

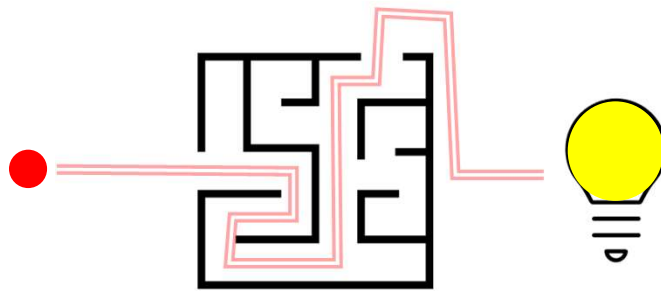


Download this chapter  
<https://bit.ly/DeconstructedCNAPP>

# The current state of cloud security

While organisations already have controls in place for safekeeping their cloud workloads, most current setups have multiple solutions that don't present their findings on a common dashboard or have a unified workflow for easy management.

The result, hard to manage and monitor cloud solution framework



Complexity is the friend of adversaries. It gives them opportunity to move through the cracks and leverage limited sharing of intelligence to make themselves invisible.

“

**Note: Complexity in security management favours the adversaries.**

# Why Change Now

Cloud adoption increased agility of cloud-native applications deployment, and complexity of processes involved.

Paradigm-shift to consider:



» Overlap of Dev,, Deployment and Operations.

Infrastructure-as-code, containerised services with app and related infra deployed together, integrated deployment of apps and related operational components.



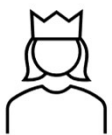
» Speed of Change

Continuous deployment, short-lived environments. Operation's need to be agile to keep up.



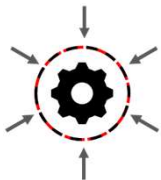
» Higher Unknowns

Lack of visibility of development pipeline, Open-source dependencies, 150% increase in reported vulnerabilities in 5 years\*



» Wider distribution of Admin-Like permissions.

Workload identities becoming more prominent and far-spread. Higher risk of code-embedded secrets and unguarded password repositories.



» Increased importance of external attack surface management

because of expansion of API surface.

\* [Skybox Report](#) based on National Vulnerability Database.


(Gartner Report) [Market Guide for Cloud-Native Application Protection Platforms](#) states that "By 2025, 60% of enterprises will have consolidated cloud workload protection platform (CWPP) and cloud security posture management (CSPM) capabilities to a single vendor, up from 25% in 2022."

Download this chapter

<https://bit.ly/DeconstructedCNAPP>


# What's the solution

## Cloud Native Application Protection Platform - CNAPP



**Get Converged Security Coverage** to protect cloud-native applications code and configuration, and its related infrastructure.

The coverage includes data stored and used by these apps, open-source libraries, IAC code, and related Identities.



**Shift-Left** to protect from development to production.

- Identify missing / risky configuration and vulnerabilities earlier.
- Bring integration and control into development pipeline.
- Enable code-to-production context linking for post deployment findings and “fix-at-source” resolution.

“CNAPP provides integrated capabilities to identify and mitigate risk for cloud-native applications and its associated infrastructure, from development to production, including artifact scanning, configuration assessment, and runtime protection. (Paraphrased from Gartner definition\*).

\* [Coined by Gartner in 2021](#) and revised in March 2023.

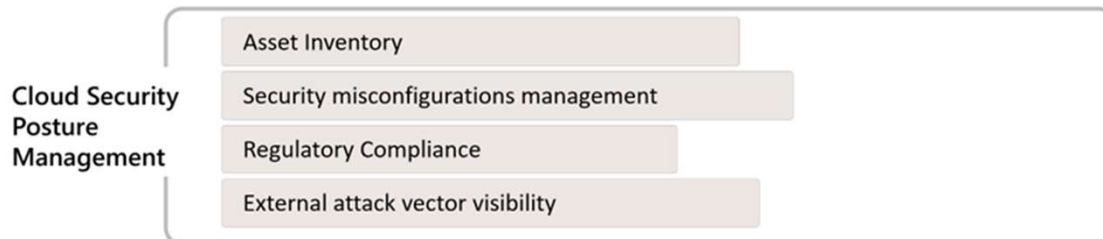
# CNAPP Deconstructed

Here's how a typical CNAPP solution is broken down.

## 1 Posture and configuration management

**Cloud Security Posture Management (CSPM) provides:**

- » **Layer of Horizontal Services** that goes across cloud services and workload types.
- » Covers discovery, configuration assessment and benchmarking of cloud resources.
- » Key services - Asset Inventory, Cloud benchmarks assessment and misconfiguration analysis, Industry and regulatory compliance check, External attack surface evaluation



**Note: CSPM provides a layer of Horizontal Services that go across cloud services and workload types.**

Download this chapter

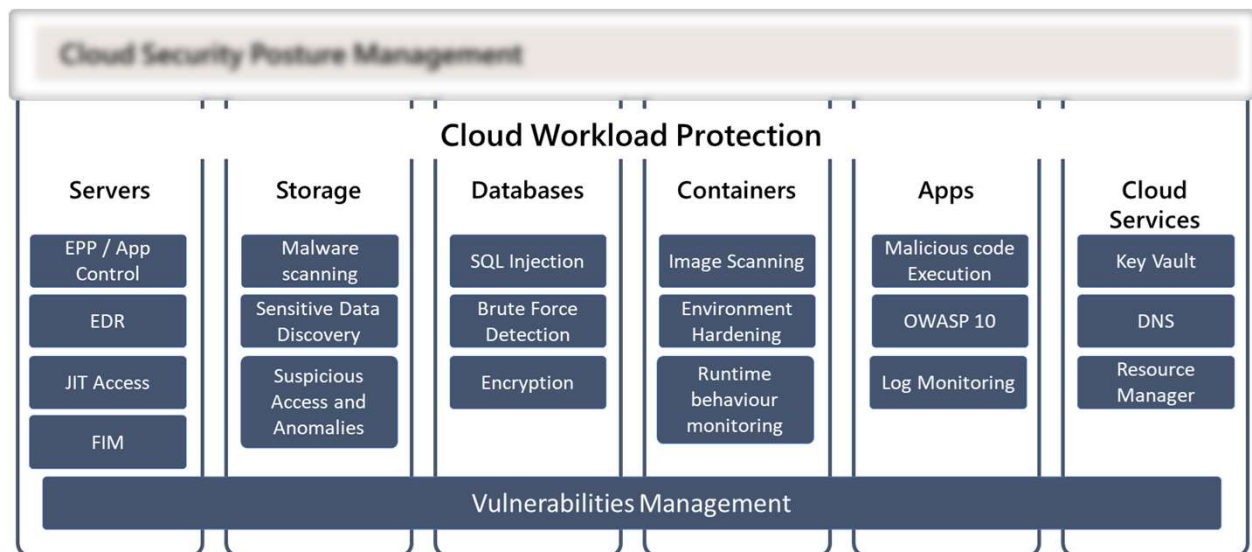
<https://bit.ly/DeconstructedCNAPP>

## 2 Workload specific protection - CWPP

The vast variation in runtime capabilities behaviour of cloud workloads (e.g., VMs, apps and containers) necessitates workload specific CWPP components for high fidelity detection and deeper response ability.

Cloud Workload Protection Platform includes **Workload-Specific services** including:

- » Detection of in-workload vulnerabilities, exposed secrets, suspicious runtime behaviour, and indicators of malware activities.
- » Response at both in-workload and control plane level.

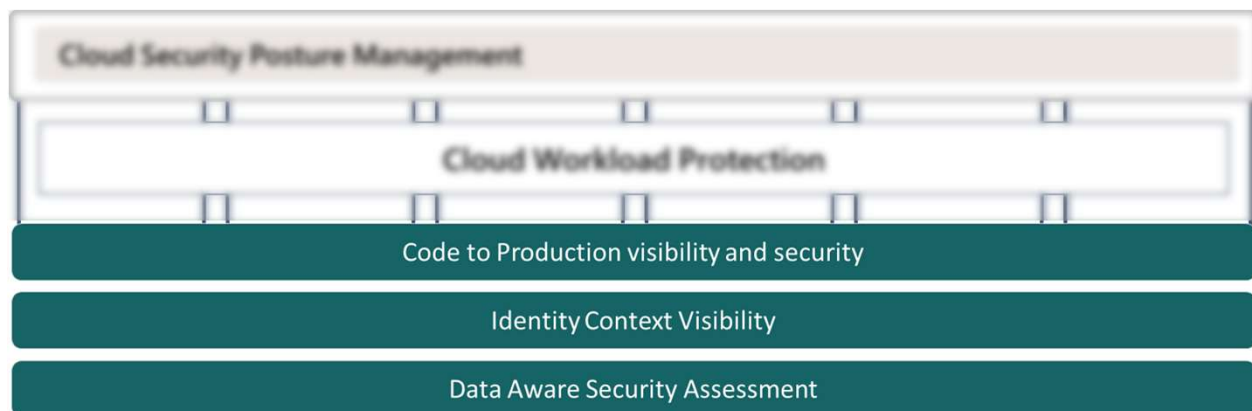


**Note:** CWPP provides workload specific detection and response capabilities.

Any CNAPP worth its salt has the ability to enrich the CSPM and CWPP findings with more context. This contextualisation helps in wider visibility and better prioritisation of risks

Some relevant inclusions are:

- » Identification of sensitive data to evaluate and prioritise risk.
- » Discovery of over-permissioned identities and unused permissions to model lateral movement and privilege escalation path.
- » Ability to connect the configuration assessment and runtime findings with development artifacts.

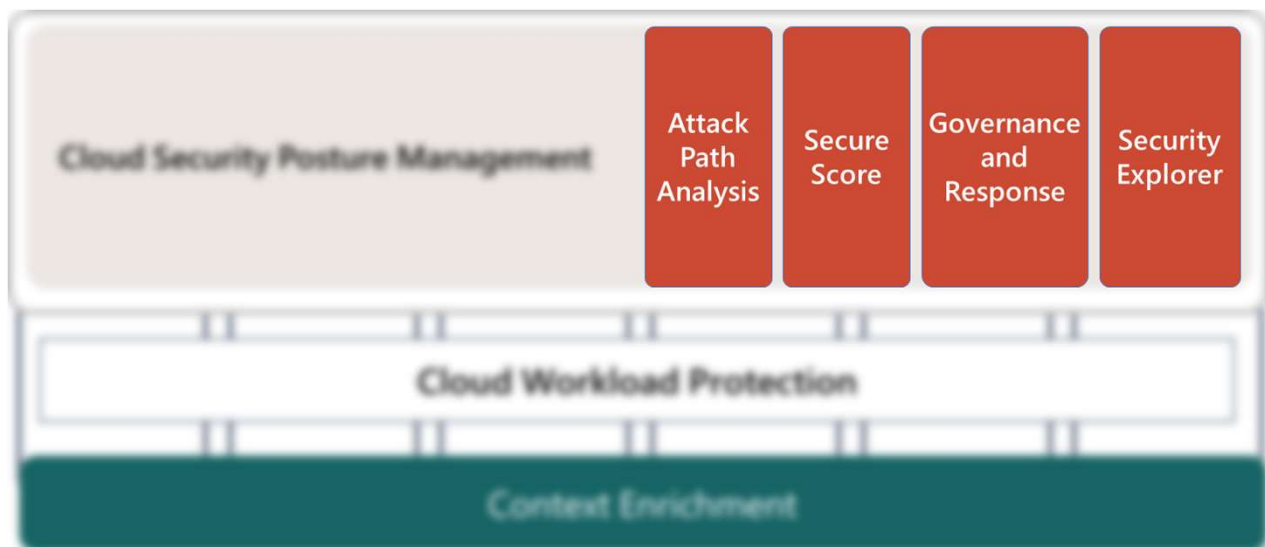


**Note: Data and permissions context helps with wider visibility and better prioritisation of risks.**

## 4 Value added solutions

CNAPP with broad coverage can leverage workload specific visibility and additional context to provide value added services such as:

- » Deeper attack path analysis to detect possibility of cross workload movement (due to permissions mismanagement) and identification of vulnerable hotspots (from presence of sensitive data).
- » Code-to-production linking to help development teams avoid ill-configuration and enable corrections at the source.
- » Consolidated scoring and recommendations - Consolidated listing of recommendations with risk, posture impact and priority rating.
- » Centralised governance and management workflow that go across workload types, team boundaries, and even across cloud services.



**Note: Enriched cross workloads visibility helps provide value added services.**

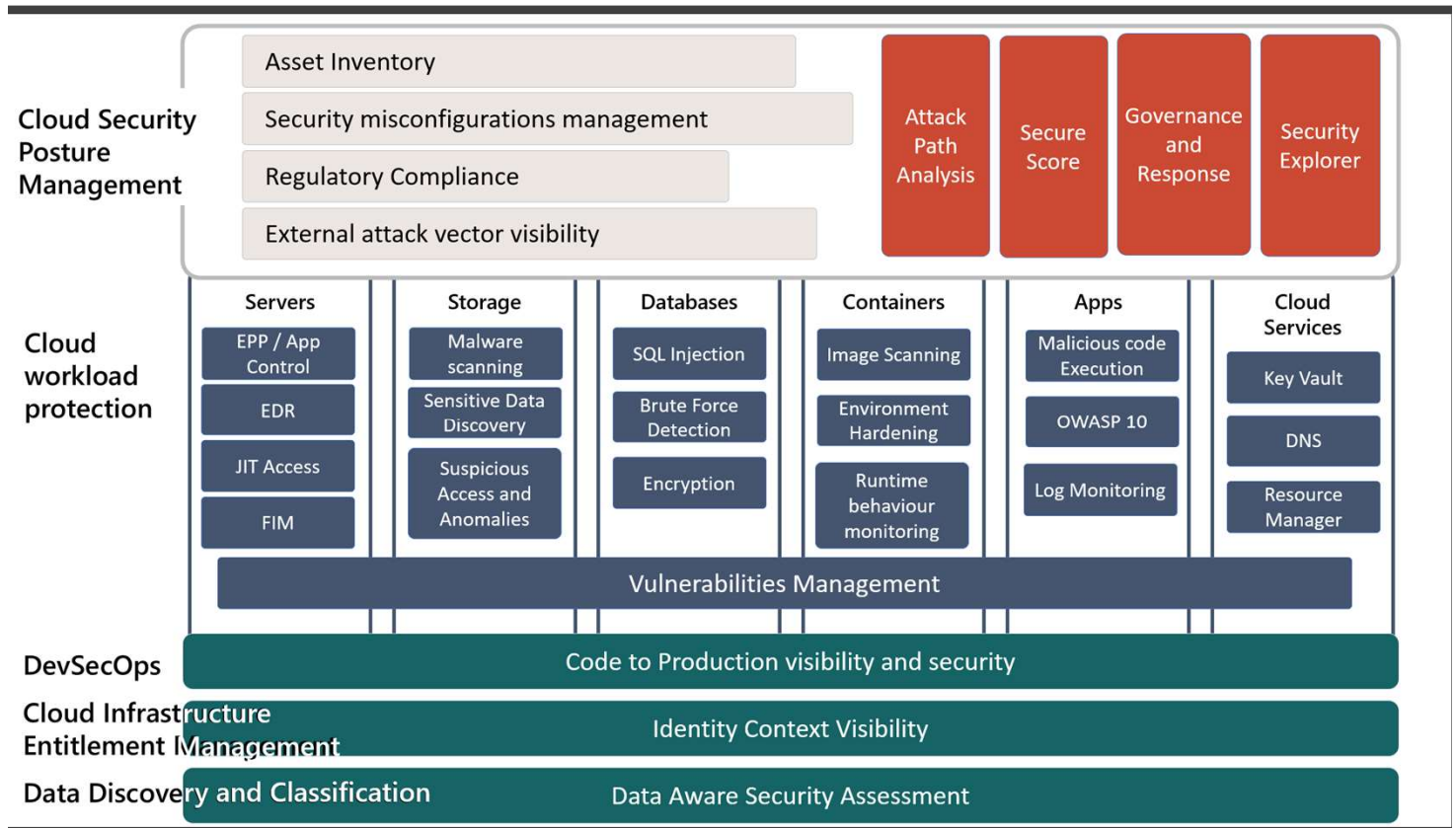
Download this chapter

<https://bit.ly/DeconstructedCNAPP>



# Cloud Native Application Protection Platform

And here's the full picture.





## Key Aspects / How to choose

Here's what to look for when choosing a CNAPP solution

- » Integrated solution - that provides Consolidated risk and recommendations, Unified policy framework, Centralised management workflow, and Shared threat intelligence overlay.
- » Common entity-model – across verticals of solutions. This results in easier correlation and ability to manually investigate across workloads. This is often missing when solution is formed from multiple acquisitions that are not integrated natively (front-end integration only)
- » Data and Identity Context - As highlighted in earlier pages, enrichment of risk with added context is a must for enhanced detection and prioritisation.
- » Regulatory compliance coverage - Compliance coverage is still a primary use case for CSPM solutions. CNAPP can assist with management and reporting by providing predefined templates for gap assessment against common compliance standards, and drift tracking.
- » Code-to-Production Linking
  - Deep understanding of the relationship between development artifacts (custom code, libraries, container images, VMs and IaC scripts) and creation, deployment and update correlation (who / when)
  - Integration into CI/CD infrastructure for code scans, build time integration and audit telemetry.
  - In-step checks with pull and deploy rejection capability
- » RiskOps\* - Risk based world-view across the protection stack and ability to continuously discover, monitor, assess and prioritize risk.
- » Mix of Agent-based and Agentless approaches - Agentless approach is great for easier rollout, reduced dependence on workload / infrastructure teams and minimal performance impact. However, for potent in-workload runtime visibility and response an agent-based solution performs better.

\* RiskOps Introduced by Gartner in [Seven Imperatives to Adopt a CARTA Strategic Approach](#) in 2018

Keen to know your thoughts

# Connect and Follow

## »LinkedIn

<https://www.linkedin.com/in/vikver/>

Connect



← Connect and follow on LinkedIn to discuss more.

## »Medium

<https://medium.com/@vikeso>



Information Security Advisor by profession. I write about Security, GRC, AI, Physics, Philosophy and more. New here but promise to be regular. Opinions my own.

## »Easy Sec Ops

<https://blogs.easysecops.com/>