Market Guide for Cloud-Native Application Protection Platforms

5 August 2025 - ID G00826547 - 39 min read

By: Dale Koeppen, Esraa ElTahawy, Neil MacDonald

Initiatives:Security of Applications and Data; Build and Optimize Cybersecurity Programs

Cloud-native application protection platforms address the full life cycle protection requirements of cloud-native applications and infrastructure from development to production. Cybersecurity leaders responsible for cloud security strategies should use this research to analyze and evaluate CNAPP offerings.

Overview

Key Findings

- The widespread adoption and increasing complexity of cloud computing represent a sophisticated attack surface. Most cloud-related issues stem from how organizations configure and use the cloud, rather than vulnerabilities inherent to the cloud provider itself.
- 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.
- Cloud security requires collaboration among technical and nontechnical stakeholders to achieve desired security outcomes. When cross-team communication is minimal, it can lead to inconsistent security practices, diminished overall strategic visibility and control, and fragmented views of risk, leading to unacceptable risk exposure.
- With operational responsibilities shifting toward developers and cloud architects, advanced tools must address vulnerabilities, securely deploy infrastructure as code and manage production workload implementations. Proactively identifying and prioritizing risks during development, while passing adequate context back to developers for corrective actions, is essential to streamlining DevSecOps and minimizing the friction of security in development.

Recommendations

Security leaders responsible for cloud security strategies should:

- Adopt CNAPP solutions to enhance the security of cloud environments and cloud-native applications by providing comprehensive visibility and control over cloud platforms and workloads. These tools protect against runtime threats, rectify cloud infrastructure misconfigurations, integrate security into development and address risk resulting from an expanding attack surface.
- Focus on comprehensive and unified CNAPPs that provide extensive capabilities and support an open integration model for additional services. This approach ensures the required breadth and depth of functionality to seamlessly integrate across the entire development ecosystem and cloud platform environment. No single vendor offers best-of-breed capabilities across these domains.
- Evaluate and select the right CNAPP offering by forming a cross-functional team comprising experts from security operations, cloud security architecture, application security and development operations (DevOps) for consensus on desired outcomes.
- 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, 40% of enterprises that successfully implement zero trust within cloud service provider environments will rely on the advanced visibility and control capabilities offered by CNAPP solutions.
- By 2029, 50% of all enterprise applications are expected to operate in containers, necessitating enhanced and unified security controls for cloud and applications.

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 and cloud infrastructure traditionally involved using multiple tools from various vendors, which often lacked cross-integration and were primarily designed for security professionals, overlocking collaboration with developers. Consequently, this lack of integration led to fragmented views of risk with limited context, making it challenging to effectively prioritize systemic risks within both the cloud infrastructure and developed applications. Using security tools that are not fully unified results in excessive alerts, which wastes developers' time, complicates remediation efforts and creates confusion for targeted roles.

One key challenge within DevSecOps 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 applications.

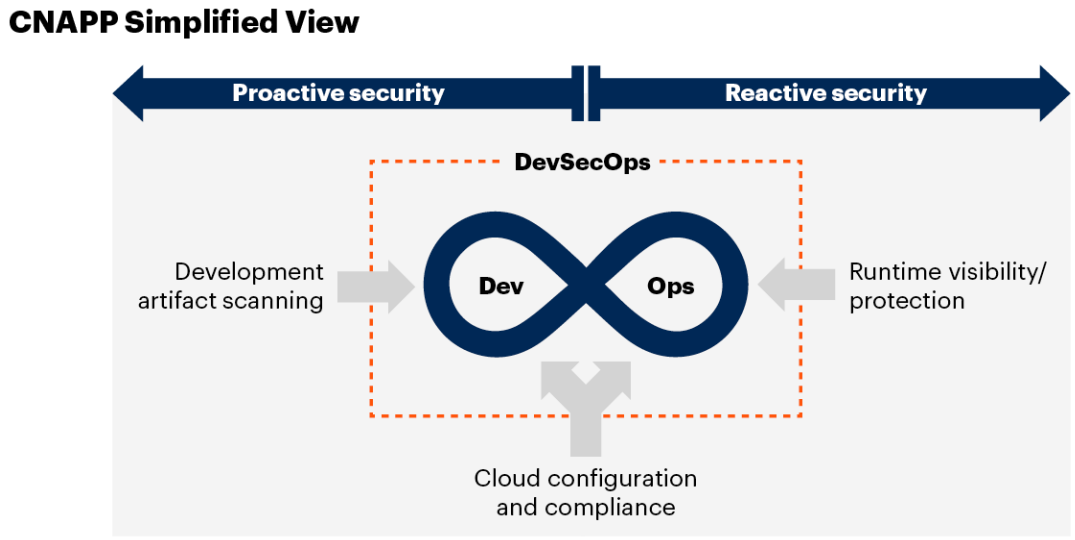
The CNAPP market has emerged to meet these challenges through integration and collaboration. [1] To that end, the development of modern cloud-native applications typically has the following characteristics:

- Constructed using discrete code functions using microservices 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.
- Used a combination of custom code and publicly sourced code from various libraries that are either open-sourced or privately sourced repositories, this can include AI artifacts (AI modes, API to AI services).
- Deployed onto programmatic cloud infrastructure, taking 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 aim to improve your security posture by proactively addressing risks that arise from known, unknown and unexpected exposures that arise from the dynamic and complex nature of developing and deploying cloud-native applications.

CNAPP platforms aim to deliver comprehensive security analysis 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 code and platform risks within the intricate logical boundaries of modern cloud-native applications.

Figure 1: CNAPP Simplified View



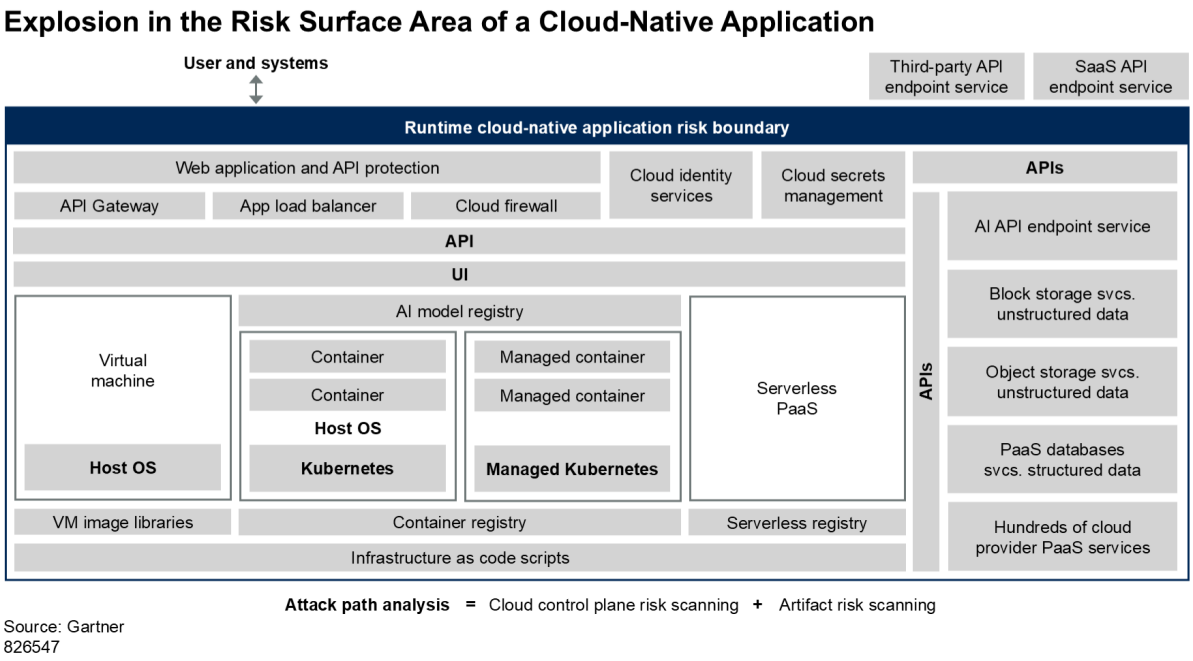
CNAPP platforms are typically sold and delivered as a single platform solution through a cloud-provided, as-a-service offering that aims to secure and protect infrastructure as a service (IaaS) and platform as a service (PaaS) platforms and the running workloads within these environments. CNAPP solutions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

- Consolidate with cloud service provider (CSP) environment 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). This is generally offered in two different deployment methods:
  - Natively offered by the CSP either through a direct embedding of the functions into the CSP platform or offered as a separate security product by the CSP and integrated via API into the CSP's own cloud environment. This method generally has a capability bias toward the CSP's own environment.
  - Alternatively, it can be offered as an enterprise-grade third-party offering that is CSP-agnostic, delivered as a cloud-as-a-service offering and integrated via API into the CSP(s) environment(s). This option generally exhibits minimal bias toward any specific CSP environment.

- Incorporate with the CSP's workload runtime environments via API to perform point-in-time analysis, or directly engage with the workload using an agent-based deployment for real-time monitoring and risk assessment. This is typically offered by cloud workload protection (CWP) solutions.
- Combine with the development pipeline tools to provide workflows and compliance guardrails for coding development teams and cloud architecture teams.
- Synergize with supplemental tooling needed by development, architecture and security operations teams for contextual enrichment, spanning from code development and application testing to cloud compliance, as well as runtime visibility and control.

CNAPP solutions address risks across both single-cloud and 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.

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

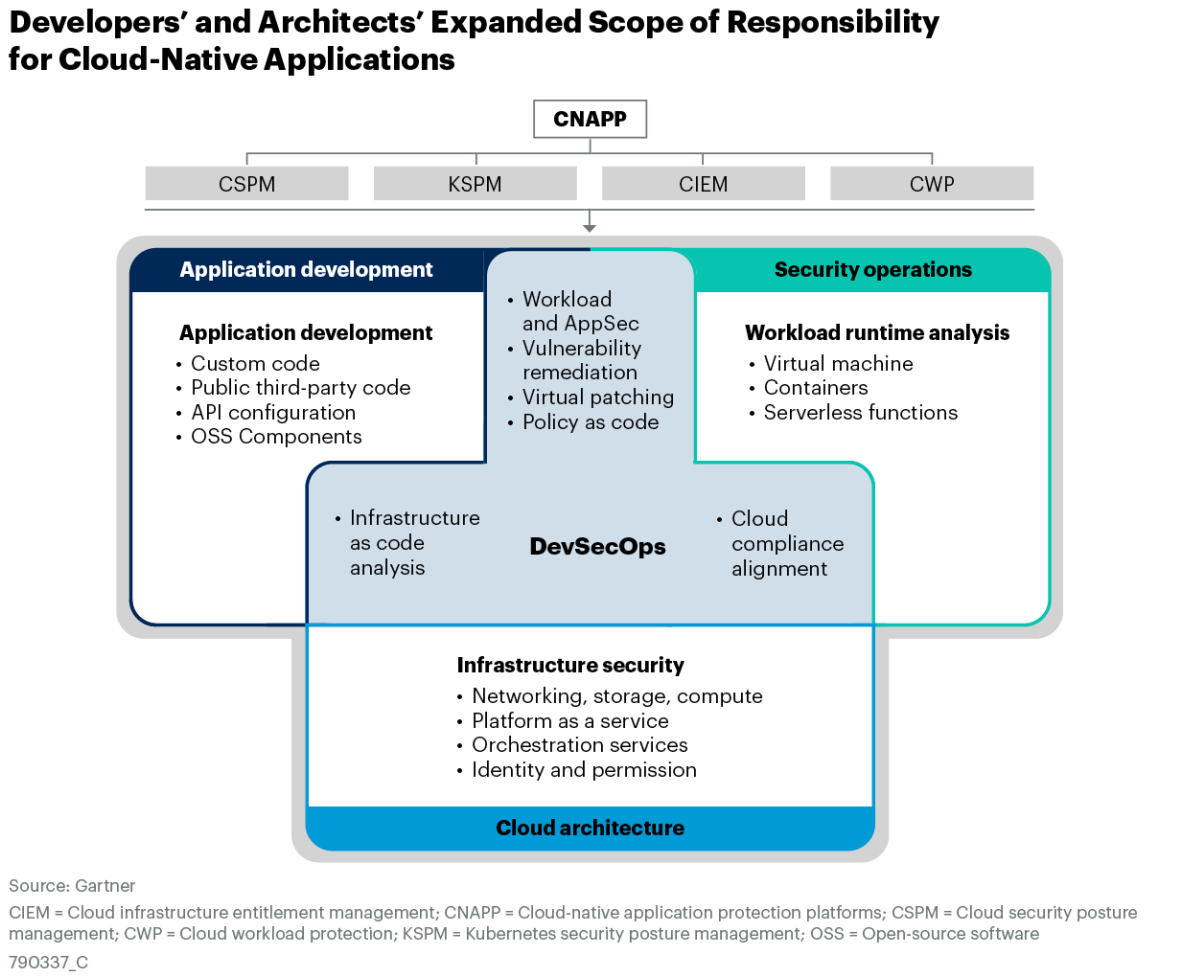


Source: Gartner
826547

Gartner

Developers and cloud architects are increasingly responsible for building more of the cloud infrastructure shown in Figure 2, including both the containers and the cloud infrastructure configuration using infrastructure as code scripts (see Figure 3). Once development pushes workloads into a production state, security operations teams are often tasked to monitor these cloud-native applications. They need the capabilities to pull contextual runtime data on behavior and threats while feeding this context into SIEM and SOC services for event correlation. Without this context, security operations (SecOps) finds it challenging to manage runtime vulnerabilities discovered within published workloads and identify abnormal workload co-pilots resulting from exploiting vulnerabilities or excessive privileges. Consequently, while SecOps teams are not responsible for code changes, they are occasionally accountable for initiating and overseeing remediation efforts with those tasked with fixing vulnerabilities identified in the cloud platforms and workloads. CNAPP implementations are only truly effective when cybersecurity leaders foster strong collaboration between SecOps, platform teams and the developer(s) responsible for workloads by prioritizing 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



Source: Gartner

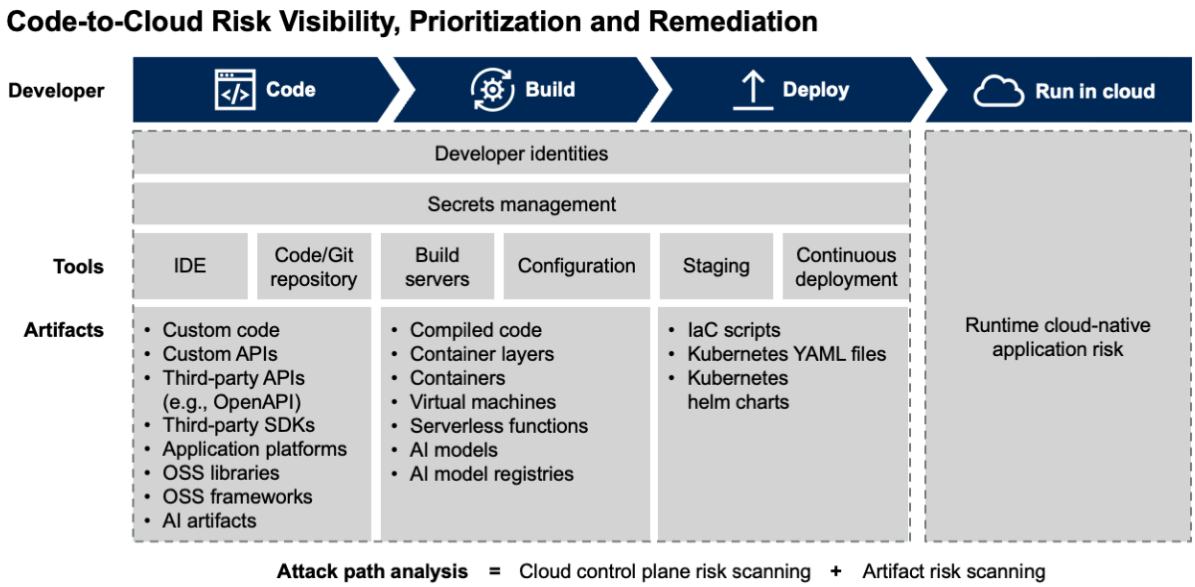
CIEM = Cloud infrastructure entitlement management; CNAPP = Cloud-native application protection platforms; CSPM = Cloud security posture management; CWP = Cloud workload protection; KSPM = Kubernetes security posture management; OSS = Open-source software

790337_C

Gartner

Because developers are creating containers, serverless functions and the instantiation parameters for cloud infrastructure as well as the workload code, CNAPP tooling has 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 1).

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

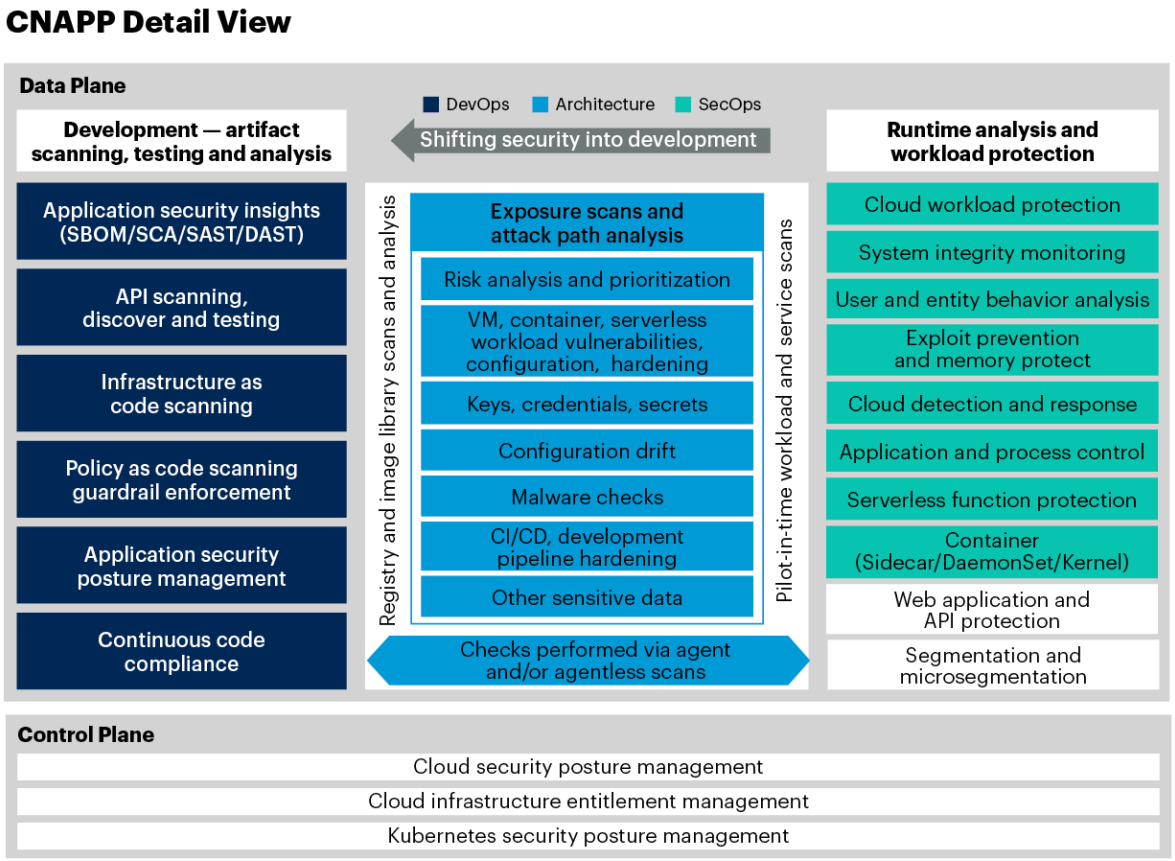


Source: Gartner
Note: IDE = integrated development environment; OSS = open-source software
826547

Gartner

To be truly effective, a complete CNAPP platform would deliver a robust set of benefits, including runtime risk visibility, cloud risk visibility and development code and artifact risk visibility, resulting in a powerful integrated set of capabilities needed for a complete CNAPP platform (see Figure 5).Today, no single vendor delivers all of the capabilities shown below in Figure 5 and in Table 2, but we expect the long-term evolution of CNAPP to deliver such capabilities.

Figure 5: 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

Gartner client interest — reflected by Gartner's inquiry volume — has remained consistent. There has been a steady flow of end-user inquiries about CNAPPs from 2023 to 2025, with no notable increase or decrease (see Note 2). The focus has been on CSPM capabilities driven by compliance needs and on integration through straightforward API CSP deployment — with expectations for runtime visibility and control, including basic workload risk visibility through the use of snapshots.

Buying Center

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 are fueling strong client interest in CNAPPs:

- The most significant is the need to unify risk visibility across IaaS and PaaS 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 into 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.

Overlap and Convergence With Application Security

On the application layer, CNAPP offerings primarily focus on scanning for known vulnerabilities, misconfigurations and hard-coded secrets in development artifacts by utilizing both static and dynamic techniques. As the CNAPP market evolves and matures over the coming years, vendors are increasingly emphasizing comprehensive code scanning within the development pipeline, extending beyond just infrastructure as code. Meanwhile, traditional static and dynamic analysis tools in application security testing concentrate on uncovering unknown vulnerabilities in custom code using similar techniques. Some vendors are expanding their capabilities to include limited code analysis, which is beginning to overlap with the application security testing market, prompting questions about the need for multiple toolsets.

CNAPP and application security offerings are increasingly converging. Organizations that predominantly or exclusively use cloud-native applications will, in the long term, rely on the same CNAPP tool both for CSPM and AST needs.

Generative AI Capabilities

CNAPP solutions are increasingly incorporating generative AI (GenAI), common language interpreters, machine learning (ML) and large language models (LLMs) to reduce management overhead, offer policy recommendations, and enhance pattern analysis for threat detection and response. Many vendors have also integrated AI-driven code analysis into their scanning processes, providing developers with tailored code corrections instead of generic examples, thus adding more value. This approach gives developers actionable code modifications based on their original work, which can be seamlessly integrated into the pipeline. The expectation is that these new AI capabilities will significantly improve risk management and reduce mean time to resolution (MTTR), resulting in quicker detection and response to cloud infrastructure and application risks both proactively and reactively.

Adjacent Products and Features

For a thorough understanding of risk, it is essential to utilize both CNAPP and application security tools. Consequently, more CNAPP vendors are either enhancing their own capabilities or integrating third-party functions. This strategy aims to deliver a comprehensive solution that addresses all facets of cloud and application risk management. Over the next several years, Gartner anticipates several CNAPP vendors will continue to expand their offerings into additional security areas. However, these areas are currently not primary drivers of the CNAPP market and serve as complements to the overall code-to-cloud security process (see Note 5):

- Application security testing (AST)
- 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 with adjacent platforms and will pull revenue from the several stand-alone markets that comprise the core of CNAPP functionality (see Table 1 and Forecast: Information Security, Worldwide, 2023-2029, 2Q25 Update). [2]

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

(Enlarged table in Appendix)

Gartner Market Forecast	Estimated Market Size at Year-End 2024, Billions of U.S. Dollars in Constant Currency	Estimated Market Percentage Growth in 2025 in Constant Currency
Cloud Security Posture Management (CSPM) *	2.1	35.1
Application Security Testing Software *	1.9	9.6
Cloud Workload Protection Platforms (CWPP) **	4.9	24.1
Vulnerability Assessment	2.5	15.4
Web Application and API Protection	1.8	12.3

* The estimated market size for CSPM was taken from Forecast: Information Security, Worldwide, 2023-2029, 1Q25 Update. Updated forecast information is now available Forecast: Information Security, Worldwide, 2023-2029, 2Q25 Update.
** 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.

Source: Gartner (August 2025)

Benefits of CNAPP Offerings

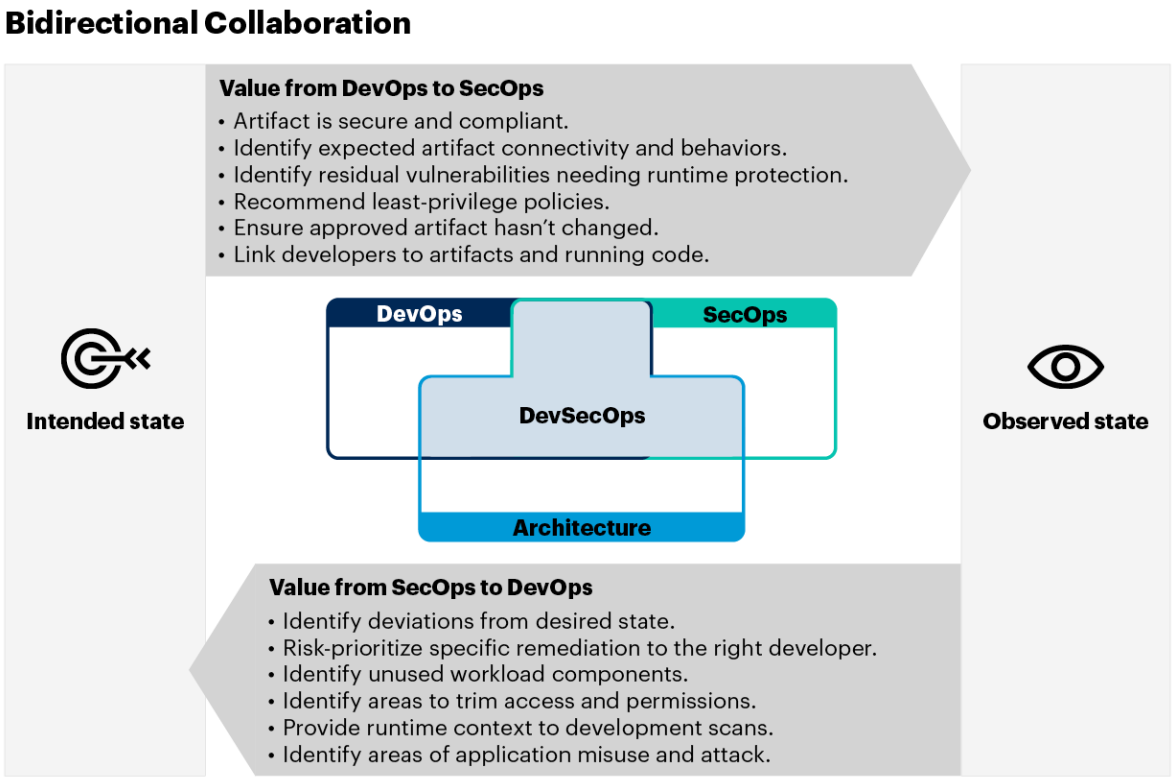
An organization could implement 10 or more tools to deliver fully against the capabilities shown below in Table 2. However, organizations have reasons to move toward the integrated convergence of a CNAPP offering:

- 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 the consolidation of vendors, consoles, policies and contracts, thereby reducing the 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
- Mature CNAPP solutions benefit from a single data lake, data model and unified graph database for all event logging, reporting, alerting and relationship mappings, which greatly improves the ability to correlate the data accurately. Combined with analytics and AI on the security graph, this enables the vendor to deliver effective risk analysis — finding the root cause of the risk, identifying the person or 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 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 ensure:
  - Proactive and preventative problem fixing earlier in the development process
  - 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 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) and application development ecosystem. (See Figure 6).

Figure 6: Bidirectional Collaboration



Source: Gartner
790337_C

Gartner

Challenges to CNAPP Adoption

- **Divergent 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.

- **Disconnection between developers and security:** Developers perceive security teams as impeding the speed of modern DevOps processes. Security controls were not designed for the speed and scale of cloud-native applications and 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 low-risk vulnerability remediation.

- **Existing investments:** Many organizations carry existing technical debt from various niche vendors that address both traditional network security and advanced cloud security and compliance tools. Early cloud adopters often viewed the cloud as an extension of their data centers and implemented threat detection and response tools, such as traditional endpoint protection (EPP) or endpoint detection and response (EDR) solutions, within their virtual machines. This approach became challenging when it was time to refactor applications and transition VMs to cloud-native environments, as these conventional tools are not compatible with cloud-native systems. Many public cloud users who had refactored applications chose container scanning tools during development and also implemented stand-alone solutions for CSPM. Most organizations rely on multiple vendors for different or sometimes overlapping functions, leading to silos of users and findings, which complicates the creation of a unified risk picture. As organizations transition to a CNAPP-based approach, the integrated platform's synergy will offer more advantages than a best-of-breed strategy, which is difficult to scale.

- **Mindset changes:** Security teams must understand and acknowledge that a perfect, risk-free application is not possible. Perfection is the enemy of good enough. Instead, security teams should focus on an approach that identifies the highest severity, highest confidence risks 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 in 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:** Over the next several years, CNAPP capabilities will continue to differ significantly, with some vendors lacking maturity in several areas. Gartner noted that this usually depends on the vendor's original area of specialization or whether the vendor has made a series of acquisitions in an attempt to develop a unified CNAPP solution, which ultimately resulted in a platform lacking internal cohesiveness. For example, sensitive-data visibility and control are often a priority capability for clients but 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 do not offer both agent and agentless integration limit their solution's adoption.

- **Legacy applications:** Older applications that are not 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:** Certain CNAPP solutions fall short in establishing strong technology partnerships and offering extensive integration options with other vendors and stand-alone tools. This shortcoming can lead to fragmented risk views and potentially disrupt the application development pipeline. Nonetheless, many CNAPP vendors are tackling this issue, investing in research and development and embracing an open integration architecture. As a result, vendors are striving to overcome the limitations of not incorporating an open integration architecture, which aims to offer consumers more options and flexibility to address their unique cloud and development environments and break down the silo's communication.

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 EPP market or were purpose-built from the ground up for container security and were previously established as CWPPs
- Vendors that initially focused on 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

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, 2025 and Hype Cycle for Workload and Network Security, 2025), 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 Functional Adoption Priorities

(Enlarged table in Appendix)

Core functions	Recommended capabilities	Optional capabilities

■ Cloud security posture management, including integration with leading hyperscale providers
■ Kubernetes security posture management providing security risk analysis of Kubernetes orchestration platforms
■ IaC scanning, including support for major IaC scripting languages and YAML/Helm for Kubernetes
■ Ability in understanding and controlling identity, roles, permissions and entitlements in cloud environments to provide better context to build risk-prioritized attack graphs
■ 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 analysisof workloads
	■ API discovery and monitoring
	■ Scanning of unstructured IaaS data repositories for risk [a]
	■ Traffic monitoring capabilities and connectivity mapping
	■ 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
	■ Support for eBPF
		■ 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
		■ AI assistant, AI agents and AI scanning engines

eBPF = Extended Berkeley Packet Filter; IaC = infrastructure as code; RASP = runtime application self-protection

[a] Risk scanning includes configuration scanning, code scanning, scanning for known vulnerabilities, secrets scanning, attack path analysis and behavioral pattern analysis.

[b] DSPM in relation to CNAPP specifically refers to the scanning and assessment of unstructured data stores, accessible by workloads within an IaaS/PaaS environment.

Source: Gartner (August 2025)

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), 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. Mapping of accountability and responsibility to code and artifacts is critical.
- Integrated advanced analytics that are combined with the graph relationships to risk-prioritize findings in development and at runtime.
- A single unified management and centralized control plane 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 or inspection into their own private cloud instances, 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 — e.g., CIS, NIST, PCI, GDPR and HIPAA.

- Support for all mainstream hyperscale providers, such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP) and Oracle Cloud Infrastructure (OCI) and other regional-specific or niche providers like Alibaba.com, IBM Cloud and others.

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 (see Solution Path for Implementing a Cloud Center of Excellence). 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 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 or development teams throughout an application's life cycle. This is critical to identifying the right developer or development team or engineering team to rectify the risks identified and provide these teams with sufficient context to understand and remediate the risks quickly and effectively.

As organizations shift to a DevSecOps life cycle for cloud-native applications, application teams are taking on greater responsibility for resolving security issues. Nevertheless, managing risk exposure remains a business obligation, with the security leadership accountable for addressing identified cloud risks. Look for a CNAPP solution that simplifies these challenges and provides business-level insight as risks are mitigated.

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 (see Note 4).

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 that provides context to security. 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, risk-prioritizing their remediation efforts and 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 the capabilities.

Table 3: Representative CNAPP Vendors

(Enlarged table in Appendix)

Vendor	Offering
Aqua Security	Aqua CNAPP
CrowdStrike	CrowdStrike Falcon Cloud Security
Cyscale	Cyscale CNAPP
Datadog	Datadog CNAPP
Data Theorem	Cloud Secure
Fortinet (Lacework)	Lacework FortiCNAPP
Google Cloud *	Security Command Center
IBM	IBM Security and Compliance Center
Microsoft	Microsoft Defender for Cloud
Orca Security	Orca CNAPP 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
Upwind	Upwind CNAPP
Wiz *	Wiz CNAPP

* Google + Wiz: Strengthening Multicloud Security, Google Cloud. Google announced on 18 March 2025 its intent to acquire Wiz. As of writing this Market Guide, the two vendors and their associated CNAPP products were still operating independently. Google has been investing in this space; first internally in Google Cloud, and in 2024, expanding the coverage of their Google Cloud-specific tooling (Security Command Center) from just Google Cloud to AWS and a more limited coverage into Azure. However, their own offering was later to the market and less feature-complete (or advanced), and the acquisition of Wiz immediately expands Google's visibility in the market and the technical capabilities it can provide.

Source: Gartner (August 2025)

Market Recommendations

Strategy and Planning

- Whether a CNAPP is adopted or not, establish a vision for DevSecOps that puts the 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 identified 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 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, e.g., common vulnerabilities and exposures (CVEs), hard-coded secrets, passwords, API keys, a high priority as this is another common source of risk in cloud-native applications. If the organization has already deployed a separate service to cover SCA, correlate the risk findings discovered by the SCA/SBOM products by integrating these products into CNAPP.
- Be pragmatic, not dogmatic, in the CNAPP deployment. Agents may provide the best visibility but are not always possible or necessary. Use inside-out workload runtime visibility where you can and agentless snapshots where you cannot, 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 2023 and 2024 and compared to the 12 months between 2024 and 2025.

[2] The estimated market size for CSPM was taken from Forecast: Information Security, Worldwide, 2023-2029, 1Q25 Update. Updated forecast information is now available: Forecast: Information Security, Worldwide, 2023-2029, 2Q25 Update.

[3] What Is the LD_PRELOAD Trick?, Baeldung.

Note 1: 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
- AI models

Note 2: Gartner's Initial 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 3: SSE, CASB, SSPM and CNAPP Overlap

Most stand-alone CASB revenue will migrate to the security service edge market (SSE). Several SSE vendors also have included limited SSPM capabilities. 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. SSE is a consolidation of access-related products to secure all users access to public and private apps irrespective of their location, which includes access to IaaS and PaaS environments. CNAPP is the consolidation of a series of platform-specific security products to secure the IaaS and PaaS environment and its associated workloads.

Note 4: Agent and Agentless Methods of Workload Integration

Agent and agentless methods of workload integration:

- 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 [3]
- 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)

Note 5: 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 developers or 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, Wiz, DevOcean, Snyk, Oligo Security, OX Security, GitLab and Tromzo.

Document Revision History

Market Guide for Cloud-Native Application Protection Platforms - 22 July 2024

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Forecast: Information Security, Worldwide, 2023-2029, 2Q25 Update

2025 Planning Guide for Security

Magic Quadrant for Application Security Testing

Emerging Tech: Security — Top Trends in the Security Market for 2023

How to Protect Your Cloud-Native Applications in Production

Guide to Application Security Concepts

Structure Application Security Tools and Practices for DevSecOps

How to Make Integrated IaaS and PaaS More Secure Than Your Own Data Center

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

Gartner Market Forecast	Estimated Market Size at Year-End 2024, Billions of U.S. Dollars in Constant Currency	Estimated Market Percentage Growth in 2025 in Constant Currency
Cloud Security Posture Management (CSPM) *	2.1	35.1
Application Security Testing Software *	1.9	9.6
Cloud Workload Protection Platforms (CWPP) **	4.9	24.1
Vulnerability Assessment	2.5	15.4
Web Application and API Protection	1.8	12.3

* The estimated market size for CSPM was taken from Forecast: Information Security, Worldwide, 2023-2029, 1Q25 Update. Updated forecast information is now available Forecast: Information Security, Worldwide, 2023-2029, 2Q25 Update.
** 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.

Source: Gartner (August 2025)

Table 2: CNAPP Functional Adoption Priorities

Core functions	Recommended capabilities	Optional capabilities

■ Cloud security posture management, including integration with leading hyperscale providers
■ Kubernetes security posture management providing security risk analysis of Kubernetes orchestration platforms
■ IaC scanning, including support for major IaC scripting languages and YAML/Helm for Kubernetes
■ Ability in understanding and controlling identity, roles, permissions and entitlements in cloud environments to provide better context to build risk-prioritized attack graphs
■ 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 analysisof workloads
	■ API discovery and monitoring
	■ Scanning of unstructured IaaS data repositories for risk [a]
	■ Traffic monitoring capabilities and connectivity mapping
	■ 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
		■ 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

	■ Software composition analysis, including software bill of materials creation ■ Application layer observability ■ Scanning of code repos ■ Support for eBPF	language interpretation ■ Digital forensics and incident response ■ AI assistant, AI agents and AI scanning engines

eBPF = Extended Berkeley Packet Filter; IaC = infrastructure as code; RASP = runtime application self-protection

[a] Risk scanning includes configuration scanning, code scanning, scanning for known vulnerabilities, secrets scanning, attack path analysis and behavioral pattern analysis.

[b] DSPM in relation to CNAPP specifically refers to the scanning and assessment of unstructured data stores, accessible by workloads within an IaaS/PaaS environment.

Source: Gartner (August 2025)

Table 3: Representative CNAPP Vendors

Vendor	Offering
Aqua Security	Aqua CNAPP
CrowdStrike	CrowdStrike Falcon Cloud Security
Cyscale	Cyscale CNAPP
Datadog	Datadog CNAPP
Data Theorem	Cloud Secure
Fortinet (Lacework)	Lacework FortiCNAPP
Google Cloud *	Security Command Center
IBM	IBM Security and Compliance Center
Microsoft	Microsoft Defender for Cloud
Orca Security	Orca CNAPP 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
Upwind	Upwind CNAPP
Wiz *	Wiz CNAPP

* Google + Wiz: Strengthening Multicloud Security, Google Cloud. Google announced on 18 March 2025 its intent to acquire Wiz. As of writing this Market Guide, the two vendors and their associated CNAPP products were still operating independently. Google has been investing in this space; first internally in Google Cloud, and in 2024, expanding the coverage of their Google Cloud-specific tooling (Security Command Center) from just Google Cloud to AWS and a more limited coverage into Azure. However, their own offering was later to the market and less feature-complete (or advanced), and the acquisition of Wiz immediately expands Google's visibility in the market and the technical capabilities it can provide.

Source: Gartner (August 2025)