfactor, DevOcean, Enso Security, Oligo, OX Security, Oxeye, Rezilion and Tromzo.