General Report

Solving the cloud-native app puzzle with CNAPP

The value of integrating cloud-native application protection into security and development

February, 2023
Trend Micro

Contents

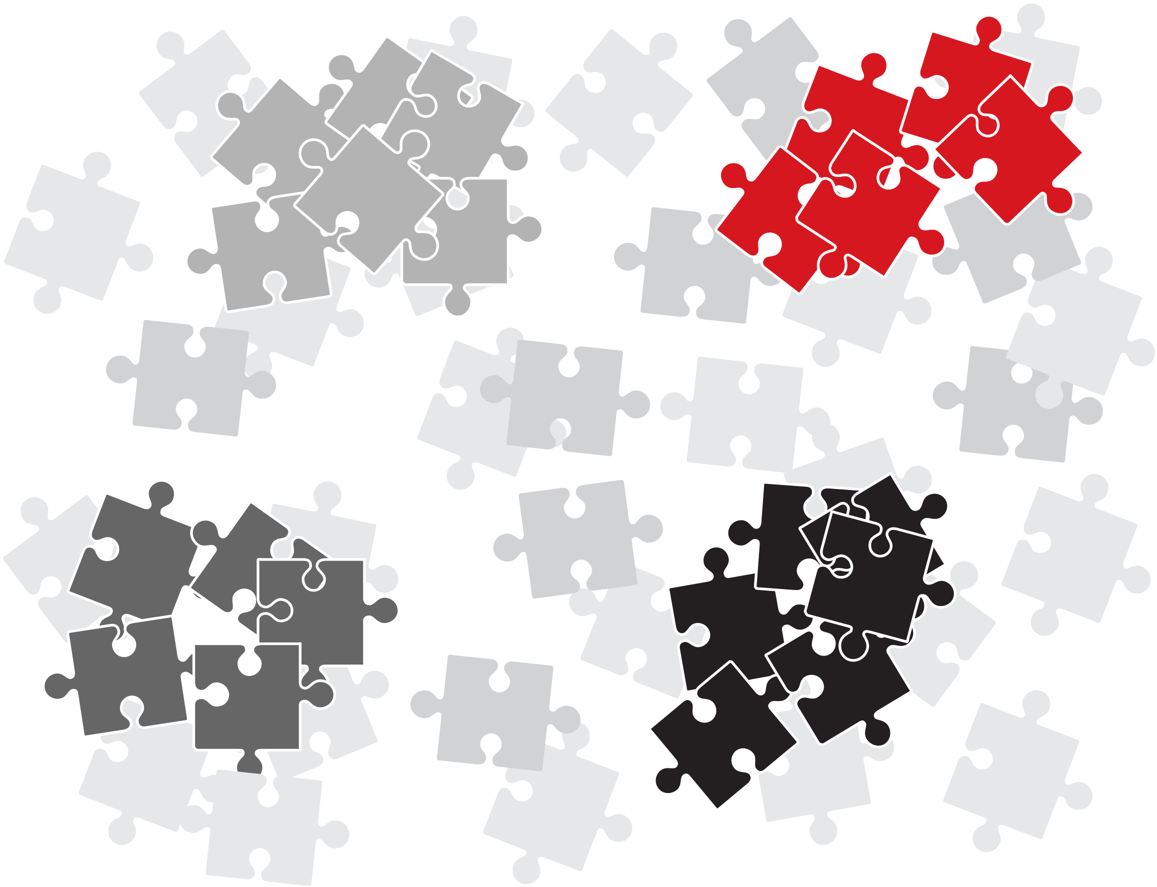
Introduction

There are a lot of pieces in the cloud security puzzle, and sometimes it can seem like it's not clear how they fit in the big picture. Think cloud access security brokers (CASBs). Or cloud workload protection platforms (CWPPs). Or cloud security posture management (CSPM). Not to mention software composition analysis (SCA), extended detection and response (XDR), and managed detection and response (MDR).

All of these have their roles in protecting your cloud environments and infrastructure. Yet many are point solutions, operating like clusters of puzzle pieces lying in different places on the card table with no edge to create the big picture.

This is where a cloud-native application protection platform (CNAPP) comes in. It not only provides the edge of the puzzle that keeps it all together, but it helps development, DevOps, cloud, and security teams sort the pieces into the big picture.

In this report, we explain CNAPP, where and how it fits with cloud security, and its value to not only security operations but also developers and DevOps. We also look at the best way to approach CNAPP so that it fits in your overall cybersecurity strategy and ecosystem.



CNAPPs: The cloud security puzzle's edge

Being a cloud-first company is fast becoming the norm. An estimated 85% of organizations are aiming to embrace a cloud-first principle by 2025, according to Gartner.[1]

Through cloud-native applications, companies unlock more agile development processes that allow them to adapt to changing needs faster. Because they often execute businesscritical workloads, cloud-native applications need top-notch security that's built into development practices.

However, dev teams bring in a lot of open-source components for these apps, and that makes them difficult to protect. To address their unique security needs, a collection of siloed, complex, and overlapping tools has appeared on the scene. Swimming in an alphabet soup of acronyms, such as SCA, CWPPs, and CSPM, they protect different aspects of cloud-native applications—just like a partially completed puzzle. However, these and other cloud security platforms do not meet the needs of the security teams who need visibility into cloud-native applications, the developers who are worried about moving quickly, or the business leaders who see the cloud as increasingly strategic to their organization.

Trend has been securing hybrid cloud environments and cloud-native applications for over a decade, and we infuse that knowledge and expertise into our approaches to today's cloud and cloud-native security challenges.

One of the more recent industry acronyms that has emerged to address the security needs of cloud-native applications is CNAPP, and it promises to shake up the puzzle box, Trend can help everything fall into line.

What is a CNAPP?

To secure cloud-native application build and deployment processes, a CNAPP consolidates important features such as runtime protection, cloud configuration, and artifact scanning from siloed tools—including CWPP and CSPM.

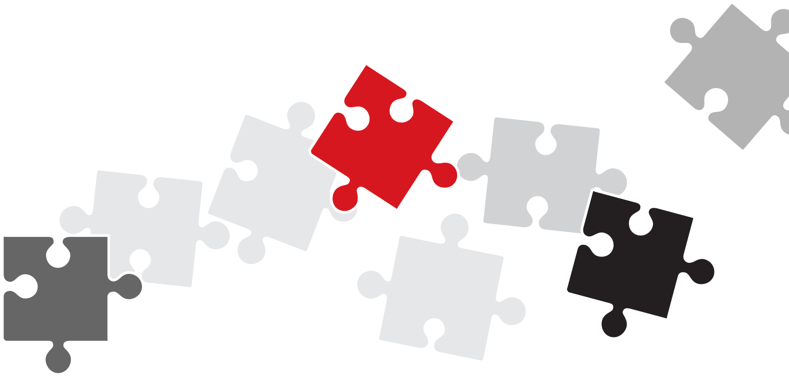
You might hear a CNAPP referred to as a cloud workload security suite or a cloud-native security platform, but the capabilities and features are similar.

A CNAPP connects multiple security features, just like the edge of a jigsaw puzzle brings other partially assembled pieces into a coherent picture. With a CNAPP, you can approach development and runtime as parts of a continuum that spans development and operations and not as separate security topics.

Trend Cloud One™ has evolved its cloud-native application protection capabilities to secure containers, serverless, code repositories, and infrastructure as code, providing thoughtful application security every step of the way. In addition to the breadth of Trend Cloud One's CNAPP capabilities, we also address security for cloud object storage, such as Amazon Simple Storage Service (Amazon S3) and cloud networks, as well as provide extended detection and response (XDR). Trend Cloud One's path forward will be defined by the needs of our customers and partners who work to securely develop and deploy cloud-native applications every day.

A CNAPP helps multiple teams contribute to the puzzle

A CNAPP delivers value to more than just your security team. It also includes all the teams across the DevOps spectrum, such as development, operations, and cloud engineering teams. Returning to the puzzle metaphor, you invite more people to the card table, making them aware of the best pieces in terms of security architectures and products. Then, you show everyone how a CNAPP lets them contribute to your cloud security strategy—the big picture—while also helping them do their jobs quickly and effectively with the tools and processes they're using already. Let's explore how.



[1] Gartner, "Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences," November 10, 2021.

The benefits of CNAPPs

The world of securing cloud-native applications is blurry and overlaps, causing confusion about the roles that different teams—like security and development—play. A CNAPP helps you draw lines, so that it's clear who will be responsible for which puzzle pieces. When everyone is working on their part of the puzzle together within a clearly defined framework, amazing things happen.

CNAPPs define a big picture based on the pieces

How do siloed point products proliferate? Generally, it's when security teams try to cover all their bases.

Already stretched teams then have to stitch together data from separate products. It's like having different groups of people show up to work on a puzzle at different times. Development workflows get delayed. And security blind spots cause risks to go undetected until it's too late. People can't see the image because they are lost in the clusters of pieces. CNAPPs correlate threats and weaknesses in a console and help security teams see risks across your cloud environments, including source code, endpoints, containers, serverless, runtime, and cloud configuration.

CNAPPs are designed to let developers keep developing naturally secure applications—they don't need to be security experts. Trend Cloud One combines a wide variety of CNAPP capabilities with a natural developer experience.

CNAPPs keep developers firing on all cylinders

Agility is the name of the cloud-native app game. Security testing should be swift and effective, so developers can keep firing on all app building cylinders. CNAPPs let developers develop by automating many tasks, scans, and checks, so detection is much quicker, and the number of false-positive alerts—those pieces that look like they fit but belong somewhere else—is reduced. CNAPPs seamlessly deliver feedback throughout development, without disrupting workflows. Trend Cloud One identifies the highest severity risks and vulnerabilities and developers can fix within the tools they are already using. Trend Cloud One lets security define policies that developer can deploy against, leaving them more time to develop and not solve security issues.

CNAPPs set up a communication flow

To deploy cloud-native apps in today's multi- and hybrid-cloud world, you need to establish a two-way communication flow between security and development teams. CNAPPs make it easy for different teams to collaborate in the tools they are already using. They can work together to investigate and remediate major open-source vulnerabilities like Log4j, as well as misconfigurations, overly permissive containers, open cloud storage objects like Amazon S3 buckets, and more. Trend Cloud One's integrated cloud-native application security tools span development through to production, ensuring that issues are fixed upon commit and everywhere after.

Now that you know the major benefits of CNAPPs, it's time to choose one that delivers them all and more.

Sorting through the CNAPP options

CNAPPs benefit developer, operations, and security teams. When considering a CNAPP, you can start with a small evaluation team that grows to include cross-team stakeholders. You'll need to weigh different options because, like jigsaw puzzles, not all CNAPPs are created equal. eWeek hinted at the differences in a recent article:

"The capabilities of CWPP and CSPM are coming together, and CNAPP solutions are emerging as a blend of the two solutions."[1]

Some solutions rely more heavily on CWPP and others on CSPM.

Here are the things to keep in mind as you explore CNAPPs.

Tips for getting a good CNAPP

Cloud-native application security needs to support the build process, not hinder it. To get the full benefits of a CNAPP approach, make sure your platform of choice has robust automation capabilities that can automate as many tasks, scans, and checks as possible. Not only is detection much quicker, but the number of false-positive alerts are reduced. Your CNAPP should give you consolidated visibility into the security posture of all the supporting pieces of your cloud-native applications and provide actionable insights and recommendations.

To enhance collaboration between teams, look for a CNAPP with turnkey, customizable integrations with your existing development toolset, pipelines, issue management, and APIs. This will provide connected protection at every stage of the software development lifecycle. In addition to broad cloud-native application protection capabilities, look for a CNAPP that offers a natural developer experience such that their interactions with the platform are nearly unrecognizable from their day-to-day tasks.

Make sure your CNAPP truly is an integrated platform that isn't just relocating your existing cloud-native application security silos, and seek out a platform that has a centralized, compliance-aligned dashboard for complete visibility of your security posture across your hybrid or multi-cloud environment.

And finally, look for a CNAPP that offers a consumption-based pricing model so that it grows with your organization as you migrate and modernize. A flexible platform that supports today's and tomorrow's cloud providers, various types of applications, and familiar DevOps tools will enable you to improve security without disrupting your developers as they adopt the latest cloud technology.

What to look for in a CNAPP

A CNAPP brings together infor- mation across artifact scanning, runtime, and cloud configuration, providing the edge of the puzzle that brings order to clusters of pieces. The following core com- ponents are not a checklist for CNAPPs; instead they are must- haves for delivering coherency to your security big picture:

- Misconfiguration checks for cloud resources like open Amazon S3 buckets, databases, and network ports.
- Runtime monitoring and protection of your cloud workloads and resources like virtual machines (VMs) and Amazon Elastic Compute Cloud (Amazon EC2).
- Automated detection of anomalies in containers and container deployments on Kubernetes clusters like Amazon Elastic Kubernetes Service (Amazon EKS), including AWS Fargate.
- Exposure scanning in artifacts, source code, and running workloads for CVEs, secrets, sensitive data, and malware.
- Exposure scanning in cloud object storage for malware.
- Infrastructure as code (IaC) scanning.
- Network layer security to inspect ingress and egress traffic.

[1] "6 Cloud Security Must-Haves – with Help from CSPM, CWPP or CNAPP," 2021. eWeek, 9 Aug.

Fitting in with your overall cybersecurity architecture

CNAPPs are most effective when they are contributing to your overall cybersecurity implementation, including advanced XDR and MDR.

XDR: Extending security across layers

Serious threats can evade detection if data is collected and analyzed in silos. XDR can automatically correlate events and related activities, delivering the cross-layered detection and investigation that can't be achieved with individual point solutions. Events that seem benign on their own suddenly become meaningful indicators of compromise, enabling swift containment of their impact, severity, and scope.

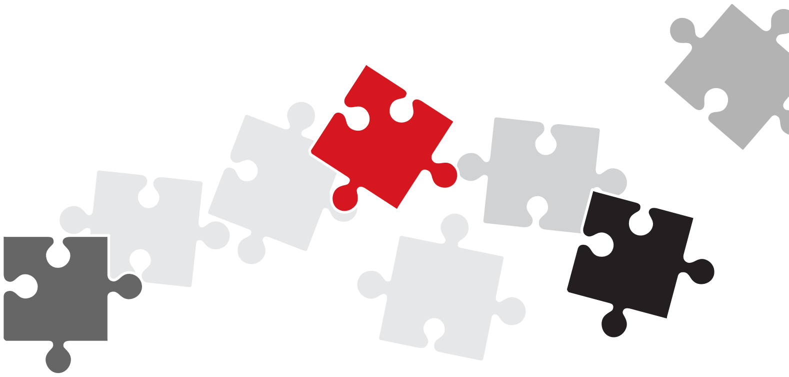
MDR: Taking a central security nervous system approach

MDR maximizes security effectiveness through a cross-layered detection and response service. It monitors and analyzes activity data from deployed XDR and protection solutions 24/7. Email, endpoint, server, cloud workload, and network sources are correlated for stronger detection and greater insight into the source and spread of complex targeted attacks.

XDR + MDR + CNAPP = Holistic cybersecurity

When XDR, MDR, and a CNAPP are combined, the result is comprehensive cloud protection. Think of your Amazon Web Services (AWS) workloads, containers, serverless architectures, cloud storage, and applications, for example. They are all safeguarded, as are your networks and anything open-source.

They are all safeguarded, as are your networks and anything open-source. Synchronization of these cloud security solutions is best done from a single platform with a focus on API-powered flexibility and automation, one that is designed to drive operational efficiencies and accelerated, streamlined compliance—a platform like Trend One.



Trend synchronizes cybersecurity

Trend is always looking at what's happening in the industry with an eye to the future. Our signature activities include threat research, and vulnerability discovery and disclosure. For example, Trend Micro Zero Day Initiative (ZDI) again dominated the number of disclosed vulnerabilities for what should be the 14th consecutive year based on Omdia's research into the vulnerability disclosure market.[1]

Our aim is to inform the public and integrate more features and capabilities into our product lines to stay up to date with changing technology. We also keep up with cloud innovations from AWS so we can be proactive with solution delivery. It all starts in the cloud.

Keeping unauthorized people off your cloud

Determined attackers are continuously looking for ways to exploit cloud environments, so they can take over your customer or administrative accounts, execute malicious code, or steal sensitive data. We want to make sure you can do business, develop, and run your apps and serve customers from the cloud safely, without having to implement and manage multiple security point solutions.

CNAPP makes it possible. Through Trend Cloud One, which predates CNAPP, you'll find the capabilities for securing cloud-native applications, workloads, and infrastructure, from source code to applications running in the cloud. It also detects threats to your web and cloud-native-based applications, minimizing your risk.

Protection beyond the cloud

And because cloud-native apps are likely connecting to or sharing data elsewhere in your IT landscape, Trend provides a unified view into your security—no matter where your data resides. Trend goes beyond the cloud to take in critical threat intelligence from email, networks, on-premises servers, and endpoints for maximum visibility and control. Integration with third-party security information and event management (SIEM) and security orchestration, automation, and response (SOAR) platforms adds even more value for customers. Our solutions also integrate with cloud services like AWS Security Hub, Amazon Simple Notification Service (Amazon SNS), or AWS Control Tower.

For example, Trend One helps you understand, communicate, and mitigate cyber risk across your enterprise. A unified cybersecurity platform, it enables consolidation with multiple market-leading security capabilities and deep integration with your IT and cloud environments, simplifying security and helping you detect and stop breaches faster.

To sum it all up, our goal is to give you everything needed to discover your attack surface, assess risk, and mitigate that risk while letting your developers develop cloud-native applications and enhancing resilience across all your environments.

[1] Jon Clay, 2021. "ZDI Tops Omdia Vulnerability Disclosures Again," Trend Micro. 19 May

Summary

Gartner defines a CNAPP as an integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications through development and production. Not all CNAPPs are the same, nor is a CNAPP a checklist of security capabilities you should implement. Instead, it provides the framework for not only keeping all your security pieces together, but also connects them. It helps development, DevOps, and security teams sort the pieces into the big picture, with security and cloud teams setting the policies and developers deploying against them.

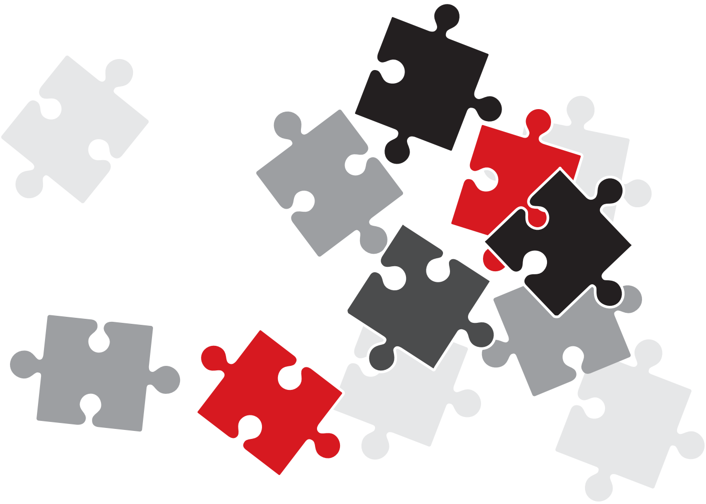
Trend has been securing hybrid cloud environments with CNAPP capabilities for over a decade, and we use that knowledge and expertise in how we approach today's cloud security challenges. We also extend our solutions beyond the cloud to email, networks, on-premises, and endpoints for maximum visibility and control. That's why we continue to be named Leaders in multiple security categories in reports from Gartner, Forrester, IDC, MITRE, and others.

For more information visit: **trendmicro.com/hybrid_cloud**

Trend and AWS

Trend has been an AWS Partner since 2012. With over 15 AWS competencies and designations, we continue to innovate with AWS and AWS Marketplace to deliver security to customers when and where they need it. We provide automated, flexible, all-in-one security designed for building and innovating securely on AWS. We're experts on cloud security and the customer role in the AWS Shared Responsibility Model—so you don't have to be.

For more information visit: **trendmicro.com/aws**



For details about what personal information we collect and why, please see our Privacy Notice on our website at: **trendmicro.com/privacy**