

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.

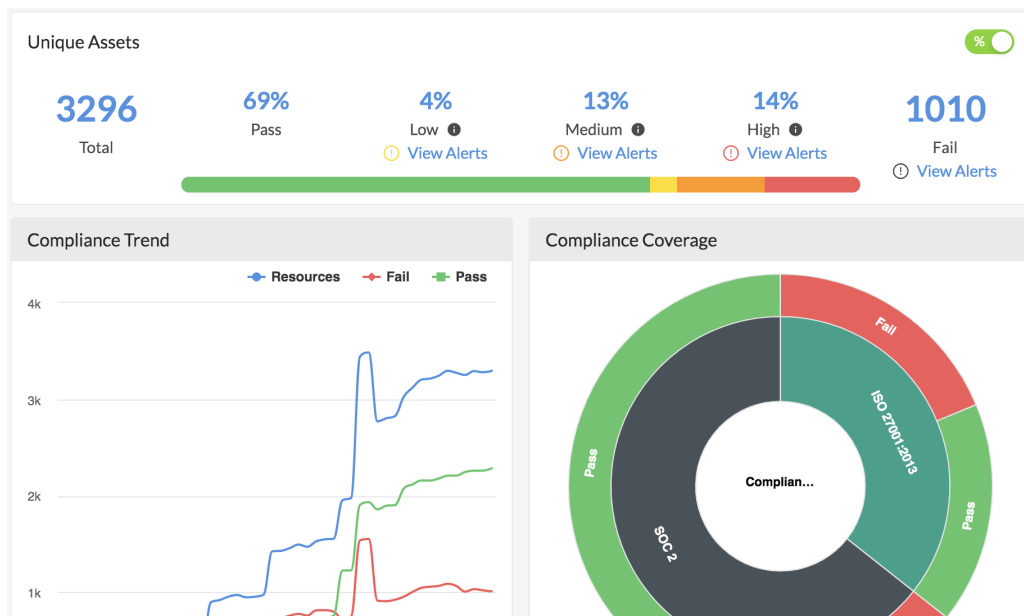


Figure 2. Conformité : tableau de bord

Priorisation contextualisée des risques

À l'inverse des outils silotés qui ne se concentrent que sur des erreurs de configuration individuelles, Prisma Cloud corréle 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.

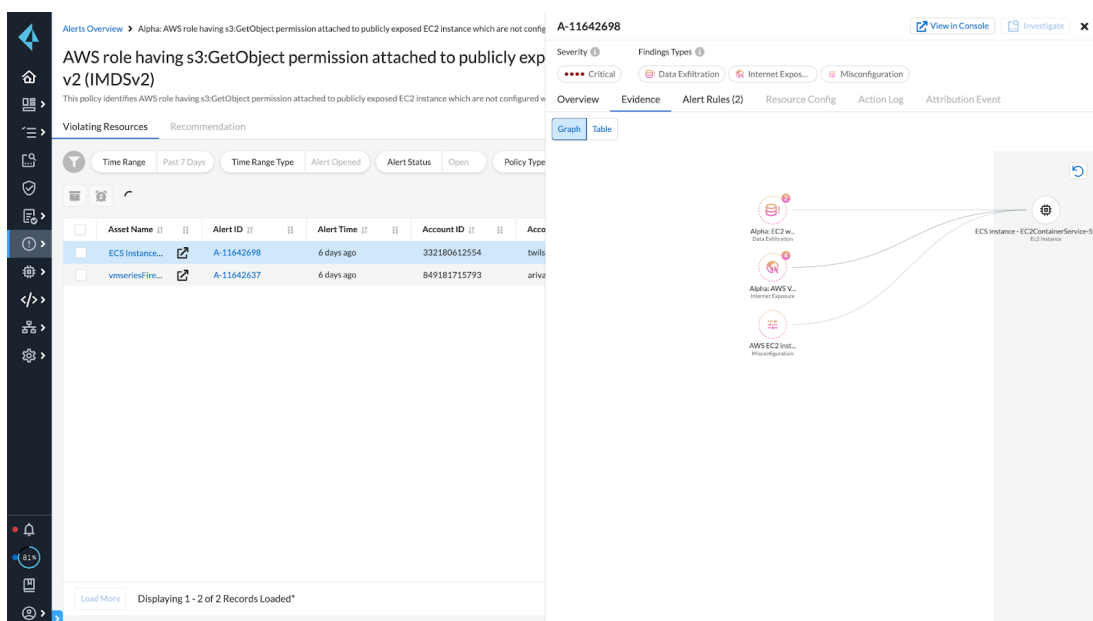


Figure 3. Investigation des alertes liées aux schémas d'attaque

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.

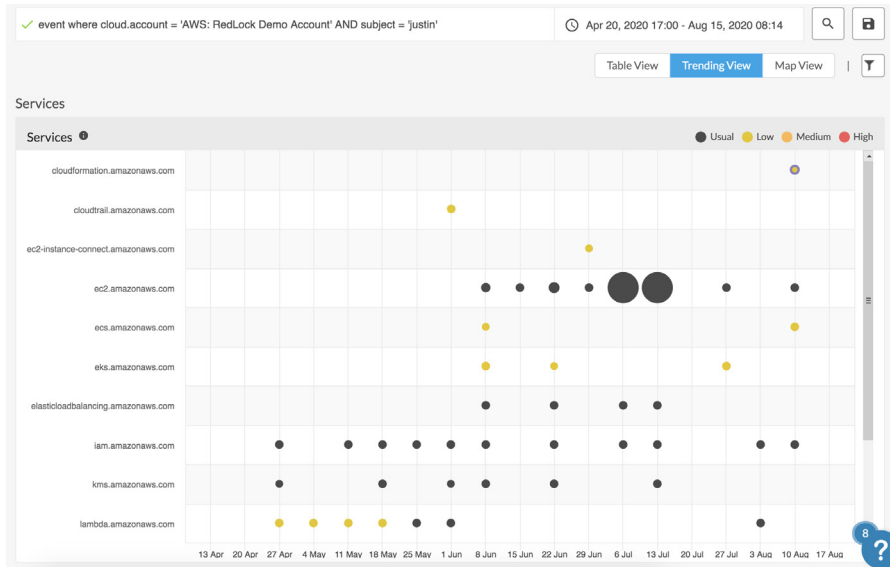


Figure 4. Suivi des activités anormales

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.

Filter(s): Policy Type = Anomaly

Port scan activity (External)

Identifies port scan attempts by inspecting inbound network traffic to your cloud environment. A host outside your environment is scanning one of your cloud hosts. Port scans are a type of discovery attack where a source host is probing a target host across multiple ports, to find out what services are running and to uncover vulnerabilities associated with those services.

Recommendation

1. Review the list of scanned ports to determine the ones to be closed. Reducing the number of ports available decreases the opportunities for adversaries to compromise your cloud resources.
2. Please review and fix any violating policy associated with the target host in the alert, as reported by Prisma Cloud.

Violating Resources

Remediate

ALERT ID	RESOURCE NAME	ACCOUNT	REGION	ALERT STATUS	RATING	OPTIONS								
<input type="checkbox"/> v P-45094	188.166.186.209	Azure: RedLock Demo Account	Azure East US	Open	N/A	<input type="checkbox"/> <input type="checkbox"/>								
<table border="1"> <thead> <tr> <th>SOURCE HOST</th> <th>SOURCE LOCATION</th> <th>TARGET HOST</th> <th>TARGET PORT COUNT</th> </tr> </thead> <tbody> <tr> <td>188.166.186.209</td> <td>Singapore</td> <td>Bastion-Host-2</td> <td>1000</td> </tr> </tbody> </table>		SOURCE HOST	SOURCE LOCATION	TARGET HOST	TARGET PORT COUNT	188.166.186.209	Singapore	Bastion-Host-2	1000					
SOURCE HOST	SOURCE LOCATION	TARGET HOST	TARGET PORT COUNT											
188.166.186.209	Singapore	Bastion-Host-2	1000											
<input type="checkbox"/> > P-44786	185.39.10.14	Azure: RedLock Demo Account	Azure West US	Open	N/A	<input type="checkbox"/> <input type="checkbox"/>								
<input type="checkbox"/> > P-44700	93.174.93.68	Azure: RedLock Demo Account	Azure East US	Open	N/A	<input type="checkbox"/> <input type="checkbox"/>								
<input type="checkbox"/> > P-44405	93.174.93.68	Azure: RedLock Demo Account	Azure West US	Open	N/A	<input type="checkbox"/> <input type="checkbox"/>								
<input type="checkbox"/> > P-44404	93.174.93.68	Azure: RedLock Demo Account	Azure West US	Open	N/A	<input type="checkbox"/> <input type="checkbox"/>								
<input type="checkbox"/> > P-44403	185.39.10.54	Azure: RedLock Demo Account	Azure East US	Open	N/A	<input type="checkbox"/> <input type="checkbox"/>								
<input type="checkbox"/> > P-44354	89.248.172.196	Azure: RedLock Demo Account	Azure East US	Open	N/A	<input type="checkbox"/> <input type="checkbox"/>								
<input type="checkbox"/> > P-44282	89.248.172.196	Azure: RedLock Demo Account	Azure West US	Open	N/A	<input type="checkbox"/> <input type="checkbox"/>								
<input type="checkbox"/> > P-44281	89.248.172.196	Azure: RedLock Demo Account	Azure West US	Open	N/A	<input type="checkbox"/> <input type="checkbox"/>								
<input type="checkbox"/> > P-44280	80.82.77.214	Azure: RedLock Demo Account	Azure East US	Open	N/A	<input type="checkbox"/> <input type="checkbox"/>								

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.

The screenshot displays the 'Violating Resources' section in the Prisma Cloud console. It features a table with columns for Alert ID, Resource Name, Account, and Options. A modal dialog is open over the table, providing a warning and a CLI command to remediate the issue.

ALERT ID ↓↑	RESOURCE NAME ↓↑	ACCOUNT	OPTIONS
P-45089	EC2ContainerService-default-test-EcsSecurityGroup-UUD683S3Z3T4	AWS: RedLo	Remediate
P-44971	launch-wizard-8		
P-44964	launch-wizard-7		
P-44617	launch-wizard-6		
P-44607	k8s-elb-a90cc32b		
P-44585	terraform-202007		
P-44279	launch-wizard-4		
P-44278	launch-wizard-5		
P-44246	Red Hat Enterpris		
P-44239	Red Hat Enterpris		
P-43969	launch-wizard-3		

Warning: Running this command may have an adverse impact on your application.

Message: "This CLI command requires 'ec2:RevokeSecurityGroupIngress' permission. Successful execution will update the security group to revoke the ingress rule records open to internet either on IPv4 or on IPv6 protocol." To resolve the alert from Prisma Cloud's console, add the permission.

```
aws --region us-east-2 ec2 revoke-security-group-ingress --group-id sg-0c7777a30125a8180 --ip-permissions [{"IpProtocol": "tcp", "FromPort": 80, "ToPort": 80, "IpRanges": [{"CidrIp": "0.0.0.0/0"}]}];
```

Buttons: Copy to Clipboard, View Resource Config, Execute Command

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.

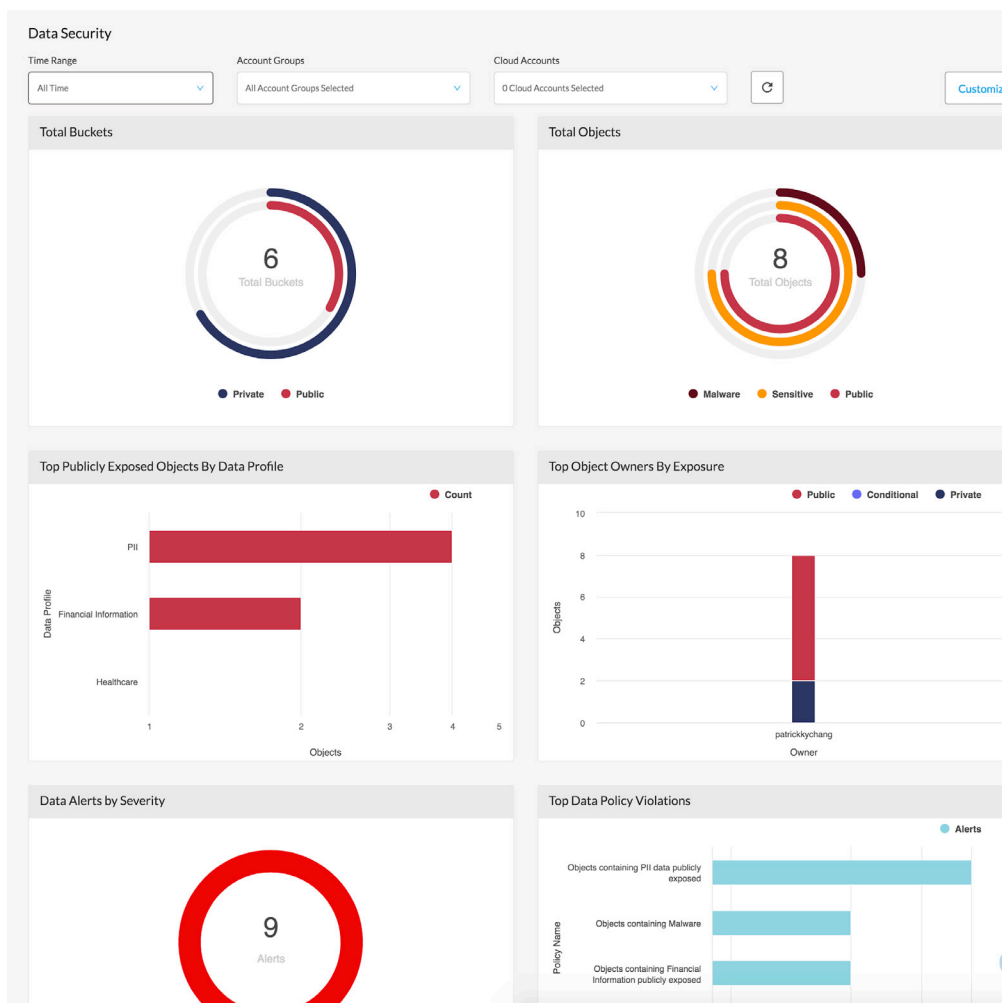


Figure 7. Sécurité des données S3 : tableau de bord

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.

PRISMA CLOUD

Data Alerts > Objects Containing PII Data Publicly Exposed

Objects Containing PII Data Publicly Exposed

This policy creates alerts if PII data is publicly exposed

Time Range: All Time | Policy Severity: All | Sub Type: All | Alert Status: Open

Violating Objects

Alert ID	Object Name	Resource Name	Object Classification	Object ID	Object Exposure	Object Owner	Malware	Alert Status
P-1448813	Monish.pdf	prisma-dlp-dev-terra	C1	Object ID 1	Conditional	Owner Name 1	Yes	Open
P-1447472	Object Name 2	memsmigration	C1	Object ID 2	Private	Owner Name 2	No	Open
P-1447161	Object Name 3	pcs-dlp-dev	C1	Object ID 3	Public	Owner Name 3	No	Open
P-1445596	Object Name 4	delp-elk	C1	Object ID 4	Conditional	Owner Name 4	No	Open
P-1445243	Object Name 5	redlock-3rdparty-migr	C1	Object ID 5	Public	Owner Name 5	No	Open
P-1444969	Object Name 6	qa3-ng-app12.qa	C1	Object ID 6	Public	Owner Name 6	No	Open
P-1443688	Object Name 7	redlock-2ndparty-migr	C1	Object ID 7	Conditional	Owner Name 7	Yes	Open
P-1443685	Object Name 8	some-resource-name	C1	Object ID 8	Conditional	Owner Name 8	Yes	Open
P-1443384	Object Name 9	resource-name	C1	Object ID 9	Private	Owner Name 9	Yes	Open
P-1448456	Object Name 10	migration-qa	C1	Object ID 10	Private	Owner Name 10	No	Open
P-1441234	Object Name 11	a.resource.1	C1	Object ID 11	Conditional	Owner Name 11	No	Open
P-1449898	Object Name 12	pcs-234-dev	C1	Object ID 12	Public	Owner Name 12	No	Open
P-1446565	Object Name 13	resource-thing1	C1	Object ID 13	Public	Owner Name 13	No	Open
P-1443625	Object Name 14	name-resource-item	C1	Object ID 14	Private	Owner Name 14	Yes	Open
P-1441245	Object Name 15	some-other-resource1	C1	Object ID 15	Conditional	Owner Name 15	Yes	Open

225 Accounts | Per page: 15 | Page: 1 of 15

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](#).