Solstice

CNAPP Unveiled: Transforming Cloud Security with Cloud-Native Application Protection Platforms

Frederik De Ryck

Accenture

Agenda

01 Introduction

02 What is CNAPP?

03 CNAPP Capabilities

04 Conclusions

05 Q&A

Frederik De Ryck

Cyber Cloud
Security Lead
GALLIA

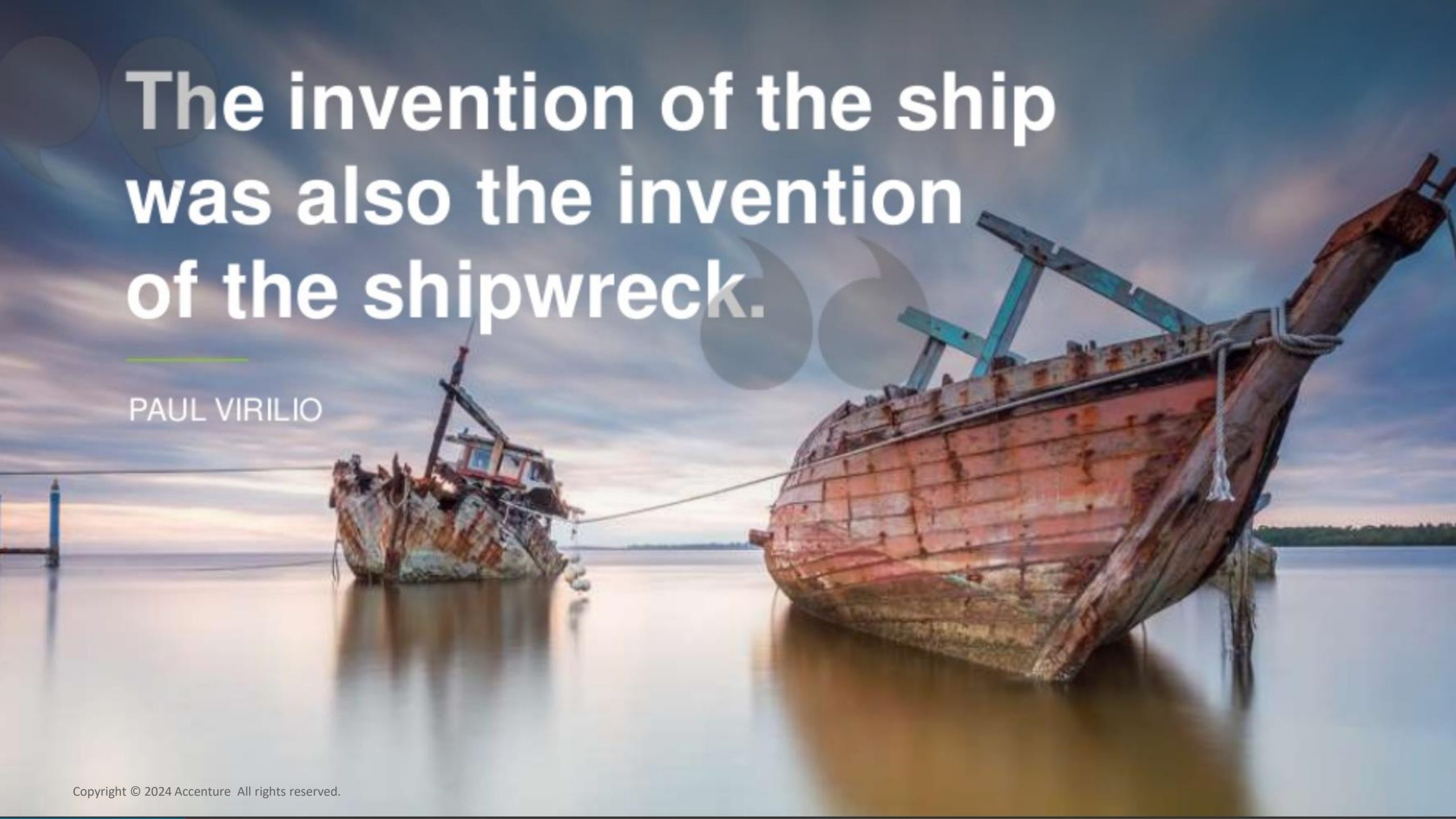
ACCENTURE SECURITY

Frederik.de.ryck@accenture.com

Frederik is a Cyber Security Manager within the CIA department of Accenture Security. He is an active member in the global Cloud Security Community.

He is an enthusiastic and motivated person with strong and in-depth knowledge in protocols and security principles. Has an analytical mind that helps in delivering and structuring complex projects.

As a fan of emerging technologies he is experimenting where he can. As a TROOPER he is convinced that together we can make the (cyber) world safe.



Navigating the Multi-Cloud Security Problem Space

Structural barriers prevent moving at the speed of business context, industry threats, technology change

Proliferation of vulnerable code into cloud application development lifecycle

Limited visibility and monitoring of privileged access to cloud environments

Siloed cloud and security operations model extends security event detection and response

Misconfigured settings

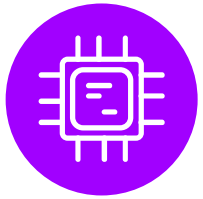
remediation efforts can be challenging and costly leaving misconfigured environments vulnerable and open to threats

Limited visibility

over the security posture of multi-cloud assets across the organisation

Configuration drift

as cloud environments scale, they become more susceptible to config drift and inadequate change control

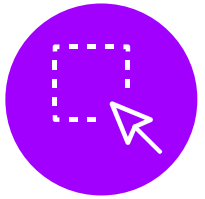


Technology jungle

with Vendor saturation and many point solutions which only address a small part of the cloud security challenges

Ever changing threats

as adversaries are constantly evolving their mode of operations, intentions, and tooling (TTP)



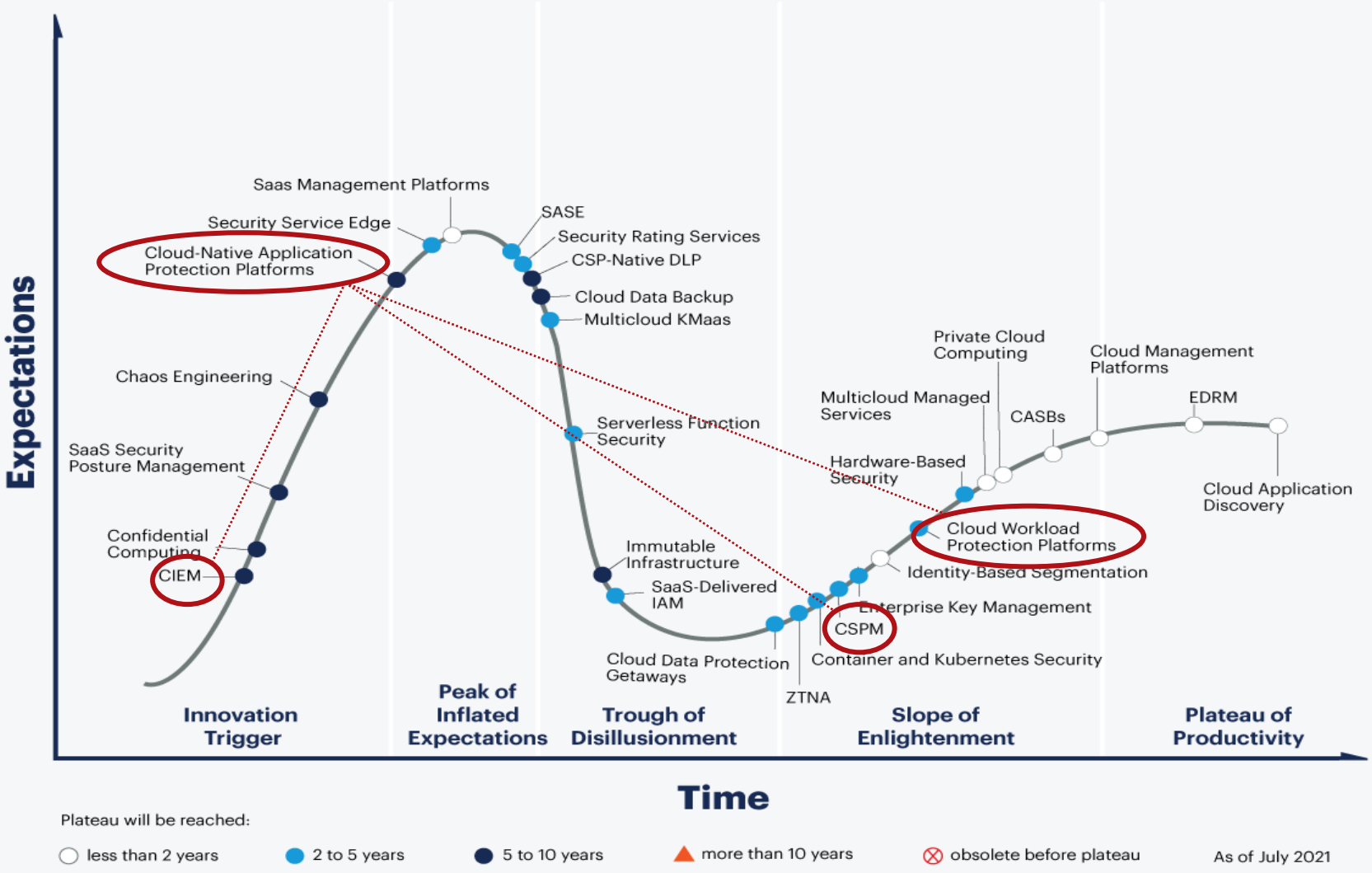
Vulnerable software

as software supply chain introduces complexity into code development lifecycle

01

What is CNAPP?

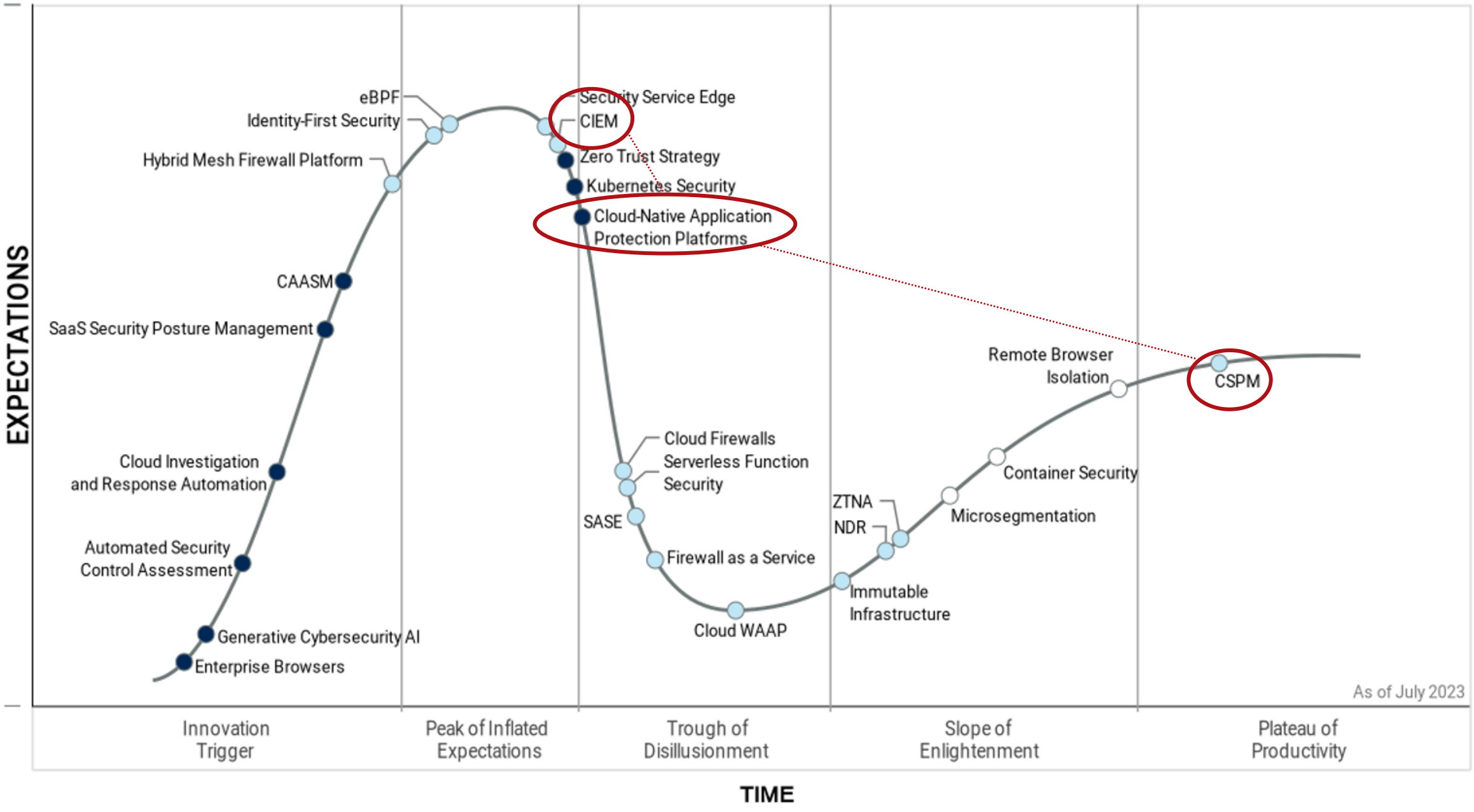
Hype Cycle for Cloud Security, 2021



gartner.com/SmarterWithGartner

Gartner

Hype Cycle for Workload and Network Security, 2023



CNAPP Definition

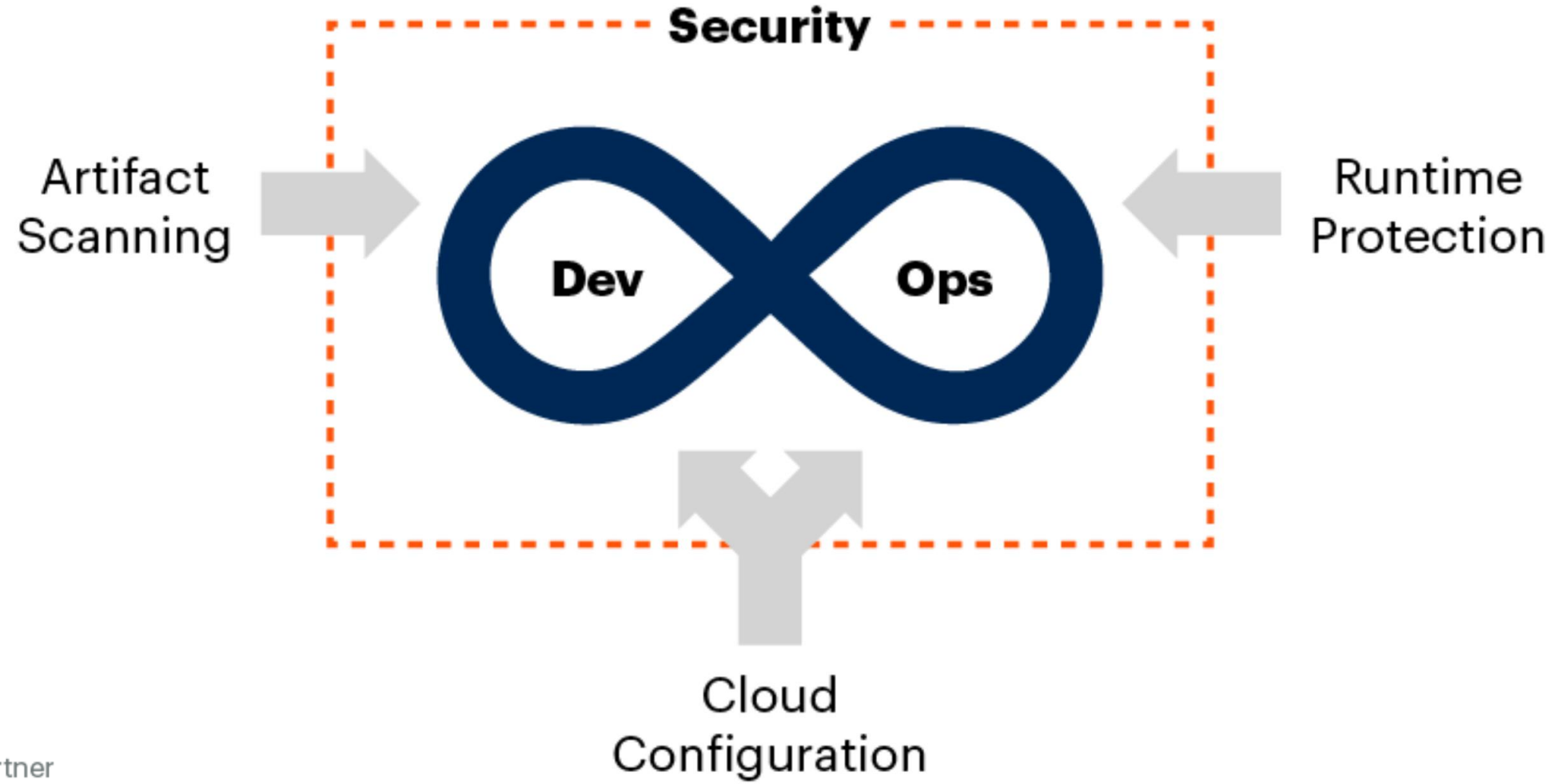
"Cloud-native application protection platforms (CNAPPs) are an integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications across development and production."

Gartner.

Gartner: **Innovation Insight for Cloud Native Application Protection Platforms** report, 08/25/21

Cloud Native Application Protection Platform (CNAPP)

CNAPP is a logical evolution for DevSecOps and “shift left” security



Source: Gartner

02

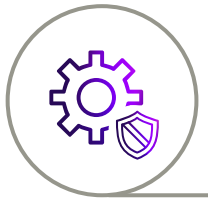
CNAPP Presentation

Capabilities

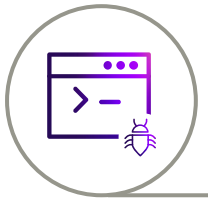
CNAPP Key Principles

A Cloud-Native Application Protection Platform (CNAPP) is an integrated set of security and compliance capabilities, designed to help secure and protect cloud-native applications across multi-Cloud setups.

CSPM
Cloud Security Posture Management



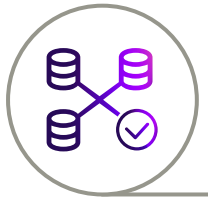
CWP
Cloud Workload Protection



TVM
Threat & Vulnerability Management

CIEM
Cloud Infrastructure Entitlement Management

CS
Code Security



NWS
Network Security

CNAPP Key Principles

A Cloud-Native Application Protection Platform (CNAPP) is an integrated set of security and compliance capabilities, designed to help secure and protect cloud-native applications across multi-Cloud setups.

CSPM
Cloud Security Posture Management

- Misconfigurations
- Non-compliance

CWP
Cloud Workload Protection

- Malware
- Threat Detection

TVM
Threat & Vulnerability Management

- Vulnerabilities Exposed
- Services

CIEM
Cloud Infrastructure Entitlement Management

- Excessive and risky privileges

CS
Code Security

- Misconfigurations
- Unsecure secrets

NWS
Network Security

- Network anomaly

CNAPP Key Principles

A Cloud-Native Application Protection Platform (CNAPP) is an integrated set of security and compliance capabilities, designed to help secure and protect cloud-native applications across multi-Cloud setups.

CSPM
Cloud Security Posture Management

- **Visibility** across multiple environments
- **Compliance** Monitoring
- Configurations Scanning
- Threat Detection
- Incident Response (leveraging integrations)

CWP
Cloud Workload Protection

- **Runtime Protection** for :
  - Virtual Machines
  - Containers
  - Serverless Functions
  - Web Applications and API
- System Integrity Protection
- Application Control
- Behavioural Monitoring
- Intrusion Prevention
- Malware Scanning
- Sensitive Data Scanning

TVM
Threat & Vulnerability Management

- Threat Analysis and **Vulnerability Management** (usually part of CWP features)

CIEM
Cloud Infrastructure Entitlement Management

- **IAM** Governance and Security
- **Privileges** Visibility
- User and Entity Behavior Analytics

CS
Code Security

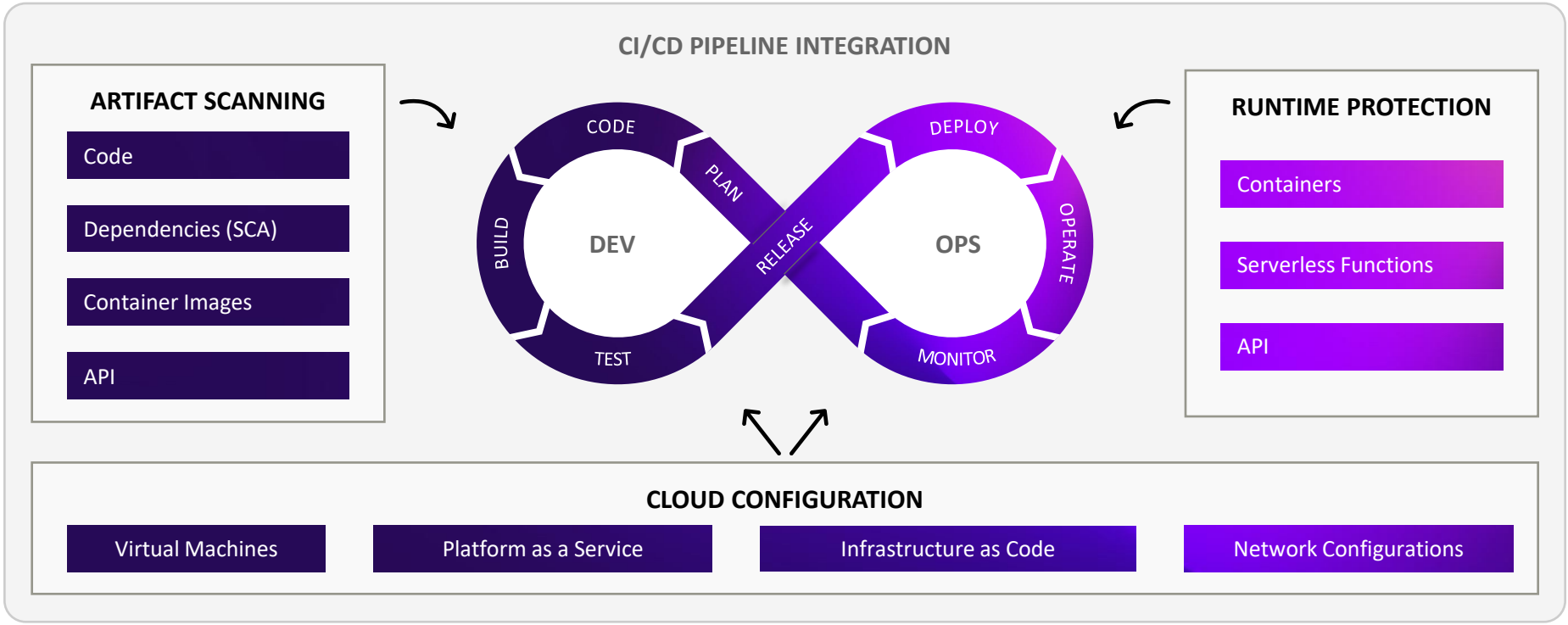
- SAST/DAST
- Software composition analysis (SCA)
- Secrets Scanning
- **IaC** Security and Policy as code
- **Container Images** Scanning

NWS
Network Security

- Visibility
- Anomalous network behavior detection
- **Micro-segmentation**

CNAPP Technical Description

CNAPP features can be split into three categories : Artifact Scanning, Runtime Protection, Cloud Configuration - allowing the platform to perform security and protection of Cloud assets along the whole lifecycle.



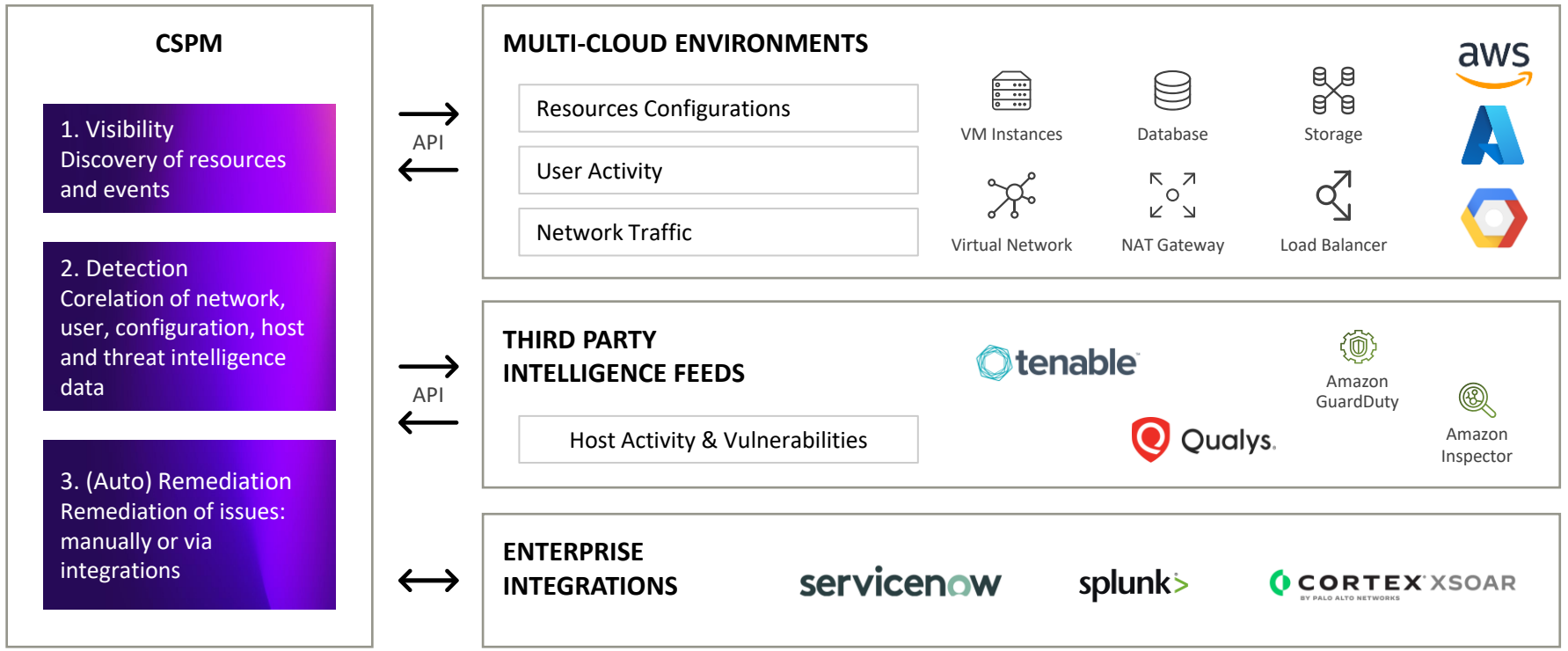
Visibility | Compliance | Protection | Detection | Prioritization | Alerting | (Auto) Remediation | Reporting

Focused Outcomes

- **Full visibility** across multi-Cloud environments, filling the existing knowledge gap
- Improved **Risk Prioritization**, enabled by centralized and contextualized risk queue (aggregating vulnerability data, extensive permissions, misconfigurations, etc.)
- Time efficiency empowered by **auto remediation**
- **Reduced complexity** and costs associated with multiple security tools
- **Seamless integration with CI/CD pipeline**, leading to better security tool acceptance from DevOps teams

Deep Dive into CSPM

A Cloud Security Posture Management (CSPM) continuously monitors public cloud environments to detect and protect cloud infrastructure from security threats as well as to maintain compliance.

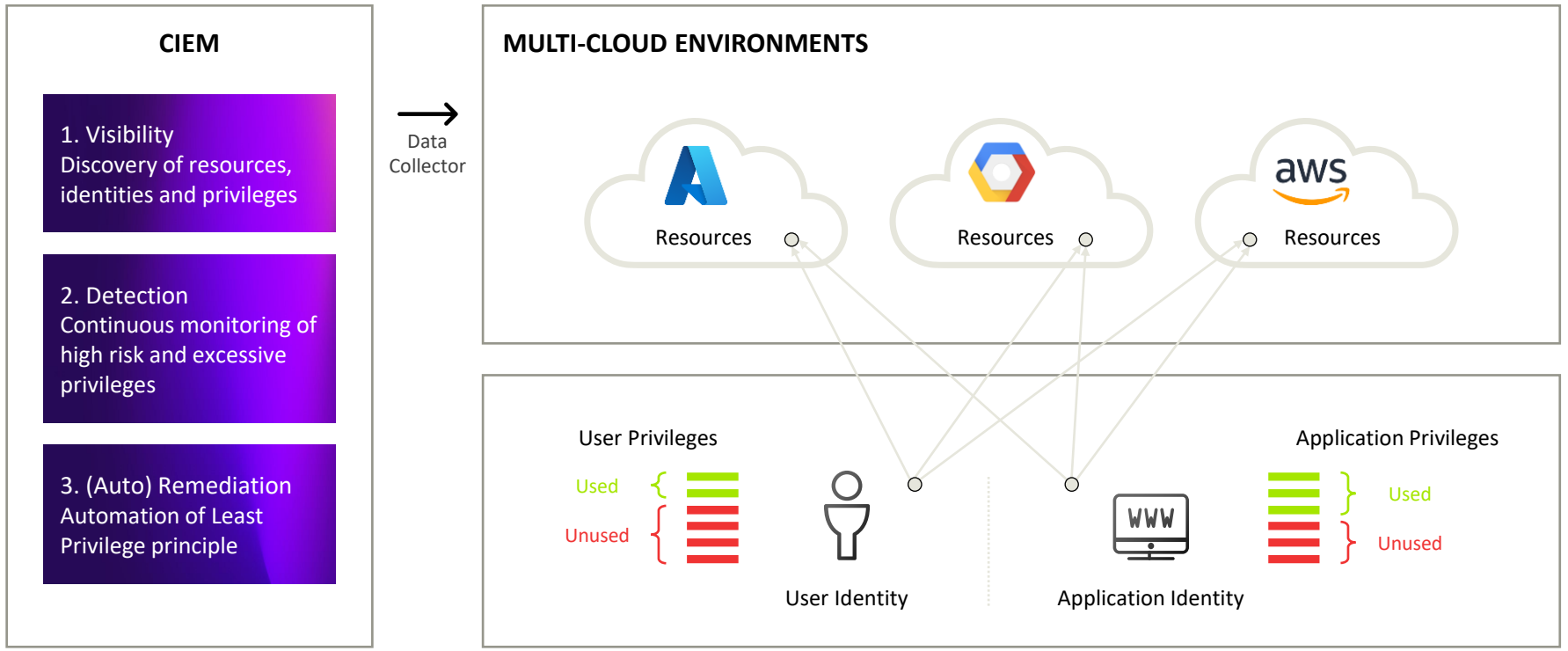


Focused Outcomes

- Multi-Cloud **Visibility**
- Policy Monitoring and **Compliance** Reporting
- **Threat Detection** (e.g. anomaly, UEBA)
- Contextual **Alerting**
- Opportunity for Rapid & Continuous **Remediation**

Deep Dive into CIEM

A Cloud Infrastructure Entitlement Management (CIEM) is supporting the process to manage identities and privileges in Cloud environments and enables a comprehensive overview of excessive or risky permissions.



Focused Outcomes

- Multi-Cloud **Identities and Privileges Visibility**
- Highlight of **excessive** and **risky** Privileges
- Automated **Least Privilege** and enabled **on-demand privilege** request

Conclusion

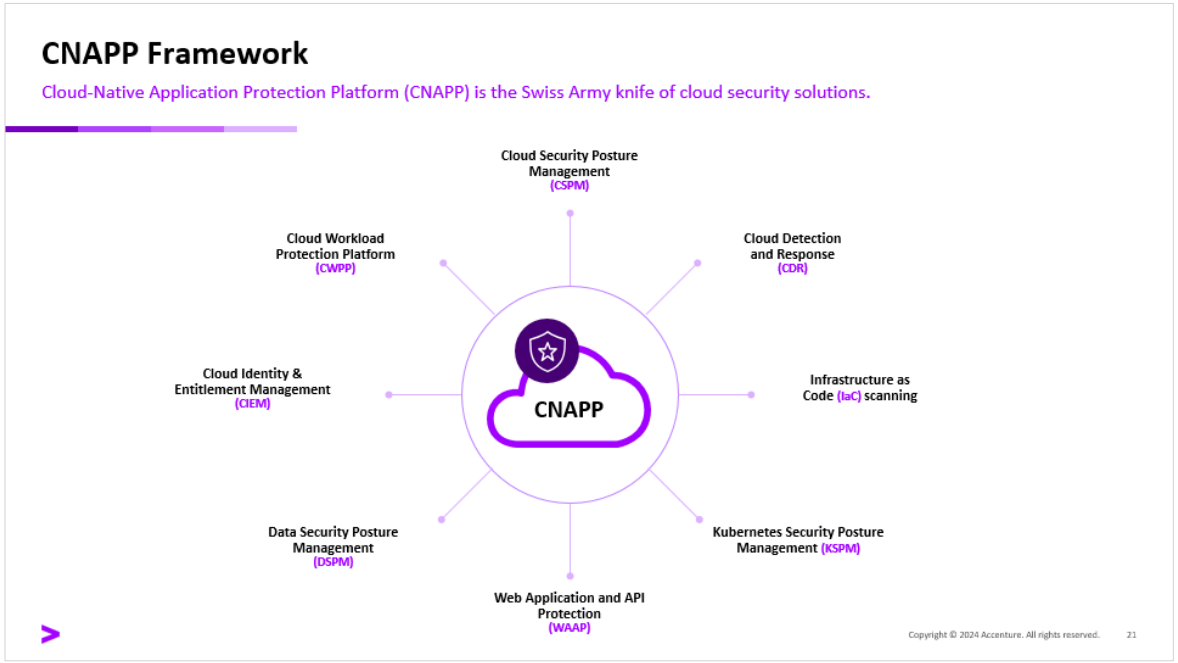
Accenture Interactive

Conclusion – CNAPP

Cloud native Application protection platforms

Is our cloud secure?

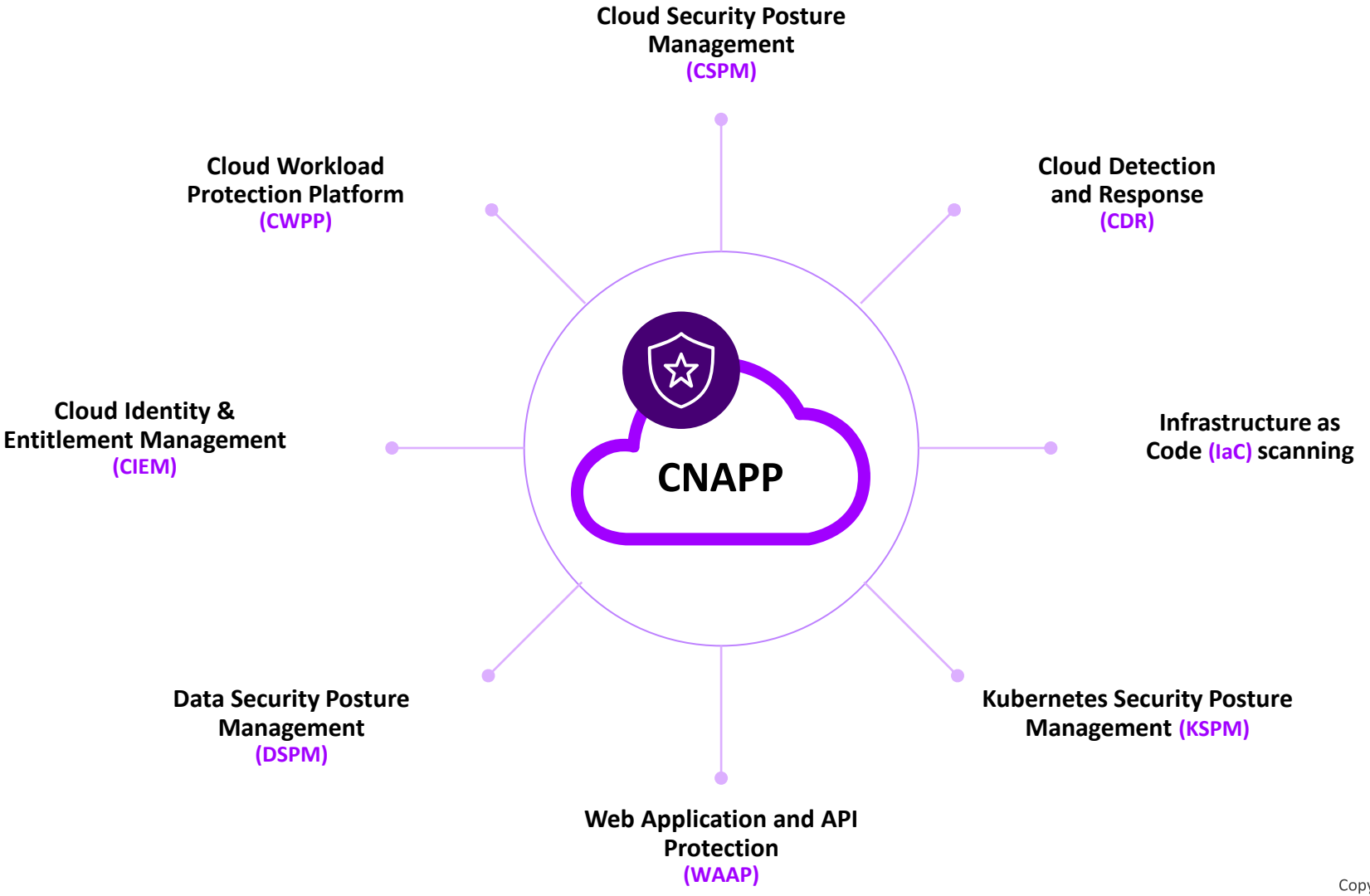
Swiss army knife?




CNAPP is not a golden bullet
Accenture

CNAPP Framework

Cloud-Native Application Protection Platform (CNAPP) is the Swiss Army knife of cloud security solutions.



Thank You

Q&A: Frederik.de.ryck@accenture.com