# Everything you need to know about CNAPP

2025 VIPSS Conference



Ed Lewis

Managing Partner, DevSecOps and Cloud Security

February 2025



## Agenda

- 1. Industry Trends for 2025
- 2. Key Technologies
- 3. Services Offerings and Success Stories

## **Industry Trends for 2025**



## Cloud changes everything



How do I get visibility into my environment?



How do I prioritize the real risks and eliminate the noise?



How do I ingrain security into our teams?

## Market Projections and Opportunity



By end of 2025, 75% of new cloud security posture management (CSPM) purchases will be part of an integrated Cloud Native Application Protection Platform (CNAPP) offering.



By end of 2025, 80% of enterprises will have adopted multiple public cloud infrastructure as a service (laaS) offerings



By end of 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.



By 2026, 80% of enterprises will have consolidated security tooling for the life cycle protection of cloud-native applications to three or fewer vendors, down from an average of 10 in 2022.



## Cloud Security Hype Cycle

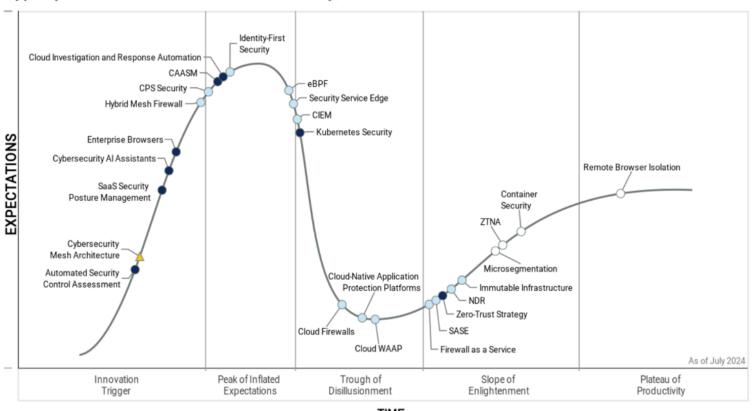


#### Matrix



### **Takeaways**

#### Hype Cycle for Workload and Network Security, 2024



TIME

Plateau will be reached: ○ <2 yrs. ○ 2-5 yrs. ● 5-10 yrs. △ >10 yrs. ⊗ Obsolete before plateau

In Production

Many vendors offering near-complete CNAPP features

Clients aren't fully taking advantage of **CNAPP** capabilities

#### **Innovation Focuses**

Cloud-focused incident detection and response automation

SaaS Application Security capabilities





## **Key Technologies**



## **CNAPP – What Good Looks Like**



### A complete platform should include...

#### To Achieve This

## Runtime Protection (CWPP)

Runtime protection at the instance/container to detect/block threats, drift, vulnerabilities, and malware.





## Entitlements Management (CIEM)

Lock down entitlements and identify and remediate IAM risks.



## Contextual Risk Analysis and Threat Detection

Combining data sources improves accuracy, enriches investigation, and reduces false positives



#### Defense in Depth

Layered protection of your most important cloud assets

## Posture Management (CSPM) Capabilities

Continuously identify and remediate risk and compliance

Integrations

Provide open APIs and

integrations with DevOps,

SIEM, ticketing systems,

and more



CNAPP Capabilities



#### public clouds, and capabilities for hybrid or private

**Multi-Environment** 

A unified platform for all



## Cloud Detection & Response (CDR)

Detect, investigate, and mitigate active cloud threats with forensic tools and automation



#### **Unified Processes**

Streamlined cloud security operations by combining many capabilities into one platform



#### **Total Oversight**

Over disparate cloud resources. Up-to-date asset inventory and compliance posture

### Network Security

Analyze networks to support Zero Trust, identify and remediate risky configurations



#### Data Security (DSPM)

Discover, catalog, and ensure protection and compliance for data stored in various repositories



## **CNAPP Players**







































Gartner, July 2024

## Services Offerings and Success Stories



## **Optiv CNAPP Services Offerings**

Secure Your Cloud with Optiv and CNAPP Solutions

Many organizations struggle to detect and respond to threats, causing challenges in identifying and prioritizing critical risks within their cloud environments. Optiv partners with CNAPP vendors to enable organizations to innovate faster, remove silos and transform their processes.

Optiv experts help clients understand the difference between good and great when it comes to Cloud Security Posture Management (CSPM) and/or Cloud Native Application Protection Platforms (CNAPP). By leveraging Optiv's advisory, implementation and configuration services, alongside the market leading CNAPP solutions, organizations can enhance their security posture and get 100% visibility into their cloud stack.

Optiv can help facilitate an efficient and seamless transition for clients looking to securely move a larger share of their business to the cloud and improve their business agility and resilience.

## **Optiv Use Cases**

- Cloud Security Architecture Assessment (CSAA)
- Cloud Strategy and Program Design
- Architecture Design
- Cloud Governance & Operating Model Design
- Product selection (e.g. vendors and modules)
- Design and Deployment
- Operationalization
- Maturity Services
- Staff Augmentation

### **Benefits of CNAPP**

- Increase workforce productivity
- Mitigate risk of cloud security breaches
- Improve collaboration across cross-functional teams
- Improve visibility across the entirety of cloud applications and services
- Operationalize CNAPP to successfully deploy, configure and upskill client teams to get the most out of the platform



## Case Study: Enhancing Cloud Security at a Global Automotive Manufacturer



#### **Client Scenario**

 Optiv worked with a global automative manufacturer to implement, configure and operationalize their Wiz Cloud Native Application Protection Platform (CNAPP) to enhance the cloud security posture for their Cloud environments.



#### **Our Solution**

- Advised on implementation design and expansion of Wiz use cases, modules and best practices.
- Assisted with 'hands on keyboard' implementation and configuration of Wiz platform and preparation, configuration, deployment and operationalization of Wiz Runtime Sensors.
- Assessed Wiz scan findings and developed prioritized vulnerability remediation plan based on severity and potential impact.
- Implemented recommended remediation actions within the Cloud environments and adjacent applications.
- Provided day-to-day operational support, trouble shooting, optimization and documentation.
- Assisted with knowledge sharing and upskilling through group sessions and 1-on-1 meetings.



#### **Value Outcome**

- Implemented, configured and operationalized Wiz within their Cloud environments.
- A secure Cloud environment configured in-line with security best practices.
- Established a robust and secure cloud foundation to enable additional migration of workloads.
- Permissions boundaries and least privilege policies for Service Control Policies (SCP) and Identity Access Management (IAM).
- Upskilled client team on usage of Wiz CNAPP and how to successfully maintain a resilient cloud security posture.

**Technology** 





## Questions?

Secure greatness®

