AYI NEDJIMI Consultants

CNAPP Cloud-Native Application Protection Platform

Catégorie : Cloud Security Lecture : 8 min Publié le : 05/03/2026 Auteur : Ayi NEDJIMI

Comparatif CNAPP 2026 : Wiz, Prisma Cloud, Orca, Lacework et Aqua Security. Critères de sélection, fonctionnalités clés et retours d'expérience.

Résumé exécutif

Les plateformes CNAPP unifient CSPM, CWPP, CIEM et sécurité des conteneurs. Ce comparatif analyse les cinq leaders du marché en 2026 : Wiz, Prisma Cloud, Orca, Lacework et Aqua Security, avec des critères objectifs et des retours terrain.
Le marché des CNAPP explose littéralement depuis trois ans, et pour cause : les équipes sécurité cloud sont noyées sous une multitude d'outils spécialisés qui ne communiquent pas entre eux. Un outil pour le CSPM, un autre pour la protection des workloads, un troisième pour la sécurité des conteneurs, un quatrième pour la gestion des droits IAM. Les plateformes Cloud-Native Application Protection promettent de consolider tout cela dans une interface unique avec un modèle de données unifié. Après avoir évalué et déployé les principales solutions CNAPP chez des clients de toutes tailles au cours des deux dernières années, je partage dans ce comparatif les forces et faiblesses réelles de chaque solution, au-delà du marketing et des quadrants analystes. Les critères d'évaluation couvrent la couverture multi-cloud, la profondeur de détection, la facilité de déploiement, l'impact opérationnel sur les équipes DevOps, le modèle de coût et bien sûr la qualité du support technique en situation de crise réelle.

Pourquoi les CNAPP dominent le marché en 2026 ?

Gartner a défini le concept de CNAPP en 2021, et depuis, la convergence des outils de sécurité cloud s'est accélérée. Les acquisitions majeures (Palo Alto rachète Bridgecrew puis Cider Security, CrowdStrike acquiert Bionic, Wiz tente de racheter Lacework) témoignent de cette consolidation. Les raisons sont pragmatiques : les **CSPM** (Cloud Security Posture Management) détectent les misconfigurations mais ne voient pas les vulnérabilités des workloads. Les **CWPP** (Cloud Workload Protection Platforms) protègent les VMs et conteneurs mais ignorent les configurations cloud. Les **CIEM** (Cloud Infrastructure Entitlement Management) gèrent les droits IAM mais ne corrèlent pas avec les vulnérabilités. Un CNAPP unifie ces trois piliers dans un *graphe de sécurité* unique qui permet de prioriser les risques en contexte.

Pour comprendre les enjeux IAM que les CNAPP adressent, notre article sur escalade de privilèges IAM cloud détaille les vecteurs d'escalade de privilèges que ces plateformes cherchent à détecter.

Quelles fonctionnalités comparer entre les CNAPP ?

Les critères d'évaluation d'un CNAPP se répartissent en huit domaines fonctionnels. Le **CSPM** évalue la configuration des ressources cloud contre des benchmarks (CIS, NIST). Le **CWPP** scanne les vulnérabilités des VMs, conteneurs et serverless. Le **CIEM** analyse les permissions IAM effectives et détecte les droits excessifs. La **sécurité des conteneurs** couvre le build (scan d'images), le deploy (admission control) et le runtime (détection comportementale). La **sécurité IaC** scanne les templates Terraform, CloudFormation et ARM avant le déploiement. La **sécurité du code** (shift-left) intègre le scan dans les pipelines CI/CD. Le **Data Security Posture Management** (DSPM) découvre et classifie les données sensibles. Enfin, l'**analyse des chemins d'attaque** corrèle toutes ces données pour identifier les risques exploitables.

Fonctionnalité	Wiz	Prisma Cloud	Orca	Lacework	Aqua
CSPM	Excellent	Excellent	Très bon	Bon	Bon
CWPP	Très bon	Excellent	Très bon	Très bon	Excellent
CIEM	Excellent	Bon	Très bon	Basique	Basique
Container Runtime	Bon	Excellent	Bon	Très bon	Excellent
IaC Scanning	Bon	Excellent	Basique	Basique	Bon
DSPM	Excellent	Bon	Très bon	Absent	Absent
Attack Path	Excellent	Bon	Très bon	Bon	Basique
Multi-cloud	AWS/Azure/GCP	AWS/Azure/GCP/OCI	AWS/Azure/GCP	AWS/Azure/GCP	AWS/Azure/GCP

Mon avis : Wiz domine le marché grâce à son approche agentless et son graphe de sécurité exceptionnellement bien conçu. Cependant, Prisma Cloud reste le choix le plus complet pour les organisations qui ont besoin d'une couverture shift-left poussée avec Bridgecrew intégré. Orca offre le meilleur rapport qualité-prix pour les entreprises mid-market.

Le déploiement d'un CNAPP dans une organisation existante nécessite une stratégie de change management bien planifiée. Les équipes DevOps peuvent percevoir le CNAPP comme un frein à leur vélocité si les findings ne sont pas correctement contextualisés et priorisés. La clé est de commencer en mode observabilité uniquement, sans bloquer aucun déploiement, pendant une période de calibrage de quatre à six semaines. Pendant cette phase, analysez les findings générés, identifiez les faux positifs récurrents, et ajustez les seuils de sévérité en fonction de votre contexte spécifique. Puis introduisez progressivement des gates bloquantes dans le pipeline CI/CD, en commençant par les findings critiques uniquement et en élargissant progressivement le périmètre. Communiquez chaque étape aux équipes de développement avec des sessions de formation sur la plateforme et des exemples concrets de vulnérabilités détectées et corrigées grâce au CNAPP, transformant la perception d'un outil de contrôle en celle d'un outil d'aide au développement sécurisé.

Wiz : le leader agentless analysé en profondeur

Wiz a révolutionné le marché en 2020 avec son approche 100% agentless qui scanne les snapshots de disques et les configurations cloud sans déployer d'agent. Son *Security Graph* corrèle les vulnérabilités, misconfigurations, permissions IAM excessives, données sensibles et exposition réseau pour identifier les combinaisons toxiques réellement exploitables. Par exemple, Wiz peut identifier qu'une VM vulnérable à Log4Shell est exposée sur Internet, dispose d'un rôle IAM avec accès admin à un bucket S3 contenant des données PII, et que ce bucket est accessible depuis un compte externe non autorisé.

Les limitations de Wiz incluent : pas de protection runtime (la détection se fait par scan périodique, pas en temps réel), une couverture IaC basique comparée à Bridgecrew, et un coût élevé qui peut atteindre plusieurs centaines de milliers d'euros par an pour les grandes organisations. Les ressources officielles d'AWS Security et de GCP Security complètent la couverture native de chaque CNAPP pour les services spécifiques à chaque provider.

Comment choisir le bon CNAPP pour votre organisation ?

Le choix d'un CNAPP dépend de cinq facteurs clés. **Maturité cloud** : si vous débutez, Wiz ou Orca avec leur approche agentless offrent un time-to-value rapide. Si vous avez une maturité DevSecOps avancée, Prisma Cloud ou Aqua s'intègrent mieux dans les pipelines CI/CD existants. **Complexité multi-cloud** : toutes les solutions couvrent les trois hyperscalers, mais la profondeur varie par provider. **Besoin runtime** : si la détection en temps réel des menaces conteneur est critique, Aqua Security et Prisma Cloud sont supérieurs. **Budget** : Orca et Lacework proposent des modèles de pricing plus accessibles. **Écosystème existant** : Prisma Cloud s'intègre naturellement avec l'écosystème Palo Alto (Cortex XDR, XSOAR), tandis que Lacework s'intègre bien avec Snowflake pour l'analytique.

La sécurité des conteneurs est un critère différenciant majeur. Notre article sur les techniques d'évasion de conteneur Docker montre pourquoi la protection runtime est critique. De même, la détection des attaques CI/CD via attaques CI/CD GitOps est une fonctionnalité que seuls Prisma Cloud et Aqua couvrent nativement.

Pour un client SaaS B2B avec 200 comptes AWS et 50 subscriptions Azure, nous avons évalué Wiz, Prisma Cloud et Orca en POC parallèle pendant 60 jours. Wiz a identifié 40% plus de chemins d'attaque critiques grâce à son graphe, mais Prisma Cloud a détecté 3 incidents runtime que Wiz a manqués par nature (approche agentless). Le client a choisi Wiz pour le CSPM/CIEM et conservé CrowdStrike Falcon pour la protection runtime — une approche best-of-breed qui fonctionne bien mais nécessite une intégration SIEM solide pour corréler les findings des deux plateformes.

Quelles sont les tendances CNAPP pour la suite de 2026 ?

Trois tendances majeures façonnent l'évolution des CNAPP. Premièrement, l'**intégration AI/LLM** pour l'analyse et la remédiation : Wiz a lancé Wiz AskAI, Prisma Cloud intègre des suggestions de remédiation IA, et Orca propose un assistant conversationnel pour l'investigation des findings.

Deuxièmement, la **convergence CNAPP-CDR** (Cloud Detection and Response) : les CNAPP ajoutent des capacités de détection en temps réel traditionnellement réservées aux CDR, brouillant la frontière entre posture et détection. Troisièmement, le **DSPM** (Data Security Posture Management) devient un pilier incontournable du CNAPP, avec la découverte automatique des données sensibles dans les datastores cloud et la corrélation avec les chemins d'accès IAM.

La sécurité des pipelines CI/CD via des outils comme ceux analysés dans notre article sur audit Terraform compliance s'intègre de plus en plus dans les CNAPP sous la catégorie Application Security Posture Management (ASPM). Cette convergence simplifie la vie des équipes sécurité mais pose la question de la profondeur versus la largeur de couverture.

À retenir : Un CNAPP ne remplace pas une stratégie de sécurité cloud. C'est un outil de visibilité et de priorisation qui doit s'intégrer dans un programme plus large incluant la formation des développeurs, les processus de revue de sécurité, la réponse aux incidents et la gouvernance des accès. Choisissez le CNAPP qui s'intègre le mieux dans votre écosystème existant plutôt que celui qui coche le plus de cases dans un tableau comparatif.

Faut-il un CNAPP en plus des outils natifs ?

Cette question revient systématiquement lors des évaluations. AWS Security Hub, Azure Defender for Cloud et GCP Security Command Center couvrent déjà une partie significative des fonctionnalités CNAPP pour leur cloud respectif. L'ajout d'un CNAPP tiers se justifie principalement dans trois cas : environnement **multi-cloud** nécessitant une vue unifiée, besoin de fonctionnalités non couvertes nativement comme l'**analyse des chemins d'attaque** cross-service, ou exigence d'une plateforme indépendante du provider pour des raisons d'audit et de séparation des responsabilités. Pour un environnement mono-cloud de taille modérée, les outils natifs bien configurés offrent souvent un rapport couverture/coût supérieur.

L'intégration d'un CNAPP avec les outils existants de l'organisation est un facteur de succès critique souvent sous-évalué lors du POC. Vérifiez la qualité des intégrations avec votre SIEM (format des logs, API bidirectionnelle, corrélation des findings), votre plateforme de ticketing (création automatique de tickets Jira, ServiceNow avec les détails du finding et la recommandation de remédiation), votre pipeline CI/CD (gates bloquantes configurables par sévérité, feedback aux développeurs dans les pull requests), et votre outil de communication (notifications Slack ou Teams contextualisées par équipe et par criticité). Un CNAPP isolé qui ne s'intègre pas dans les workflows existants génère une fatigue d'outil supplémentaire et un taux d'adoption faible qui annule les bénéfices théoriques de la plateforme et ne justifie pas l'investissement réalisé.

Avant d'investir dans un CNAPP coûteux, avez-vous vérifié que les outils natifs de votre cloud provider sont correctement configurés et pleinement exploités par vos équipes ?

Comment évaluer le ROI d'un CNAPP ?

L'évaluation du retour sur investissement d'un CNAPP doit considérer quatre dimensions quantifiables. Premièrement, la **réduction du temps de détection** (MTTD) : un CNAPP bien configuré détecte les misconfigurations critiques en minutes contre des jours ou semaines avec

des audits manuels. Deuxièmement, la **consolidation des outils** : remplacer quatre ou cinq outils spécialisés (CSPM, CWPP, CIEM, scanner de conteneurs, scanner IaC) par une plateforme unique réduit les coûts de licence et de formation. Troisièmement, l'**efficacité opérationnelle** : la priorisation contextuelle des risques via l'analyse des chemins d'attaque permet aux équipes de se concentrer sur les vulnérabilités réellement exploitables au lieu de traiter des milliers de findings non contextualisés. Quatrièmement, l'**évitement des incidents** : chaque compromission cloud évitée représente un coût évité de remédiation, de notification RGPD, de perte de réputation et potentiellement de sanctions réglementaires.

Le coût d'un CNAPP varie considérablement selon la solution et l'échelle de déploiement. Wiz facture par workload protégé avec des contrats annuels débutant aux alentours de cent mille euros pour une organisation mid-market. Prisma Cloud utilise un modèle de crédits basé sur les ressources protégées, avec une complexité tarifaire qui nécessite une simulation détaillée avant engagement. Orca propose des forfaits par compte cloud, généralement plus accessibles pour les PME. Pour justifier l'investissement auprès du management, construisez un business case qui compare le coût du CNAPP au coût moyen d'un incident de sécurité cloud dans votre secteur, en utilisant les données du rapport annuel IBM Cost of a Data Breach qui chiffre le coût moyen d'une violation à plus de quatre millions d'euros dans le secteur technologique européen.

Sources et références : CISA · Cloud Security Alliance

Conclusion : grille de décision CNAPP

Le choix d'un CNAPP en 2026 se résume à quatre profils types. Organisation multi-cloud mature avec budget confortable : Wiz. Organisation mono-cloud AWS avec pipeline DevSecOps avancé : Prisma Cloud. Organisation mid-market cherchant le meilleur rapport qualité-prix : Orca Security. Organisation avec des exigences runtime conteneur fortes : Aqua Security ou Prisma Cloud. Quelle que soit la solution choisie, prévoyez trois à six mois de déploiement progressif, une équipe dédiée de deux à trois personnes pour l'exploitation quotidienne, et un budget formation conséquent pour exploiter pleinement les capacités de la plateforme.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr