FORTINET

Exploring CNAPPs for Comprehensive AWS Cloud Security

Discover the value of integrating cloud-native application protection into your AWS Cloud security toolkit

Table of Contents

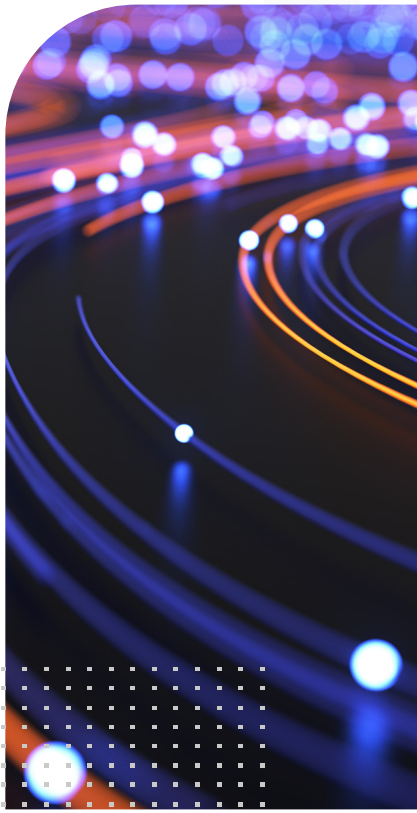
Introduction	3
What is a CNAPP?	4
Uncover the Future of Cybersecurity: Exploring the Innerworkings of a CNAPP	5
Enhanced and Integrated Security Operations in the Cloud: Harnessing the Power of CNAPPs	6
Move Confidently into the Dynamic Future of the Cloud with FortiCNP from Fortinet	7

Introduction

As an organization's presence in the cloud evolves, so do limitless opportunities for growth. Customers of the Amazon Web Services (AWS) Cloud consistently experience benefits in cost-efficiency, an accelerated time-to-market, transformative differentiation, and the capacity to power more innovation in a fraction of the time. While customers may leverage the embedded security provided through AWS, augmenting this with an additional security solution can provide even greater protection against incidents in the cloud. In our dynamic cybersecurity landscape, new anomalies are constantly emerging, and the modern attack surface is expanding. Organizations often address security challenges by continuously adding security tools and point solutions to their infrastructure. These often come from separate vendors that don't integrate. This saddles customers with the management of tools and solutions that have distinct features, interfaces, and functions, and that often operate in silos.

This results in fractured visibility and security blind spots across cloud environments. Most significantly, the lack of cohesion among these tools leads to delayed incident responses and increases the probability that anomalies may not be properly detected and mitigated. While managing and operating this wide array of security tools, organizations may have a hard time identifying and prioritizing the most pressing risks, leading to inefficient and ineffective security coverage.

This eBook will explore the benefits of adopting a Cloud Native Application Protection Platform (CNAPP) and its unique approach to enhancing cloud security by enabling security teams to proactively address anomalies in their cloud infrastructure. A CNAPP resolves some of the challenges inherent in operating disparate security solutions by providing a centralized, integrated risk management platform. By implementing security earlier in the application lifecycle across public and private cloud infrastructures, a CNAPP can also make risk management simpler, and more effective with deep integrations across AWS services.



What is a CNAPP?

Several cloud-native security point solutions have been introduced to address distinctive areas of the threat landscape. These include CSPM (Cloud Security Posture Management), XDR (Extended Detection and Response),MDR (Managed Threat Detection and Response), and CWPPs (Cloud Workload Protection Platforms). As we've explored, the lack of cohesion among these solutions keep security teams from accessing a comprehensive view of the risks they're facing. The limitations of these solutions also leave teams ill-equipped to operate effectively and efficiently in the current cyber landscape.

A CNAPP is a new level of cloud security that combines and integrates CSPM with CWPP capabilities and other security solutions. CNAPPs deliver unified visibility, as well as asset and data protection for containers and Kubernetes clusters, providing an end-to-end approach to cloud security.

As a comprehensive solution that is specifically designed to meet the security demands of complex cloud environments and cloud-native applications, a CNAPP enables an organization to consolidate its security practices. It also empowers an organization with a bird's eye view of its security posture in the cloud. Security teams can identify and preemptively address security issues as early in the application lifecycle as possible. This fortified approach to risk management also supports compliance and streamlines workflows for DevOps and DevSecOps like never before. With ninety-five percent of new digital workloads being deployed on cloud-native platforms, CNAPPs are widely regarded as the future of cloud security.

Uncover the Future of Cybersecurity: Exploring the Innerworkings of a CNAPP

As an all-in-one, integrated security and compliance solution for cloud-native applications and environments, a CNAPP helps organizations maintain and augment their security posture and consolidate their security tools practices for more efficacy and control. It provides a central source of truth, reduces complexity, and offers comprehensive coverage in a broad range of contexts. Here are some standard characteristics and components of CNAPPs:

- Data protection that supports visibility and inspection capabilities, and escalates the most critical cybersecurity anomaly indicators.
- A CWPP that supports continuous identification and resolution for workloads in hybrid, cloud, and on-premises environments, as well as servers and virtual machines.
- IaC security that automates configuration and deployment processes to reduce and detect any mistakes or potential security risks in code in its earliest stages.
- CSPM that supports security teams in overseeing and adjusting cloud security policies. It also automates detection and remediation and provides AI-driven insights on an organization's security posture.
- Governance and compliance support to streamline alignment with compliance requirements and identity when activities across an organization's single, multi-cloud, hybrid, and on-premises environments are diverging from established security policies and protocols.
- Cloud Infrastructure Entitlement Management (CIEM) that supports the management of permissions and access for all identities across an organization.
- Kubernetes Posture Management (KSPM) and related tools to streamline container scanning prior to deployment.
- Cloud Service Network Security (CSNS) for real-time cloud infrastructure protection.

Enhanced and Integrated Cloud Security Operations: Harnessing the Power of CNAPPs

A security leader may be wondering what value a CNAPP can bring to an already secure AWS Cloud environment. The most effective CNAPP solutions enable enterprise security teams to transform their operations in significant ways:

- **Bolster agility**: It enables the organization to easily manage risk without slowing down or disrupting operations.
- **Improve productivity:** Security teams are no longer obliged to sift through countless alerts and can access consolidated, high-priority alerts to make the best decisions for their organization in a fraction of the time.
- **Power better security operations:** It supports seamless collaboration between development and operations teams, and simplifies risk management.
- **Prioritize security in the earliest phases of development for proactive risk management:** It supports shift-left security, and bi-directional communication with ease.
- **Overcome common security blind spots:** Where other security solutions falter, a CNAPP can be especially effective – such as protection for container security.
- **Reinforce the capabilities of existing security tools and practices:** Seamless integration with AWS security tools makes CNAPP a breeze for teams to integrate into their practices, with no learning curve.
- **Provides a single source of truth:** A CNAPP can help organizations overcome common perils of traditional security solutions including visibility gaps, alert fatigue, disparate tools, and poor or outdated security approaches.
- **Identity and Access Management (IAM):** That ensures that access to organization's assets and data are exclusively accorded to the appropriate users.

Move Confidently into the Dynamic Future of the Cloud with FortiCNP from Fortinet

As a world leader in cybersecurity solutions, Fortinet offers customers a comprehensive set of products slated specifically for cloud infrastructure security needs.

Fortinet Cloud Native Protection (FortiCNP), is a built-in-the-cloud service that integrates and prioritizes security findings across an organization's cloud environment. It enables more seamless, effective, and efficient security operations. This cloud security tool boasts deep integrations with a broad range of cloud security products, and services from AWS. These services include AWS Security Hub and Amazon GuardDuty, among others. FortiCNP also supports the delivery of near-real-time threat protection with zero-permission capabilities to actively scan running workloads.

FortiCNP supplies customers with heightened and comprehensive visibility into their security posture that is reliable, automated, and centralized. It prioritizes resources with the highest risk across cloud environments that cover workloads, virtual machines, databases, gateways, containers, and more. FortiCNP also continuously monitors the workloads to identify new and evolving risks. For organizations in highly regulated industries, FortiCNP provides reports to identify policy violations—enabling organizations to comply with regulatory demands with ease.

Ready to embark on the future of cloud security? Learn more and get started today with a test drive through AWS Marketplace.

January 2023