Prisma Cloud
En bref

Protection des applications du code au cloud

Véritable alternative aux ensembles hétéroclites de produits spécialisés, Prisma® Cloud est une plateforme de protection des applications cloud-native (CNAPP). Intégrant un large éventail de fonctionnalités, elle garantit une sécurité unifiée et inégalée dans tout environnement cloud privé, public, hybride ou multicloud. À la clé : réduction des risques et des compromissions, collaboration plus étroite entre les équipes Dev et Sec, efficacité maximisée, conformité et sécurité renforcées, etc.

Figure 1. Approche Code to Cloud™ unifiée de Prisma Cloud

Prisma Cloud : les cas d'usage

Prévention des risques

Misez sur une approche « shift-left » pour sécuriser vos applications dès la conception. Dans cet esprit, Prisma Cloud s'intègre aux écosystèmes d'ingénierie pour empêcher les vulnérabilités et les erreurs de configuration d'entrer en production. Une approche qui offre de multiples avantages :

- **Sécurité IaC (Infrastructure-as-Code) :** identifiez et corrigez les erreurs de configuration dans Terraform, CloudFormation, ARM, Kubernetes et autres modèles IaC
- **Sécurité des secrets :** détectez et sécurisez les secrets exposés et vulnérables dans tous les fichiers de vos référentiels et pipelines CI/CD
- **Sécurité CI/CD :** renforcez vos pipelines CI/CD, réduisez votre surface d'attaque et protégez votre environnement de développement applicatif
- **Analyse de la composition logicielle (SCA) :** éliminez les vulnérabilités et les problèmes de conformité des licences open-source à l'aide d'une priorisation contextualisée.

Visibilité et contrôle

Erreurs de configuration, identités et accès, données, vulnérabilités, terminaux d'API… vous devez assurer une visibilité et un contrôle continus sur tous les facteurs influençant votre environnement cloud. C'est pourquoi Prisma Cloud sécurise l'infrastructure dématérialisée en conjuguant :

- **Gestion de la posture de sécurité du cloud (CSPM) :** surveillez l'environnement cloud, identifiez et prévenez les risques, et maintenez la conformité
- **Gestion des droits sur l'infrastructure cloud (CIEM) :** maîtrisez les autorisations sur les environnements multicloud
- **Analyse sans agent des workloads :** débusquez les vulnérabilités et les menaces en passant au crible les hôtes, les containers, les plateformes Kubernetes et les systèmes sans serveur
- **Sécurité des données cloud :** identifiez les données sensibles et détectez la présence de malwares sur les systèmes de stockage dans le cloud public
- **Visibilité sur les API :** recensez, profilez et sécurisez les API sur l'ensemble des applications cloud-native
- **CDEM (Cloud Discovery and Exposure Management) :** gagnez en visibilité et en contrôle sur les assets cloud inconnus et non gérés exposés à Internet

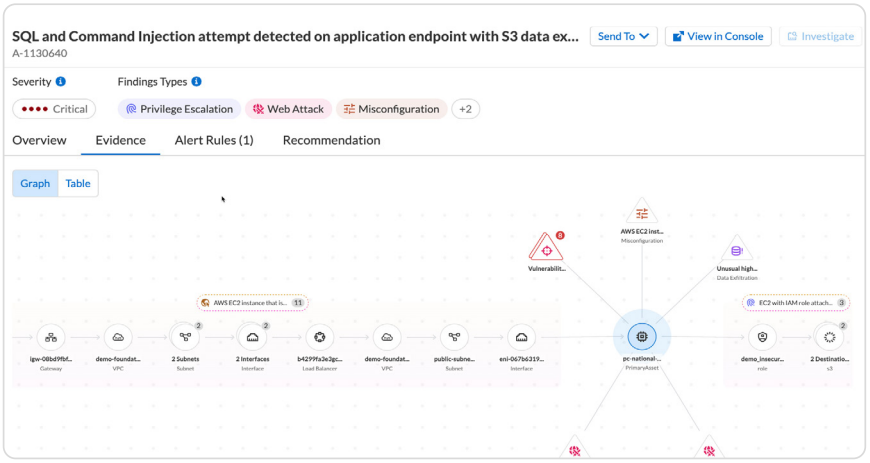

Figure 2. Analyse des chemins d'attaque

Prisma Cloud
En bref

Protection du runtime

Neutralisez les compromissions pendant le runtime et protégez les applications contre les attaques. À cette fin, Prisma Cloud offre une protection contre les menaces sur les clouds publics et privés grâce aux fonctionnalités suivantes :

- **Détection des menaces cloud :** détectez les menaces avancées, les attaques zero-day et les anomalies sur les environnements multicloud
- **Sécurité des hôtes :** protégez vos machines virtuelles dans tous les environnements cloud publics et privés
- **Sécurité des containers :** sécurisez les containers et les plateformes Kubernetes sur n'importe quel cloud public ou privé
- **Sécurité des architectures sans serveur :** sécurisez les fonctions sans serveur tout au long du cycle de vie des applications
- **Sécurité des API et des applications web :** protégez les API et les applications web dans tous les clouds publics ou privés

Visibilité du code au cloud

Notre approche unique repose sur une visibilité code-to-cloud qui corrèle les informations tout au long du cycle de vie applicatif dans un double objectif : limiter les risques et prévenir les compromissions. En pratique, Prisma Cloud contextualise les alertes, priorise les risques critiques et recommande différentes étapes de remédiation.

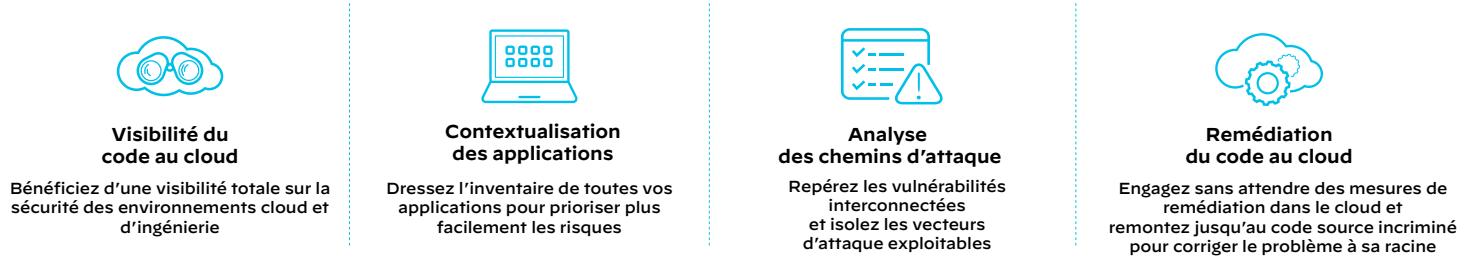

Figure 3. Visibilité du code au cloud

« Avec Palo Alto Networks, c'est simple comme bonjour. La visibilité est totale, l'intégration native parfaitement fluide, et l'automatisation prend en charge la majorité de la surveillance. Le tout sans aucun impact sur nos ressources. »

– Oussama Benzaouia, RSSI, Teads
Lire l'étude de cas complète

« Les solutions Palo Alto Networks répondent à toutes les problématiques. Grâce à elles, nous n'avons plus besoin d'outils de protection spécialisés. Nous disposons d'une suite de technologies de sécurité interconnectées qui ont fait leurs preuves. Notre équipe peut ainsi se concentrer sur les tâches créatrices de valeur tout en sachant que les processus de sécurité critiques s'exécutent en arrière-plan et donc, que notre nouvelle infrastructure numérique reste protégée. »

– Bob Bowden, Architecte sécurité, Registers of Scotland
Lire l'étude de cas complète