CNAPP: de nieuwe hype voor security in de cloud



Koen Tamsyn



Business Unit Lead Cybersecurity | CISSP



Koen.tamsyn@inetum-realdolmen.world

02 801 53 97

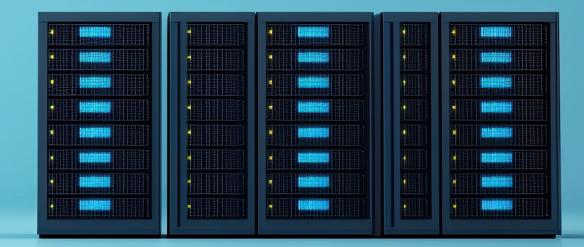


Cloud Native Application Protection Platform

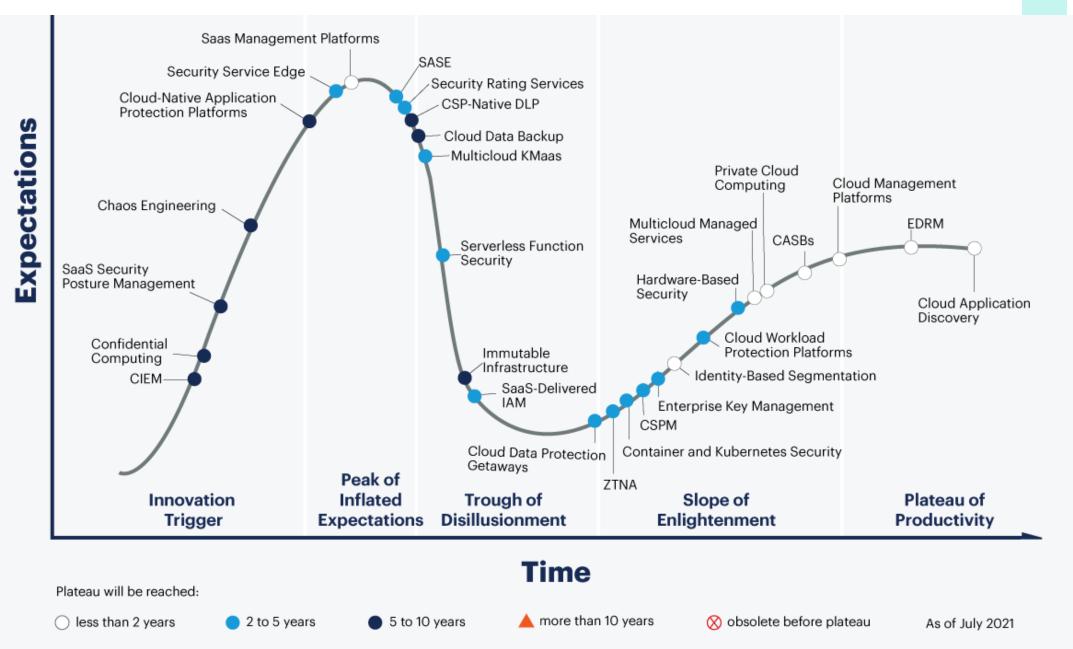


Firewall

EDR



Hype Cycle for Cloud Security, 2021



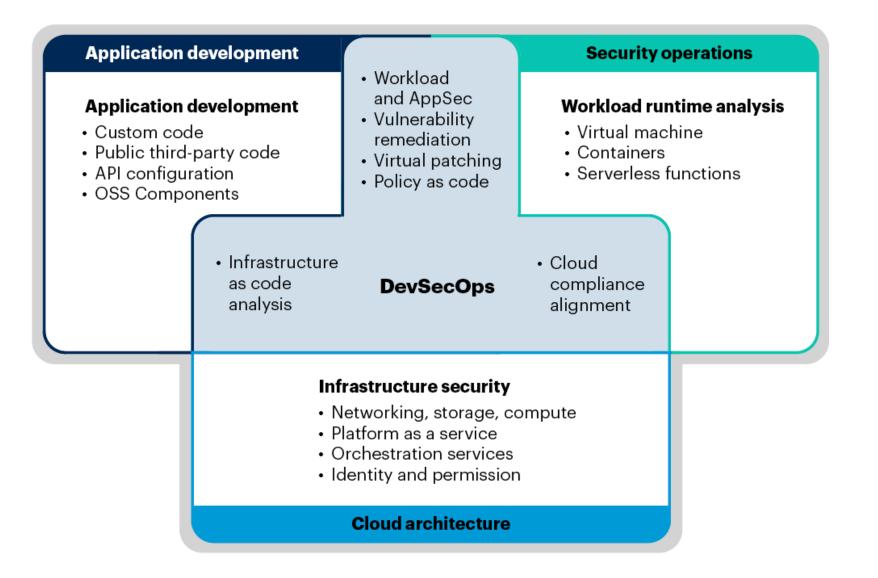
inet

5

Users and Systems Third-Party SaaS API **API Endpoint** Endpoint Service Service **Runtime Cloud-Native Application Risk Boundary** Web Application APIs and API Protection **Cloud Identity Cloud Secrets** Services Management App Load Cloud API Balancer Firewall Gateway Block Storage Svcs Unstructured Data API UI **Object Storage Svcs** Managed Container Unstructured Data Container APIs Virtual Managed Machine Container Serverless Container PaaS PaaS Database Svcs Host OS Structured Data Managed Host OS **Kubernetes Kubernetes** VM Image Libraries **Container Registry** Serverless Registry Hundreds of Cloud Provider PaaS Services Infrastructure as Code Scripts

Explosion in the Risk Surface Area of a Cloud-Native Application

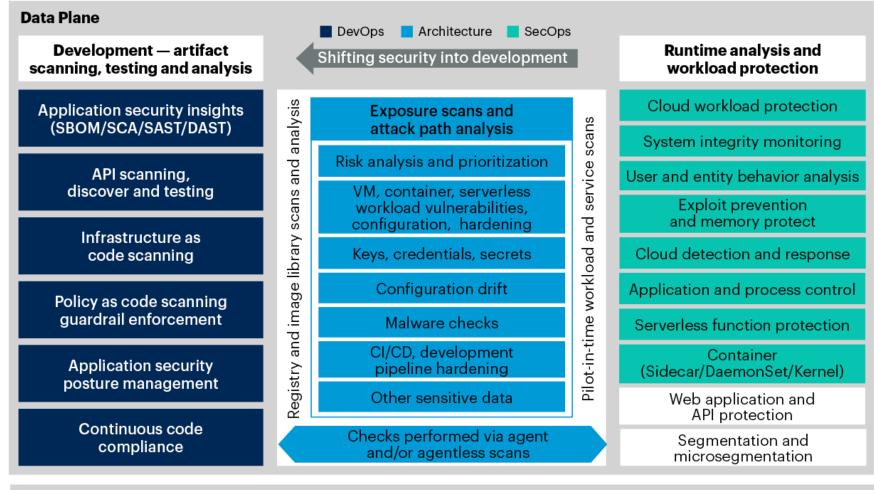
Developers' and Architects' Expanded Scope of Responsibility for Cloud-Native Applications



Code-to-Cloud Risk Visibility, Prioritization and Remediation

Developer	Code			Build		Deploy	Run in Cloud
	Developer Identities						
	Secrets Management						
Tools	IDE	Code/Git Repository	Build Servers	Configuration	Staging	Continuous Deployment	
Artifacts	 Custom Code Custom APIs Third-Party APIs Declarative APIs (e.g., OpenAPI) Third-Party SDKs Application Platforms OSS Libraries OSS Frameworks 		 Compiled Code Container Layers Containers Virtual Machines Serverless Functions 		 IaC Scripts Kubernetes YAML Files Kubernetes Helm Charts 		Runtime Cloud-Native Application Risk

CNAPP Detail View



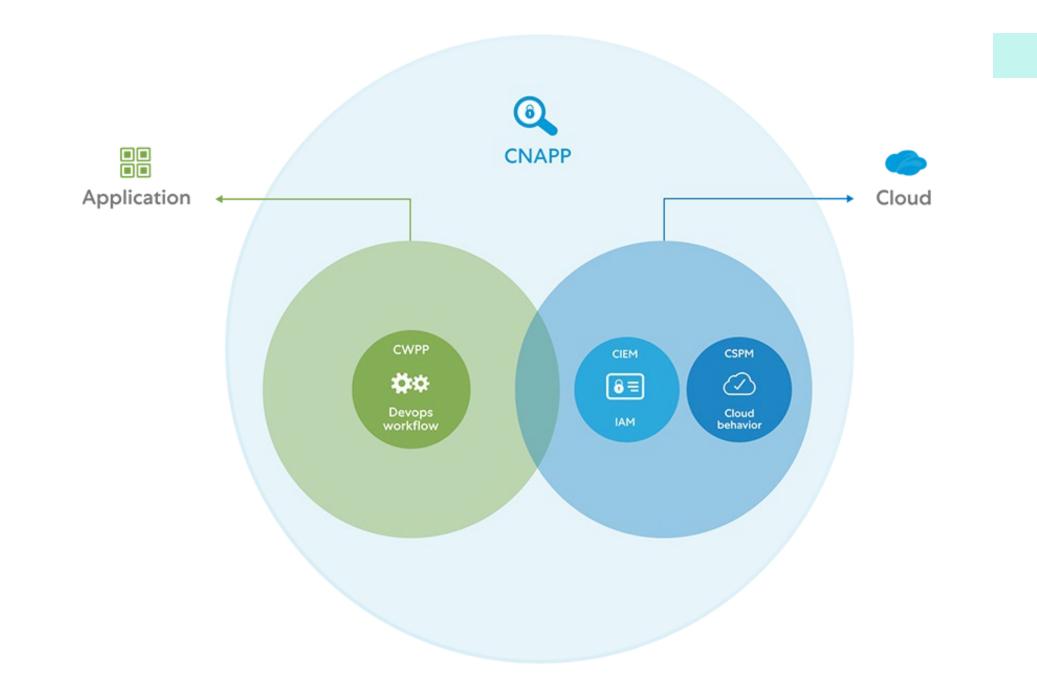
Control Plane

Cloud security posture management

Cloud infrastructure entitlement management

Kubernetes security posture management

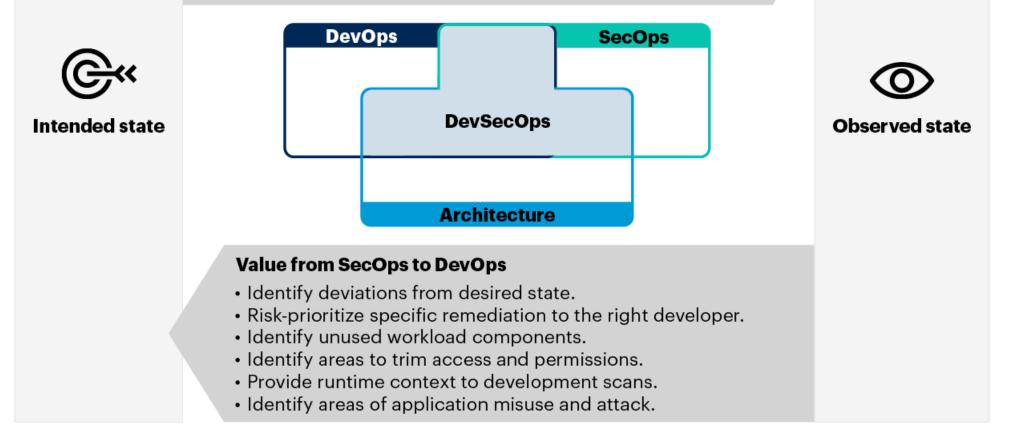
API = Application programming interface; CNAPP = Cloud-native application protection platform; DAST = Dynamic application security testing; SAST = Static application security testing; SBOM = Software bill of materials; SCA = Software composition analysis; VM = Virtual machine



Bidirectional Collaboration

Value from DevOps to SecOps

- Artifact is secure and compliant.
- Identify expected artifact connectivity and behaviors.
- Identify residual vulnerabilities needing runtime protection.
- Recommend least-privilege policies.
- Ensure approved artifact hasn't changed.
- Link developers to artifacts and running code.



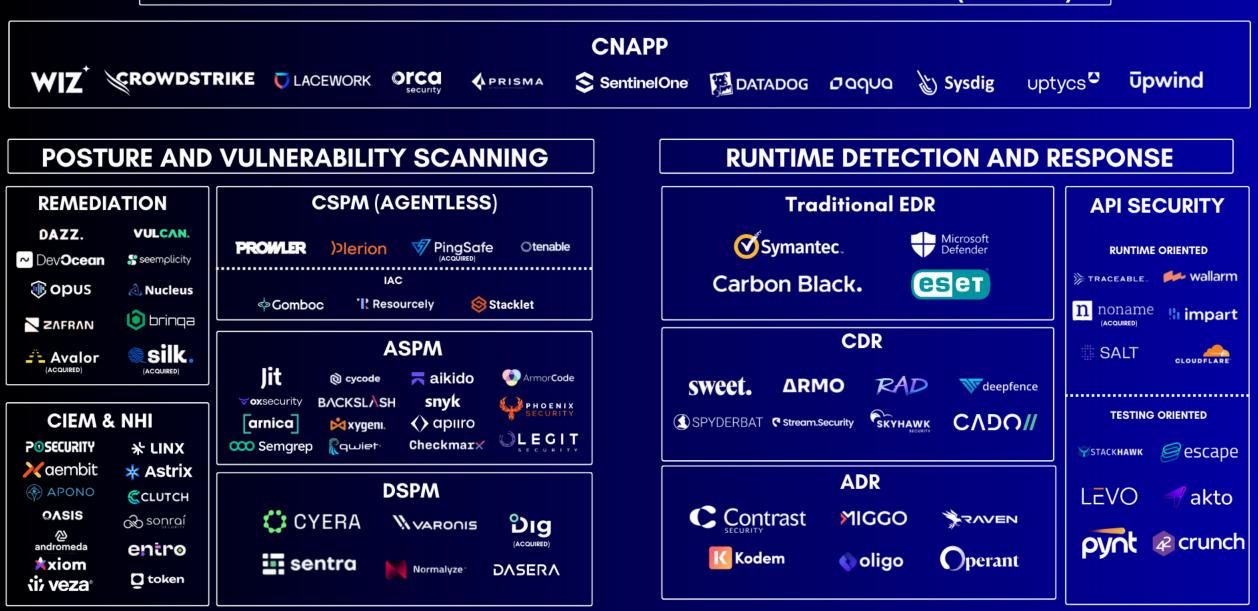
Benefits of CNAPP adoption

X Better identification, priorization and remediation X Reduces operational complexity through consolidation Consistent enforcement of security policy X Single data lack shortens remediation times X X Reduces developer friction and improves experience X Shortens application deployment time X Minimizes runtime vulnerabilities X Eliminates redundant capabilities Bridges the communication gap of siloed teams X

Challenges to CNAPP adoption

X	Security organizational buying personas				
X	Adversarial relationship between developers and security				
X	Existing investments				
X	Mindset changes				
X	Architecture				
X	Maturity				
X	Legacy applications				
X	Immature single vendor offerings				
X	Stand-alone tools Integration				





SOURCE: SOFTWARE ANALYST RESEARCH & LATIO TECH

