

Le meilleur niveau de sécurité dans le cloud

Les outils de sécurité conventionnels ne permettent pas d'obtenir une sécurité complète pour les environnements multi-cloud, à la complexité toujours croissante. Avec Prisma Cloud, Palo Alto Networks fournit désormais une plateforme de sécurité cloud native innovante à gestion centralisée pour tous les types de réseaux en cloud imaginables.

Les workloads cloud connaissent une croissance constante. En même temps, la complexité des environnements cloud s'accroît en permanence, tandis que les cycles de développement et des applications se font plus courts. En conséquence, chaque organisation voit augmenter sa responsabilité en matière de protection de ses biens numériques. Une approche efficace pour améliorer la sécurité des réseaux en cloud consiste à associer des facteurs tels que la prévention et la transparence.

Prisma Cloud de Palo Alto Networks est une plateforme de sécurité cloud native (CNSP) complète qui protège les applications, les données et les technologies comme les containers au moyen de fonctions de sécurité et de conformité leaders dans le secteur, pendant toute la durée du cycle de vie dans les environnements multi-cloud. Prisma Cloud repose pour cela sur cinq piliers : gestion du niveau de sécurité du cloud (CSPM), protection des workloads cloud (CWPP), gestion des droits d'accès à l'infrastructure (CIEM), sécurité du réseau (CNS) ainsi que sécurité selon les approches DevSecOps et Shift Left.

CSPM: gérer le niveau de sécurité du cloud

Une sécurité de cloud efficace nécessite d'avoir une vue d'ensemble complète sur toutes les ressources utilisées de tous les prestataires de cloud impliqués. Un inventaire global constitue alors la base de la gestion du niveau de sécurité du cloud. Le module CSPM de Prisma Cloud surveille et consigne les ressources en matière de configuration et de conformité. Pour cela, la solution analyse et normalise les données de journal et d'audit des différentes sources de données du cloud.

L'analyse des comportements des utilisateurs et des objets, associée à la surveillance des charges de travail et des réseaux, permet de détecter les activités suspectes. Les connaissances ainsi acquises – renforcées par un apprentissage automatique – sont ensuite combinées les unes aux autres avant d'être évaluées. Ainsi, les risques et les problèmes de sécurité des ressources utilisées deviennent visibles de façon centralisée. Prisma Cloud aide les responsables de la sécurité à corriger ces problèmes en leur soumettant des propositions et en mettant automatiquement en œuvre les mesures nécessaires sur la base de consignes.

CWPP: protéger les workloads cloud

Les entreprises disposent aujourd'hui d'une large palette d'outils et de technologies afin d'exploiter leurs workloads dans le cloud et de mettre des applications modernes à disposition. En complément, elles utilisent souvent une combinaison de machines virtuelles, d'offres de Platform as a Service, de containers et de fonctions sans serveur pour des tâches spécifiques. Toutes ces workloads doivent être protégées.

Prisma Cloud intègre sous un même toit toutes les fonctions d'une plateforme de sécurité des workloads cloud complète. Un framework d'agents homogène surveille pour cela l'ensemble du cycle de vie des applications. Les entreprises peuvent ainsi intégrer la gestion des vulnérabilités et la conformité dans leurs processus d'intégration et de déploiement continus. Les référentiels de codes et les registres de containers sont surveillés en permanence.

La solution observe le comportement des workloads sur la base de profils, par exemple pour les systèmes de processus, de réseau et de fichiers. Ainsi, des directives runtime permettent de protéger les applications et



