Guide des outils de gestion de la sécurité du cloud

paloalto NETWORKS | PRISMA BY PALO ALTO NETWORKS

Sommaire

PRISMA BY PALO ALTO NETWORKS

Une bonne hygiène de sécurité du cloud, c'est d'abord une visibilité complète sur la sécurité et la conformité de chaque ressource déployée dans votre environnement. Dans une configuration monocloud, les outils de surveillance et d'audit de votre fournisseur cloud permettent généralement d'obtenir ce niveau de visibilité. Des solutions externes peuvent alors servir à combler d'éventuelles lacunes, notamment au niveau de la détection des menaces. Mais dès que l'on entre dans l'univers du multicloud, le maintien d'une sécurité robuste devient un tout autre défi.

Il est en effet beaucoup plus difficile d'obtenir une visibilité centralisée et d'homogénéiser les politiques et les règles de conformité dans un environnement multicloud. Idem pour la détection des menaces et la correction rapide des vulnérabilités, compte tenu de la nature complexe et protéiforme des menaces ciblant les architectures distribuées et multicouches.

Vous pouvez toutefois relever ces défis. Et non seulement vous le pouvez, mais vous le devez : il en va de votre capacité à concrétiser les avantages des architectures multicloud sans compromettre la sécurité. Ce guide vous invite à découvrir les problématiques spécifiques à la gestion de la sécurité du cloud (CSPM, Cloud Security Posture Management) dans une architecture multicloud. Nous verrons ensuite comment développer des outils et une stratégie CSPM capables de résoudre efficacement ces problématiques autour de différents axes : visibilité centralisée, gestion de la conformité, détection des menaces, protection des données, automatisation dédiée aux environnements multicloud, etc.

Problématiques spécifiques à la sécurité multicloud

Une approche CSPM monocloud ne peut pas simplement monter en puissance pour répondre aux besoins d'une architecture multicloud. Sécuritairement parlant, ces deux types d'environnements diffèrent fondamentalement à bien des égards.

Données disparates et distribuées

Dans un environnement multicloud, les données sont réparties sur plusieurs clouds. Vous pouvez par exemple stocker vos big data dans un cloud pour bénéficier de tarifs avantageux, tout en conservant vos données actives dans un cloud plus coûteux mais qui offre un accès plus rapide. Vous pouvez également distribuer des données entre différentes régions pour les placer au plus près des utilisateurs.

Lorsque des données sont distribuées, il est plus difficile d'assurer leur sécurité et de les protéger contre les malwares. Vous devez notamment veiller à la mise en place de règles IAM (gestion des identités et des accès) appropriées pour chaque datastore sur chaque cloud. De même, tous les compartiments (buckets) doivent être configurés selon certaines règles, sachant que chaque fournisseur de services cloud (CSP) place le curseur différemment dans ce domaine.

Applications distribuées

Les applications et les outils qui les sous-tendent, sont souvent distribués au sein d'environnements multicloud. Par exemple, vous pouvez exécuter des instances redondantes de la même application dans différents clouds afin que celle-ci reste disponible en cas de défaillance d'un cloud. Vous pouvez également héberger une chaîne d'outils de développement dans un cloud, mais déployer vos applications dans un autre.

Dans ce contexte, une CSPM efficace nécessite de comprendre l'environnement de sécurité de tous les services et ressources individuels qui composent l'application. Il ne suffit pas de surveiller séparément chaque instance d'une application multicloud. Vous devez savoir quel impact le niveau de sécurité de telle instance peut avoir sur telle autre. Étant donné les interactions entre ces instances, la compromission d'un environnement cloud peut-elle par exemple s'étendre à un autre ? Pour éviter ce genre de risque, il faut constamment vérifier que la configuration des applications respecte bien les règles de sécurité en place.

De même, le déploiement d'applications sur plusieurs clouds étant plus complexe, il devient plus crucial d'intégrer la sécurité à chaque étape du pipeline de développement, plutôt qu'après coup. Une fois l'application en production, il faut beaucoup plus de temps pour corriger une vulnérabilité, a fortiori si le code vulnérable s'étend sur de multiples environnements. En intégrant les contrôles de sécurité au pipeline de développement, vous réduisez le risque associé à la correction d'une application en production.

Multitude de menaces et de vulnérabilités

Usages abusifs d'API en interne, cryptojacking, exfiltration de données, malwares dans les images de containers, injections SQL dans les applications… les menaces actuelles sont si diverses qu'aucun système de détection ne peut à lui seul les neutraliser toutes. Les analyses anti-malware et les audits de configuration ne suffisent pas non plus à protéger vos environnements. Une protection efficace nécessite de recueillir les données CTI d'une variété de sources, de les analyser et d'établir des recoupements avec des menaces connues. Aux politiques basées sur des règles doivent également s'ajouter des politiques orientées machine learning, seules capables de détecter les menaces inconnues.

Multitude d'utilisateurs et d'autorisations

Dans les environnements monocloud, le maintien d'une bonne hygiène IAM est une pratique exigeante pour les équipes de sécurité. Entre les politiques gérées par le CSP ou par les utilisateurs d'une part, et les politiques rattachées à d'autres groupes, rôles, ressources ou listes de contrôle d'accès d'autre part, la diversité des règles rend difficile l'application du principe du moindre privilège.

Dans les environnements multicloud, les autorisations et les droits utilisateurs diffèrent selon les CSP, ce qui ajoute encore un degré de complexité. Non seulement vous devez surveiller des configurations IAM différentes pour chaque cloud, mais vous devez également être en mesure de cadrer les rôles et autorisations utilisateur définis par les différents CSP sur les besoins de chaque utilisateur. Vous ne pouvez pas vous contenter de vérifier les identifiants d'un même utilisateur sur tous les clouds.

Élargissement de la surface d'attaque

Qui dit plus de clouds, dit plus de comptes, de politiques de contrôle d'accès, de services, etc. Résultat : la surface d'attaque s'étend et les opportunités se multiplient pour les attaquants (ressources mal configurées, autorisations trop permissives, vulnérabilités du code, etc.).

Parallèlement, l'absence de visibilité et de contrôle centralisés dans un environnement multicloud rend les vulnérabilités et les menaces plus difficiles à détecter. Lorsque les outils d'un CSP ne vous permettent pas de surveiller et d'auditer toutes les configurations de tous vos services, il devient compliqué de prévenir les erreurs de configuration pouvant conduire à une compromission.

Gestion de la sécurité multicloud : quatre fonctionnalités indispensables

La résolution des problématiques de sécurité multicloud que nous venons d'évoquer passe par l'adoption d'une stratégie et d'outils CSPM agissant simultanément sur quatre tableaux.

Conformité, gouvernance et visibilité totale

Le fondement d'une approche efficace de la sécurité multicloud réside dans la capacité à surveiller et à auditer en permanence toutes les ressources de tous les CSP. Chaque fois qu'un nouveau service ou workload est déployé ou qu'une configuration est modifiée, vos outils doivent pouvoir détecter et analyser la mise à jour pour s'assurer de sa conformité aux exigences et bonnes pratiques de sécurité.

En cas de non-conformité, ces outils doivent signaler l'anomalie à votre équipe et proposer des actions correctives. Mise à jour d'une adresse IP mal saisie, ajout d'une déclaration manquante à une politique IAM… vos outils doivent également pouvoir effectuer eux-mêmes des remédiations simples pour résoudre ces problèmes sans que les équipes de sécurité n'aient à intervenir.

Pour réduire le nombre d'alertes générées dans l'environnement d'exécution (runtime), il est également important de bloquer toute mise en production de configurations non sécurisées. Enfin, les outils CSPM doivent être capables de détecter les erreurs de configuration dans les modèles IaC (Infrastructure as Code) et d'appliquer des politiques non seulement dans l'environnement d'exécution, mais aussi en amont, tout au long du cycle de développement logiciel.

Détection complète des menaces

Face à la complexité des menaces ciblant les environnements multicloud, les outils CSPM doivent collecter les données CTI d'une variété de sources pour dresser un constat précis des risques en présence. Ces sources comprennent les configurations IaC, les images de containers et les images de machines virtuelles (VM) cloud, déjà passées au crible par de nombreuses équipes à la recherche de vulnérabilités.

Ceci dit, il ne suffit pas d'analyser ces éléments pour obtenir des informations complètes sur les menaces et les détecter. Votre entreprise doit également maintenir une Threat Intelligence haute-fidélité pour identifier les menaces émergentes et évaluer leur niveau de gravité. Pour placer les menaces en contexte et évaluer leur impact potentiel, vous devez pouvoir détecter les anomalies sur le réseau et les corréler avec d'autres types de données CTI. Idem avec les données d'analyse du comportement des utilisateurs et des entités (UEBA).

Autrement dit, toute détection des menaces nécessite de passer de multiples sources de données au peigne fin, puis de corréler et de contextualiser ces données. L'intérêt est non seulement d'identifier les menaces dans des environnements complexes et multicouches, mais aussi d'aider les équipes à identifier rapidement les risques et les menaces à traiter en priorité. Seule une détection complète des menaces permet d'associer les anomalies du réseau à une image de container non sécurisée, par exemple, ou de déterminer quel compte est à l'origine d'une compromission. Lorsque votre équipe cerne les menaces plus rapidement, vous pouvez aussi les neutraliser plus rapidement, ce qui réduit le délai moyen de résolution.

Sécurité intégrée des données

Personnelles ou non, quel que soit le type de données que vous stockez dans le cloud, vous devez adopter une approche de sécurité multifacette, seule garante d'une visibilité approfondie sur l'état et le statut de ces données. La première étape consiste à surveiller la configuration de chaque compartiment rattaché à vos différents services de stockage. L'objectif : veiller à ce que les données ne soient pas accidentellement exposées à des utilisateurs ou des applications non autorisés. Parallèlement, vous devez examiner le contenu de ces compartiments pour vérifier s'ils contiennent des données personnelles soumises à des règlementations spécifiques ou à d'autres exigences, RGPD en tête.

Autre aspect important, mais souvent négligé : la détection des malwares dans les données au repos. Identifier des malwares exige non seulement de passer au crible les compartiments de stockage, mais également les bases de données, les systèmes de fichiers de VM, les volumes de stockage des containers, voire les systèmes de fichiers éphémères des containers.

Enfin, parce que la sécurité des données cloud nécessite souvent de trouver le juste équilibre entre protection et disponibilité, vos outils CSPM doivent vous permettre de calculer le risque d'exposition des données et de formuler des recommandations pour limiter l'impact potentiel d'une compromission. Quel est le niveau de contrôle d'accès le plus adapté au caractère sensible de vos données cloud ? Devriez-vous définir des politiques d'accès moins granulaires pour en simplifier la gestion ? Des outils capables de calculer le risque d'exposition vous aideront à répondre à ce type de questions.

Automatisation du traitement des alertes

Par définition, les environnements multicloud sont complexes et de grande taille. D'où l'impossibilité de mettre en œuvre les contrôles et processus de sécurité que nous venons d'évoquer sans des outils capables de détecter et neutraliser automatiquement les risques.

Cela ne veut pas dire qu'une gestion de la sécurité multicloud doit être totalement automatisée. Une intervention humaine sera toujours nécessaire pour répondre à des incidents de sécurité complexes ou pour évaluer des risques trop nébuleux pour que vos outils CSPM puissent les gérer seuls. Toutefois, la surveillance, les audits et les mesures correctives de routine doivent être automatisés pour permettre à votre équipe de se focaliser sur ses missions prioritaires.

PRISMA BY PALO ALTO NETWORKS

Limites des outils des fournisseurs cloud

Les CSP proposent une variété d'outils permettant de gérer certains des risques décrits dans ce guide. Par exemple, des services de protection des données comme Amazon Macie® et Google Cloud DLP peuvent évaluer les vulnérabilités des données dans les compartiments de stockage et les bases de données. De leur côté, des outils de surveillance tels qu'Amazon CloudWatch et Azure® de Microsoft Monitor peuvent générer des alertes pour certains types d'évènements signalant d'éventuels risques de sécurité. Très utiles, ces instruments peuvent renforcer votre arsenal d'outils CSPM. Ceci dit, ils présentent deux grandes lacunes :

1. **Ils ne sont pas conçus pour constituer des solutions CSPM complètes et de bout en bout**. Ils peuvent auditer certains fichiers de configuration ou détecter des données personnelles dans certains datastores, mais ils sont incapables d'analyser en permanence les images de containers, détecter les anomalies réseau ou neutraliser automatiquement les menaces.
2. **Ils ne fonctionnent que dans le cloud du CSP en question**. En d'autres termes, les outils Google ne fonctionnent que sur Google Cloud, ceux d'Amazon uniquement sur Amazon Web Services, ceux de Microsoft exclusivement sur Azure, etc.

Bref, le recours aux seuls outils des CSP dans un environnement multicloud revient à jongler entre de multiples outils disparates, avec toutes les difficultés et l'inefficacité que cela implique. Vous n'avez en effet aucun moyen de corréler efficacement les données entre tous ces outils. Et faute de corrélation, impossible de détecter toutes les menaces à partir de toutes les sources de données disponibles dans votre environnement multicloud.

Conclusion

En résumé, une sécurité multicloud efficace exige une plateforme complète et capable de détecter en permanence les erreurs de configuration, les vulnérabilités et les menaces, puis de les signaler avec une extrême précision.

Prisma® Cloud par Palo Alto Networks offre l'automatisation et la visibilité centralisée nécessaires pour relever efficacement les défis de sécurité des environnements multicloud. En ingérant les données des journaux de flux, de configuration et d'audit stockés sur chacun des clouds de votre écosystème, Prisma Cloud fournit une vue centralisée qui permet à vos équipes de surveiller la sécurité et l'état de conformité de tout votre environnement.

Et parce que Prisma Cloud permet de détecter les activités suspectes et d'évaluer leur impact potentiel, cette solution aide votre équipe à cerner la gravité de chaque menace et à agir en conséquence. Avec Prisma Cloud, vous ne perdez plus votre temps à deviner quelles menaces doivent être traitées en priorité, ni à essayer d'identifier la cause racine d'incidents de sécurité complexes.

Les fonctionnalités Prisma Cloud de remédiation automatisée peuvent résoudre rapidement et automatiquement une grande partie des erreurs de configuration impactant la sécurité. Votre équipe n'a alors plus qu'à suivre l'avancement de leur résolution sur un tableau de bord centralisé.

Pour en savoir plus sur Prisma Cloud et sa capacité à aider votre équipe à gérer la sécurité d'environnements multicloud complexes, découvrez la plateforme en action ou demandez un rendez-vous avec un expert Palo Alto Networks.

paloalto NETWORKS

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

Téléphone : +31 20 888 1883

www.paloaltonetworks.fr

prisma_eb_guide-to-cloud-security-posture_042621-fr