GÉRER LA SÉCURITÉ À GRANDE ÉCHELLE

ÉTUDE SUR LES PLATEFORMES DE PROTECTION DES APPLICATIONS CLOUD NATIVES (CNAPP)

SYNTHÈSE

Les entreprises de toutes tailles adoptent actuellement la transformation numérique pour se doter d'un avantage concurrentiel. Les équipes DevOps jouent un rôle important dans ce processus, car leurs activités ont un impact immédiat sur l'entreprise. En parallèle, les équipes de sécurité doivent s'assurer que les risques pour la sécurité des applications cloud natives sont maîtrisés lors des phases de développement et de test avant la mise en production des applications. Les risques sont d'autant plus élevés que les applications cloud natives reposent sur une architecture basée sur des containers et des microservices, or ce sont généralement des centaines, voire des milliers d'instances qui en sont déployées. Cela n'a plus rien à voir avec le fonctionnement des applications monolithiques traditionnelles, dont la conception est plus simple, mais qui sont moins agiles et n'offrent aucune évolutivité à grande échelle.

À qui les entreprises peuvent-elles faire appel pour bénéficier des niveaux de sécurité les plus élevés pour leurs applications cloud natives ? À quels risques sont-elles le plus exposées : les pipelines CI/CD (intégration et développement continus), les enjeux de conformité ou d'autres types de violations susceptibles d'entraîner des failles ? Ces risques existent bel et bien, et il y en a sûrement d'autres. De nouvelles plateformes de protection des applications cloud natives (CNAPP) sont actuellement créées pour relever ces défis de sécurité. Cependant, toutes les solutions ne se valent pas. Cette synthèse définit les fonctionnalités, les fonctions et les capacités globales des CNAPP, les problèmes qu'elles visent à résoudre et les types d'utilisation spécifiques pour lesquels elles peuvent avoir un impact mesurable.

DÉFINITION D'UNE CNAPP COMPLÈTE

Les CNAPP intègrent et automatisent la sécurité du cloud en regroupant toutes les fonctionnalités souhaitées dans une même plateforme intégrée, et ce tout au long du cycle de vie d'une application cloud native, du développement à la gestion continue, en passant par les tests et le déploiement. Il s'agit d'une rupture par rapport aux approches des années passées consistant à rechercher des solutions de pointe, car cela favorisait les problèmes de fragmentation et de gestion du fait de la prolifération de solutions de

sécurité isolées. Ces dernières n'offraient en effet plus d'intérêt pour les entreprises, car elles les obligeaient à gérer une multiplicité de tableaux de bord et d'alertes. Étant donné la nature complexe des applications cloud natives, l'approche traditionnelle se traduit par des postures de gestion non proactives, avec les carences en matière de visibilité et de couverture du système de sécurité qui en résultent.

Les CNAPP sont nées du désir de rassembler des outils disparates afin de faciliter la supervision de la sécurité du cloud, les alertes, les dispositifs et le contrôle, ainsi que la prévention et la maîtrise des failles éventuelles. Quant aux plateformes de protection des workloads dans le cloud (CWPP), elles utilisent un agent sur une machine de calcul physique ou virtuelle et des containers. Elles ciblent uniquement la sécurité des workloads. Leur inconvénient ? Elles ne peuvent pas toujours être appliquées lors de l'exécution d'une application cloud native dans le cadre du cycle de développement.

Selon Moor Insights & Strategy, une CNAPP complète se compose de quatre éléments cruciaux.

1. Elle doit sécuriser les architectures de microservices, les containers et les déploiements sans serveur.
2. Elle doit inclure la fonctionnalité CWPP que nous venons d'évoquer, mais aussi deux éléments supplémentaires : la gestion de la sécurité dans le cloud et la gestion des droits d'accès à l'infrastructure cloud. La gestion de la sécurité dans le cloud identifie et traite les risques lorsque l'automatisation est appliquée à l'observabilité et aux menaces qui en résultent.
3. La gestion des droits d'accès à l'infrastructure cloud 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 cloud native, du développement, aux tests et à la production. Ce faisant, chaque CNAPP est conçue pour identifier les vulnérabilités dès le début du cycle de développement et surveille l'exécution en permanence pour détecter les vulnérabilités ou les erreurs de configuration.

LA VALEUR DES CNAPP

Les bénéfices du déploiement d'une CNAPP sont incalculables. La centralisation des fonctionnalités de sécurité du cloud simplifie la gestion des activités SecOps. En outre, la visibilité sur les angles morts s'est grandement améliorée, ce qui réduit le nombre de failles de sécurité. Votre entreprise améliore ainsi sa rentabilité, puisque vous bénéficiez d'un délai de déploiement plus rapide pour vos applications cloud natives ainsi que d'une réduction du nombre de violations de la conformité (aux conséquences parfois coûteuses) et d'interruptions d'activité. Les CNAPP peuvent être utiles à toutes les entreprises, mais elles conviennent particulièrement bien à celles qui évoluent dans des environnements hautement réglementés, tels que la production industrielle, les services financiers, l'assurance, ainsi que la santé et les produits pharmaceutiques.

IL EST TEMPS D'AGIR

Les applications cloud natives offrent l'évolutivité et les fonctionnalités nécessaires aux entreprises modernes, mais il peut être difficile d'en garantir la sécurité tout en donnant les moyens aux équipes DevOps de faire preuve de créativité. Les surfaces d'exposition aux menaces vont continuer à croître en raison de la nature hautement distribuée des nouveaux modèles de travail hybrides, mais aussi de l'adoption et du déploiement d'un nombre croissant d'applications cloud natives. Les entreprises ont besoin d'une approche simplifiée pour gérer la sécurité des applications cloud natives tout au long du cycle de vie. Les CNAPP sont parfaitement positionnées pour répondre à ce besoin. En outre, les CNAPP ne présentent pas toutes le même niveau de qualité. Il est donc important de vous assurer que toute plateforme choisie fournit les capacités et les fonctionnalités nécessaires pour couvrir vos besoins du point de vue de la sécurité du cloud.

Moor Insights & Strategy estime que Cisco est bien positionné pour répondre aux besoins des entreprises en matière de CNAPP avec Panoptica, la solution de sécurité applicative multicloud d'Outshift by Cisco. Panoptica offre une protection complète du cycle de vie, du développement à l'exécution, couvrant les applications et l'infrastructure qui inclut les containers, les environnements sans serveur et les API. Associée à Cisco AppDynamics, les entreprises peuvent également observer et gérer les risques de sécurité à l'aide d'un système de remédiation automatisé. Toutes ces fonctionnalités ont le potentiel de faciliter la collaboration des développeurs et des équipes de sécurité, éliminant ainsi certaines difficultés du processus de développement.

Pour en savoir plus, rendez-vous sur le site web consacré aux solutions pour les applications Cisco Reimagine.

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

ÉDITEUR
Patrick Moorhead, fondateur, président et analyste principal chez Moor Insights & Strategy

DEMANDES
Contactez-nous si vous souhaitez discuter de ce rapport. Moor Insights & Strategy vous répondra rapidement.

CITATIONS
Ce document peut être cité par la presse et les analystes accrédités, mais doit être cité en contexte, en indiquant le nom de l'auteur, le titre de l'auteur et « Moor Insights & Strategy ». Les autres utilisations hors presse et analystes doivent faire l'objet d'une autorisation écrite préalable de Moor Insights & Strategy pour toute citation.

AVERTISSEMENTS
Ce document a été commandé par Cisco. Moor Insights & Strategy fournit des services de recherche, d'analyse et de conseil à de nombreuses entreprises du secteur des hautes technologies. Aucun collaborateur de notre cabinet n'occupe de poste dans une entreprise citée dans ce document.

AVERTISSEMENT
Les informations présentées dans ce document sont fournies à titre informatif uniquement et peuvent contenir des inexactitudes techniques, des omissions et des erreurs typographiques. Moor Insights & Strategy exclut toute garantie quant à l'exactitude, à l'exhaustivité ou à la pertinence de ces informations et décline toute responsabilité en cas d'erreurs, d'omissions ou de manquements dans ces dernières. Ce document contient les opinions de Moor Insights & Strategy et ne doit pas être interprété comme une déclaration de fait. Les opinions exprimées ici sont sujettes à modification sans préavis.

Moor Insights & Strategy réalise des prévisions et des déclarations prospectives à titre d'indicateurs directionnels et non de prédictions précises des événements futurs. Bien que nos prévisions et nos déclarations prospectives correspondent à notre jugement actuel sur ce que l'avenir nous réserve, elles sont soumises à des risques et à des incertitudes qui pourraient entraîner des différences considérables avec les résultats réels. Vous êtes prié de ne pas vous fier indûment à ces prévisions et à ces déclarations prospectives, qui reflètent nos opinions uniquement à la date de publication de ce document. Nous ne nous engageons pas à réviser ou à publier les résultats de toute révision de ces prévisions et déclarations prospectives à la lumière de nouvelles informations ou d'événements futurs.