Guide

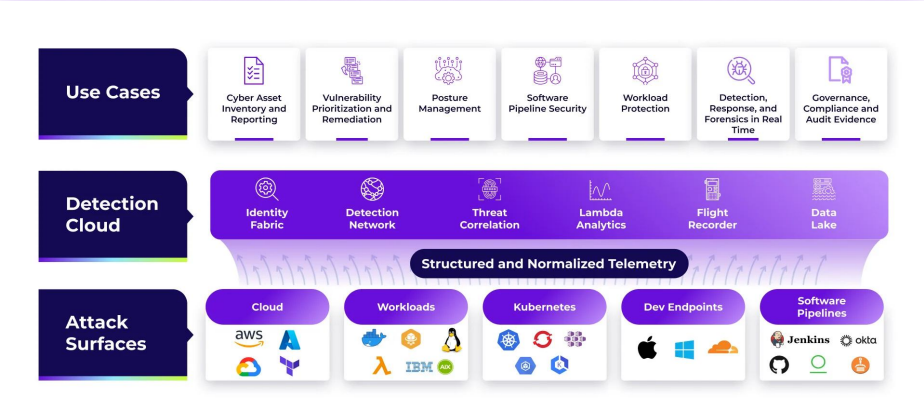
Cloud-Native Application Protection Platforms (CNAPP): Everything You Need to Know in 10 Pages

uptycs

Table of Contents

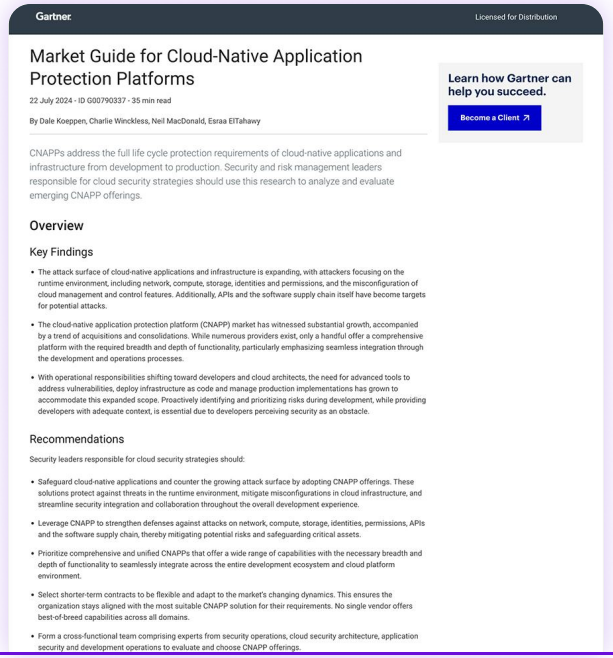
What is a CNAPP?

A **cloud-native application protection platform (CNAPP)** is a unified suite of security solutions designed specifically for cloud-native environments. It provides comprehensive protection across the entire lifecycle of cloud-native applications, from development to deployment and ongoing management. CNAPP combines various security disciplines into a cohesive platform, ensuring robust defense against a wide spectrum of threats.



Gartner introduced a Cloud-Native Application Protection Platform as a holistic approach to address cloud-native application security challenges throughout the development lifecycle. Gartner's CNAPP definition combines various security capabilities, such as development artifact scanning, Cloud Security Posture Management (CSPM), Infrastructure as Code (IaC) scanning, Cloud Infrastructure Entitlement Management (CIEM), and Cloud Workload Protection Platform (CWPP), to provide a unified approach to securing cloud environments.

Gartner forecasts that by 2029, "60% of enterprises that do not deploy unified CNAPP solutions within their cloud architecture will lack extensive visibility into the cloud attack surface and consequently fail to achieve their desired zero-trust goals.


Gartner

Licensed for Distribution

Market Guide for Cloud-Native Application Protection Platforms

22 July 2024 - ID G00790337 - 35 min read

By Dale Koeppen, Charlie Winckless, Neil MacDonald, Esraa ElTahawy

Learn how Gartner can help you succeed.

Become a Client

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.

Cloud-native Application Protection Platform: Features and Capabilities

Understanding CNAPP requires a closer look at its core components, each designed to tackle specific aspects of cloud security:

CIEM (Cloud Infrastructure Entitlement Management)

Cloud infrastructure entitlement management (CIEM) manages and controls access rights within cloud environments, focusing on enforcing the principle of least privilege. CIEM continuously monitors cloud infrastructures, identifying excessive or inappropriate access permissions and remediating them, thereby reducing the risk of data breaches due to insider threats or compromised credentials.

CDR (Cloud Detection and Response)

Cloud detection and response (CDR) focuses on detecting and responding to threats within cloud environments, using advanced analytics and automated response mechanisms. CDR tools analyze vast amounts of cloud data to identify potential security incidents and automatically orchestrate responses to mitigate threats.

CWPP (Cloud Workload Protection Platform)

Cloud workload protection (CWPP) is designed to protect cloud workloads, including servers, virtual machines, containers, and serverless functions. CWPP offers real-time visibility and security for cloud workloads, ensuring they are protected against vulnerabilities, malware, and unauthorized changes.

KSPM (Kubernetes Security Posture Management)

Kubernetes security posture management (KSPM) secures Kubernetes environments, a popular container orchestration platform. It ensures Kubernetes configurations are secure, compliance standards are met, and best practices are followed to prevent misconfigurations and vulnerabilities.

XDR (Extended Detection and Response)
Extended detection and response (XDR) consolidates security data from multiple sources across the network, cloud, endpoints, and other environments to provide advanced threat detection and response. XDR correlates and analyzes data from various security layers, offering an integrated and comprehensive response to complex, multi-stage threats.

By integrating XDR with cloud-native application protection platforms (CNAPP), security teams can streamline threat detection and response processes across their entire environment. XDR enhances visibility by correlating data from cloud workloads, endpoints, and other assets, enabling faster and more effective threat remediation. With 85% of organizations recognizing the value of CNAPP in mitigating risk, combining it with XDR provides a unified platform that not only improves response times but also strengthens overall security posture management, driving efficiency and reducing complexity in managing modern cloud security challenges.

The significance of CNAPP in today's cloud landscape

CNAPP's relevance in the current cloud ecosystem cannot be overstated. Its significance is highlighted by the following factors:

Evolving Cyber Threat Landscape
As cyber threats become more sophisticated, CNAPP provides advanced protection mechanisms, keeping pace with evolving attack vectors.

Regulatory Compliance
CNAPP aids in meeting stringent compliance requirements and industry standards, essential for businesses operating in regulated sectors.

Increased Cloud Adoption
With more businesses moving to the cloud, CNAPP ensures a secure transition and operation in cloud environments.

DevSecOps Integration
CNAPP integrates seamlessly with DevSecOps practices, embedding security into the software development lifecycle and facilitating secure application development.

Benefits of Implementing a Cloud-native Application Protection Platform

Implementing CNAPP offers a range of benefits, making it an invaluable asset for businesses:

Comprehensive Cloud Security

CNAPP cloud security provides end-to-end security coverage, from securing infrastructure and workloads to protecting against advanced threats across the cloud ecosystem.

Enhanced Visibility and Control

With its integrated approach, CNAPP offers greater visibility into cloud environments, enabling more effective control and management of security risks.

Operational Efficiency

By consolidating multiple security tools into a unified platform, CNAPP reduces complexity and streamlines security operations.

Improved Compliance Management

CNAPP facilitates easier adherence to compliance standards, reducing the risk of non-compliance penalties.

Proactive Threat Detection and Response

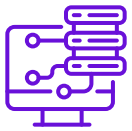
Advanced analytics and automated response capabilities enable CNAPP to quickly identify and mitigate threats, minimizing potential damages.

Cost-Effectiveness

By integrating various security functions, CNAPP can be more cost-effective compared to managing multiple standalone security solutions.

CNAPP's impact on DevSecOps and securing the CI/CD process

The adoption of DevSecOps and CI/CD pipelines has revolutionized the way applications are developed, deployed, and maintained. With the increasing complexity and speed of these pipelines, the demand for integrated security solutions that align with DevSecOps principles has risen. This is where CNAPP offers its transformative benefits.



Seamless integration with CI/CD pipelines

At the core of DevSecOps is the principle of integrating security measures directly into the CI/CD pipelines. CNAPP tools are designed to align with this integration-first approach. By doing so, it ensures that security checks and remediations are carried out continuously, right from the coding phase to deployment, thereby optimizing both development speed and security.

Unified security platform for DevSecOps teams

Instead of juggling multiple security tools, DevSecOps teams can leverage CNAPP's unified platform. It amalgamates various security components, ensuring that every stage of the CI/CD pipeline is covered. This not only reduces the overhead of managing multiple tools but also ensures a consistent security posture across the entire pipeline.

Proactive cloud security posture management (CSPM)

One of the primary challenges in the CI/CD process is maintaining a cloud security posture management (CSPM). With cloud infrastructure being dynamic and evolving, security configurations can often be left vulnerable. CNAPP acts as a vigilant watchdog, constantly monitoring cloud configurations, identifying potential misconfigurations, and immediately flagging them. This proactive approach ensures that security risks are mitigated even before they pose any tangible threat.

Agility and flexibility

In the fast-paced world of DevSecOps, agility is key. Cloud-Native Application Protection Platform offers are tailored to provide flexible solutions that adapt to the unique needs of each organization. Whether it's integrating with existing tools or scaling up as per the application demands, cloud-native application protection ensures that the CI/CD process remains agile without compromising on security.

Collaborative security culture
CNAPP reinforces the "shift left" approach of DevSecOps, encouraging developers, operations, and security teams to collaborate from the outset. By offering real-time insights and feedback, CNAPP security becomes an integral part of the development lifecycle, rather than an afterthought.

As organizations look to accelerate their application development without compromising on security, the integration of cloud-native protection into the DevSecOps and CI/CD processes becomes indispensable. CNAPP offers a proactive CSPM approach and seamless alignment with CI/CD pipelines, ensuring that businesses can operate at peak efficiency while maintaining a robust security posture in the cloud.

Introducing: Uptycs Cloud-native Application Protection Platform (CNAPP)

If you're looking for a comprehensive solution that combines all the necessary security components into a unified platform, look no further than Uptycs. A proven leader in the CNAPP space, Uptycs provides Gartner's five core capabilities and goes beyond with additional features for a holistic cloud-native application security approach.

Uptycs presents the following advanced features to ensure robust cloud security:

- Development artifact scanning: Identifies vulnerabilities in early application development stages.
- Cloud Security Posture Management (CSPM): Assesses, manages, and rectifies cloud security configurations, ensuring compliance.
- Infrastructure as Code (IaC) Scanning: Validates security best practices in cloud setup and deployment.
- Cloud Infrastructure Entitlement Management (CIEM): Regulates access to cloud resources, ensuring least privilege and automating permissions.
- Runtime Cloud Workload Protection Platform (CWPP): Protects cloud workloads and provides continuous visibility and security.

More Than Just a CNAPP

Beyond the core Cloud-native Application Protection Platform capabilities, Uptycs provides a comprehensive laptop-to-cloud security approach with additional capabilities:

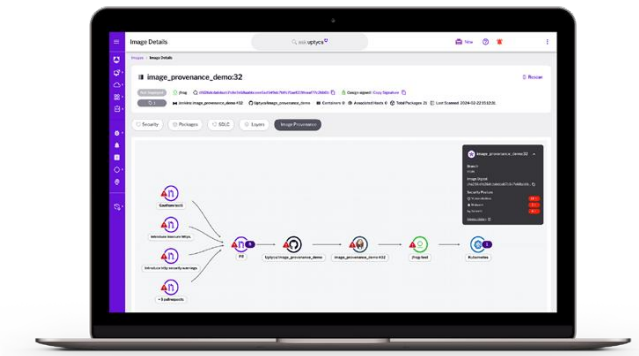
- **Cloud Detection and Response (CDR):** Uptycs CDR offers visibility, analytics, and threat detection capabilities within cloud environments, continuously analyzing cloud logs and telemetry to identify malicious activities and unauthorized access.
- **Extended Detection and Response (XDR):** Uptycs XDR expands the scope of threat detection beyond endpoints by consolidating and correlating data from multiple sources, including networks, cloud environments, and applications.
- **Kubernetes Security Posture Management (KSPM):** Uptycs KSPM extends the capabilities of CSPM to secure Kubernetes environments, addressing misconfigurations and enforcing best practices.

With Uptycs, organizations benefit from a unified platform that combines the core capabilities plus the crucial CDR, XDR, and KSPM functionality.

This approach streamlines security operations, reduces complexity, and ensures comprehensive protection for cloud-native applications and infrastructure.

By choosing Uptycs as your CNAPP solutions provider, you'll benefit from a unified platform that combines cloud-native security and XDR capabilities, simplifies management and visibility, and integrates seamlessly with your existing tools and infrastructure. With Uptycs, you can rest assured that your cloud-native applications are well protected against current and future threats.

Don't wait for a security incident to happen before taking action. Explore Uptycs as your go-to solution provider today. Our team of experts is ready to help you safeguard your applications, reduce risk, and ensure the continued success of your business in the cloud.



Uptycs is dedicated to leading security innovations in hybrid cloud environments, ensuring robust protection and enabling our customers to innovate safely and efficiently. Included in the 2024 CNAPP Market Guide, Uptycs provides comprehensive security solutions that bridge the gap from code to cloud. Our platform excels in Cloud Workload Protection (CWPP), Vulnerability Management, Cloud Security Posture Management (CSPM), Detection & Response, Software Pipeline Security, XDR, and Risk & Compliance. Trusted by leading enterprises like PayPal and Comcast, Uptycs transforms potential vulnerabilities into fortified security, ensuring your digital environments are safeguarded from development through runtime.

Secure Everything from Dev to Runtime

Learn more at Uptycs.com