Akamai

LIVRE BLANC

Respecter la promesse des conteneurs

Simplification et accélération de la segmentation des ressources et des applications critiques

Introduction

La conteneurisation s'est rapidement imposée comme la solution idéale pour le déploiement d'applications dans les environnements cloud et hybrides, et la prolifération des conteneurs continue de s'accélérer. Selon Gartner, 90 % des organisations mondiales exécuteront des applications conteneurisées en production d'ici 2026, contre 40 % en 2021.[1] Et selon une étude de Forrester pour Capital One, **86 % des responsables informatiques interrogés ont donné la priorité à l'utilisation élargie des conteneurs pour davantage d'applications**.[2]

> Selon Gartner, **90 % des entreprises internationales** déploieront des applications conteneurisées en production d'ici 2026, contre 40 % en 2021

Tout cela, bien sûr, met une pression supplémentaire sur les responsables de la sécurisation des environnements informatiques pour faire face au déploiement des conteneurs, en particulier dans un modèle DevOps qui donne la priorité à l'adoption et à l'expansion rapides. Bien qu'un certain nombre de solutions spécialisées dans la sécurité des conteneurs aient vu le jour, ces entités spécifiques à une plateforme ou à un conteneur finissent par alourdir la complexité et les frais de gestion, sans prendre en compte le centre de données de l'entreprise dans son ensemble, ce qui complique la vie des équipes chargées de la sécurité. Ce qu'il faut, c'est une solution de sécurité unique et complète, fonctionnant de manière cohérente avec toutes les applications et technologies exécutées dans des environnements sur site, cloud et hybrides, y compris les conteneurs.

Mais avant de nous pencher sur les solutions, examinons rapidement le phénomène des conteneurs, les forces qui l'animent et ses implications du point de vue de la sécurité.

La pression monte : les demandes des entreprises, moteur de l'adoption

La tendance à l'adoption des conteneurs et leur croissance prévue peuvent être attribuées aux exigences commerciales imposées aux services informatiques des entreprises. Les entreprises actuelles s'attendent à pouvoir agir avec rapidité et agilité en réponse aux menaces concurrentielles et aux opportunités du marché. Elles ont besoin de solutions soutenant l'innovation et accélérant la mise sur le marché. Et elles cherchent en permanence à améliorer leur efficacité. Dans un monde de plus en plus interconnecté, elles veulent faciliter les transactions digitales avec leurs fournisseurs, leurs partenaires commerciaux et surtout leurs clients.

Ce sont là les principales raisons pour lesquelles les services informatiques des entreprises se tournent vers le cloud, ou plus précisément vers des modèles hybrides sur site/cloud. Ce sont également les principaux moteurs de la tendance DevOps, qui cherche à accélérer le déploiement des applications critiques en éliminant les points de friction entre les idées et la mise en œuvre, en tirant parti de l'automatisation et de la mise à l'échelle automatique pour mettre les applications en production plus rapidement.

> « Les organisations sous-estiment souvent l'effort requis pour utiliser les conteneurs en production. »
>
> — Gartner

Tout cela explique pourquoi les services informatiques ont adopté la conteneurisation. Par rapport aux machines virtuelles, les conteneurs sont beaucoup plus faciles et rapides à lancer, ce qui permet une livraison juste à temps avec pratiquement aucune latence et permet aux équipes de se concentrer sur la « mise en place de services, et non de serveurs ». L'un des principaux avantages des conteneurs est leur portabilité dans les environnements dynamiques des centres de données d'aujourd'hui ; ils facilitent la migration des applications entre les installations sur site et les instances multicloud. Cet avantage est encore renforcé par l'orchestration des conteneurs via Kubernetes, ou « K8s », qui permet aux équipes de déployer et gérer des volumes plus importants d'applications conteneurisées à l'échelle dans plusieurs environnements. L'orchestration est de plus en plus considérée comme la meilleure pratique en matière de mise en œuvre et de gestion des conteneurs.

En résumé, les conteneurs permettent aux services informatiques de mieux répondre aux exigences des entreprises en matière de rapidité, d'automatisation, de résilience et de disponibilité, et ce pour un coût total de possession inférieur à celui d'autres technologies. Les efforts de mise en œuvre ne sont toutefois pas sans inconvénient. « Les organisations sous-estiment souvent les efforts requis pour utiliser les conteneurs en production », indique un rapport de Gartner de 2019 sur les meilleures pratiques en matière de conteneurisation.[3] Malgré la popularité de la conteneurisation, la technologie est encore quelque peu naissante et les meilleures pratiques pour un déploiement sécurisé n'ont pas encore été entièrement harmonisées. Selon le rapport 2022 State of Kubernetes Security de Red Hat, « la sécurité est [encore] l'une des plus grandes préoccupations liées à l'adoption des conteneurs, et les problèmes de sécurité continuent d'entraîner des retards dans le déploiement des applications en production ».[4] Il est clair que les entreprises ne peuvent pas récolter tous les avantages potentiels des conteneurs sans une stratégie de mise en œuvre incluant nécessairement la cybersécurité.

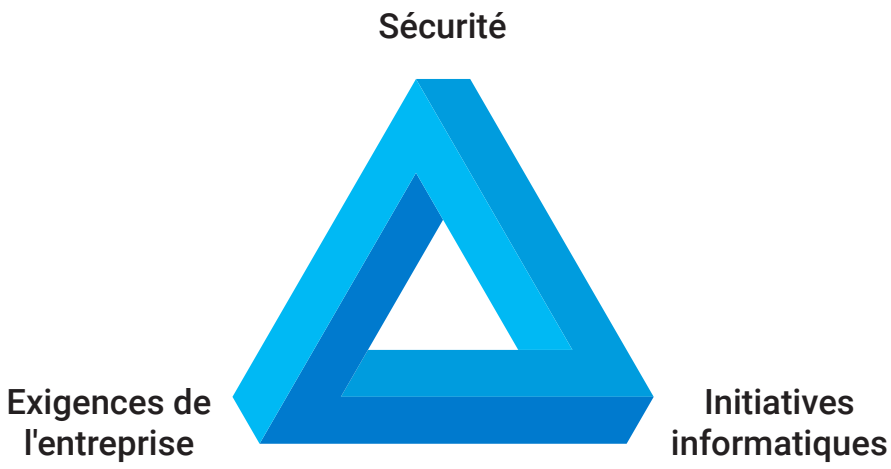
> Selon le rapport 2022 State of Kubernetes Security de Red Hat, « **la sécurité est [toujours] l'une des plus grandes préoccupations liées à l'adoption des conteneurs** et les problèmes de sécurité continuent de causer des retards dans le déploiement des applications en production »

Qu'est-ce que cela signifie pour l'équipe chargée de la sécurité ?

« La sécurité ne peut pas être envisagée après coup », affirme Gartner dans son rapport sur les meilleures pratiques. « Elle doit être intégrée au processus DevOps. » Trop souvent, cependant, ce n'est pas le cas. Dans la précipitation de la mise en œuvre de la conteneurisation, les équipes de sécurité peuvent parfois avoir l'impression de se trouver au sommet d'un « triangle impossible », une illusion d'optique également connue sous le nom de triangle impossible de Penrose (également connu chez Akamai sous le nom de triangle impossible de Klein & Howard).

> Les solutions de sécurité traditionnelles ne sont pas adaptables à l'entreprise contemporaine. Elles doivent être rapides, adaptables, dynamiques et s'intégrer parfaitement dans une approche « DevSecOps ».

De la même manière que le sommet du triangle semble illusoirement plus éloigné que les deux autres coins, la sécurité semble être à la traîne par rapport aux exigences de l'entreprise et aux initiatives informatiques pour y répondre. Mais tout comme le triangle est une illusion d'optique, les solutions de sécurité sont en fait plus proches qu'il n'y paraît. Les équipes doivent simplement aller au-delà des solutions lourdes et anciennes sur lesquelles elles se sont appuyées par le passé et se tourner vers des solutions correspondant à la manière dont l'informatique d'entreprise fonctionne aujourd'hui et s'intégrant parfaitement dans une approche « DevSecOps ». Il s'agit donc d'une solution rapide, adaptable et dynamique, qui utilise elle-même l'approche DevOps. Mais surtout, une solution découplée des systèmes d'exploitation et de la plateforme sous-jacents, afin de simplifier la mise en œuvre et la gestion.



Triangle impossible de Klein et Howard

Pourquoi le concept « natif » n'est-il pas suffisant ?

Dans les premiers temps de la virtualisation et de la migration vers le cloud, les entreprises ont souvent été amenées à croire que les contrôles natifs du cloud étaient suffisants pour visualiser, gérer et protéger leurs charges de travail. Ce n'est qu'après de nombreux essais et erreurs que les responsables informatiques ont réalisé qu'ils avaient besoin d'un modèle de gestion superposé, intégrant des solutions tierces qui offrent une sécurité supérieure aux contrôles natifs.

Comme l'ont indiqué Gartner et Forrester Research, une stratégie réussie de mise en œuvre des conteneurs repose sur le « tiercé des conteneurs » :

- Exécuter les conteneurs d'une manière portable, indépendante de la plateforme, pouvant être mise en œuvre partout dans de multiples architectures cloud et sur site, de manière fluide
- Tirer parti de l'orchestration pour exécuter et gérer les conteneurs à grande échelle
- Utiliser des outils tiers pour la gestion, la visibilité et la sécurité des conteneurs

Contrairement aux efforts passés en matière de virtualisation et de cloud, l'industrie des conteneurs a reconnu dès le début que les systèmes de gestion natifs du cloud, et les contrôles de sécurité en particulier, sont inadéquats pour une stratégie de conteneurs efficace. Dans l'étude de Gartner sur les solutions de gestion des conteneurs, **65 % des personnes interrogées ont déclaré avoir l'intention d'exploiter des outils de gestion tiers pour visualiser, gérer et sécuriser les charges de travail conteneurisées**.[5] Toutefois, ces outils tiers doivent fonctionner de manière fluide dans les instances sur site et dans le cloud, et adopter une approche granulaire pour éviter les pièges des méthodes lourdes et mixtes utilisées par le passé, comme les groupes de sécurité, les VLAN et les pare-feu, qui offrent une visibilité nulle et une granularité négligeable.

Favoriser l'adoption des conteneurs avec Akamai Guardicore Segmentation

Akamai Guardicore Segmentation a été conçu pour relever les défis des infrastructures dynamiques et hybrides des centres de données actuels. Nous offrons une visibilité complète sur toutes les applications et charges de travail s'exécutant dans plusieurs environnements, et permettons une segmentation logicielle granulaire facile à mettre en œuvre grâce à la création, au déploiement et à l'application rapides de règles de sécurité autour d'applications individuelles ou regroupées logiquement.

Soyons clairs : Akamai Guardicore Segmentation n'est pas un produit ponctuel réservé aux conteneurs. Au contraire, la sécurité des conteneurs est une fonctionnalité clé de la plateforme, qui fonctionne de manière cohérente dans des environnements mixtes pouvant également inclure des serveurs bare-metal, des machines virtuelles, des charges de travail sans serveur et des terminaux distants. Par conséquent, nous fournissons aux organisations une solution unique et complète pour sécuriser tous les actifs du centre de données et du cloud, quel que soit leur emplacement ou leur mode de déploiement, éliminant ainsi la nécessité de gérer plusieurs solutions ponctuelles. De plus, comme notre solution est découplée des plateformes et systèmes d'exploitation sous-jacents, les règles de sécurité accompagnent les applications et les charges de travail lorsqu'elles se déplacent entre les environnements sur site et dans le cloud, améliorant ainsi le facteur de portabilité qui rend les conteneurs attrayants pour le déploiement d'applications dans les infrastructures de cloud hybride.

> La sécurité des conteneurs est une capacité clé de la plateforme Akamai Guardicore Segmentation, qui fonctionne de manière cohérente dans les environnements dynamiques et hétérogènes des centres de données

En ce qui concerne les conteneurs, Akamai Guardicore Segmentation place des agents sur les nœuds hôtes des conteneurs, ce qui permet d'avoir une visibilité sur l'ensemble du cluster de conteneurs, y compris les flux de communication entre pods et entre pods et machines virtuelles. Il est ainsi possible de mettre en œuvre et d'appliquer une règle de sécurité très granulaire par processus, utilisateur et nom de domaine pleinement qualifié (FQDN). Dans un scénario d'orchestration, nous prenons en charge l'orchestration K8s et permettons une visibilité sur les métadonnées Kubernetes et OpenShift pour un contexte amélioré. Un modèle d'étiquetage flexible permet aux opérateurs d'exprimer des règles en utilisant la terminologie native de K8s. Pour la mise en œuvre de K8s, nous nous appuyons sur l'interface native Container Network Interface (CNI), une méthode non intrusive de mise en œuvre des règles dans K8s sans limitation d'échelle. Des modèles dédiés permettent aux utilisateurs de protéger leurs applications stratégiques Kubernetes, qu'il s'agisse d'espaces de noms, d'applications ou de tout autre objet. Nous nous adaptons également aux charges de travail et aux taux de changement de K8s. Comme notre solution fonctionne également sur toutes les autres charges de travail de l'entreprise de la même manière, elle sert de solution unique pour visualiser, gérer et sécuriser les actifs dans l'ensemble de votre entreprise.

Dans un environnement DevOps, les règles de sécurité que vous créez s'intègrent efficacement dans les processus d'intégration et de déploiement continus (CI/CD), ce qui permet de s'assurer que la sécurité n'est pas envisagée après coup, mais qu'elle est pleinement intégrée au modèle de livraison.

Conclusion

Les conteneurs sont de plus en plus présents dans de nombreux environnements d'entreprise. Ils permettent d'accroître l'efficacité de l'utilisation des ressources, de rationaliser les processus et d'améliorer la portabilité et l'évolutivité. Dans le même temps, la sécurité intégrée qu'ils fournissent n'est pas suffisante, en particulier pour les entreprises qui utilisent un environnement hybride.

Lorsque vous recherchez une solution de sécurité capable d'évoluer avec votre entreprise, veillez à choisir un outil indépendant de la plateforme, qui fournit des informations granulaires sur vos processus de bout en bout, quel que soit l'endroit où ils se déroulent. C'est ce que fait Akamai Guardicore Segmentation, et bien plus encore, en offrant la gamme de fonctionnalités et de capacités dont les entreprises actuelles ont besoin pour être prêtes à affronter le présent et l'avenir.

Grâce à Akamai Guardicore Segmentation, votre équipe de sécurité peut assurer une sécurité cohérente dans des environnements de centres de données dynamiques et hétérogènes. Ce faisant, vous pouvez aider les équipes informatiques à tenir les promesses de la conteneurisation, en réalisant le développement et le déploiement rapides, rentables et sécurisés d'applications critiques essentielles aux exigences métier de votre entreprise.

Simplifiez la sécurité dans l'ensemble de votre environnement. En savoir plus sur notre solution de sécurité unifiée performante pour les conteneurs et plus encore : akamai.com/guardicore.

1 Chandrasekaran, Arun et Wataru Katsurashima. « The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem », Gartner, 18 août 2021.

2 « Cloud Container Adoption In The Enterprise », Forrester, juin 2020.

3 « Best Practices for Running Containers and Kubernetes in production », Gartner, 25 février 2019.

4 « State of Kubernetes Security Report », Red Hat, mai 2022.

5 « Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024 », 25 juin 2020.