CHECK POINT™
YOU DESERVE THE BEST SECURITY

Cloud Infrastructure Entitlement Management

Droits d'accès et identités Zero Trust

Il existe de nombreux facteurs permettant de déterminer les mesures les plus efficaces pour protéger un actif dans le cloud. Par ailleurs, la protection de ces actifs devient de plus en plus complexe à mesure que l'environnement cloud s'agrandit et que de nouveaux utilisateurs et charges de travail sont ajoutés. Ainsi, les équipes DevOps accordent souvent des autorisations d'accès excessives aux actifs dans le cloud, agrandissant alors la surface attaquable. Les outils de gestion des identités et des accès (IAM) traditionnels, les autorisations préconfigurées dans les paramètres développeur et la configuration manuelle des autorisations ne suffisent plus pour protéger le cloud à l'échelle et à la vitesse des DevOps. Les entreprises ont besoin d'une solution de gestion des droits d'accès à l'infrastructure cloud (CIEM) pour automatiser et déployer des modèles basés sur le principe du moindre privilège afin de réduire la surface d'attaque et d'atteindre une sécurité Zero Trust.

Visualiser, détecter, prioriser et corriger les risques IAM

Grâce à Check Point CloudGuard, optimisez la gestion des accès utilisateurs et charges de travail et des privilèges pour accorder uniquement les autorisations nécessaires et d'appliquer rapidement des recommandations pour les rôles possédant trop d'autorisations d'accès. CloudGuard vous fournit une visibilité sur les autorisations effectives, identifie les droits d'accès trop permissifs et vous suggère des mesures de correction.

La technologie Check Point CloudGuard CIEM optimise la gestion des privilèges, les accès utilisateurs et les accès aux charges de travail :

Avec CloudGuard, vous obtenez une meilleure visibilité sur les autorisations effectives des utilisateurs et des actifs avec des recommandations concernant les rôles ayant trop d'autorisations. Ces informations vous permettent ensuite de mettre facilement en œuvre une gestion des droits d'accès basée sur le principe du moindre privilège.

La technologie CIEM CloudGuard vous aide à identifier et à gérer les autorisations en :

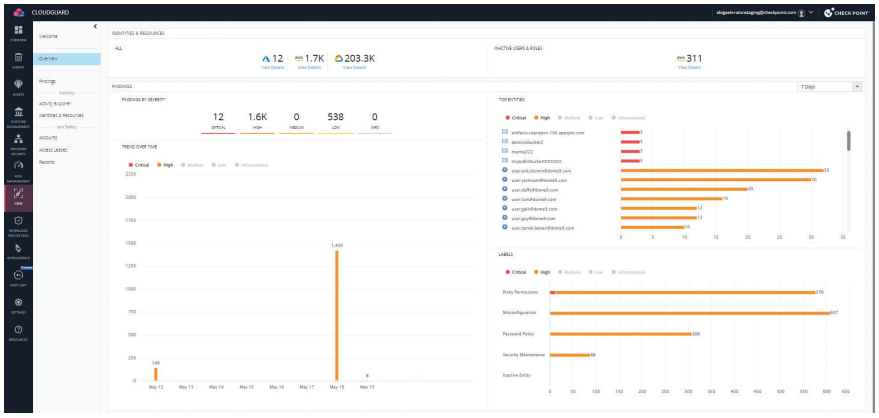
- visualisant les autorisations effectives des utilisateurs et des services cloud ;
- détectant les rôles non utilisés, les rôles avec trop d'autorisations et les droits d'accès potentiellement risqués ;
- générant automatiquement des recommandations de rôles basées sur le principe du moindre privilège en fonction de l'usage réel.

Comprendre vos autorisations et appliquer le principe du moindre privilège dans tous vos clouds

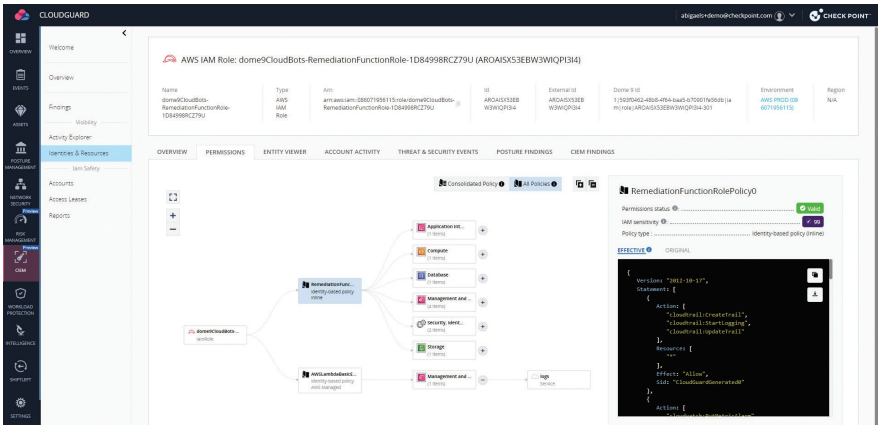
Comprenez les autorisations effectives des utilisateurs et des services cloud, identifiez l'exposition et les risques et générez automatiquement des recommandations explicites sur les rôles selon le principe du moindre privilège pour réduire le nombre d'accès et révoquer les autorisations non utilisées.

Simplifier la gestion des droits d'accès pour réduire le risque

Les capacités CIEM de CloudGuard permettent de supprimer les complexités inhérentes à la correction des identités et droits d'accès mal configurés. En calculant automatiquement les mesures les plus efficaces pour chaque actif et en automatisant la gestion des accès basée sur le principe du moindre privilège, CloudGuard aide les utilisateurs à minimiser la surface d'attaque.



Le CIEM de CloudGuard s'appuie sur l'apprentissage machine pour analyser les journaux d'activité des comptes afin de repérer les anomalies et de suggérer les bons paramètres de stratégie pour assurer un accès basé sur le principe du moindre privilège.



Avec le CIEM de CloudGuard, les entreprises peuvent :

- Réduire le coût total de possession (TCO)
- Automatiser la correction des risques liés aux identités
- Implémenter automatiquement le principe du moindre privilège
- Gagner en visibilité sur les droits d'accès en analysant les autorisations par apprentissage machine
- Appliquer les bonnes pratiques à suivre concernant le principe du moindre privilège SANS impact sur les fonctionnalités
- Arrêter de chercher et de supprimer manuellement les comptes utilisateurs redondants

Solution de sécurité unifiée pour réduire les risques dans le cloud

Les capacités de CIEM font partie des outils de sécurité cloud native unifiée fournis dans CloudGuard. Check Point est conscient que l'unification est un moyen de parvenir à une fin. C'est pour cela que notre CIEM tire sa force du moteur Effective Risk Management. Ce moteur regroupe tous les résultats de la gestion de la posture, de l'analyse des vulnérabilités et des logiciels malveillants ainsi que du CIEM, pour fournir un score à chaque risque basé sur les priorités et l'architecture de l'entreprise. CloudGuard hiérarchise ensuite la correction des risques pour l'entreprise afin de permettre aux équipes de sécurité d'assurer un niveau de protection optimal.

Contexte approfondi, sécurité concrète et prévention plus intelligente

Du **code au cloud**, Check Point CloudGuard fournit une sécurité cloud native, **automatisée** et unifiée dans toutes vos applications, charges de travail et réseaux : **gérez les risques, maintenez votre posture de sécurité et prévenez les menaces** avec le contexte approprié, à la vitesse du cloud et à grande échelle. L'approche axée sur la prévention de CloudGuard protège les applications et les charges de travail dans tout le cycle de développement logiciel. Elle comprend un moteur de gestion efficace des risques qui hiérarchise automatiquement les mesures correctives pour permettre aux utilisateurs de se concentrer sur les risques de sécurités les plus importants.

Pour plus d'informations à propos de CloudGuard, consultez www.checkpoint.com/cloudguard

