CLOUD SECURITY

WHITEPAPER

Trends, ontwikkelingen, uitdagingen en de rol van CNAPP in public cloud security

YOU CAN'T SECURE WHAT YOU CAN'T SEE

VISIBILITY IS THE FOUNDATION OF CLOUD SECURITY

INHOUDSOPGAVE

Inleiding **4**

1 Trends en ontwikkelingen **5**

1.1 Toename complexiteit in multicloud-omgevingen 5

1.2 Adoptie van ‘Shift-Left’ security 5

1.3 Focus op runtime security 6

1.4 Toename gebruik van AI en Machine Learning 6

1.5 Compliance als prioriteit 6

2 De uitdagingen van cloud security **7**

2.1 Gebrek aan volledige zichtbaarheid 7

2.2 Silovorming tussen teams 7

2.3 Trage reactietijden door handmatige processen 8

2.4 Kwetsbaarheid voor misconfiguraties 8

2.5 Beperkingen in compliance en risicobeheer 8

3 Wat is CNAPP en hoe adresseert het de uitdagingen? **9**

3.1 Posture en vulnerability scanning 9

3.2 Runtime detection en respons 9

3.3 Hoe ziet het CNAPP-landschap eruit? 10

3.4 Hoe CNAPP de uitdagingen van cloud security aanpakt 10

4 De rol van CNAPP in hedendaagse cloudomgevingen **12**

4.1 Ontwikkelingen 12

4.2 Wat betekent dit voor jouw organisatie en hoe nu verder? 13

INLEIDING

Steeds meer organisaties kiezen ervoor om over te stappen op een (hybride) cloud infrastructuur vanwege de voordelen die deze biedt, zoals flexibiliteit, schaalbaarheid en toegankelijkheid. In 2023 hadden 54% van de EMEA-regio gevestigde bedrijven, cloud technologie geïmplementeerd in alle of de meeste onderdelen van hun bedrijfsvoering en de verwachting is dat 73% van de bedrijven binnen twee jaar al hun operaties in de cloud hebben.[1] Cloudtechnologie biedt organisaties de mogelijkheid om applicaties en data op te slaan en te beheren zonder dat ze afhankelijk zijn van dure fysieke infrastructuur. Deze flexibiliteit stelt organisaties in staat om sneller te schalen en processen te optimaliseren, wat bijdraagt aan een hogere efficiëntie en innovatie. Bovendien speelt de cloud een sleutelrol in digitale transformatie, doordat organisaties toegang krijgen tot geavanceerde technologieën zoals kunstmatige intelligentie en machine learning, wat met traditionele IT-omgevingen vaak lastig te realiseren is.[2]

Cloud security is een essentieel onderdeel geworden van de security stack in een tijd waarin steeds meer organisaties de publieke cloud omarmen. De overgang naar de cloud brengt tegelijkertijd de nodige risico's en uitdagingen met zich mee. Deze uitdagingen kunnen grote gevolgen hebben voor de integriteit, vertrouwelijkheid en beschikbaarheid van bedrijfsdata en systemen. De snelle adoptie van cloudomgevingen vergroot de aanvalsoppervlakte aanzienlijk. Wanneer bedrijven data en applicaties naar de cloud migreren worden deze vaak toegankelijk via het internet, wat hen blootstelt aan een breed scala van cyberdreigingen.

Cloudtechnologie heeft organisaties enorme flexibiliteit en schaalbaarheid geboden, maar het beveiligen van deze dynamische omgevingen brengt unieke uitdagingen met zich mee. Traditionele beveiligingsmethoden zijn vaak niet ontworpen voor de complexiteit en snelheid van multicloud-omgevingen.

Cloud security is complex, maar er is een cloud-agnostische oplossing: Cloud-Native Application Protection Platforms (CNAPP). Deze oplossing biedt een geïntegreerde aanpak om de complexiteit van moderne cloudbeveiliging te verminderen en te vereenvoudigen. In deze whitepaper bespreken we in **hoofdstuk 1** de trends en ontwikkelingen in cloud security, in **hoofdstuk 2** de uitdagingen van cloud security, in **hoofdstuk 3** CNAPP als oplossing en tenslotte in **hoofdstuk 4** waarom CNAPP essentieel is voor organisaties die hun cloudomgevingen willen beschermen tegen hedendaagse bedreigingen.

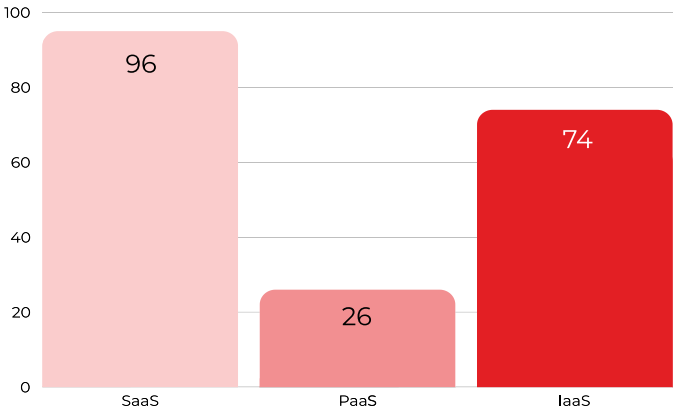
Of u nu een IT-professional bent die grip zoekt op multicloud-complexiteit, of een DevOps-team dat beveiliging wil verbeteren zonder snelheid te verliezen, deze whitepaper biedt essentiële inzichten in de toekomst van cloudbeveiliging en de rol van CNAPP daarin.

[1] PwC, "PwC EMEA Cloud Business Survey 2023: How Businesses Will Unlock the Transformational Power of Cloud."

[2] Giemzo et al., "How CIOs and CTOs Can Accelerate Digital Transformations Through Cloud Platforms."

1 TRENDS EN ONTWIKKELINGEN

Voordat we het kunnen hebben over het beveiligen van cloud omgevingen is het eerst belangrijk om in kaart te brengen hoe cloud omgevingen er bij de Europese organisaties uitzien. Allereerst kan er onderscheidt gemaakt worden tussen drie verschillende types van cloudservices, namelijk: Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) en Platform-as-a-service (PaaS). Elk type cloudservice biedt verschillende niveaus van controle, flexibiliteit en beheer.



Grafiek I - % van Europese organisaties dat gebruik maakt van welk type cloudservices

Bij SaaS-services wordt een compleet product afgenomen dat uitgevoerd en beheerd wordt door de serviceprovider. Bij PaaS-services worden de onderliggende infrastructuur (meestal hardware en besturingssystemen) beheerd door de serviceprovider. PaaS-services worden voornamelijk gebruikt binnen DevOps omgevingen om zo efficiënt applicaties te kunnen ontwikkelen. IaaS-services bevatten de basisbouwstenen voor cloud-IT. IaaS geeft de hoogste mate van flexibiliteit en beheerscontrole over de IT-resources.[3,4,5]

Uit cijfers van Eurostat[6] blijkt dat SaaS-services door bijna alle Europese organisaties gebruikt worden zoals te zien is in bovenstaande grafiek. Waar IaaS-services nog door bijna driekwart van de Europese organisaties gebruikt wordt, blijft het gebruik van PaaS-services nog uit.

1.1 TOENAME COMPLEXITEIT IN MULTI CLOUD-OMGEVINGEN

Uit onderzoek van Microsoft[7] blijkt dat 86% van de organisaties al gebruik maakt van een multi-cloud strategie om flexibiliteit en innovatie te stimuleren. Dit houdt in dat de eerdergenoemde cloudservices bij tenminste twee of meerdere cloudproviders worden afgenomen.

Cloud omgevingen bevatten vaak complexe configuraties bestaande uit verschillende SaaS-, IaaS- en PaaS-services. Wanneer organisaties migreren naar de cloud, zijn verkeerde configuraties van cloudservices een veelvoorkomende valkuil. Simpele fouten in configuraties kunnen leiden tot inbreuken, gegevensverlies en compliance-overtredingen. Daarnaast zorgen deze complexe omgevingen ook voor een groter en meer verspreid aanvalsoppervlak, waarbij traditionele beveiligingstools moeite hebben om volledige zichtbaarheid te bieden over meerdere platformen en systemen.

1.2 ADOPTIE VAN 'SHIFT-LEFT' SECURITY

Nu organisaties massaal gebruik maken van de cloud, neemt ook het aantal organisaties toe dat applicaties direct in de cloud ontwikkelt. De ontwikkeling van cloud-native applicaties benadrukt ook het belang van het integreren van security practices vroeg in het ontwikkelproces. Dit zorgt voor een duidelijke trend om beveiliging eerder in de ontwikkelingscyclus te integreren, oftewel "shift-left security".

Door beveiligingscontroles toe te passen tijdens de ontwikkeling (bijvoorbeeld via Infrastructure-as-Code-scans), kunnen kwetsbaarheden vroegtijdig worden geïdentificeerd, wat kosten en risico's in latere stadia vermindert.[8] Waar veel organisaties nog tegenaan lopen op dit moment is dat DevOps en security afdelingen in silo's opereren. Deze traditionele scheiding leidt tot systematische problemen, waarbij elk team zich beperkt tot zijn eigen doelstellingen in plaats van naar gezamenlijke doelen toe te werken.[9] Echter, door beveiliging een integraal onderdeel van de ontwikkelingslevenscyclus te maken, kunnen organisaties risico's beter beheren, compliance garanderen en een concurrentievoordeel op de markt behouden.[10]

[3] "PaaS Vs IaaS Vs SaaS: What's the Difference? | Google Cloud."

[4] "SaaS Vs PaaS Vs IaaS – Types of Cloud Computing – AWS."

[5] "What Is IaaS? Infrastructure as a Service | Microsoft Azure."

[6] Eurostats, "Cloud Computing - Statistics on the Use by Enterprises."

[7] Microsoft, "2024 State of Multicloud Security Report."

[8] Sandler, "How to Modernize Your Cloud Security Posture."

[9] Nahmias, "Better Cloud Security Means Breaking Down Silos Between Dev and SecOps."

[10] Lucanus, "The Role of DevSecOps in Enhancing CNAPP Efficiency - Security Boulevard."

1.3 FOCUS OP RUNTIME SECURITY

Runtime security legt de focus op het beschermen van applicaties en systemen tegen dreigingen en kwetsbaarheden terwijl ze actief draaien in een productieomgeving. De focus op runtime security in cloud security groeit door de dynamische aard van moderne cloudomgevingen en de toename van geavanceerde cyberaanvallen. Traditionele beveiligingsmethoden, zoals statische code-analyse en configuratiecontroles, zijn vaak onvoldoende omdat bedreigingen zich pas tijdens runtime manifesteren.

Runtime security is daarom essentieel om kwetsbaarheden te detecteren en aanvallen te blokkeren terwijl applicaties actief draaien (in productie zijn). In moderne cloud-native omgevingen, zoals microservices en containerplatformen, veranderen workloads constant, wat de nodige risico's met zich meebrengt. Daarnaast worden zero-day aanvallen pas tijdens de runtime zichtbaar. Hoewel preventieve beveiliging belangrijk blijft, groeit het belang van realtime monitoring en runtime security. Moderne oplossingen moeten daarom bedreigingen actief detecteren en erop reageren terwijl applicaties worden uitgevoerd.[11]

1.4 TOENAME GEBRUIK VAN AI EN MACHINE LEARNING

Een andere trend op het gebied van cloud security is een toename in het gebruik van AI en Machine Learning (ML), dit is een direct gevolg van de toenemende complexiteit van cloud-omgevingen. Met het toenemende volume aan dreigingen en data wordt het moeilijker voor teams om alles handmatig te beheren. AI en ML worden steeds vaker ingezet om bedreigingen te identificeren, prioriteren en erop te reageren. Dit versnelt het opsporen van aanvallen en vermindert menselijke fouten.[12,13]

Daarnaast zal er steeds meer ingezet worden op AI-gedreven cloud management. Door voorspellende analyses en automatiseringen kan AI dynamisch resources toewijzen, op storingen anticiperen en workloads efficiënter beheren. Naarmate cloudomgevingen complexer worden, zijn traditionele handmatige beveiligingsmethoden niet langer toereikend, waardoor de rol van AI in het beheer van deze systemen ook meer onmisbaar wordt.[14]

1.5 COMPLIANCE ALS PRIORITEIT

Strengere regelgeving zoals GDPR, DORA & NIS-2 zorgt er mede voor dat bedrijven meer aandacht moeten besteden aan compliance-eisen bij het inregelen en onderhouden van cloud security. Een andere reden voor de toegenomen aandacht voor compliance is het kosten en concurrentievoordeel dat het kan opleveren. Volgens PWC[15] kunnen bedrijven door middel van compliance meer vertrouwen uitstralen, met nieuwe en loyale(re) klanten als bewezen resultaat.

Deze trends laten zien dat traditionele beveiligingsmethoden tekortschieten in met name multi-cloud en hybride omgevingen. Ze onderstrepen de noodzaak van geïntegreerde oplossingen om geautomatiseerd uniforme compliance checks te kunnen doen in multi-cloud omgevingen.

[11] Gartner, "Market Guide for Cloud-Native Application Protection Platforms."

[12] Gartner, "Market Guide for Cloud-Native Application Protection Platforms."

[13] Bradley, "Leveraging AI for Better Cloud Runtime Security."

[14] Sfondrini, "Eight Emerging Trends Shaping the Future of Cloud Computing."

[15] PricewaterhouseCoopers, "EMEA Cloud Business Survey 2023."

2 DE UITDAGINGEN VAN CLOUD SECURITY

Met de snelle opkomst van cloud computing is ook de vraag naar cloud security veranderd. Waar organisaties voorheen veelal eigen datacenters hadden en de focus voornamelijk lag op het goed dichtzetten de omgeving naar buiten toe, is dat door het open karakter van de cloud veranderd. Door de algehele acceptatie van cloud computing is de verwachting dat medewerkers ongeacht de locatie of tijd toegang kunnen hebben tot de omgeving van hun organisatie. Dit heeft als resultaat dat data en applicaties vaak toegankelijk worden via het internet, met blootstelling aan een breed scala van cyberdreigingen als gevolg.

Traditionele security tools zijn voornamelijk gericht op Endpoint Detection and Respons (EDR) en netwerk security via firewalls. Hoewel deze technologieën fundamenteel waren, bieden ze onvoldoende zichtbaarheid en controle over cloudomgevingen, vooral met de verschuiving naar containers en microservices. Hieronder bespreken we de belangrijkste beperkingen:

2.1 GEBREK AAN VOLLEDIGE ZICHTBAARHEID

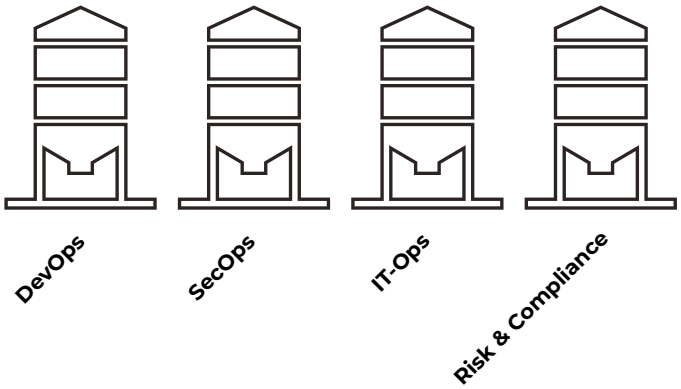
Traditionele tools bieden vaak beperkte zichtbaarheid over cloud-assets, vooral in multicloud-omgevingen. Dit gebrek aan overzicht maakt het moeilijk om bedreigingen of misconfiguraties tijdig te identificeren en aan te pakken. Zonder een holistisch beeld blijven kwetsbaarheden onopgemerkt. Cloudomgevingen maken vaak gebruik van microservices, zoals containers en serverless architecturen die niet direct zichtbaar zijn voor traditionele security tooling.[16]

Bovendien bieden ze beperkte ondersteuning voor cloud-native logbestanden en API's, waardoor correlatie en analyse van gebeurtenissen in cloudomgevingen moeilijk wordt. Verder vereisen cloudomgevingen ook een diepgaand inzicht in Identity and Access Management (IAM), misconfiguraties en compliance eisen, iets waar traditionele tools vaak tekortschieten. Tenslotte zijn traditionele tools slecht afgestemd op de schaalbaarheid en snelheid van moderne DevOps-praktijken, zoals CI/CD-pipelines en Infrastructure as Code (IaC).[10]

2.2 SILOVORMING TUSSEN TEAMS

In veel organisaties werken ontwikkelings- (DevOps), security (SecOps), en IT Operationsteams in aparte silo's. Dit leidt tot inefficiënties en een gebrek aan coordinatie bij het beveiligen van cloudomgevingen. Elk team heeft zijn eigen doelen, tools en werkmethodiek. Zo richten DevOps-teams zich voornamelijk op snelheid en innovatie, vaak via CI/CD-pipelines. Terwijl ITOps-teams streven naar stabiliteit en prestaties van de infrastructuur., en vaak pas laat in het proces worden betrokken. Een gebrek aan samenwerking kan leiden tot inefficiënties zoals miscommunicatie, tegengestelde prioriteiten en fragmentatie van verantwoordelijkheden.

In de praktijk blijkt echter dat er, met name binnen de grotere organisaties, meerdere silo's bestaan. Zo zijn er naast DevOps en SecOps nog meer afzonderlijke entiteiten met hun eigen verantwoordelijkheden en prioriteiten, zoals bijvoorbeeld IT-Ops en Risk & Compliance. IT-Ops richt zich op het beheer en onderhoud van IT-systemen, waaronder netwerkbeheer, opslag en algemene infrastructuurvoorzieningen, en werkt vaak los van zowel DevOps als SecOps. Risk & Compliance houdt zich bezig met regelgeving, audits en risicobeheersing, wat betekent dat zij vaak strikte kaders opleggen die niet altijd in lijn zijn met de agile werkwijzen van DevOps-teams. Deze extra laag complexiteit vergroot de uitdagingen rondom samenwerking en afstemming, waardoor securitymaatregelen gefragmenteerd en reactief blijven in plaats van proactief en geïntegreerd.



Traditionele security tools versterken deze fragmentatie doordat ze slechts specifieke lagen of onderdelen van de infrastructuur beschermen (bijvoorbeeld netwerk security of endpoint security). Daarnaast biedt het geen geïntegreerde zichtbaarheid voor teams, wat samenwerking en communicatie bemoeilijkt. Dit zorgt er vaak voor dat beveiligingsteams geen inzicht hebben in hoe ontwikkelaars cloud infrastructuren configureren, wat tot blootstelling leidt, zoals slecht geconfigureerde IAM-regels. Daarnaast vertraagt een mogelijk gebrek aan coördinatie het identificeren en oplossen van beveiligingsincidenten.

[10] Lucanus, "The Role of DevSecOps in Enhancing CNAPP Efficiency - Security Boulevard."

[16] Berthoty, "Redefining CNAPP: A Complete Guide to the Future of Cloud Security."

2.3 TRAGE REACTIETIJDEN DOOR HANDMATIGE PROCESSEN

Veel traditionele beveiligingsmethoden vertrouwen sterk op handmatige processen, zoals regelmatige audits of handmatige configuraties. Dit is niet schaalbaar in dynamische cloudomgevingen waar systemen voortdurend veranderen, waardoor reactietijden vertragen en risico's toenemen.

2.4 KWETSBAARHEID DOOR MISCONFIGURATIES

In de cloud leiden kleine configuratiefouten, zoals open S3-buckets of slecht ingestelde firewalls, snel tot grote beveiligingsrisico's. Traditionele tools missen vaak de mogelijkheid om deze fouten dynamisch te identificeren en te corrigeren, wat tot datalekken of blootstelling leidt.

2.5 BEPERKINGEN IN COMPLIANCE EN RISICOBEHEER

Met steeds strengere regelgeving en toenemende complexiteit van cloudomgevingen is het moeilijk om compliance te waarborgen. Traditionele tools bieden vaak geen geïntegreerde manier om compliance-eisen real-time te monitoren, waardoor organisaties risico's lopen op boetes of reputatieschade.

3 WAT IS CNAPP EN HOE ADRESSEERT HET DE UITDAGINGEN?

Een technologische ontwikkeling die inspeelt op eerdergenoemde trends en uitdagingen zijn Cloud Native Application Protection Platforms (CNAPP). Waar het Security Framework 'Secure Access Service Edge' (SASE)[16] beveiligt hoe gebruikers toegang krijgen tot cloudapps en -diensten, beveiligt CNAPP als Security Framework de cloud-native applicaties en de onderliggende infrastructuur zelf. CNAPP is een term die Gartner in 2021 voor het eerst heeft gebruikt als een allesomvattend cloud security platform dat meerdere security tools en functies consolideert in één geïntegreerde oplossing. Het concept is ontstaan uit een combinatie van Cloud Security Posture Management (CSPM) en Cloud Workload Protection Platforms (CWPP) en evolueert voortdurend om de groeiende uitdagingen binnen cloud security te adresseren.[17] CSPM richt zich oorspronkelijk op het identificeren van misconfiguraties en compliance risico's in cloud omgevingen, terwijl CWPP aanvankelijk werd gezien als EDR voor containers. Inmiddels heeft CWPP zich uitgebreid met vulnerability scans en netwerk security scans waardoor het een cruciale rol speelt in cloud security.

De kernfunctionaliteiten van CNAPP kunnen onderverdeeld worden in twee hoofdgebieden (1. posture en vulnerability scanning en 2. runtime detection en response), elk met subcategorieën:

3.1 POSTURE EN VULNERABILITY SCANNING:

- **Cloud Security Posture Management (CSPM):**
  Biedt inzicht in cloud-workload configuraties en kwetsbaarheden, met een focus op het detecteren van misconfiguraties, asset management en vulnerability scans.
- **Application Security Posture Management (ASPM):**
  Bevat tools voor het testen en beveiligen van applicaties, vaak met verschillende scanners en talen.
- **Cloud Infrastructure Entitlement Management (CIEM) & Non-Human Identities (NHI):**
  Richt zich op het traceren van machtigingen en activiteiten van zowel menselijke als niet-menselijke entiteiten in de cloud.
- **Data Security Posture Management (DSPM):**
  Biedt inzichten in dataplatforms, zoals object en relational storage.
- **Unified Remediation:**
  Werkt samen met security tools en developer workflows om duidelijke remediation stappen te bieden voor issues die door scans zijn geïdentificeerd.

3.2 RUNTIME DETECTION EN RESPONSE

- **Traditionele EDR:**
  Functioneert als EDR, maar dan in de cloud, met een focus op statische servers en bestand gebaseerde detecties.
- **eBPF Agent of Sensor:**
  Een lichte eBPF-gebaseerde sensor die runtime zichtbaarheid en bescherming biedt, native geïntegreerd met CNAPP. De Extended Berkeley Packet Filter (eBPF) is een Linux-kernel technologie waarmee software-ingenieurs programma's veilig kunnen uitvoeren en updaten in de kernel. Het biedt veilige toegang tot de werking van het besturingssysteem, waardoor ontwikkelaars netwerk-, observatie- en beveiligingsuitdagingen kunnen aanpakken, zonder impact op het operationele systeem (bijvoorbeeld op server of database workloads).
- **Cloud Detection and Response (CDR):**
  Speciaal ontwikkeld voor dreigingsdetectie en –respons binnen cloudomgevingen, waarbij container security een essentieel onderdeel is.
- **Application Detection and Response (ADR):**
  Richt zich op het monitoren van applicatieactiviteiten voor dreigingen, inclusief gebruikersinteracties en communicatie tussen services.
- **API Security:**
  Richt zich op het beschermen van API's binnen CNAPP tegen misconfiguraties, ongeautoriseerde toegang en exploits.

[10] "Definition of Secure Access Service Edge (SASE) - Gartner Information Technology Glossary."

[16] Berthoty, "Redefining CNAPP: A Complete Guide to the Future of Cloud Security."

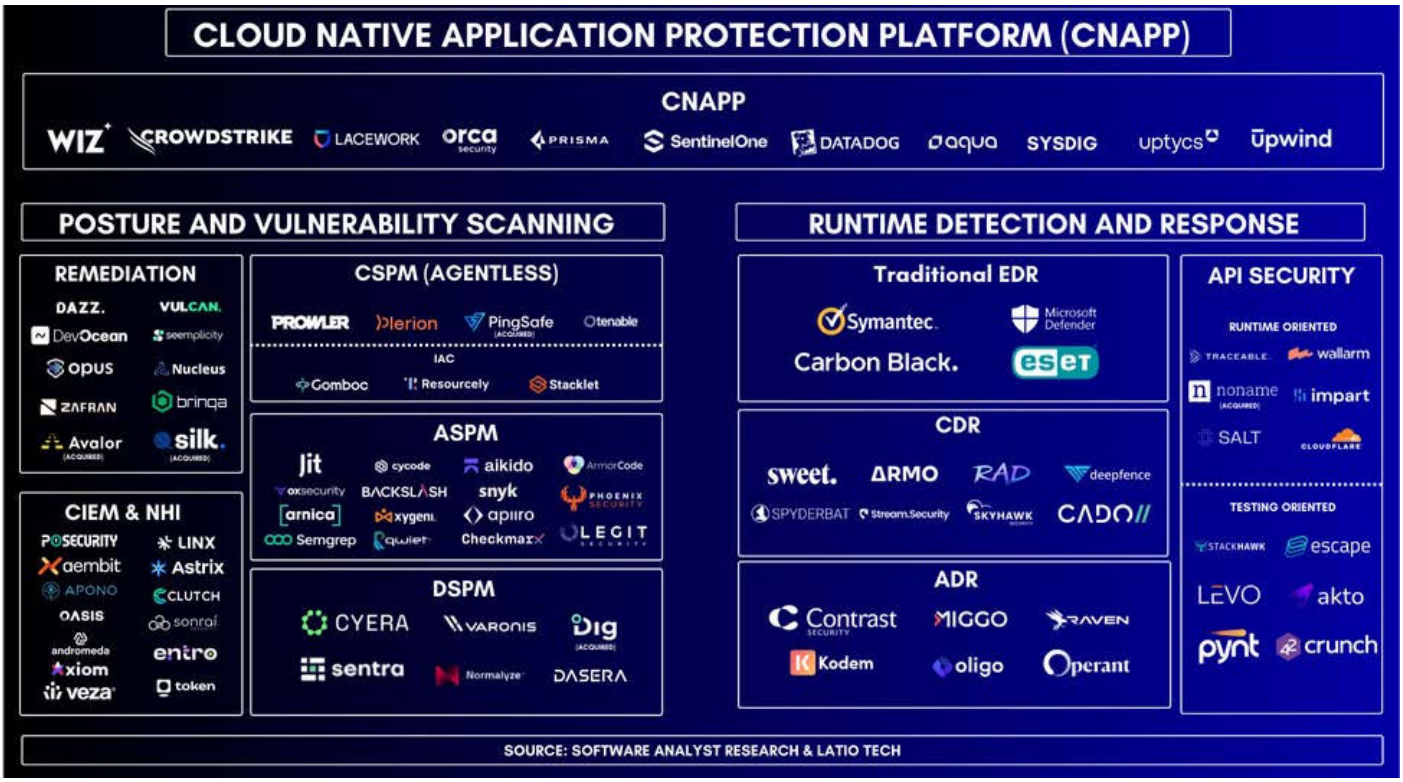
3 WAT IS CNAPP EN HOE ADRESSEERT HET DE UITDAGINGEN?

3.3 HOE ZIET HET CNAPP-LANDSCHAP ERUIT?

Zoals in onderstaande afbeelding te zien is zijn er verschillende aanbieders binnen CNAPP als security framework. Enerzijds zijn er de CNAPP-oplossingen die overkoepelend zijn, anderzijds zijn er puntoplossing aanbieders voor de eerder genoemde specifieke functionaliteiten. Deze oplossingen tezamen vormen het huidige cloud security landschap.

3.4 HOE CNAPP DE UITDAGINGEN VAN CLOUD SECURITY AANPAKT

CNAPP kan (in zijn beste vorm) de uitdagingen van cloud security aanpakken door een geïntegreerde en holistische oplossing te bieden op basis van een Unified Data Model (UDM), in tegenstelling tot gefragmenteerde puntoplossingen. Gefragmenteerde puntoplossingen richten zich op specifieke beveiligingsproblemen, maar werken vaak los van elkaar, wat kan leiden tot blinde vlekken, hogere complexiteit en inefficiënte beveiliging. CNAPP voorkomt dit door alle cloudbeveiligingsfuncties te bundelen in één geïntegreerd platform, waardoor bedreigingen beter zichtbaar en beheersbaar zijn.



Afbeelding I - Bron: Berthoty, “Redefining CNAPP: A Complete Guide to the Future of Cloud Security.”

3 WAT IS CNAPP EN HOE ADRESSEERT HET DE UITDAGINGEN?

CONSOLIDATIE VAN SECURITY TOOLS

CNAPP streeft naar consolidatie van verschillende security tools in één platform. In het verleden gebruikten securityteams meerdere tools voor verschillende aspecten van cloud security, zoals CSPM, CWPP en andere tools. CNAPP is erop gericht deze samen te brengen om de complexiteit van het beheer van meerdere security tools te verminderen en het aantal tools waarmee securityteams te maken hebben te reduceren.

VISIBILITY VAN CLOUDOMGEVING

Daarnaast biedt CNAPP uitgebreide visibility in cloudomgevingen. Waardoor er diepgaande inzichten verkregen worden, op workload niveau, op alle lagen (SaaS, PaaS, IaaS) van de cloud estate. Traditionele security tools hebben vaak niet de mogelijkheid om end-to-end configuraties van resources te zien. CNAPP-tools zijn ontworpen om 100% zichtbaarheid te bieden op alle cloud assets. Om daarmee eventuele misconfiguraties, compliance-risico's en security gaps te identificeren en zo een overzicht te bieden van de gehele security posture van de cloudomgeving.

CNAPP combineert agent-based en agentless oplossingen om verschillende niveaus van zichtbaarheid te bieden. Agentless scanning zorgt voor razendsnel inzicht in alle cloudresources, terwijl een cloudsensor ('light' agent) een nog gedetailleerder beeld geeft binnen de runtime-omgeving van workloads. Door primair vanuit een agentless-benadering te werken en alleen waar nodig light sensors (eBPF agents) in te zetten, ontstaat een compleet beeld van de cloudomgeving met minimale impact op de runtime omgeving.

HET OVERBRUGGEN VAN POSTURE EN RUNTIME

CNAPP overbrugt de kloof tussen posture management en runtime protection. Posture management richt zich op het voorkomen van kwetsbaarheden en misconfiguraties voordat ze kunnen worden uitgebuit, terwijl runtime protection bedoeld is om bedreigingen te detecteren en erop te reageren wanneer ze zich voordoen. CNAPP biedt een uniforme aanpak voor deze beide essentiële onderdelen van cloud security.

WORKLOAD SECURITY

CNAPP beveiligt cloud workloads en richt zich specifiek op containers. Containers zijn lichtgewicht, geïsoleerde omgevingen die alle benodigde applicatiecomponenten bevat, zoals code, runtime en afhankelijkheden, waardoor applicaties consistent kunnen draaien in verschillende omgevingen. Containers zijn populair geworden dankzij technologieën zoals Docker en Kubernetes, die flexibiliteit en schaalbaarheid in de cloud mogelijk maken. Traditionele security tools schieten tekort omdat containers kortlevend en dynamisch zijn, waardoor statische beveiligingsmaatregelen niet volstaan. CNAPP-tools helpen door misconfiguraties op workloadniveau te detecteren en bieden runtime protection om actieve bedreigingen te blokkeren

ADRESSEREN VAN SILO VORMING

De Silos tussen DevOps, ITOps en SecOps kunnen leiden tot frustraties, inefficiëntie en uiteindelijk security gaps. Elk team heeft behoefte aan andere context en prioritering van risico's en CNAPP kan hierop inspelen. Hierdoor ontvangen DevOps-teams bijvoorbeeld alleen meldingen over echte kritieke problemen en kunnen SecOps-teams zich richten op strategische risico's in plaats van op eindeloze foutmeldingen. Ook kan CNAPP integereren met bestaande DevOps-tools en workflows zoals Kubernetes, Terraform, GitHub en CI/CD-piplines, waardoor security geautomatiseerd kan worden zonder dat het impact heeft op de snelheid van de ontwikkeling.

RISK & COMPLIANCE

CNAPP speelt een cruciale rol binnen Risk & Compliance Management door risico's zoals misconfiguraties, kwetsbaarheden en bedreigingen in cloudomgevingen te detecteren en deze te koppelen aan relevante compliance frameworks zoals DORA, CIS, NIS-2 en ISO27001. Dit onderdeel binnen CNAPP helpt organisaties bij het naleven van regelgeving door geautomatiseerde controles uit te voeren, afwijkingen snel te signaleren en risico's te prioriteren op basis van hun impact op bedrijfscontinuïteit en compliance. Daarnaast biedt dit organisaties near-real-time inzicht in de compliance status, vermindert de afhankelijkheid van handmatige audits en versnelt het detecteren en oplossen van security- en compliance-issues, waardoor organisaties efficiënter en veiliger opereren binnen de geldende regelgeving.

4 DE ROL VAN CNAPP IN HEDENDAAGSE CLOUDOMGEVINGEN

4.1 ONTWIKKELINGEN

CNAPP-platformen maken steeds vaker gebruik van AI & Machine Learning om het beveiligen van (multi) cloudomgevingen te automatiseren en risico's proactief te beheren. Volgens Gartner behoren geavanceerde detectie-algoritmen en machine learning tot belangrijke trends in cloud security. AI kan helpen bij:

- Automatische threat detection, door patronen in gedrag en anomalieën te herkennen.
- False positives verminderen, zodat securityteams zich op echte bedreigingen kunnen richten.
- Snellere incident respons, door geautomatiseerde playbooks en aanbevelingen. Hierdoor worden security processen minder afhankelijk van interventie en kunnen organisaties efficiënter dreigingen aanpakken.

Daarnaast verwacht Gartner[12] dat in 2029, 60% van de organisaties die geen uniforme CNAPP oplossing implementeren binnen hun cloud architectuur geen uitgebreid inzicht hebben in het aanvalsoppervlak van de cloud en daardoor hun gewenste zero-trust doelstellingen niet halen. Verder verwacht Gartner dat in 2029 35% van alle bedrijfsapplicaties in containers draaien, een stijging van 15 procentpunt vergeleken met de voorspelling van 2023. Er kan niet uitgesloten worden dat de voorspellingen de aankomende jaren nogmaals bijgesteld worden.

Verder zegt Gartner[12] dat de markt voor CNAPP een aanzienlijke groei heeft doorgemaakt, die gepaard ging met een trend van overnames en consolidaties. Hoewel er veel aanbieders zijn, biedt slechts een handjevol een uitgebreid platform met de vereiste breedte en diepte van functionaliteit, met de nadruk op naadloze integratie in het ontwikkelings- en operationele proces. Daarnaast is er slechts een select aantal aanbieders met verregaande cloud-native functionaliteiten die niet alleen door overnames tot stand zijn gekomen.

Naarmate steeds meer organisaties cloud-native applicaties ontwikkelen, zal de rol van CNAPP in Dev, Sec and IT Ops-strategieën de komende jaren alleen maar belangrijker worden. De samenwerking tussen development en operations wordt essentieel, en CNAPP biedt de geïntegreerde beveiliging die nodig is om kwetsbaarheden snel te identificeren en te verhelpen, zonder de snelheid van ontwikkeling te vertragen.

Nu steeds meer organisaties kiezen voor een multi-cloudstrategie, waarbij ze meerdere cloudproviders zoals AWS, Azure en GCP combineren om flexibiliteit en schaalbaarheid te vergroten en de afhankelijkheid te verkleinen, brengt dit ook grotere risico's met zich mee. In deze ontwikkeling speelt CNAPP, als cloud-agnostische oplossing, een belangrijke rol, doordat het één platform biedt dat alle cloudomgevingen ondersteunt. Dit maakt het mogelijk om beveiligingsstrategieën consistent toe te passen over verschillende clouds heen, terwijl organisaties de risico's van vendor lock-in vermijden.

[12] Gartner, "Market Guide for Cloud-Native Application Protection Platforms."

4.2 WAT BETEKENT DIT VOOR UW ORGANISATIE EN HOE NU VERDER?

Organisaties staan voor de uitdaging om cloudomgevingen niet alleen snel, maar ook veilig te laten groeien. Vaak hebben organisaties al de nodige security tooling in huis gehaald om de public cloudomgevingen te beveiligen. Zodoende willen we het volgende meegeven:

- **Evalueer de in gebruik zijnde (cloud) security tooling:** Vallen alle onderdelen die horen bij posture and vulnerability scanning & runtime detection and response (Hoofdstuk 3.1 & 3.2) binnen de scope? Is de huidige security stack zo efficiënt mogelijk ingericht, of is er toch sprake van veel overlap?
- **Evalueer de inzet van AI security:** Wordt er al gebruik gemaakt van AI om de cloudomgeving te beveiligen?
- **Evalueer het (jaarlijkse) pentest-beleid:** Valt de cloud binnen de scope van de pentest? Wordt een cloud assessment uitgevoerd door een CNAPP-partner?

Mocht u meer informatie willen over cloud security, CNAPP of wilt u weten wat Acora op dat gebied voor u kan betekenen, neem dan gerust contact met ons op.

CONTACT

Leon Smit
General Manager
Acora Cyber Security, Acora Netherlands

e: leon.smit@acora.com
t: 0031 (0)651220533

acora