Gestion de la posture de sécurité du cloud

Maintien de la conformité pour les applications, workloads et données

Prisma Cloud réduit la complexité et protège les ressources des environnements hybrides et multicloud. Adoptée par plus de 1 900 entreprises leaders à travers le monde, notre plateforme complète de protection des applications cloud-native (CNAPP) sécurise plus de 7 milliards de ressources cloud et analyse plus de 1 000 milliards d'évènements par jour. Prisma Cloud élimine les angles morts et détecte les menaces que d'autres outils laissent passer. À la clé : visibilité complète sur l'environnement, détection continue des menaces, et automatisation des réponses.

Gestion complète de la posture de sécurité dans les environnements multicloud

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. Or, à mesure que les entreprises adoptent des méthodologies cloud-native et exploitent la flexibilité des architectures multicloud, la disparité des outils utilisés rend difficile la corrélation des données de sécurité. D'où l'importance d'une solution intégrée pour les équipes DevOps et SecOps. C'est là que Prisma Cloud entre en jeu.

Cette plateforme va bien au-delà d'une simple gestion de la conformité et des configurations pour créer une nouvelle approche de la gestion de la posture de sécurité du cloud (CSPM). Les flux CTI provenant de plus de 30 sources de données fournissent une vue claire et immédiate sur les vulnérabilités et problèmes de sécurité critiques, tandis que les contrôles sur le pipeline de développement empêchent les configurations non sécurisées d'être mises en production.

Fonctionnalités CSPM

Visibilité, conformité et gouvernance

Inventaire des ressources cloud

Prisma Cloud offre une visibilité et un contrôle complets sur la posture de sécurité de chaque ressource déployée. Tandis que certaines solutions se contentent d'agréger les données des ressources, Prisma Cloud analyse et normalise les sources de données disparates pour fournir une vue incomparable sur les risques en présence.

Amazon EFS	aws	24	0	ⓘ 24	0	ⓘ 24	0	0%
AWS Secrets Manager	aws	7	7	0	0	0	0	100%
Amazon EKS	aws	1	0	ⓘ 1	0	ⓘ 1	0	0%
Amazon SQS	aws	5	0	ⓘ 5	0	ⓘ 5	0	0%
Amazon S3	aws	66	0	ⓘ 66	ⓘ 66	0	0	0%
Azure Virtual Network		120	87	ⓘ 33	ⓘ 18	ⓘ 15	0	73%
Azure Network Watcher		31	31	0	0	0	0	100%
Azure Resource Manager		9	7	ⓘ 2	0	0	ⓘ 2	78%
Azure Policy		3	3	0	0	0	0	100%
Azure SQL Database		2	0	ⓘ 2	ⓘ 2	0	0	0%
Azure Compute		31	17	ⓘ 14	ⓘ 5	ⓘ 9	0	55%
Azure Storage		13	0	ⓘ 13	ⓘ 1	ⓘ 12	0	0%
Azure App Service		1	1	0	0	0	0	100%
Azure Security Center		2	0	ⓘ 2	0	ⓘ 2	0	0%
Google Resource Manager		114	91	ⓘ 23	ⓘ 12	ⓘ 11	0	80%

Figure 1. Inventaire des ressources

Suivi de la conformité et reporting

Prisma Cloud surveille en permanence l'état de conformité de l'environnement cloud et permet de générer des rapports en un clic depuis une console centralisée. Plus de 65 cadres réglementaires et normatifs sont intégrés par défaut, mais vous pouvez également créer vos propres cadres de conformité.

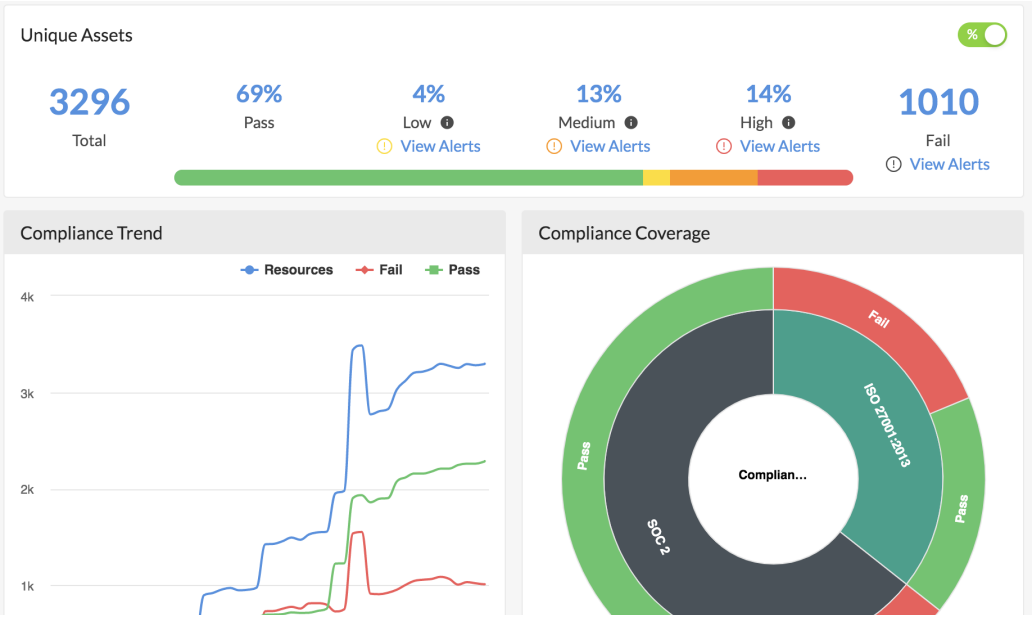

Figure 2. Conformité : tableau de bord

Priorisation contextualisée des risques

À l'inverse des outils silotés qui ne se concentrent que sur des erreurs de configuration individuelles, Prisma Cloud corrèle une grande variété d'informations pour mieux prioriser les différents risques : erreurs de configuration, expositions du réseau, autorisations excessives et autres vulnérabilités menant à des attaques potentielles. Basée sur les risques, cette analyse repose sur le moteur de contextualisation de Prisma Cloud pour identifier les multiples vulnérabilités du cloud pouvant être exploitées dans le cadre d'une attaque sophistiquée.

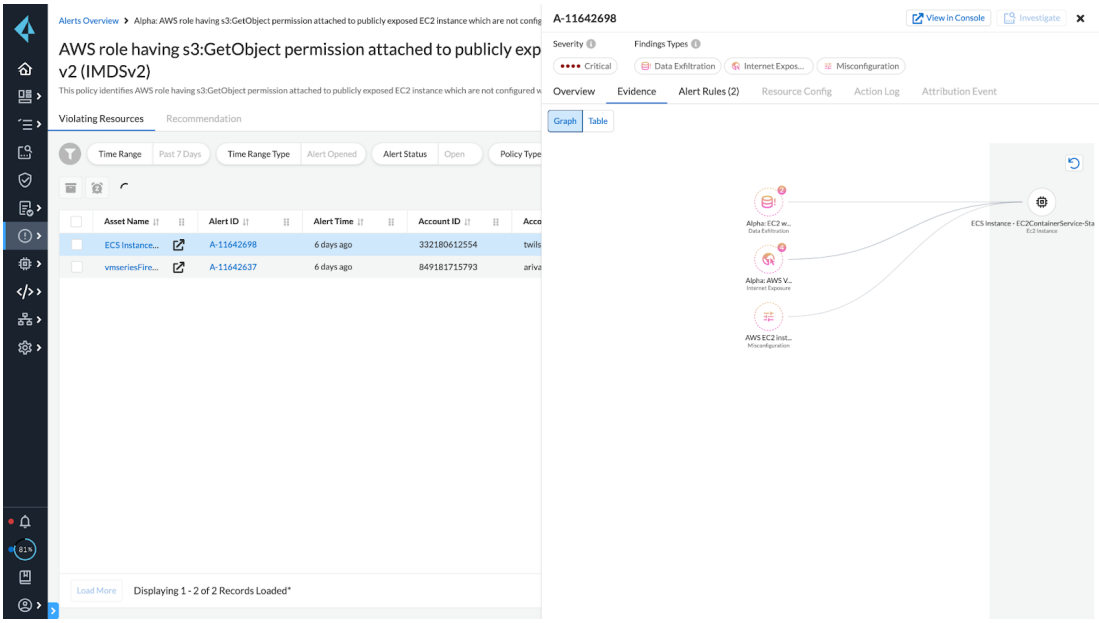

Figure 3. Investigation des alertes liées aux schémas d'attaque

Détection des menaces

Analyse du comportement des utilisateurs et des entités (UEBA)

Prisma Cloud analyse des millions d'évènements d'audit, puis utilise le machine learning (ML) pour détecter les activités symptomatiques d'une compromission de compte, de menaces internes, d'un vol de clés d'accès, etc.

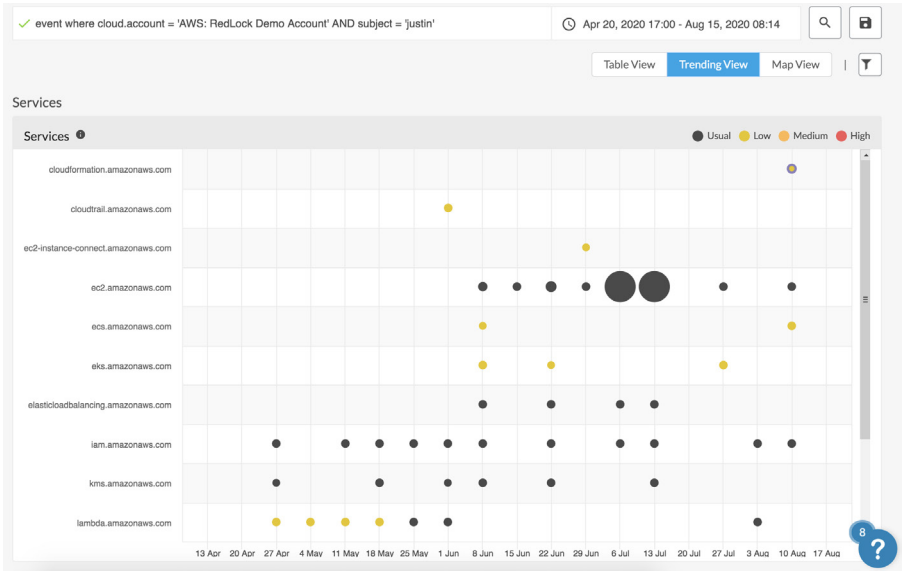

Figure 4. Suivi des activités anormales

Détection des menaces et des anomalies sur le réseau

Prisma Cloud surveille les comportements sur le réseau et s'appuie sur le ML et des flux CTI avancés pour détecter les menaces et les anomalies sur le réseau. La solution repère les scans et les balayages de ports qui permettent de rechercher les ports ouverts sur un serveur ou un hôte. Elle détecte également les menaces cachées dans le trafic DNS (Domain Name System) telles que les algorithmes de génération de noms de domaines (DGA) et les activités de cryptominage.

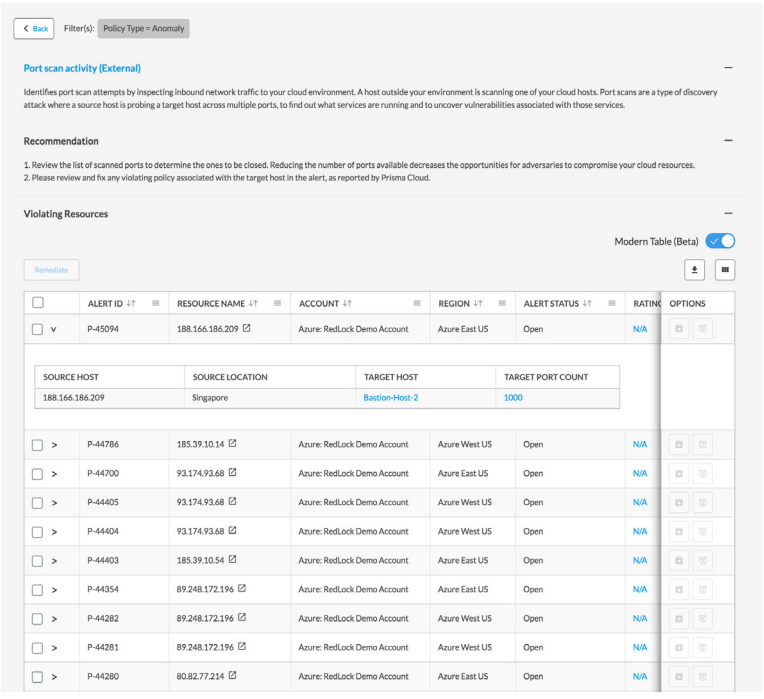

Figure 5. Détail des analyses de ports

Réponse et investigation automatiques

Prisma Cloud intègre des fonctionnalités de corrélation, de remédiation automatique et d'analyses forensiques approfondies. En combinant les informations provenant des workloads, des réseaux, de l'activité des utilisateurs, des données et des configurations, la plateforme accélère le processus d'investigation et de réponse aux incidents.

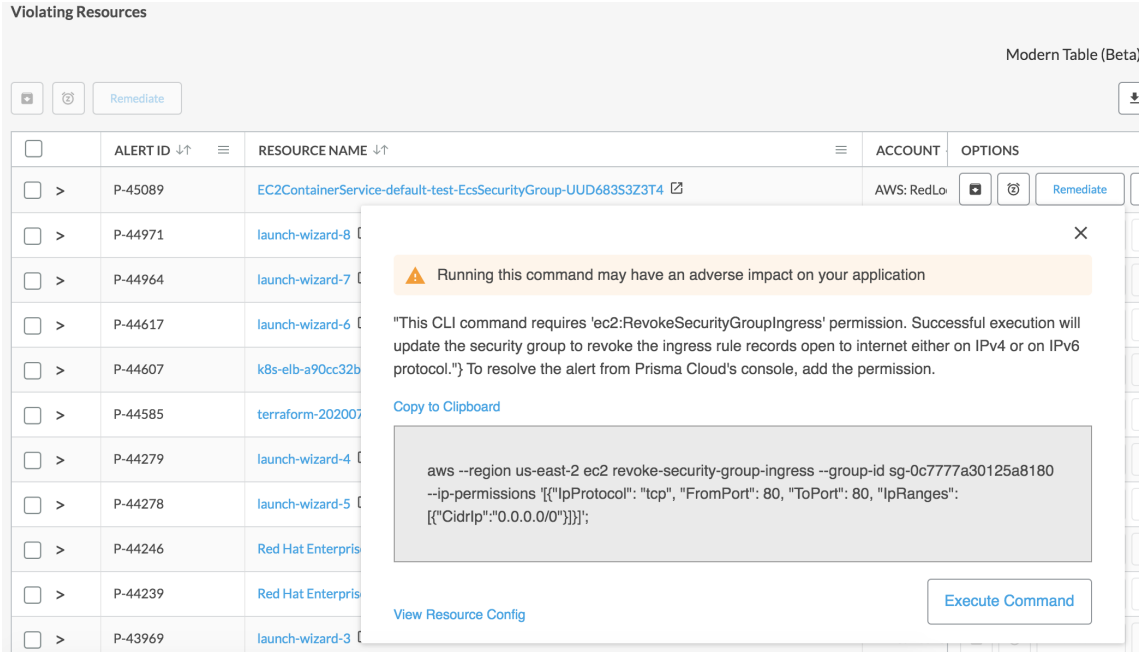

Figure 6. Détail des investigations automatisées

Sécurité des données

Visibilité sur les données et classification

Prisma Cloud offre une visibilité complète sur tous les objets et compartiments Amazon S3 et Microsoft Azure Storage, y compris les contenus par région, propriétaire et niveau d'exposition.

Vous pouvez affiner la granularité des données (permis de conduire, numéro de sécurité sociale, numéro de carte de crédit, etc.) pour identifier et surveiller les contenus sensibles.

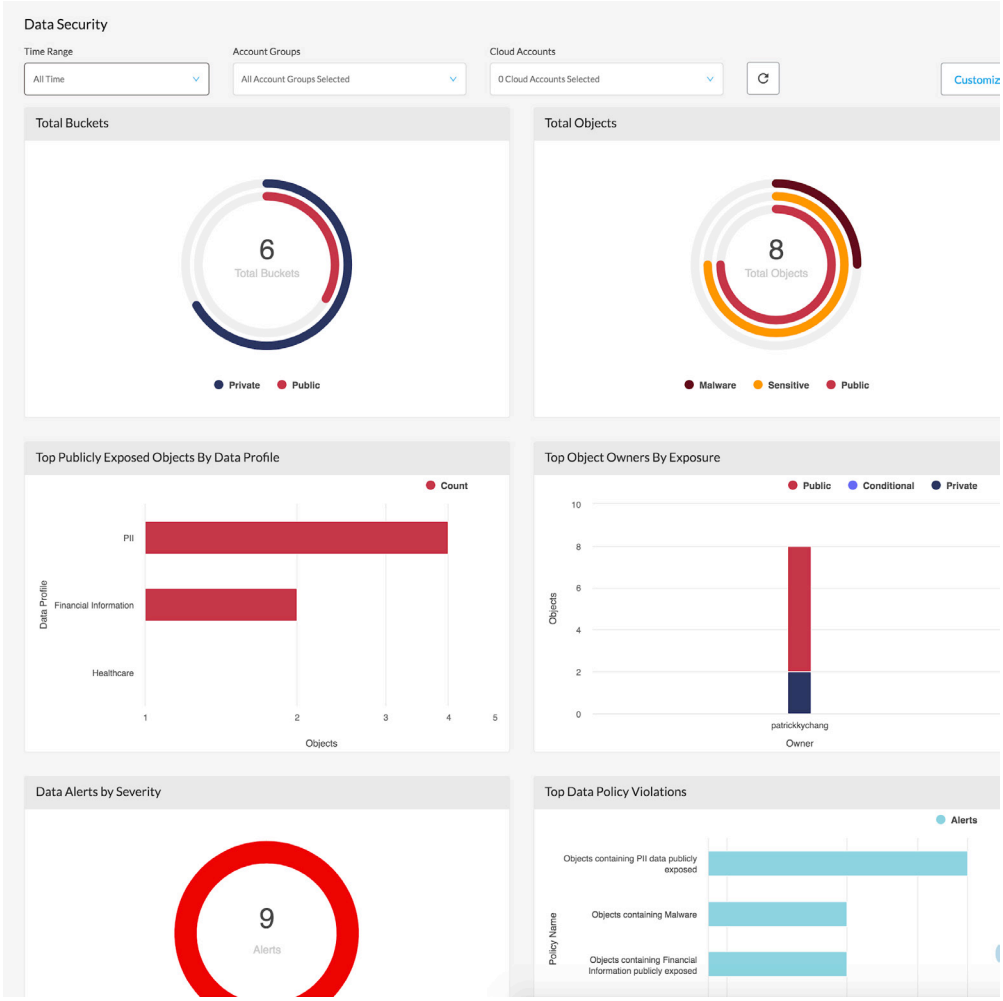

Figure 7. Sécurité des données S3 : tableau de bord

Gouvernance des données

Prisma Cloud intègre des politiques spécifiques permettant de déterminer rapidement votre profil de risque en fonction de la classification des données et des types d'exposition/de fichier. Il vous suffit d'activer et de désactiver les profils d'évaluation du niveau de conformité des données (PCI, RGPD, SOC 2, HIPAA, etc.) selon vos besoins, avec la possibilité de générer des rapports pré-audits en un seul clic.

Détection des malwares

Grâce au service WildFire, Prisma Cloud aide les utilisateurs à identifier et neutraliser les menaces connues et inconnues introduites dans des compartiments S3 et Azure Storage Blob, notamment des fichiers et objets contenant un malware.

Alertes et remédiation

Prisma Cloud génère automatiquement des alertes pour chaque objet selon la classification des données, l'exposition de ces dernières et les types de fichiers. Ces alertes permettent aux analystes de corriger rapidement la situation, d'avertir les équipes DevOps fautives et de supprimer tous les objets contenant des malwares.

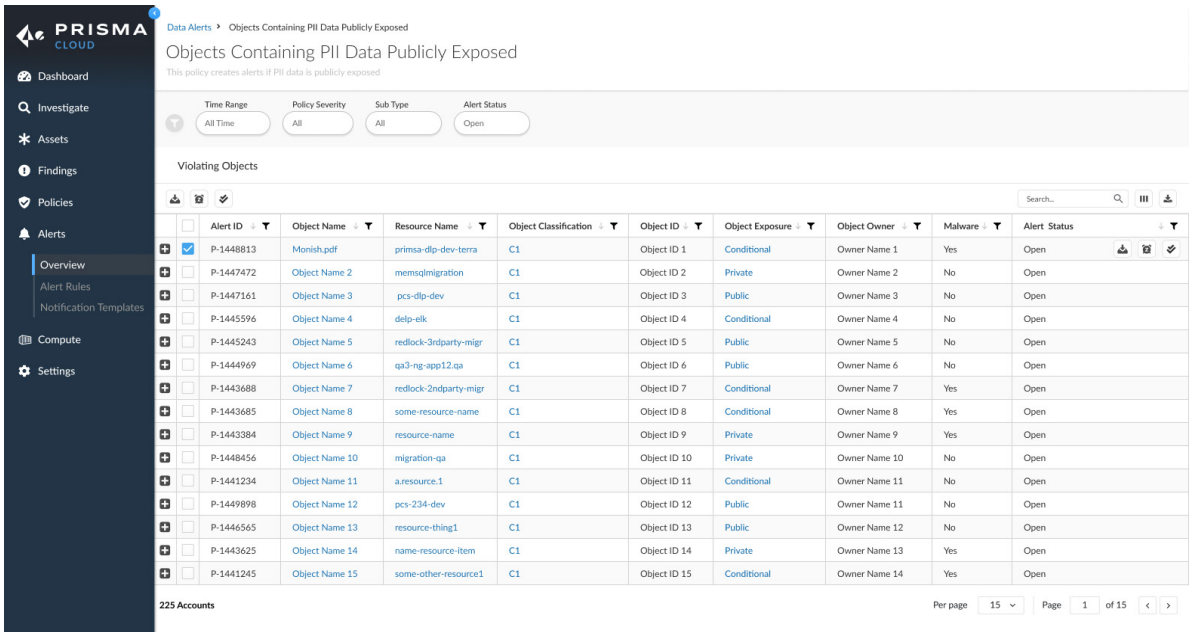

Figure 8. Résultats d'analyse d'objets pour les données personnelles

« En tant que responsable, je peux dormir sur mes deux oreilles, car je sais qu'un outil s'occupe de la surveillance continue pour moi. Mes équipes se sont vraiment approprié l'outil et certains de nos collaborateurs sont sur Prisma Cloud tous les jours. Cela a transformé notre manière de maintenir la conformité et la visibilité. »

– John Hluboky, VP de la sécurité de l'information, Veradigm Health
Lire l'étude de cas complète

À propos de Prisma Cloud

Prisma® Cloud est la plateforme de protection des applications cloud-native (CNAPP) la plus complète du marché. Sa mission : assurer la sécurité et la mise en conformité de vos utilisateurs, applications, données et technologies cloud-native tout au long du cycle de développement sur vos environnements cloud hybrides et multicloud. Au lieu de s'assujettir aux contraintes de sécurité des architectures 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.

Pour en savoir plus, rendez-vous sur notre site web ou visionnez une démo.

paloalto® NETWORKS

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam, Pays-Bas

Téléphone : +31 20 888 1883
www.paloaltonetworks.fr