CNAPP vs CSPM vs CWPP: Understanding Key Cloud Security Tools

Cloud computing has changed the way business operates. They have introduced a new layer of ease in capturing and storing data but with this ease, it has also introduced a new layer of complexity and vulnerabilities to cyber security. As more and more threats are aimed at cloud environments, organizations require strong solutions to protect their infrastructure and apps. Three significant cloud security technologies came into picture.

Cloud-Native Application Protection Platform (CNAPP), Cloud Workload Protection Platform (CWPP), and Cloud Security Posture Management (CSPM). It is vital to understand the differences between CNAPP vs CSPM vs CWPP in order to choose the right solution specific to your organization's needs.

In this blog, we will try to understand the difference between CNAPP vs CWPP vs CSPM, their distinct functions, and how they leverage one another as part of a comprehensive security posture.

What is CNAPP Security?

A Cloud-Native Application Protection Platform (CNAPP) is a set of security tools that protects the entire lifecycle of cloud-native applications. Instead of being single-purpose tools, CNAPP cloud security brings together workload protection, posture management and runtime security into a cohesive platform. This makes it possible for organizations to surface vulnerabilities, misconfigurations, and compliance issues in real time and securing workloads and applications for the complete lifecycle.

Key Features of CNAPP

- **Integrated Security Across Environments**

  CNAPP offers visibility and protection across applications running in hybrid and multi-cloud settings, delivering common security policies.

- **Proactive Vulnerability Management**

  Through the combination of scanning, detection, and prioritization, CNAPPs enable users to find vulnerabilities and remediate them before the operation of the environment is compromised.

- **Runtime Protection**

  CNAPP security extends application security to the runtime environment, enabling real-time monitoring and threat mitigation to prevent breaches or disruptions.

Fidelis Halo® is the only complete CNAPP solution covering the entire lifecycle of your cloud-native applications. Fidelis Halo® with integrated security, pre-emptive vulnerability management, and in-line runtime protection protects your applications in hybrid and multi-

clouds. One unified platform that brings it all together; to stay ahead of threats and minimize risks.

Struggling to Maintain Cloud Security and Compliance?

- Discover how to:
- Monitor for Risks
- Ensure Compliance in Real Time
- Strengthen your Cloud Infrastructure

Download the Whitepaper Now!

What is CWPP Security?

Cloud Workload Protection Platform (CWPP) refers to a security solution that safeguards workloads across various cloud hosting environments, including public cloud, private cloud, and hybrid cloud platform. CWPP security provides protection for workloads such as virtual machines, containers, serverless functions and more. Its workload-centric approach to threat detection, vulnerability management and compliance provides a way to address those challenges with a workload-focus. CWPP works on the infrastructure layer, protecting assets regardless of the cloud architecture under it.

Key Features of CWPP

- **Workload-Centric Security**

  CWPP safeguards assets such as containers, VMs, and serverless functions from runtime threats and exploits.

- **Integrated vulnerability scanning**

  It also scans workloads for security vulnerabilities, to catch day zero risk and helps in prioritizing remediation.

- **Runtime Threat Detection**

  CWPP security monitors workloads in real-time, detecting and responding to anomalous behavior or attacks.

Choose Fidelis Server Secure™ to provide your cloud environment advanced, workload-based protection. This solution aims to protect critical workloads be it VMs, containers or serverless functions from runtime threats and vulnerabilities. Fidelis Server Secure™ delivers continuous scanning, prompt threat detection and integrated workload protection to the cloud that keeps your assets secure and minimizes risk for any cloud environment.

What is CSPM Security?

Cloud security posturing management (CSPM) is a service used to identify and fix security threats across cloud technologies. Its main focus is on compliance with security and governance standards of cloud environments like GDPR, HIPAA, CIS benchmarks, etc., by monitoring configurations on a continuous basis and scanning them to identify potential misconfigurations or vulnerabilities.

CSPM security correlates at configuration and ensures that no breach is a result of human errors, policy violations, and mismanagement. CSPM is an important element of keeping secure cloud infrastructure running, able to provide insights into the security for gaps and noncompliance issues.

Key Features of CSPM

- **Configuration Assessment**

  CSPM detects and alerts on misconfigurations (e.g., overly permissive access controls) in real-time.

- **Compliance Monitoring**

  The tools offer real-time tracking and reporting capabilities to ensure compliance with industry standards and regulations.

- **Automated Remediation**

  CSPM security also helps organizations respond to risks rapidly with automated remediation or actionable recommendations.

Fidelis Security CSPM solution helps organizations prevent security risks in their cloud infrastructure by ensuring continuous compliance and risk management practices. Fidelis Cloud Secure™ is the one-cloud-native comprehensive CSPM solution that keeps your cloud environment secure and compliant. It identifies real-time misconfigurations, policy violations, and noncompliance risks by monitoring and assessing cloud-wide configurations continuously.

CNAPP Vs CSPM Vs CWPP: Key Differences

The table below highlights the essential points of comparison among CNAPP vs CSPM vs CWPP.

Feature CNAPP CSPM CWPP

Goals

Provide an integrated security platform for cloud-native applications across their lifecycle. Identify, monitor, and remediate misconfigurations in cloud environments. Protect cloud workloads (e.g., VMs, containers) from threats and vulnerabilities.

Key Capabilities

Combines CWPP, CSPM, runtime protection, and compliance into one platform. Continuous posture management, compliance reporting, and remediation recommendations.

Vulnerability scanning

, runtime protection, and threat detection for workloads.

Attack Vectors

- Misconfigurations in cloud environments.
- Insecure APIs.
- Runtime threats and vulnerabilities.

- Misconfigured cloud services.
- Open storage buckets.
- Non-compliant access controls.

- Malware targeting workloads.
- Container runtime exploits.
- Ransomware attacks on cloud workloads.

Threats Covered

- Misconfigurations and compliance violations.
- Runtime threats like malicious code injection.
- Application lifecycle vulnerabilities.

- Misconfigurations in cloud services.
- Exposed or unsecured cloud assets.
- Non-compliance with security policies.

- Malware and ransomware attacks.
- Unauthorized workload access.
- Exploits targeting workloads like containers and VMs.

Best For

Organizations looking for an all-in-one security solution for cloud-native applications. Businesses focusing on securing cloud configuration and ensuring compliance. Teams aiming to protect specific workloads (e.g., containers or VMs) in a cloud environment.

Scope

Broad coverage across cloud applications, workloads, and environments. Limited to security posture and governance in cloud configurations. Specialized in workload protection irrespective of the underlying cloud or data center.

Proactive/Reactive

Both proactive (risk mitigation) and reactive (runtime threat detection). Primarily proactive in addressing misconfigurations and non-compliance issues. Primarily reactive, focusing on detecting and mitigating workload-level threats in runtime

Compliance Support

In-depth, unified compliance and monitoring throughout the application lifecycle. Focused on identifying and fixing compliance violations. Supports workload-specific compliance without encompassing broader environments.

Integration

Combines CSPM, CWPP, and additional features into one unified platform. Integrates with cloud providers for posture and compliance management. Typically, standalone but integrates well with CNAPP for broader coverage.

You can refer to the table above even if you are trying to differentiate between CNAPP vs CSPM or CNAPP vs CWPP. This table will help you understand which solutions your business requires and once you reach the conclusion and look for the CSPM, CWPP, or CNAPP cloud security vendor then you don’t have to look beyond Fidelis Security. Let’s see what makes Fidelis Security the best CNAPP cloud security solution in the industry.

Why Choose Fidelis Cloud Security?

Fidelis Cloud Security enables complete protection across all environments (and the applications and data running in them). Whether it’s protecting workloads with Fidelis Server Secure™, defending cloud-native applications with Fidelis Halo®, or ensuring compliance with Fidelis Cloud Secure™, Fidelis provides real-time threat detection, vulnerability management, and automated remediation as part of an integrated solution.

Key Benefits

- Unified security platform for hybrid, multi-cloud environments.
- Real-time threat monitoring and vulnerability management.
- Automated remediation for rapid response.
- Strong compliance monitoring for industry standards (GDPR, HIPAA, etc.).
- Scalable, adaptable solutions for evolving cloud environments.

Why settle for less when you can have it all? Fidelis Halo® offers:

- Real-time security for cloud environments
- Automated protection for servers and containers
- Continuous compliance for hassle-free audits

Book a Demo Now!

Frequently Ask Questions

What is the difference between CNAPP vs CSPM?

CNAPP provides a complete security solution which integrates CSPM, CWPP, and runtime protection, in contrast CSPM concentrates on detecting and correcting cloud misconfigurations and compliance-related security problems.

What is the difference between CNAPP vs CWPP?

CNAPP cloud security refers to a single solution for application lifecycle security that includes both runtime protection and posture management. On the other hand, CWPP specializes in protecting cloud workloads like containers and VMs from runtime threats and vulnerabilities.

Can CNAPP replace CWPP or CSPM entirely?

CNAPP combines both CWPP and CSPM features, but more than those, therefore, this is a much wider solution. That said, some organizations will likely continue to use standalone CSPM or CWPP tools based on their needs.