PRÉSENTATION DE LA SOLUTION AKAMAI

Visualisez et sécurisez Kubernetes avec la solution Guardicore Segmentation d'Akamai

Kubernetes (K8s) reste l'une des technologies les plus répandues dans le domaine du déploiement et de la gestion des applications dans les centres de données basés sur le cloud. Elle offre une vitesse et une flexibilité qui n'avaient jamais été atteintes auparavant. Selon Gartner, 90 % des entreprises internationales déploieront des applications conteneurisées en production d'ici 2026, contre 40 % en 2021. En outre, d'ici 2026, 20 % de l'ensemble des applications d'entreprise seront exécutées à l'aide de conteneurs, contre moins de 10 % en 2020.[1] La popularité croissante de cette plateforme a attiré non seulement les utilisateurs, mais également les pirates, obligeant les équipes de sécurité à faire face à des défis auxquels elles n'étaient pas initialement préparées.

De nouvelles technologies, de nouveaux défis de sécurité

Les clusters K8s offrent un écosystème complet, incluant des services DNS, l'équilibrage de la charge, la mise en réseau, la mise à l'échelle automatique ainsi que d'autres fonctionnalités requises pour l'exécution des applications. Il n'est pas surprenant que les clusters K8s soient aussi largement adoptés, ceux-ci permettant aux entreprises d'innover rapidement et de réaliser des économies. Toutefois, ces caractéristiques qui rendent K8s si attrayant, complexifient également sa sécurisation.

En effet, ce réseau plat par nature implique que chaque pod puisse communiquer avec n'importe quel autre pod du cluster. Après une violation initiale, les hackers peuvent se déplacer latéralement et accéder à tous les centres de données connectés. Il s'agit d'un processus typique des attaques par ransomware, mais cette même stratégie peut être facilement appliquée par d'autres vecteurs d'attaque.

Lors d'un sondage mené pour le Rapport sur l'état de la sécurité de Kubernetes 2022 auprès de 300 professionnels DevOps, ingénieurs et professionnels de la sécurité, 93 % des personnes interrogées ont déclaré avoir subi au moins un incident de sécurité dans leurs environnements K8s au cours des 12 derniers mois, entraînant parfois des pertes de revenus ou de clients.

La solution : la micro-segmentation

Le concept de déploiement des applications de K8s étant par lui-même différent, il nécessite des méthodes de sécurité innovantes. Les équipes de sécurité ne peuvent pas simplement redéployer une solution de sécurité existante et s'attendre à ce qu'elle fonctionne avec cette nouvelle technologie. La sécurisation des clusters K8s nécessite une approche native.

C'est pourquoi Akamai propose une solution de segmentation logicielle qui prend en charge la sécurisation des clusters K8s. C'est une solution qui se comporte de la même manière avec les autres charges de travail de votre environnement, y compris avec les systèmes hérités, les clouds, les charges de travail sur site et les conteneurs. Ainsi, vous pouvez visualiser, sécuriser et gérer les ressources de votre entreprise de manière centralisée.

Avantages

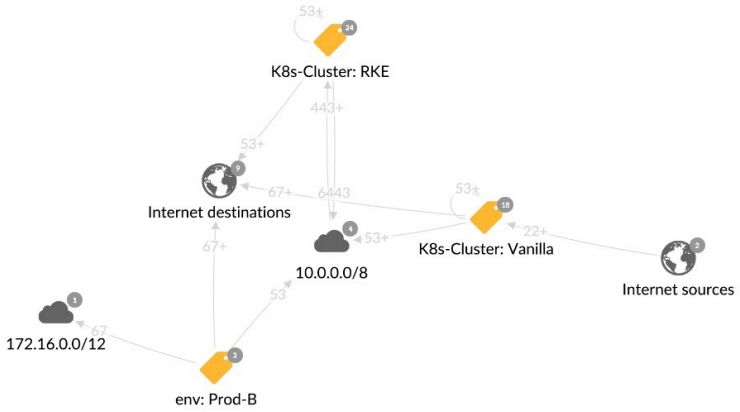
- Visualisez, appliquez et surveillez vos clusters K8s depuis un point unique et en utilisant les mêmes processus que pour toute autre ressource
- Protégez simplement vos applications des attaques avancées qui exploitent les vulnérabilités de K8s
- Affichage en temps réel ou chronologique de toutes les connexions entre les pods, les services, les hôtes ou les espaces de noms
- Modèles prêts à l'emploi pour protéger facilement les clusters K8s
- Gestion unifiée des règles et de la console au niveau des K8s, des points de terminaison et des charges de travail dans le cloud ou sur site
- Recevez des données d'exploitation concernant les clusters déployés, notamment sur le nombre d'agents de surveillance et sur l'état de l'orchestration de Kubernetes

Akamai

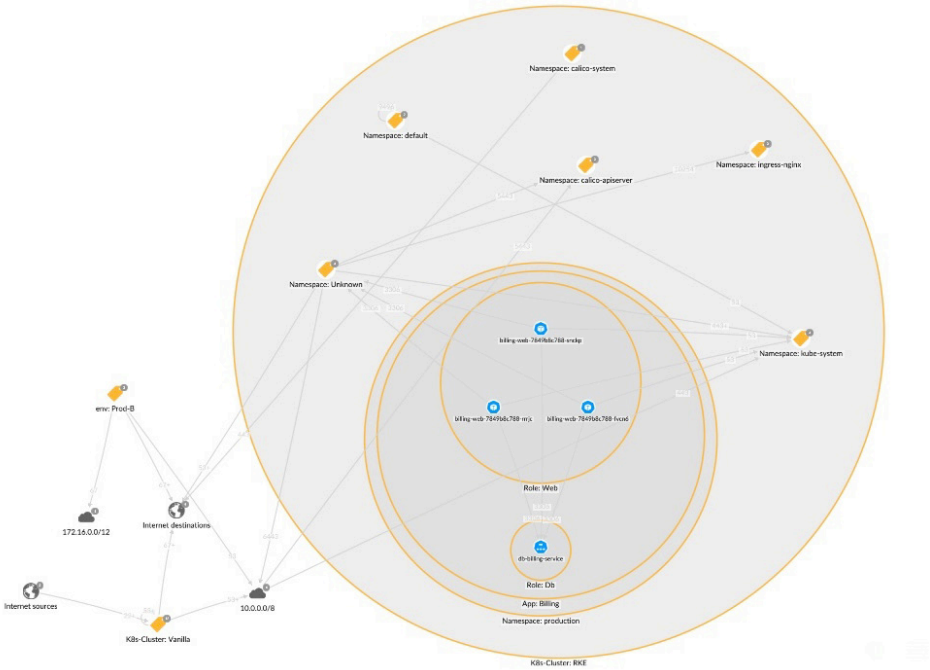
Principales fonctionnalités pour la segmentation des clusters Kubernetes

Visibilité. Guardicore Segmentation d'Akamai vous indique ce qui est en cours d'exécution dans votre environnement K8s et vous confirme que votre trafic se dirige uniquement là où vous le souhaitez, ce qui est essentiel pour une création de règles réussie.

- **Cartes d'interdépendance :** Akamai fournit une carte permettant de visualiser les communications en interne ou entre les centres de données pour tous les types de technologies comme les machines virtuelles, les K8s, les conteneurs Docker et plus encore. Ces cartes permettent de rendre visible et de détecter toute connexion suspecte entre les pods, les services, les hôtes ou les espaces de noms.
- **Étiquettes :** les cartes reflètent avec précision la façon dont les applications sont déployées dans le cluster grâce à l'utilisation de plusieurs couches d'étiquettes. Cette carte présente la hiérarchie K8s telle qu'elle a été établie par les gestionnaires de l'application. Ce niveau de détail aide les utilisateurs d'Akamai à comprendre exactement ce qui est déployé dans le cluster et à connaître les relations de réseau entre les applications déployées et le reste de l'infrastructure.



Clusters représentés sur la carte Reveal. En double-cliquant sur un cluster, les espaces de noms et leurs interconnexions au sein du cluster s'affichent.



Carte Reveal fournissant des informations sur les pods

> 93 % des personnes interrogées ont subi au moins un incident de sécurité au sein de leurs environnements K8s au cours des 12 derniers mois, entraînant parfois des pertes de revenus ou de clients.

Application. Afin de réduire la surface d'attaque dans les clusters K8s, une règle de segmentation stricte est nécessaire. Une solution appliquant la segmentation doit répondre à deux critères principaux : elle doit être non intrusive, sans aucune limitation d'échelle ou de performances, et elle doit protéger les objets K8s à tous les niveaux de manière flexible, y compris les espaces de noms, les contrôleurs et les étiquettes K8s.

Akamai exploite l'interface réseau des conteneurs (IRC) native Kubernetes. L'IRC est constituée d'un plug-in de règle de sécurité réseau qui avait été à l'origine conçu pour l'application de la segmentation du réseau dans K8s. Il s'agit d'une méthode non intrusive 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.

Ring Fence a K8s Application by whitelisting inbound and outbound flows for an application on K8s cluster K8s-Cluster within Namespace

Modèle de protection des applications de Kubernetes

Surveillance avancée. Grâce à un système de journalisation et de surveillance avancé, un journal réseau dédié est ajusté à la mise en réseau K8s et affiche la destination des services, les adresses IP des nœuds, les ports source et de destination ainsi que les processus pour chaque événement. Ceci permet d'examiner facilement les activités anormales sur le réseau et d'exporter des données vers une application tierce comme un SIEM.

Synthèse

Kubernetes fait désormais partie intégrante de nombreux environnements d'entreprise. Il s'agit d'une nouvelle approche qui permet une utilisation efficace des ressources et qui offre des processus de développement plus rationalisés ainsi qu'une portabilité et une évolutivité accrues. Mais cette approche différente en matière de développement d'applications nécessite également de revoir l'approche sécuritaire.

Guardicore Segmentation d'Akamai offre une solution globale qui permet de visualiser les flux de communication entre les différents types de déploiements (serveurs physiques, machines virtuelles, K8s, etc.), à partir d'une seule et même carte. Elle offre une approche native K8s non intrusive et évolutive permettant la visibilité, la surveillance et l'application, tout en allégeant la charge des équipes de sécurité et de développement, pour permettre à votre entreprise d'innover rapidement sans laisser la sécurité de côté.

Selon le Rapport sur l'état de la sécurité de Kubernetes 2022, la sécurité est l'une des principales préoccupations des professionnels avec l'adoption de K8s. Par ailleurs, les problèmes de sécurité continuent de provoquer des retards dans le déploiement des applications en production.

Pour en savoir plus, rendez-vous sur akamai.com ou contactez votre équipe commerciale Akamai.

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