Cloud Native Security Model

Best Practice approach for designing ultimate cloud security environment
Cloud Security Architecture Building Blocks

4C Model

CNAPP Model – Gartner (CSPM/CWPP/CNS)

Cloud Native Security Architecture
The 4C model – Cloud Security Concepts

**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](https://kubernetes.io/docs/concepts/security/overview/) computing approach to security, which is widely regarded as a best practice for securing software systems.

[Diagram showing the 4C layers: Cloud Provider, K8s Cluster, Container, Code]

[https://kubernetes.io/docs/concepts/security/overview/](https://kubernetes.io/docs/concepts/security/overview/)
CNAAP – Cloud Native Application Protection Platform

1. Cloud Security Posture Management
   Powerful visualization of network topology and flows for rapid security assessment; Cloud-native and agentless technology that protects all cloud assets along with in-place remediation.

2. Cloud-Native Network (IaaS) Security
   ADC, LB, WAF/WAAP, DoS, FW, IPS

3. Cloud Workload Protection Platform
   Security technologies and solutions to protect server workloads by CI/CD security, scanning code/images, behavior analysis, Run-time protection, Threat Hunting and more.
Cloud security transformation

- **CSPM**: Cloud Native Security Posture monitoring, control and remediation
- **CSNS**: Cloud Native Access Control, segmentation, NS/EW security, K8s containers network policies
- **CWPP**: Cloud Native Protection of VMs/Containers and Vulnerability/Threats mitigation, Shift-Left / CI-CD security for DevOps

Legacy Data Center

- Lift and Shift
- Firewalls internal and external, IPS/IDS, perimeter Internet access protection, proxy.
Cloud Native Security Model - 4C and CNAPP adjacency

<table>
<thead>
<tr>
<th>Layer</th>
<th>1c Cloud</th>
<th>2c Cluster</th>
<th>3c Container</th>
<th>4c Code</th>
</tr>
</thead>
</table>

Cloud Security Posture Management (CSPM)

Cloud Workload Protection Platform (CWPP)

Cloud Service Network Security (CSNS)

Cloud Security Operations

<table>
<thead>
<tr>
<th>Cloud Security</th>
<th>DevSecOps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Security / Network / Data Center</td>
<td>Applications Team (DevOps)</td>
</tr>
<tr>
<td>Security Operations (SOC)</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Governance</td>
<td></td>
</tr>
</tbody>
</table>
## CNAPP Security Functions

<table>
<thead>
<tr>
<th>Layer</th>
<th>Security Function</th>
<th>1c Cloud</th>
<th>2c Cluster</th>
<th>3c Container</th>
<th>4c Code</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Security Platform / Components</th>
<th>Security Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CSPM</strong></td>
<td>Automated Posture Management</td>
</tr>
<tr>
<td></td>
<td>Visibility / Flows</td>
</tr>
<tr>
<td></td>
<td>Tamper Protection</td>
</tr>
<tr>
<td></td>
<td>Auto Remediation</td>
</tr>
<tr>
<td></td>
<td>Compliance and Governance</td>
</tr>
<tr>
<td></td>
<td>Dynamic access leases</td>
</tr>
<tr>
<td></td>
<td>IAC Scanner</td>
</tr>
<tr>
<td></td>
<td>Entity Behavior Analytics</td>
</tr>
<tr>
<td></td>
<td>IAM Insights</td>
</tr>
<tr>
<td></td>
<td>Clarity for Assets</td>
</tr>
<tr>
<td><strong>CWPP</strong></td>
<td>Image scan</td>
</tr>
<tr>
<td></td>
<td>Code scan</td>
</tr>
<tr>
<td></td>
<td>K8s API protection</td>
</tr>
<tr>
<td></td>
<td>Admission Controller</td>
</tr>
<tr>
<td></td>
<td>Behavioral analysis and Machine Learning</td>
</tr>
<tr>
<td></td>
<td>VM Protection</td>
</tr>
<tr>
<td></td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td></td>
<td>Container Runtime Protection</td>
</tr>
<tr>
<td></td>
<td>Serverless Run-time Protection</td>
</tr>
<tr>
<td><strong>CSNS</strong></td>
<td>NG + Native Firewall</td>
</tr>
<tr>
<td></td>
<td>WAAP</td>
</tr>
<tr>
<td></td>
<td>CNI Security</td>
</tr>
<tr>
<td></td>
<td>VMware DFW</td>
</tr>
<tr>
<td></td>
<td>CloudBots</td>
</tr>
<tr>
<td></td>
<td>Automated Micro/Macro Segmentation</td>
</tr>
<tr>
<td><strong>Dev/Cloud Operations</strong></td>
<td>IAC Scanner, Ansible/Terraform</td>
</tr>
<tr>
<td></td>
<td>CLI tools, Plugins, 3-rd party lib scan</td>
</tr>
</tbody>
</table>
Cloud Native Security Design Model

1c Cloud
- Inventory, Assets and Posture management for Clouds, Clusters, Containers, Code; Configuration risks (Vulnerable dependencies, Excessive Permissions); Cloud Identity and Access Management reporting and dashboards; Compliance and Governance

2c Cluster
- Native FW management (NACL, NSG, Security Groups)

3c Container
- Web, antivot, API Protection
- K8s Runtime assurance
- K8s Intrusion detection

4c Code
- Serverless runtime protection

Unified management: Assets, Zones, Rules, Best practices
CI/CD pipeline security

**Risks and attack vectors**
- Vulnerable code / libraries
- Incompliant infrastructure-as-a-code
- Vulnerable code / images / other dependencies / permissions
- Insecure posture, compliance/governance violations, permissions misuses, network attacks, improper behavior, various threats

**CI/CD pipeline stages**
- **Code**
  - CSPM: IAC Scan
  - CWPP: Code, 3rd party library scan
  - DevOps: IDE plugins
- **Commit**
  - CSPM: IAC Scan
  - CWPP: Code & 3PP scan
- **Build**
  - CSNS: Image Assurance
  - DevOps: CLI Tool
- **Deploy**
  - Posture Management & Visibility
  - Clarity for Assets
  - IAM Insights
  - Entity Behavior Analytics
  - K8s Runtime Assurance
  - Serverless
  - Container Image Assurance
  - K8s Intrusion Detection
  - VM Protection
  - Container Runtime Protection
  - CGI Orchestrator, Integration
  - Automated Micro/Macro Segmentation
  - Web & API Protection
  - Terraform
  - Cloud Bots
  - CloudGuard API

**Tools and technologies**
- DevOps: IDE plugins, CLI Tool
- CWPP: Code, 3rd party library scan, Code & 3PP scan
- CSPM: IAC Scan
- CSNS: Image Assurance
- Posture Management & Visibility
- Clarity for Assets
- IAM Insights
- Entity Behavior Analytics
- K8s Runtime Assurance
- Serverless
- Container Image Assurance
- K8s Intrusion Detection
- VM Protection
- Container Runtime Protection
- CGI Orchestrator, Integration
- Automated Micro/Macro Segmentation
- Web & API Protection
- Terraform
- Cloud Bots
- CloudGuard API
Operations Model

Security layer (People, Process and Technology)

User Layer

Test Layer

Publishing layer

Data & Identity Layer

Code

CI/CD

Containers / SaaS / PaaS / FaaS

Test Dev Layer

Prod Dev Layer

Transport / Network layer

Cloud Infrastructure

API

Security/layer

Security layer (People, Process and Technology)

App Owner

DevOps

Network Engineering

Operations / Support

Functiona Teams

Threat Intelligence

External Audit

External

Security Office

Security Assurance

Governance

Operations / Support

Security layer

Code

CI/CD

SaaS / PaaS

FaaS

K8s / IaaS

Functional Teams
Cloud security architecture Design Process

1. Design Principles
   - Standards
   - Design Patterns
   - 4C Model - Google
   - CNAPP Model - Gartner

2. Technical Security
   - References
   - K8s best-practices
   - Check Point Best Practice
   - CIS Container Security
   - NIST SP 800-190
     Application Container Security Guide
   - AWS/Azure/GCP
     architecture guides

Cloud Native Security Architecture

©2020 Check Point Software Technologies Ltd.
Cloud Transformation Phase IV

Cloud-Centric Security Services
- Security Management (MaaS)
- SASE / SDWAN / ZTNA
- WAAP / Data protection
- Network Access Policies
- SaaS/CASB security
- Web / Internet secure access (Appi/URLF)
- Threat prevention (AV/AB/TE/TX/IPS)

Cloud Native Application Protection Platform (API)
- Network Access control Management NS / EW via API integration with Cloud native FW and K8s CNI + VMware NSX
- WAAP agent API control
- Cloud Security Posture Management (CSPM)
- Cloud Security Workload Protection (K8s/Containers / CI-CD integration
- K8s / Serverless protection

Check Point Secure Cloud Transformation
ONE CLOUDGUARD MULTI CLOUD SECURITY

Private & Public Cloud Network Security (CSNS)

Cloud Intelligence & Threat Hunting

High Fidelity Context

Shift Left

Advanced Prevention

Cloud Security Posture Management (CSPM)

CNAAP

Workload Protection (CWPP)

WAAP
Security Best Practice Starts With a Strong Architecture

Leverage our architects’ security best practices to strengthen your security infrastructure and future proof your business against fifth generation cyber-attacks.

https://www.checkpoint.com/architecture/best-practices/

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.

https://www.checkpoint.com/support-services/security-workshop/