GESTION DE LA SÉCURITÉ À GRANDE ÉCHELLE

CONSIDÉRATIONS RELATIVES À LA PLATEFORME CNAPP (CLOUD NATIVE APPLICATION PROTECTION PLATFORM)

RÉSUMÉ

Les entreprises de toutes tailles adoptent la transformation numérique pour acquérir un avantage concurrentiel. Les équipes DevOps jouent un rôle important dans ce processus, car leurs efforts ont une incidence immédiate sur l'entreprise. Cependant, les SecOps doivent s'assurer que les risques de sécurité des applications natives en nuage sont atténués à la fois dans les phases de développement et de test avant que les applications ne soient mises en production. Le défi est d'autant plus grand que l'architecture conteneurisée et de microservices sous-jacente des applications natives en nuage entraîne une exposition incrémentielle aux menaces, étant donné que des centaines, voire des milliers d'instances sont généralement déployées. Le contraste est frappant avec les applications patrimoniales et monolithiques du passé, plus simples dans leur conception, mais qui ne sont pas aussi agiles ni massivement évolutives.

Vers qui les entreprises se tournent-elles pour garantir les niveaux de sécurité les plus élevés pour les applications en nuage? En outre, qu'est-ce qui est le plus risqué : les pipelines d'intégration et de livraison continues de l'entreprise (CI/CD), les considérations de conformité et d'autres violations qui mènent à des violations à la vie privée? C'est probablement tout cela et plus encore. Les plateformes de protection des applications natives du nuage (CNAPP) émergent pour relever ces défis de sécurité. Cependant, toutes les solutions ne sont pas égales. Ce document définit les caractéristiques, les fonctions et les capacités globales de la CNAPP, les objectifs qu'elle poursuit et les cas d'utilisation spécifiques dans lesquels elle peut avoir une incidence mesurable.

DÉFINITION D'UN CNAPP COMPLET

La CNAPP intègre et automatise la sécurité infonuagique, en rassemblant toutes les fonctionnalités requises dans une plateforme unique et intégrée et, surtout, sur l'ensemble du cycle de vie d'une application native en nuage, couvrant le développement, les tests, le déploiement et la gestion continue. Il s'agit d'une rupture par rapport aux meilleures approches des années précédentes, qui favorisaient la fragmentation et les problèmes de gestion en raison de la prolifération des solutions de sécurité ponctuelles. Cette dernière solution est devenue intenable pour les entreprises, d'où la nécessité de gérer

de multiples tableaux de bord et alertes. Compte tenu de la nature complexe des applications natives en nuage, ce phénomène engendre des postures de gestion réactives et des lacunes subséquentes en matière de visibilité et de couverture de sécurité correspondante.

En approfondissant, l'origine de la CNAPP peut être retracé à un désir de consolider les outils disparates qui facilitent la surveillance, l'alerte, la posture et le contrôle de la sécurité des nuages, ainsi que la prévention et l'atténuation des violations si elles se produisent. En comparaison, les plateformes de protection des charges de travail en nuage (CWPP) utilisent un agent sur une machine de calcul physique ou virtuelle et des conteneurs, ciblant uniquement la sécurité des charges de travail. Son inconvénient est qu'il ne peut pas toujours être appliqué au moment de l'exécution d'une application native en nuage au cours du cycle de développement.

Moor Insights & Strategy affirme qu'une CNAPP complet comprend quatre éléments essentiels.

1. Elle doit sécuriser toute architecture de microservices, tout conteneur et tout déploiement sans serveur.
2. Elle doit inclure la fonctionnalité CWPP mentionnée précédemment comme base et deux éléments supplémentaires : la gestion de la posture de sécurité en nuage (CSPM, pour Cloud Security Posture Management) et la gestion des droits d'utilisation de l'infrastructure en nuage (CIEM, pour Cloud Infrastructure Entitlement Management). La CSPM détermine et traite les risques lors de l'application de l'automatisation à l'observabilité et aux menaces qui en découlent.
3. La CIEM vise à fournir une analyse en temps réel des alertes générées par les applications ainsi que par le matériel sous-jacent.
4. Les CNAPP doivent couvrir l'ensemble du cycle de vie d'une application native en nuage, du développement à la production en passant par les tests. Ce faisant, la CNAPP détecte idéalement les vulnérabilités dès le début du cycle de développement et surveille en permanence l'exécution pour détecter les vulnérabilités ou les mauvaises configurations.

LA VALEUR DE LA CNAPP

Les avantages du déploiement d'une CNAPP sont incommensurables. La consolidation des fonctionnalités de sécurité en nuage simplifie la gestion des opérations de sécurité (SecOps). De plus, la visibilité des angles morts est considérablement améliorée, ce qui permet de réduire le nombre de failles de sécurité. Il en résulte un déploiement plus rapide des applications natives de l'informatique en nuage, ainsi qu'une réduction des violations coûteuses de la conformité et des perturbations de l'activité, ce qui se traduit par une amélioration de la rentabilité de l'entreprise. La CNAPP peut être utile à toutes les organisations, mais surtout à celles qui se trouvent dans des environnements très réglementés, tels que les secteurs de la fabrication, des services financiers, de l'assurance, des soins de santé et des produits pharmaceutiques.

APPEL À L'ACTION

Les applications natives en nuage offrent l'évolutivité et les fonctionnalités nécessaires aux entreprises modernes, mais garantir la sécurité tout en permettant aux équipes DevOps d'innover peut s'avérer difficile. Les surfaces de menaces continueront de croître compte tenu de la nature hautement distribuée des nouveaux modèles de travail hybride ainsi que de l'adoption et du déploiement d'applications natives en nuage. Les entreprises ont besoin d'une approche simplifiée pour gérer la sécurité des applications natives en nuage tout au long de leur cycle de vie, et la CNAPP est prête à répondre à ce besoin. De plus, toutes les CNAPP ne sont pas créées égales. Il convient donc de s'assurer que toute plateforme offre les capacités et les fonctionnalités nécessaires pour couvrir ce qui est requis du point de vue de la sécurité de l'informatique en nuage.

Moor Insights & Strategy estime que Cisco est bien positionnée pour fournir ce que les entreprises attendent d'une CNAPP avec Panoptica, une solution de sécurité des applications multinuage d'Outshift par Cisco. Panoptica offre une protection complète du cycle de vie, du développement à l'exécution, couvrant les applications et l'infrastructure qui comprend des conteneurs, des environnements sans serveur et des environnements d'interface de programmation d'applications (API). Associées à AppDynamics de Cisco, les entreprises peuvent également observer et traiter les risques de sécurité par le biais d'une correction automatisée. Toutes ces capacités peuvent faciliter la collaboration entre les développeurs et les équipes de sécurité, en éliminant les frictions dans le processus de développement.

Pour en savoir plus, visitez le site Web des solutions d'applications Cisco Reimagine.

CONTRIBUTEUR

Will Townsend, vice-président et analyste principal, Pratiques de réseau et de sécurité chez Moor Insights & Strategy

ÉDITEUR

Patrick Moorhead, président, fondateur et analyste en chef chez Moor Insights & Strategy

DEMANDES DE RENSEIGNEMENTS

Communiquez avec nous si vous souhaitez discuter de ce rapport. Un représentant de Moor Insights & Strategy vous répondra rapidement.

CITATIONS

Des extraits de ce document peuvent être cités par des analystes et des représentants accrédités de la presse, à condition qu'ils soient cités en contexte et que le nom de l'auteur, le titre de l'auteur et « Moor Insights & Strategy » soient affichés. Les personnes qui ne sont ni des analystes ni des représentants accrédités de la presse doivent avoir obtenu de Moor Insights & Strategy une autorisation écrite avant de citer des extraits du présent document.

LICENCES

AVERTISSEMENTS

Ce document a été commandé par Cisco. Moor Insights & Strategy fournit des recherches, des analyses, des conseils et des services de consultation à de nombreuses entreprises de haute technologie, comme celles mentionnées dans ce document. Aucun salarié de l'entreprise ne détient des positions en titres de participation dans les entreprises citées dans ce document.

AVERTISSEMENT

Les renseignements présentés dans ce document sont fournis à titre informatif seulement et peuvent contenir des inexactitudes techniques, des omissions et des erreurs typographiques. Moor Insights & Strategy décline toute garantie quant à l'exactitude, à l'exhaustivité ou à la pertinence de ces renseignements et n'assume aucune responsabilité pour les erreurs, les omissions ou les lacunes de ces renseignements. Le présent document contient les opinions de Moor Insights & Strategy et ne doit pas être interprété comme une déclaration de fait. Les opinions exprimées dans ce document peuvent être modifiées sans préavis.

Moor Insights & Strategy présente des prévisions et des énoncés prospectifs à titre d'orientations. Il ne s'agit pas de prévisions précises d'événements futurs. Bien que nos prévisions et nos énoncés prospectifs témoignent de notre opinion actuelle sur ce que l'avenir nous réserve, ils sont assujettis à des risques et à des incertitudes qui pourraient faire en sorte que les résultats réels diffèrent considérablement de nos projections. Vous êtes priés de ne pas vous fier indûment à ces prévisions et à ces énoncés prospectifs, qui reflètent nos opinions uniquement à la date de publication du présent document. Veuillez garder à l'esprit que nous ne nous engageons pas à réviser ou à publier les résultats de toute révision de ces prévisions et énoncés prospectifs à la lumière de nouveaux renseignements ou d'événements futurs.