Prisma Cloud
En bref

Sécurité cloud-native complète. Sur tout le cycle de vie. Pour tous les clouds.

Prisma™ Cloud est la plateforme de sécurité cloud-native la plus complète du marché. Sa mission : assurer la protection et la mise en conformité de vos applications, données et technologies cloud-native tout au long du cycle de développement sur vos environnements cloud hybrides et multi-cloud.

Son approche intégrée permet aux équipes DevOps et de sécurité opérationnelle de collaborer efficacement et d'accélérer le développement d'applications cloud-native en toute sécurité.

Prisma Cloud protège et s'intègre aux architectures et outils cloud-native pour assurer une couverture complète de l'environnement, brisant au passage les silos opérationnels d'un bout à l'autre du cycle de vie des applications. La plateforme favorise ainsi l'adoption de pratiques DevSecOps et permet de réagir plus rapidement aux besoins de sécurité changeants des architectures cloud-native.

Piliers de Prisma Cloud

Gestion de la sécurité cloud

Une sécurité cloud efficace exige une visibilité complète sur chaque ressource déployée, de même qu'une confiance absolue dans leur configuration et leur état de conformité. Prisma Cloud va bien au-delà d'une simple gestion de la conformité et des configurations pour créer une nouvelle approche de la sécurité cloud. Les flux CTI provenant de plus de 30 sources fournissent une vue claire et immédiate sur les risques et vulnérabilités, tandis que les contrôles sur le pipeline de développement empêchent les configurations non sécurisées d'être mises en production. Fonctions de Prisma Cloud :

- Visibilité, conformité et gouvernance
  - » Inventaire des ressources cloud
  - » Évaluation des configurations (environnement d'exécution)
  - » Suivi de la conformité et reporting
  - » Analyse des configurations IaC (IDE, SCM, CI/CD)
- Détection des menaces
  - » Analyse du comportement des utilisateurs et des entités (UEBA)
  - » Visibilité, analyse et détection des anomalies du trafic réseau basées sur les API
  - » Réponse et investigation automatiques
- Sécurité des données (AWS® uniquement)
  - » Classification des données
  - » Analyses anti-malware
  - » Gouvernance des données

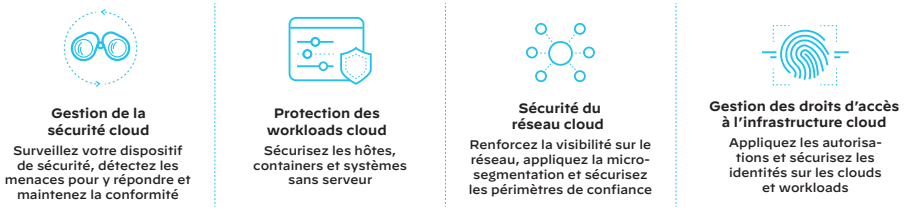

Figure 1 : Piliers de Prisma Cloud

Protection des workloads cloud

Les environnements cloud-native ne cessent d'évoluer. Des plateformes et technologies de nouvelle génération permettent aujourd'hui aux entreprises d'accélérer leurs déploiements et d'élargir leur périmètre comme jamais auparavant. Prisma Cloud offre une protection complète des environnements cloud (publics et privés) et sur site. La sécurité est intégrée en toute simplicité aux principaux workflows d'intégration et de déploiement continus (CI/CD), registres et environnements d'exécution. Modules de sécurité :

- Sécurité des hôtes
  - » Gestion des vulnérabilités
  - » Sécurité des environnements d'exécution
  - » Gestion de la conformité
  - » Contrôle des accès
- Sécurité des containers
  - » Gestion des vulnérabilités
  - » Sécurité des environnements d'exécution
  - » Gestion de la conformité
  - » Contrôle des accès
  - » Analyse des référentiels Git

Prisma Cloud

En bref

- Sécurité des systèmes sans serveur
  - » Gestion des vulnérabilités
  - » Sécurité des environnements d'exécution
  - » Gestion de la conformité
  - » Contrôle des accès
- Sécurité des API et des applications web
  - » Protection contre le top 10 des risques de l'OWASP
  - » Protection des API

Sécurité du réseau cloud

La protection du réseau doit être adaptée aux spécificités des environnements cloud-native, tout en appliquant des politiques homogènes dans les environnements hybrides. Pour détecter et prévenir les anomalies réseau, Prisma Cloud applique la microsegmentation au niveau des containers, inspecte les journaux de flux de trafic et prévient les menaces sur la couche L7 :

- Visibilité sur le réseau et détection des anomalies
- Microsegmentation basée sur les identités
- Pare-feu cloud-native

Gestion des droits d'accès à l'infrastructure cloud

Les méthodes manuelles traditionnelles d'application du principe du moindre privilège compliquent le travail des équipes de sécurité à mesure qu'elles doivent gérer de plus en plus de droits associés aux services cloud. Prisma Cloud détecte continuellement et corrige automatiquement les risques liés aux identités et aux accès sur les infrastructures IaaS (Infrastructure as a Service) et les plateformes PaaS (Platform as a Service). La solution recherche toutes les identités humaines et machines dans les environnements cloud, puis analyse les droits, les rôles et les politiques. Fonctions de Prisma Cloud :

- Visibilité sur les permissions
- Gouvernance IAM
- Réponse automatisée
- Analyse du comportement des utilisateurs et des entités (UEBA)

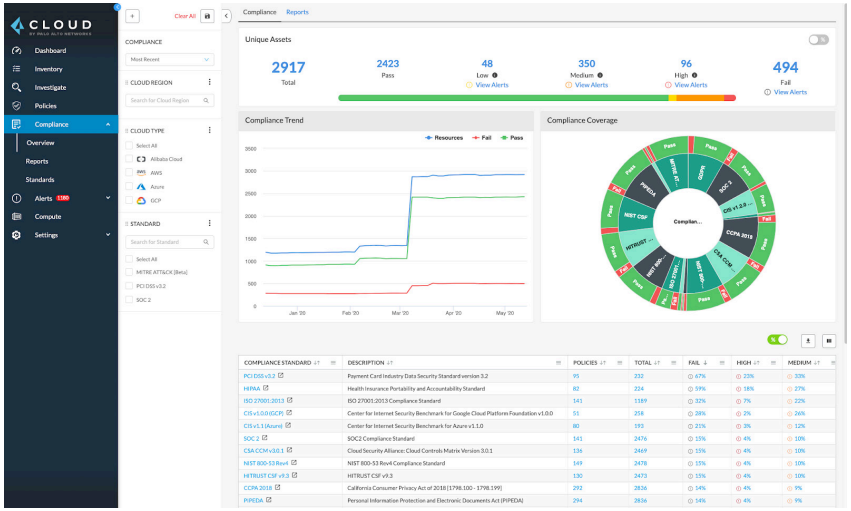

Figure 2 : Tableau de bord de Prisma Cloud

« Lorsque nous nous sommes penchés sur Prisma Cloud, nous n'avons pas seulement pris en compte les capacités actuelles de l'outil, mais aussi la feuille de route et la vision à terme. Cela fait une énorme différence, car il s'agit d'une collaboration à long terme. »

– Experian

Lire l'étude de cas complète

À propos de Prisma Cloud

Prisma™ Cloud est la plateforme de sécurité cloud-native la plus complète du marché. Sa mission : assurer la protection et la mise en conformité de vos applications, données et technologies cloud-native tout au long du cycle de développement sur vos environnements cloud hybrides et multi-cloud. Au lieu de s'assujettir aux contraintes de sécurité des architectures du cloud-native, l'approche intégrée de Prisma Cloud les élimine et brise les silos de sécurité opérationnelle tout au long du cycle de vie des applications. Vous pouvez ainsi évoluer vers une approche DevSecOps et réagir plus rapidement aux besoins de sécurité changeants des architectures cloud-native.