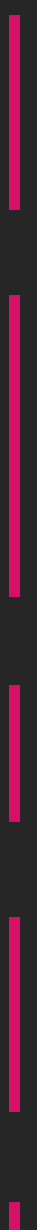


# CLOUD NATIVE SECURITY MODEL

Best practice approach  
for designing ultimate  
cloud security environment



Moving to the cloud is more than a technical transition to a new platform. It is a core part of an enterprise's growth strategy and while strategically important, it can also be potentially disruptive.

For cloud transformation to be successful, enterprises must be aware of their organizational and technology challenges, and security teams must carefully plan their strategy and approach. This playbook aims to provide important principles of cloud-native security modeling based on the most advanced and common cloud security trends and concepts, which will lead organizations towards reliable cloud security architecture implementation.

## Cloud Security Architecture Building Blocks

Secure and reliable environment must be built on a strong basis using standardized building blocks. And there are two popular models, two approaches to build cloud-native security architecture.



# The 4C's of Cloud Native Security

Each layer of the Cloud Native security model builds upon the next outermost layer. The Code layer benefits from strong base (Cloud IaaS, Cluster, Container, Code) security layers.

**Design Principle:** This layered approach augments the *defense in depth* computing approach to security, which is widely regarded as a best practice for securing software systems.

The first one is the 4C model, proposed by Google for the popular Kubernetes platform invented by them. It defines 4 layers.

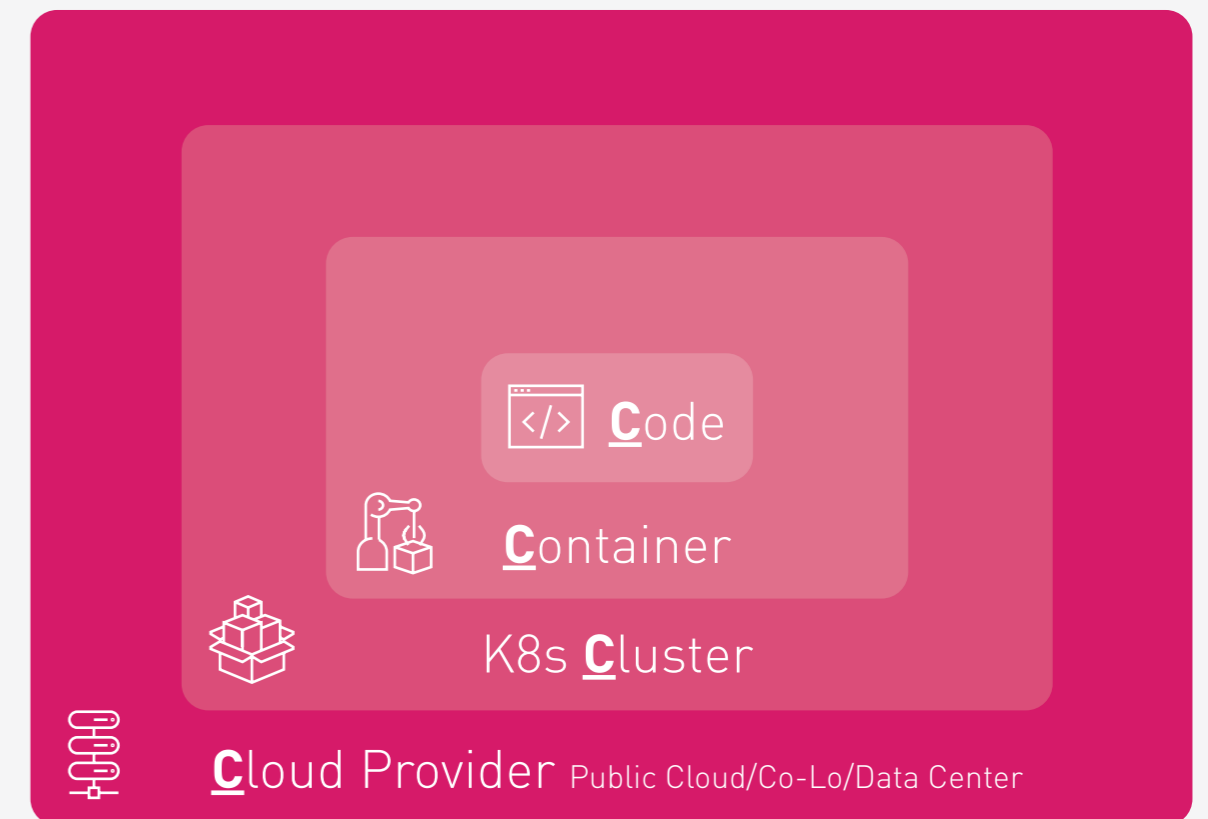
**#1** is Cloud/Co-location/Data Center. Obviously, we need a strong base to build our systems on top of it. If the cloud or Data Center is insecure the whole system can be compromised.

**#2** is a Kubernetes cluster. Doesn't matter if it is a vanilla Kubernetes on-prem or a managed Kubernetes cluster like AKS/EKS/GKE. It brings additional risks which must be addressed. If somebody can compromise the Kubernetes cluster he can own all the infrastructure.

**#3** Containers.

**#4** Code.

All these layers are important, base on the previous one and require different protections. We will discuss them soon.



# CNAPP – Cloud Native Application Protection Platform

CNAPP model was proposed by Gartner and separate 3 pillars we need to pay attention for.

The first one is Cloud Security Posture Management (CSPM). Obviously, the control plane must be protected. And as we are talking about Cloud-Native, these protections must be mostly agentless, protect assets wherever they are placed, provide powerful visualization for many aspects of the environment.

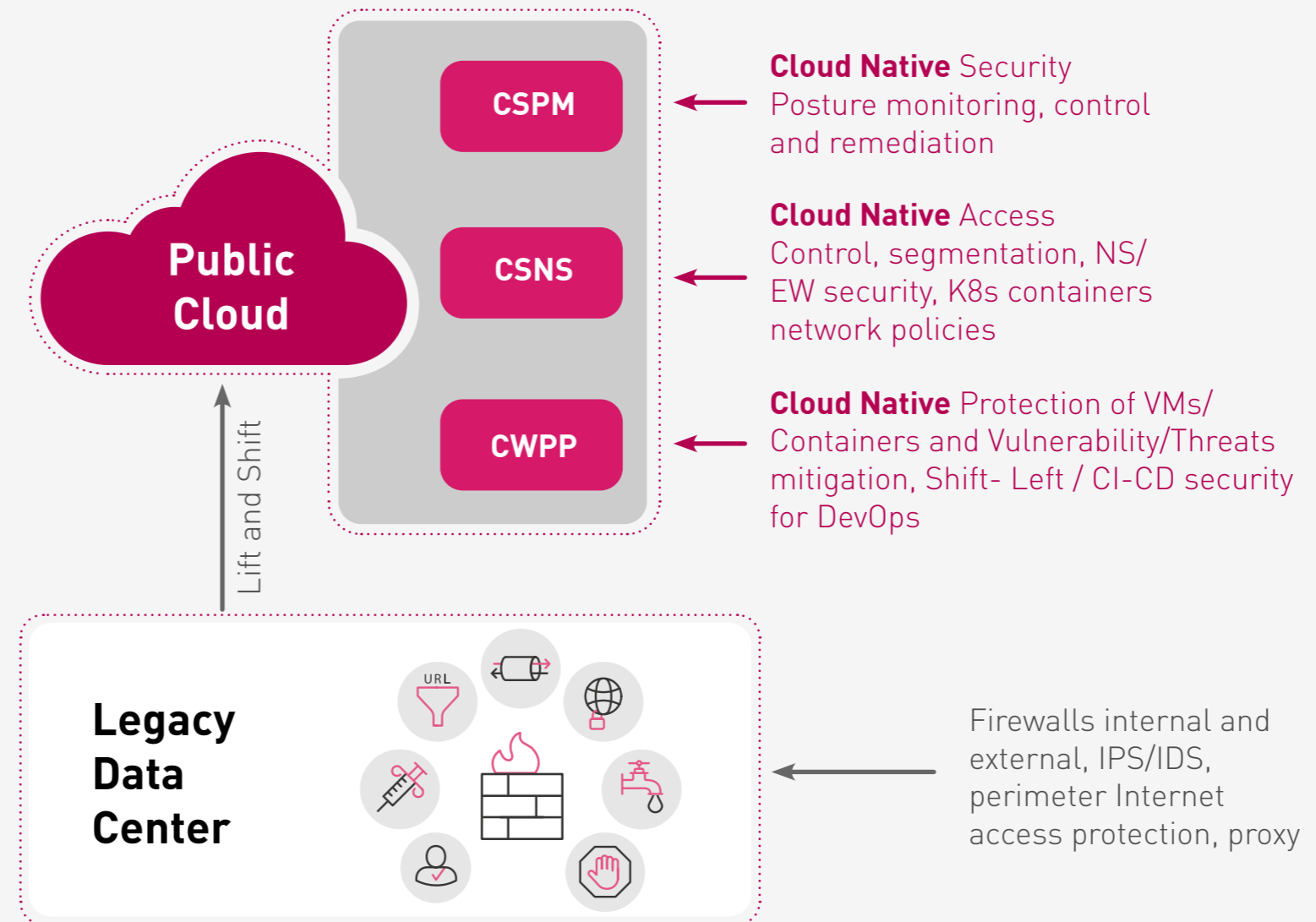
The second pillar is Network Security (CNS). It includes traditional solutions like load balancers, security gateways/firewalls, and web application firewalls, which still may be adopted for cloud-native environments.

And the third one is the Cloud Workload Protection Platform (CWPP) - It is about securing workloads themselves which includes protection to avoid breaches as well as threat hunting technologies to quickly identify and respond if we were compromised.



# Cloud security transformation

As soon as we “lift and shift” legacy environments to clouds, traditional security solutions firewalls, IPS and others must be adopted and in many cases replaced or expanded with the new cloud-native tools covering 3 pillars (CSPM, CNS, CWPP) discussed earlier.



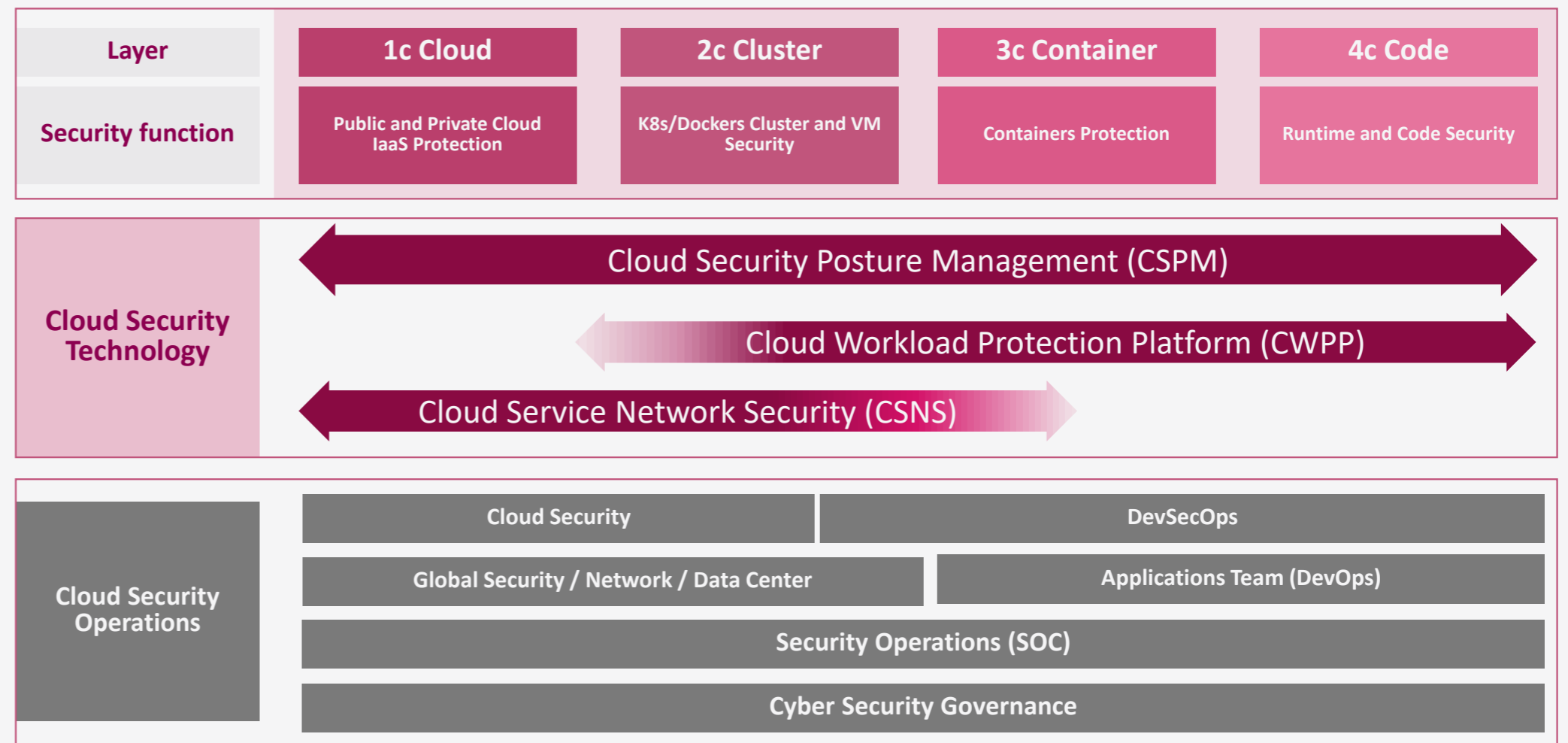
## Cloud Native Security Model - 4C and CNAPP adjacency

We've talked about 2 models: 4C and CNAPP, Every model covers its aspect, and Check Point combine them and fill with real security products. Let's look at the matrix with 4 columns according to the 4C model, and rows of CSMP, CWPP and CNS.

It gives us a good understanding what we really need to build a security architecture.

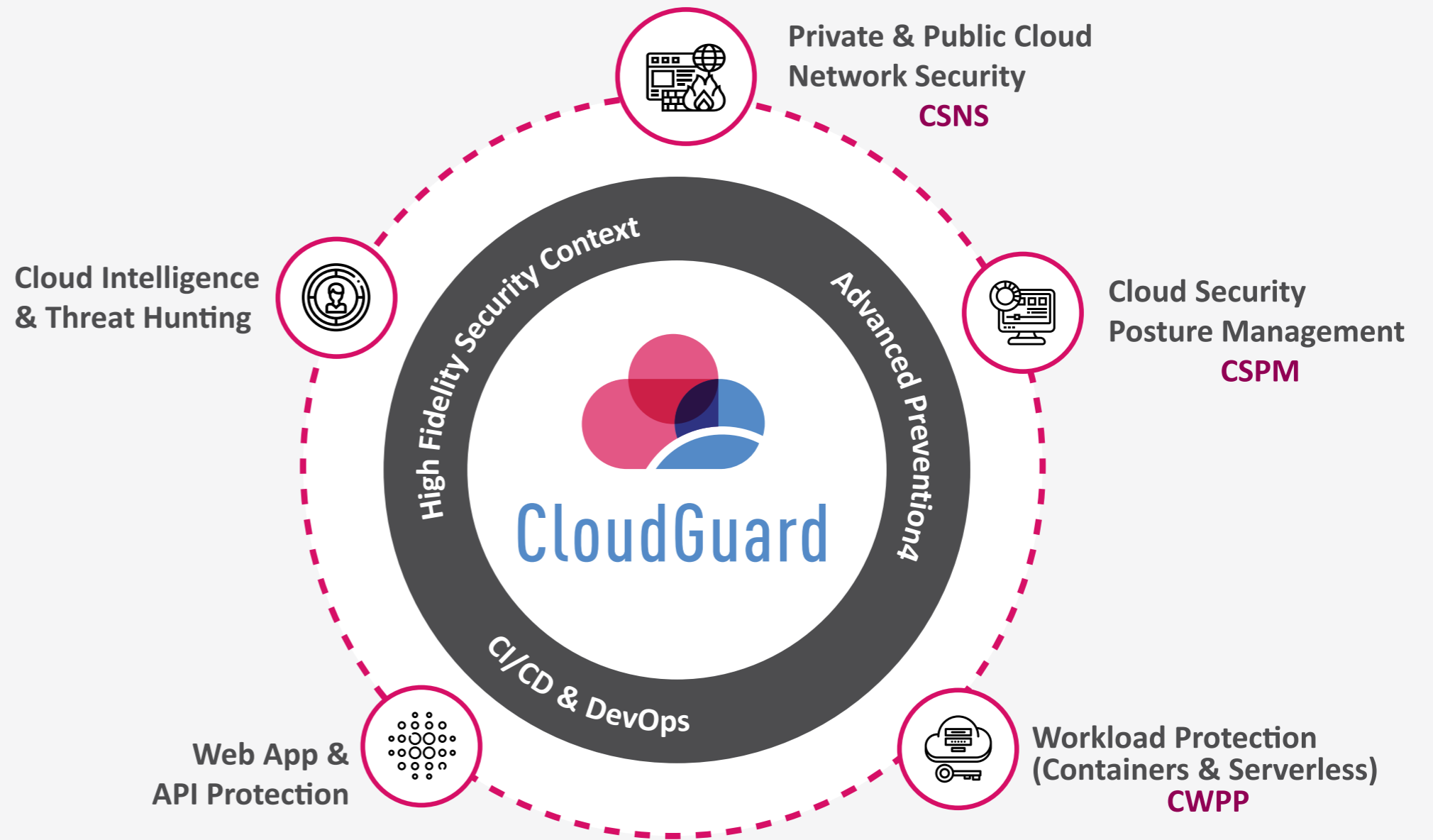
Secured Posture is important for all 4C pillars. Workload protection is not relevant for 1C because we definitely should not protect the public cloud infrastructure. And Network security is less relevant to the 4c Code layer. Other solutions at other layers must be used to secure it.

Additionally, we'd always remember of Security Operations. Many teams are involved, they are responsible for different aspects and must cover all 4c layers.



# One CloudGuard Multi Cloud Security

Number of solutions is growing. They cover different aspects of security. And it is important to keep the great Check Point advantage of the unified management. That's why we are talking about the single CloudGuard platform covering various aspects of the Cloud-Native security, wherever we are talking about CSPM, CNS or CWPP.





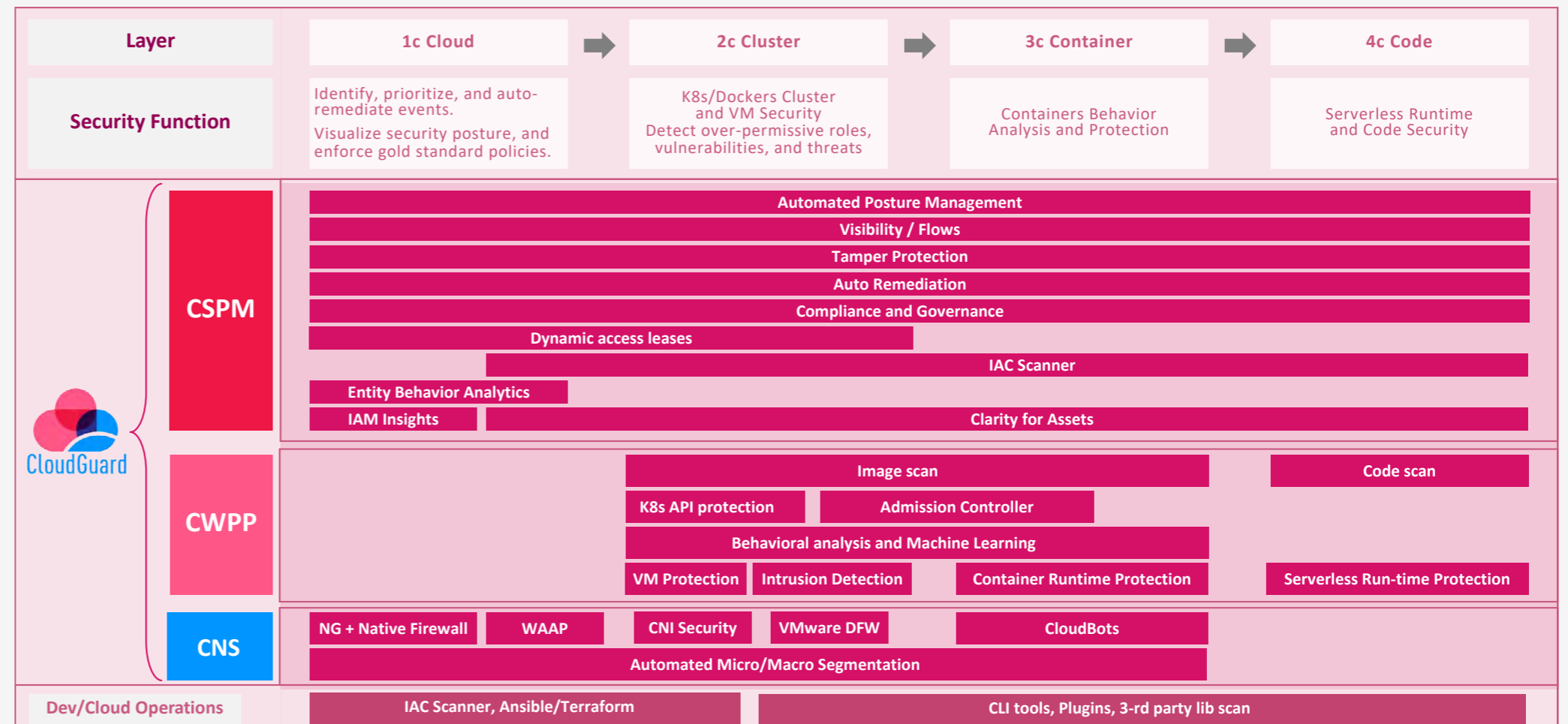
# CNAPP Security Functions

Now let's go deeper to the intersections of 4C and CNAPP models and talk about security features required to protect every cell of this matrix.

Some features like Posture Management, Visibility, Compliance and governance are important for all layers. Of course, specific checks will be different. CIS Kubernetes benchmark or NIST 800-190 is relevant for 2C. While AWS or Azure should be checked against different standards.

But anyway we must ensure that all settings follow best practices.

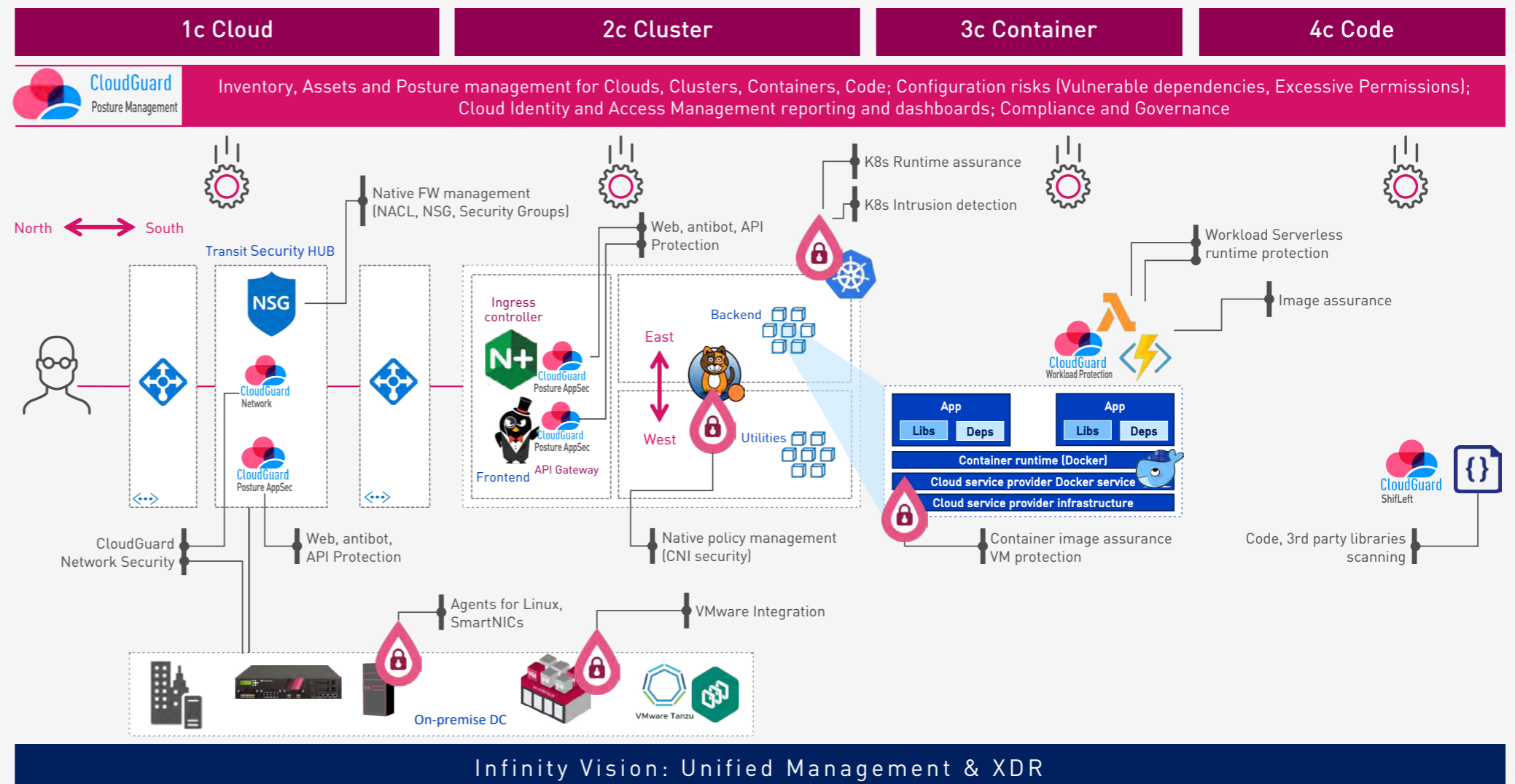
As Check Point CloudGuard Posture Management (formerly Dome9) for public clouds is well-known, let's focus on relatively new Workload protection, which became important with the growth of Containers popularity in companies of different sizes.



# Cloud Native Security Design Model

The drawing below represents Cloud Native architecture design model using Check Point solution deployed per relevant level according to the 4C concept.

- 1C Cloud IaaS layer provides network access security and is protected with CloudGuard Network and Quantum appliances.
- 2C layer secures Kubernetes cluster against intrusions and other threats using agents, like Application Security (AppSec)
- 3C layer refers to containers and assures their images security during build and runtime
- 4C is about code and includes ShiftLeft to scan own code as well as 3rd parties dependencies

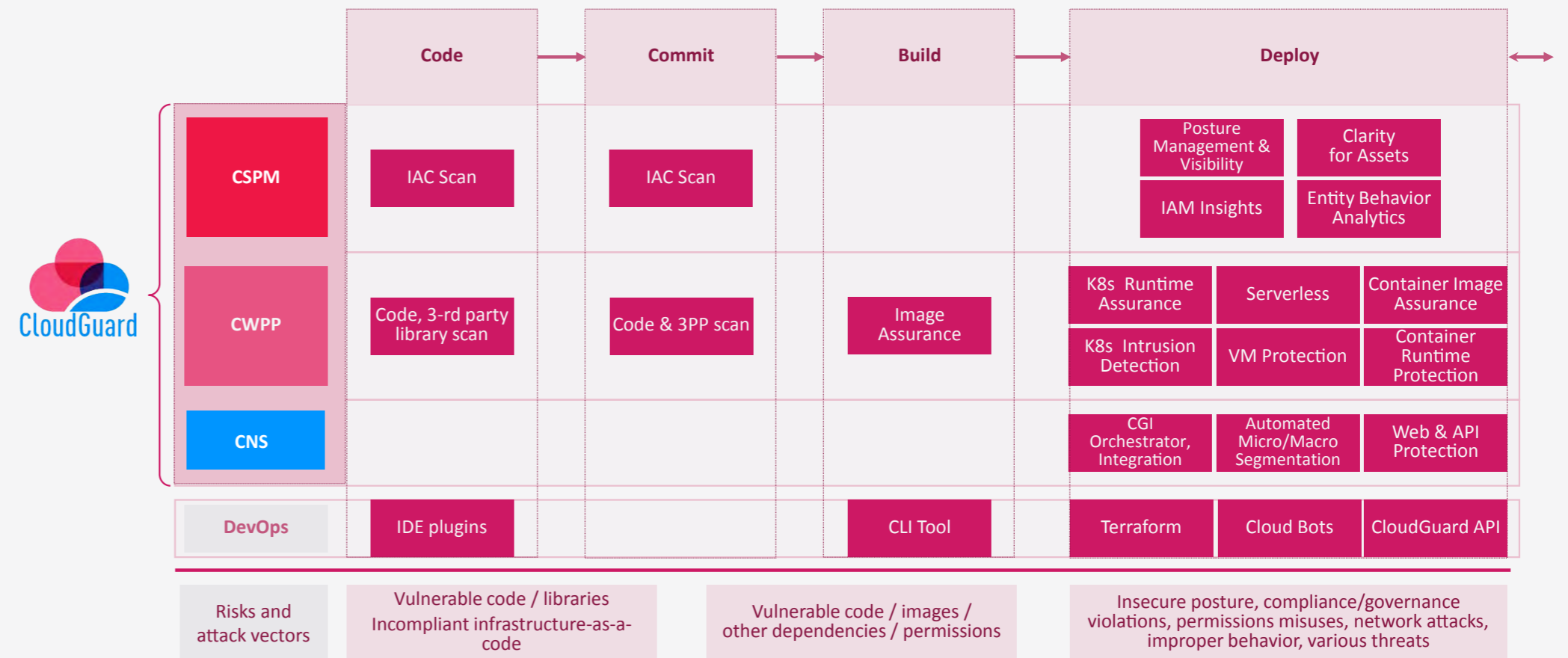


©2020 Check Point Software Technologies Ltd.

# CI/CD pipeline security

A typical development workflow includes the following steps: Develop, test locally, commit code to the version control system. CI/CD system takes this code, builds it, pushes it to the Docker compose which builds a container also using images and packages from public repositories and places it into the public or private registry. After successfully staging the container goes to production.

Every step brings additional security risks which are addressed with Check Point Native security solution from the early development stage to production as shown at the figure below:

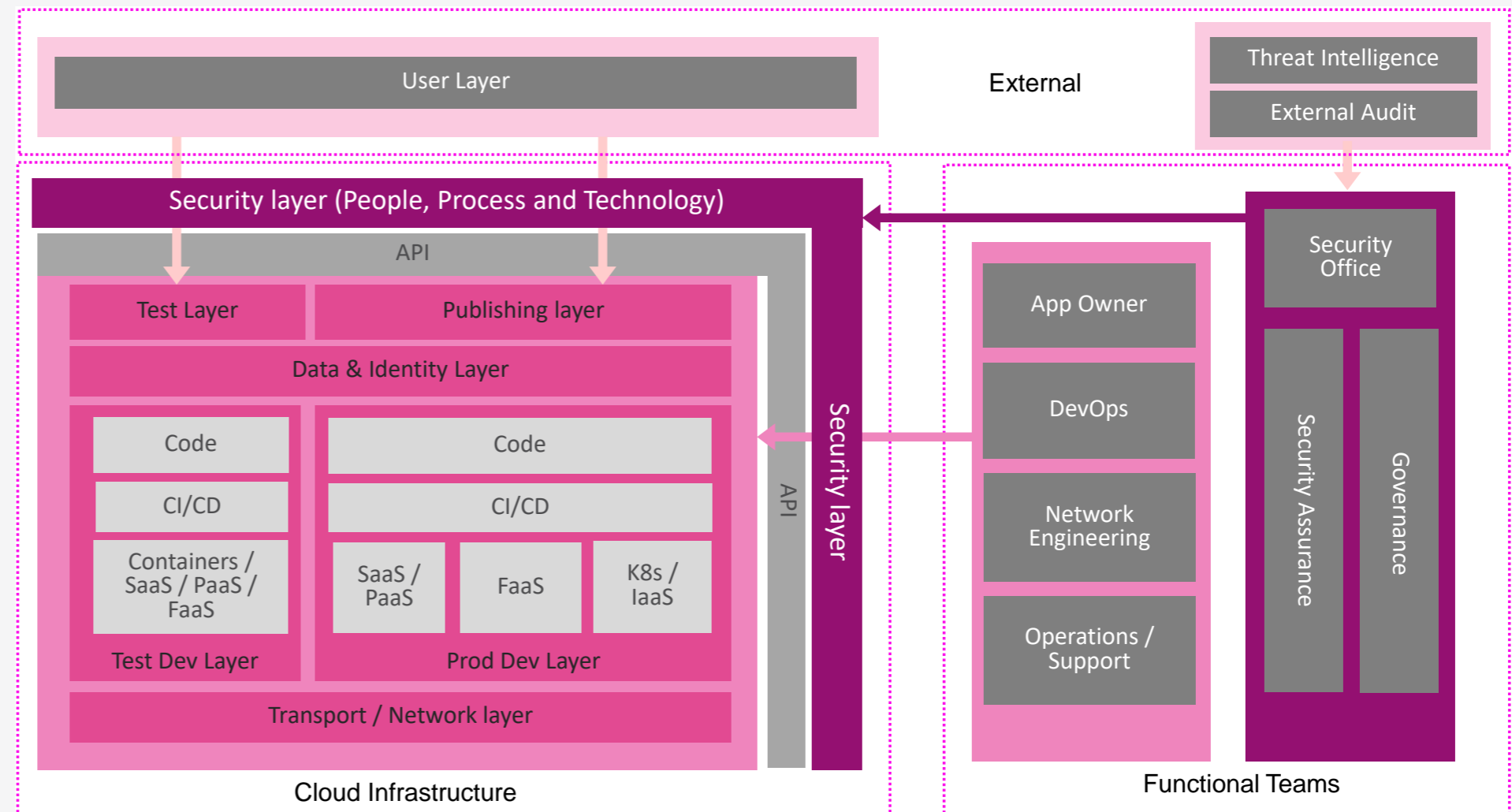


# Operations Model

The network security team has become the security compliance and governance team that oversee security but do not sit directly between the dev team and the workload.

The security layer (physical or logical) is still owned by the security team and protects the cloud environment but doesn't interfere with dev teams

This operation is done through the api where security teams define guidelines and policies for devops and constantly verify the enforcement



# Cloud security architecture Design Process

## 01

Design Principles  
Standards  
Design Patterns

**4C Model - Google**

**CNAPP Model - Gartner**



## 02

Technical  
Security  
References

**K8s security model**

**Check Point  
Best Practice**

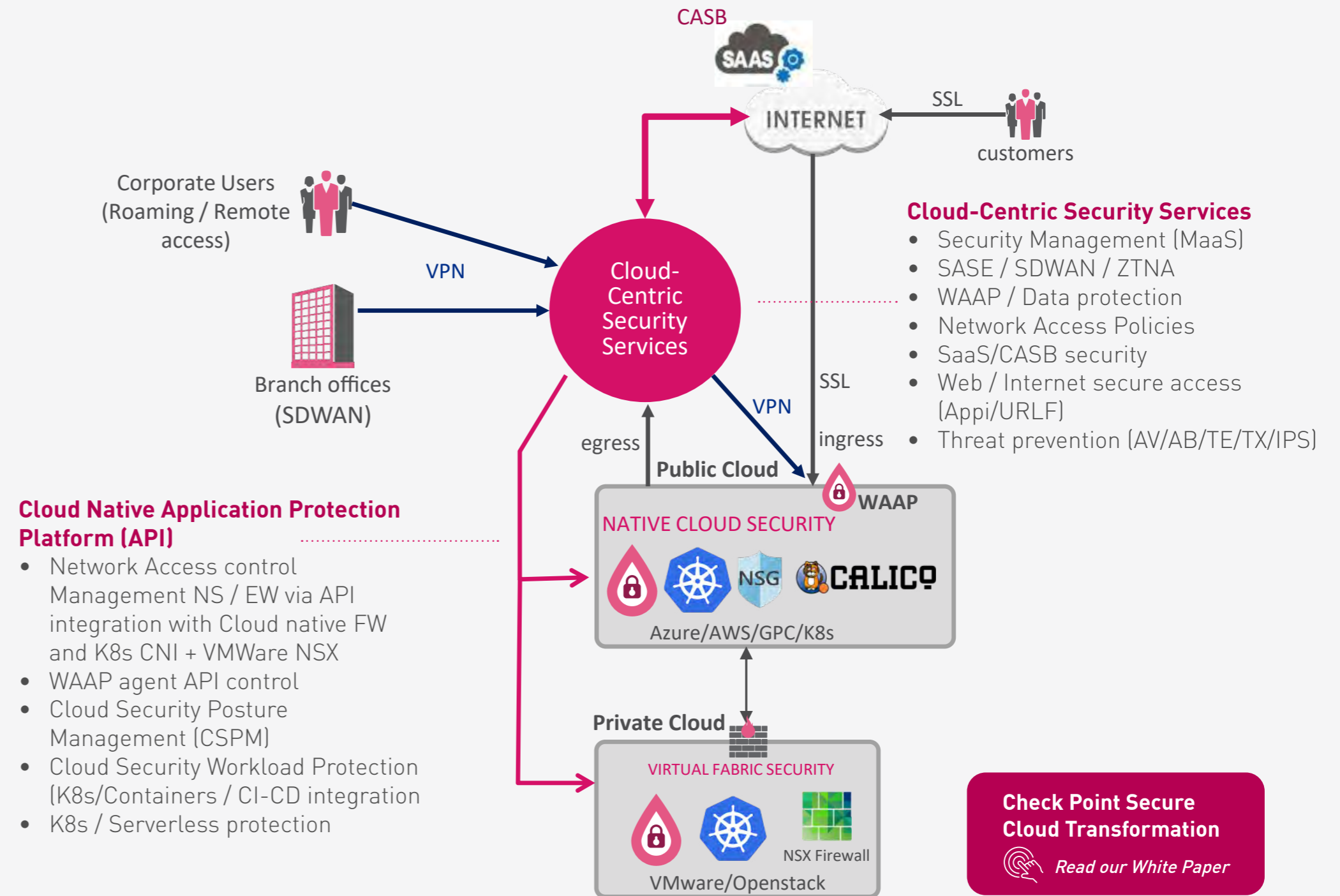
**CIS Container Security**

**NIST SP 800-190**  
Application Container Security Guide

**AWS/Azure/GCP**  
architecture guides

Cloud Native Security Architecture

# Security as a Service Vision



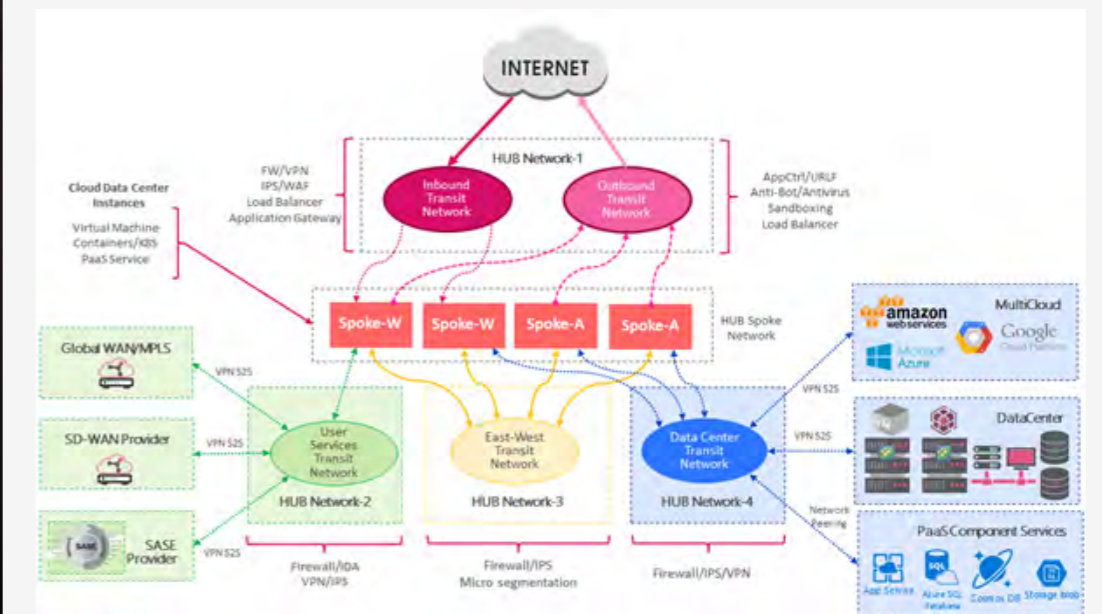
# Cloud Architecture References



**Security Reference Architectures for Public Clouds Using CloudGuard Network Security**

Guide for a Successful Lift and Shift Secure Migration Model for Microsoft Azure, Amazon Web Services, and Platform

This white paper aims to provide the reader with reference architectures using different technical examples taken from Microsoft Azure, Amazon Web Services, the Google Cloud Platform, and Check Point Software Technologies, as well as from a variety of technical blogs.

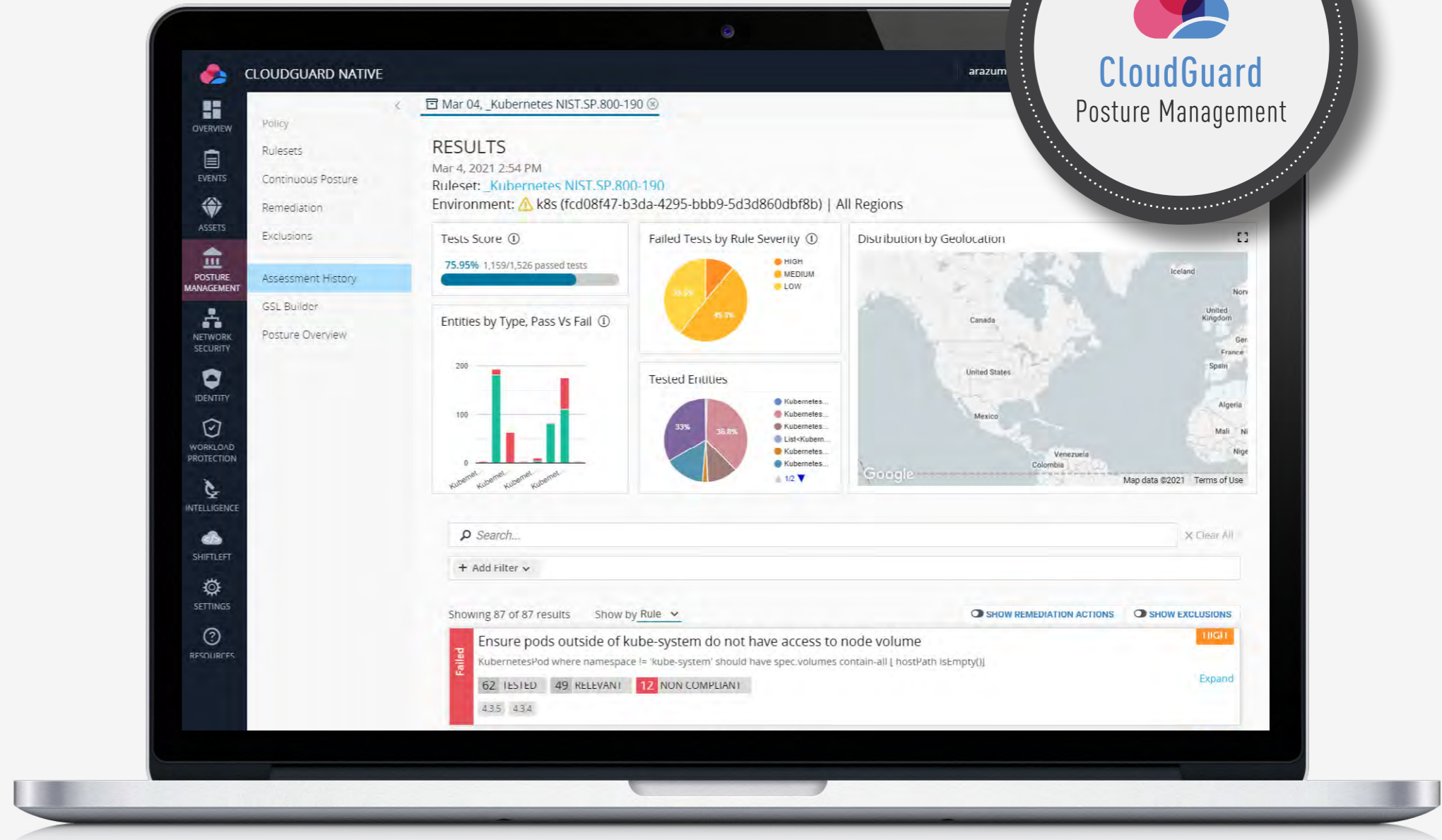


**Security Architecture References for Public cloud IaaS**

*Read our White Paper*

# Posture Management

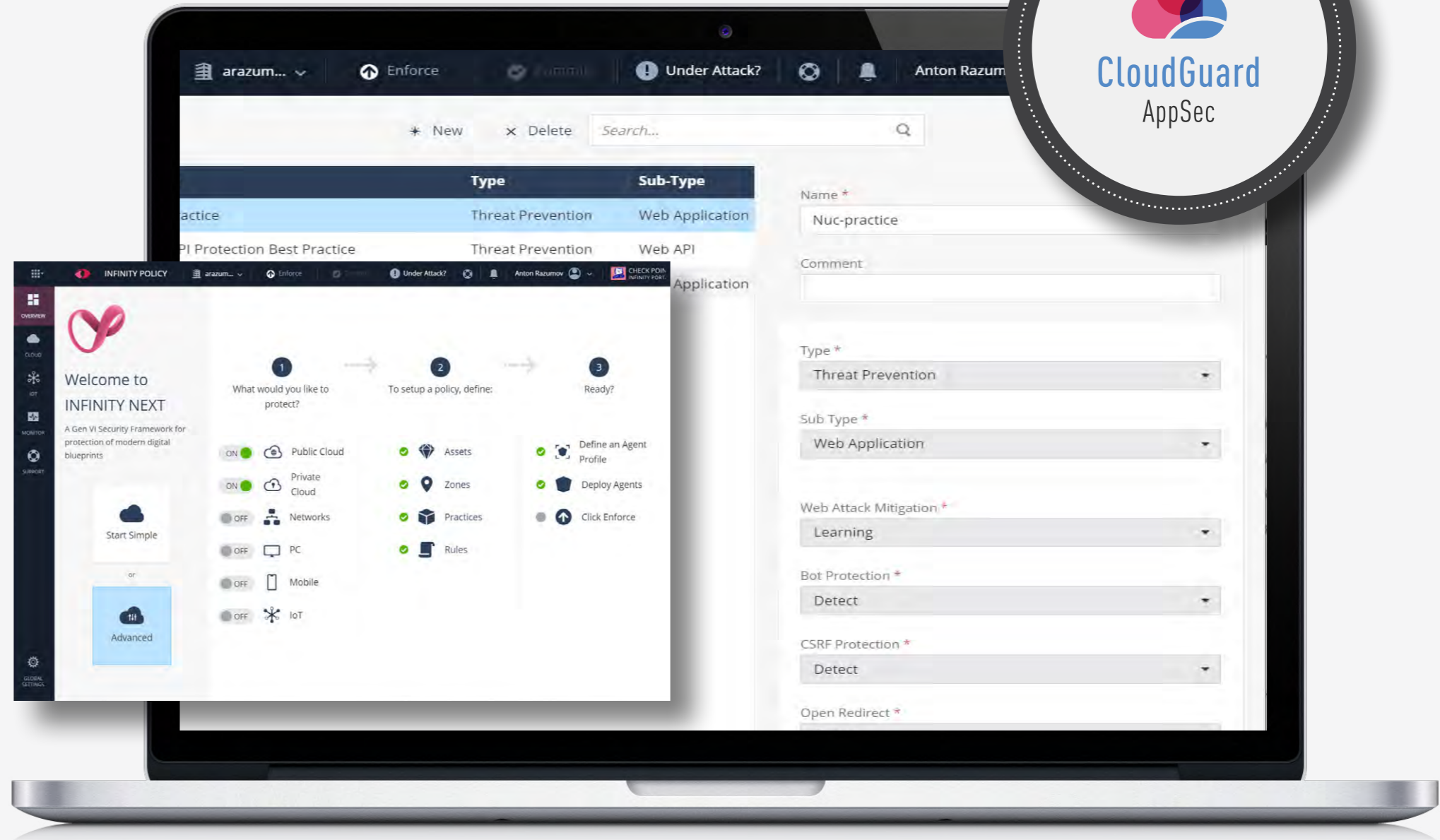
Read more





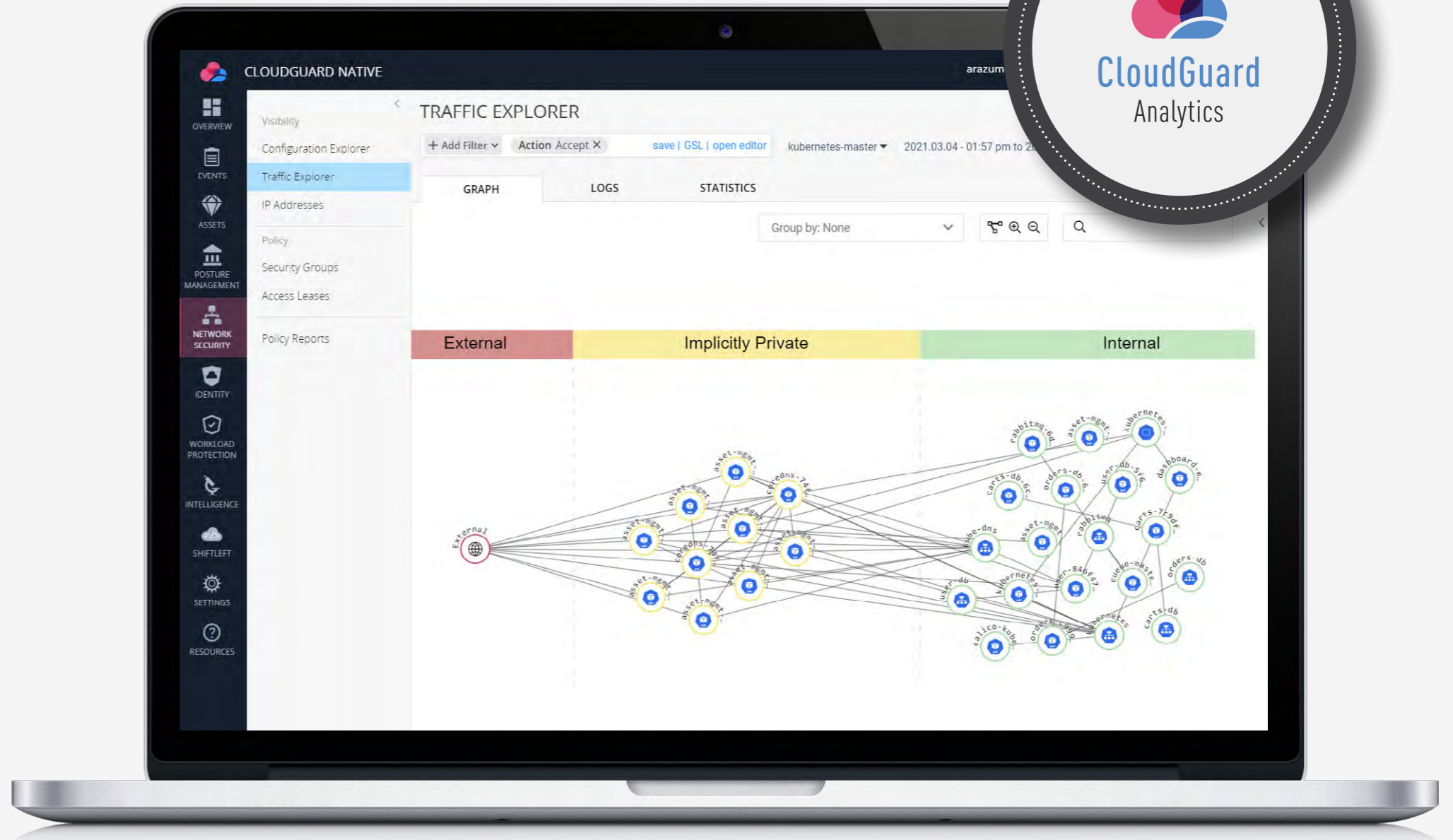
# AppSec

[Read more](#)



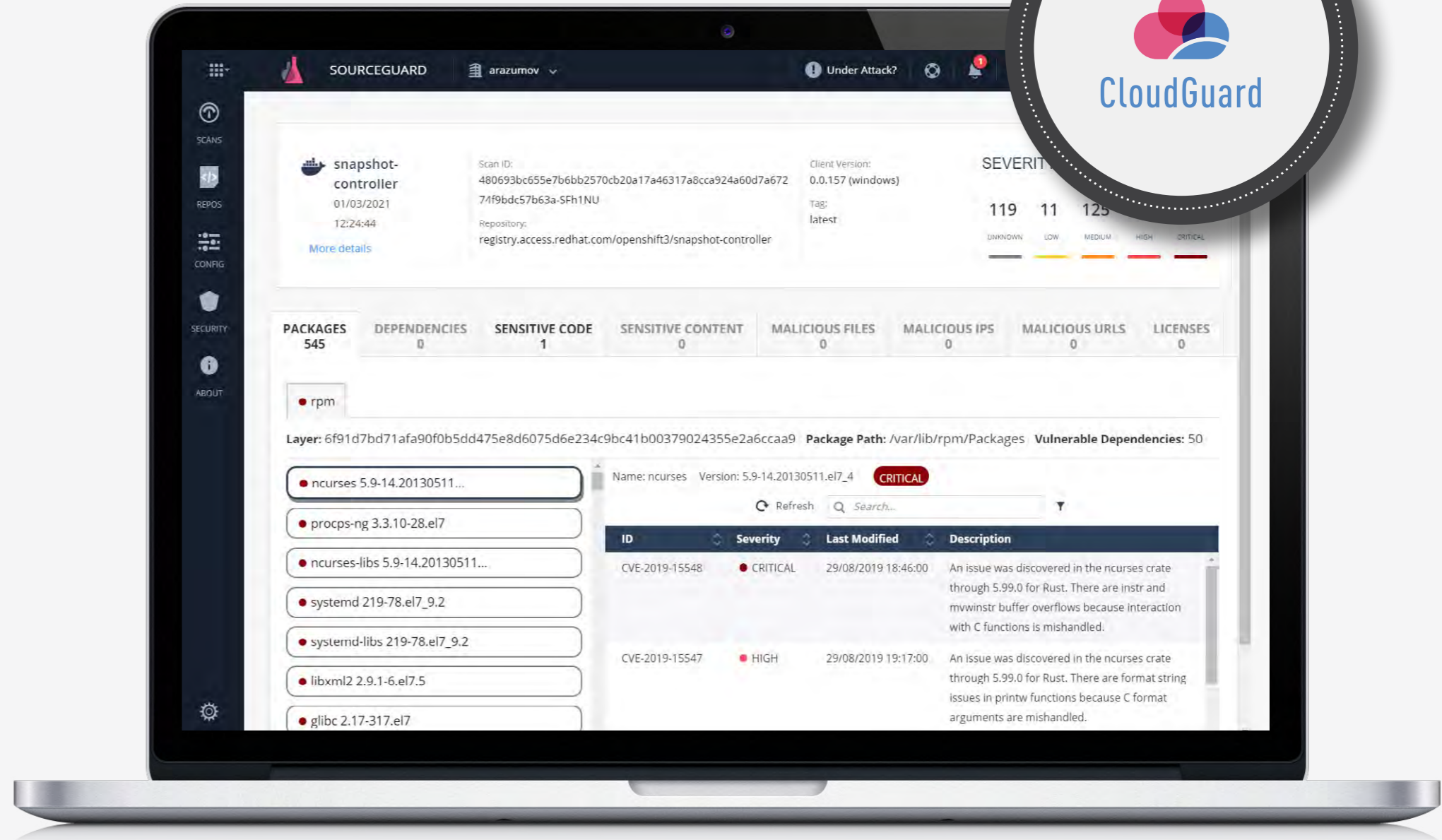
# Traffic Explorer

[Read more](#)



# Image Scan

Read more



## Resources

### Check Point Security Consulting Services

For nearly thirty years, Check Point has set the standard for Cyber Security. Across the ever-evolving digital world, from enterprise networks through cloud transformations, from securing remote employees to defending critical infrastructures, we protect organizations from the most imminent cyber threats. Check Point Security Consulting leverages this experience along with independent frameworks, such as NIST CSF, SABSA and Zero Trust Architecture, to provide advisory and assessment services to the company's global customer community.

[READ MORE](#)

### Security Best Practices and Architecture References

Security best practices start with the strong architecture. This resource contains ultimate Security Best Practices and Architecture Reference white papers that provide a deep dive into designing efficient and secured private and public cloud infrastructures.

[READ MORE](#)