La sécurité native pour Kubernetes

Définition et avantages

Introduction

Ces cinq dernières années, les logiciels d'infrastructure ont bénéficié d'innovations majeures dans le domaine des technologies et architectures cloud-native. Ces nouvelles approches permettent aux entreprises de développer et d'exécuter leurs applications avec des niveaux de flexibilité, d'évolutivité et de dynamisme jamais atteints auparavant. Les conteneurs, les microservices, les API déclaratives et les fonctions logicielles font abstraction des ressources sous-jacentes de calcul, de stockage et de mise en réseau. À cela s'ajoutent la distribution continue et les pratiques DevOps, qui ont permis aux entreprises de toutes tailles et de tous secteurs d'activité de distribuer leurs logiciels de façon plus fiable et rapide.

Au cœur de cette transition généralisée se trouve Kubernetes, le système d'orchestration de conteneurs Open Source. La technologie Kubernetes est devenue la norme pour automatiser le déploiement et la gestion des applications cloud-native en production.

L'adoption des technologies cloud-native génère de nouveaux défis en matière de sécurité, mais aussi des possibilités d'amélioration des stratégies de sécurité existantes. Cette évolution cloud-native engendre quant à elle un nouveau contexte de menaces, dans lequel la surface d'attaque est aussi rapide, active et dynamique que les conteneurs. Plutôt que d'être délimitées, les applications sont désormais intentionnellement décomposées, souvent en microservices. Cette approche implique de sécuriser tout un ensemble de composants interconnectés qui communiquent de façon autonome. En parallèle, des acteurs malveillants peuvent exploiter certaines caractéristiques clés des conteneurs pour mener des attaques plus rapides et importantes qu'auparavant.

À l'instar des machines virtuelles et des environnements de cloud public, les conteneurs et Kubernetes introduisent de nouvelles couches dans l'infrastructure, qui ont chacune des exigences de sécurité particulières. Pour répondre à ces changements, les solutions de sécurité suivent généralement l'une de ces trois approches :

1. Les solutions basées sur l'hôte ou sur le réseau étendent leur protection aux conteneurs.
2. Les solutions privilégient la sécurisation des environnements de conteneurs.
3. Les solutions privilégient la sécurisation des conteneurs et de Kubernetes.

Comparaison des approches en matière de sécurité des conteneurs

À retenir : la sécurité native pour Kubernetes va au-delà des approches existantes de la sécurité des conteneurs pour protéger également les environnements Kubernetes.

La première catégorie d'outils de sécurité protègent les environnements cloud en contrôlant les machines virtuelles et points de terminaison (ou leurs réseaux) par l'intermédiaire de fonctionnalités telles que les pare-feu. La majorité de ces outils répondent à un besoin spécifique, comme la gestion des vulnérabilités, la détection des intrusions ou la protection des applications web par pare-feu. Ils sont moins adaptés pour la sécurisation des conteneurs, puisque la protection couvre les charges de travail et les données associées, et non les adresses IP ou les serveurs.

Ces solutions ne sécurisent pas la totalité du cycle de vie des applications cloud-native, et ne sont pas conçues pour répondre aux besoins des applications conteneurisées qui sont dynamiques, hautement évolutives et éphémères.

La deuxième catégorie de solutions sécurisent la totalité du cycle de vie des conteneurs et présentent une architecture conçue spécialement pour les conteneurs. La majorité des outils de sécurisation des conteneurs appartiennent à cette catégorie. Leurs fonctions de protection couvrent chacun des conteneurs de manière individuelle, l'environnement ou le moteur d'exécution (par exemple, Docker), et les artefacts servant à leur exécution, c'est-à-dire les images de conteneurs. L'inconvénient de cette approche est qu'elle n'apporte pas de protection au niveau de Kubernetes.

La troisième catégorie va plus loin que les solutions axées sur les conteneurs pour fournir une sécurité spécialement adaptée aux environnements Kubernetes. Cette approche, basée sur une architecture native pour Kubernetes, sécurise la totalité du cycle de vie des applications cloud-native et traite les vecteurs de menaces au niveau des conteneurs et de Kubernetes. La solution Red Hat® Advanced Cluster Security for Kubernetes est à l'origine de cette approche native pour Kubernetes.

Définition de la sécurité native pour Kubernetes

À retenir : une solution de sécurité doit respecter six critères essentiels pour être considérée comme native pour Kubernetes.

La sécurité native pour Kubernetes repose sur le principe que la sécurité est plus efficacement mise en œuvre lorsqu'elle est en adéquation avec le système responsable de la gestion de l'ensemble des applications conteneurisées d'une entreprise. Une plateforme de sécurité doit présenter les caractéristiques suivantes pour être considérée comme native pour Kubernetes :

1. S'intégrer directement au serveur de l'API Kubernetes pour obtenir une visibilité sur les charges de travail et l'infrastructure Kubernetes
2. Évaluer les vulnérabilités dans le logiciel Kubernetes
3. Baser ses fonctionnalités de sécurité, notamment la gestion des politiques, sur les ressources du modèle objet Kubernetes (déploiements, espaces de noms, services, pods, etc.)
4. Analyser les données déclaratives provenant des artefacts propres à Kubernetes (par exemple, les fichiers manifestes de charge de travail) et des configurations
5. Utiliser les fonctions de sécurité intégrées de Kubernetes afin de gérer l'application des politiques pour renforcer l'automatisation, l'évolutivité et la fiabilité
6. Se déployer et s'exécuter en tant qu'application Kubernetes, notamment l'intégration et la prise en charge des outils courants dans les chaînes d'outils cloud-native

Les entreprises qui cherchent à sécuriser leurs environnements Kubernetes doivent évaluer et hiérarchiser leurs besoins en matière de sécurité selon leurs cas d'utilisation spécifiques : visibilité, gestion des vulnérabilités, segmentation du réseau, gestion des configurations, conformité, détection des menaces et résolution des incidents. Une plateforme de sécurité native pour Kubernetes qui remplit ces six critères peut répondre de manière exhaustive à ces besoins de sécurité spécifiques.

Avantages de la sécurité native pour Kubernetes

À retenir : une solution de sécurité native pour Kubernetes offre plusieurs avantages clés exclusifs : renforcement de la protection, réduction des coûts et des délais, et diminution des risques pour l'exploitation.

Les entreprises qui adoptent une approche de sécurité native pour Kubernetes en tirent trois avantages majeurs :

1. **Renforcement de la protection :** la sécurité native pour Kubernetes élimine les zones d'ombre sur la surface d'attaque de l'outil d'orchestration, permettant ainsi aux équipes de sécurité de détecter les vulnérabilités critiques et les vecteurs de menace qu'elles ne verraient pas autrement.
2. **Réduction des coûts et des délais :** l'approche native pour Kubernetes réduit le temps, le travail et le personnel nécessaires à la mise en œuvre de la sécurité. De plus, elle simplifie les analyses de sécurité, les recherches et les corrections en recueillant des informations supplémentaires sur le contexte spécifique des applications et de l'infrastructure Kubernetes.
3. **Diminution des risques pour l'exploitation :** les solutions de sécurité native pour Kubernetes limitent les effets sur les tâches d'exploitation essentielles par une application des politiques qui s'appuie sur l'évolutivité et la résilience de l'outil d'orchestration. Cette approche permet également d'éviter les conflits et la complexité pouvant exposer les applications essentielles à des risques pour l'exploitation.

Une protection renforcée grâce à la sécurité native pour Kubernetes

Lorsque les entreprises passent de l'exécution de conteneurs individuels à leur orchestration avec un système tel que Kubernetes, elles sont en mesure de les exécuter sur la quasi-totalité des infrastructures. Elles bénéficient aussi de davantage de cohérence au niveau de la découverte des services et de l'équilibrage de charge, ainsi que de mises à niveau et de déploiements automatisés. En parallèle, l'introduction de cette nouvelle plateforme entraîne l'élargissement de la surface d'attaque de l'infrastructure. Des vulnérabilités peuvent naître au niveau des logiciels Open Source, des configurations non maîtrisées ou de nouveaux vecteurs d'attaque.

Kubernetes donne accès à des abstractions facilitant le développement et l'exploitation, qui génèrent facilement des zones d'ombre pour les spécialistes de la sécurité habituels. Les conteneurs et applications créés ne sont plus associés à des limites et ressources physiques telles que les serveurs. Et parce que Kubernetes permet de programmer tout ce qui concerne le calcul, la mise en réseau et le stockage, les failles de sécurité peuvent persister si le niveau de visibilité est insuffisant.

Plus de visibilité et de données, moins de zones d'ombres

À retenir : les solutions de sécurité native pour Kubernetes permettent aux entreprises de comprendre toute la sécurité de leur environnement Kubernetes.

Pour une sécurité efficace, il faut d'abord disposer d'une bonne visibilité sur l'environnement et son niveau de protection global. La sécurité native pour Kubernetes apporte une visibilité directe sur Kubernetes, qui s'obtient en intégrant le serveur de l'API Kubernetes. Cette fonctionnalité permet de surveiller non seulement les conteneurs qui s'exécutent dans les clusters Kubernetes, mais aussi et surtout les ressources et les objets, qui sont visibles par Kubernetes. Ces abstractions (déploiements, ensembles de démons, services, pods et autres ressources) renvoient à des contrôleurs, des groupes de réseaux et des charges de travail. Une meilleure visibilité permet d'obtenir des données clés sur le contexte au niveau de l'application.

De leur côté, les solutions de sécurité axées sur les conteneurs offrent une visibilité au niveau de chaque conteneur éphémère et des images correspondantes, et donnent peu d'informations sur les applications dans leur ensemble. La solution Red Hat Advanced Cluster Security complète la surveillance des activités de chaque conteneur en offrant une visibilité centrée sur le déploiement. Les utilisateurs disposent alors d'une vue globale et à la demande des applications Kubernetes et de leur sécurité.

Visibilité sur les configurations

Avec une visibilité directe sur Kubernetes, les entreprises peuvent évaluer le niveau de sécurité du système lui-même en contrôlant les configurations et les paramètres. La sécurité native pour Kubernetes automatise les contrôles de politiques pour appliquer les meilleures pratiques de sécurité et identifier les erreurs de configuration qui pourraient augmenter le risque d'exposition des données d'applications. La solution Red Hat Advanced Cluster Security évalue continuellement des centaines de configurations Kubernetes pour déterminer le niveau de sécurité global des environnements Kubernetes. Ces configurations comprennent notamment :

- les autorisations des rôles ;
- l'accès aux secrets ;
- le trafic réseau autorisé ;
- les paramètres des composants du plan de contrôle ;
- d'autres paramètres.

De leur côté, les solutions axées sur les conteneurs se concentrent sur les configurations du moteur d'exécution des conteneurs et de chaque conteneur individuel (privilèges et capacités du noyau par exemple). Parce qu'elles peuvent omettre certaines catégories de contrôles Kubernetes, les configurations non sécurisées peuvent être exploitées.

Visibilité sur la conformité

Avec Kubernetes, la visibilité doit aussi couvrir la conformité, notamment aux normes PCI, SOC 2, FedRAMP et à la loi HIPAA. Même lorsque l'entreprise dispose d'une posture de sécurité solide, elle doit correctement tenir compte de la sécurité des applications et de l'infrastructure Kubernetes pour une mise en conformité adaptée. Les audits et les certifications peuvent nécessiter la mise en place de mesures de contrôle renforcées, dont une visibilité complète sur Kubernetes.

L'approche native pour Kubernetes de la solution Red Hat Advanced Cluster Security prévoit l'application de contrôles spécifiques aux clusters qui sont automatiquement associés aux contrôles de conformité existants. Les entreprises peuvent ainsi connaître instantanément leurs taux de réussite et d'échec. Par exemple, il peut s'agir de restreindre l'accès au réseau entre Internet et les services traitant des données sensibles, ou d'identifier des vulnérabilités dans la version de Kubernetes utilisée.

Lorsque la sécurité est axée sur les conteneurs, les contrôles de conformité compatibles avec le système d'orchestration reposent généralement sur les critères CIS (Center for Internet Security) Docker, ce qui entraîne une évaluation incomplète de la conformité globale des environnements.

Visibilité sur l'isolation des charges de travail

Par essence, les conteneurs offrent un plus faible niveau d'isolation que les machines virtuelles, en particulier dans les situations nécessitant une architecture multi-client. L'un des avantages de Kubernetes réside dans la multitude d'options disponibles pour assurer l'isolation entre les charges de travail durant l'exécution des

conteneurs. Point de départ essentiel dans la sécurisation des environnements Kubernetes de tous types, l'isolation peut être assurée par le biais de limites physiques (clusters, nœuds) ou virtuelles. Ces deux types de limites peuvent être mises en place à l'aide de fonctions telles que les politiques réseau et les espaces de noms.

La sécurité native pour Kubernetes permet aux équipes de comprendre et de mettre en œuvre des charges de travail isolées au sein de Kubernetes de différentes façons.

La sécurité axée sur les conteneurs ignore en grande partie ces limites. Elle privilégie plutôt les hôtes d'exécution des conteneurs, sans tenir compte du niveau d'isolation des applications et de leurs services.

La solution Red Hat Advanced Cluster Security fournit des informations clés qui :

- s'appuient sur la compréhension des clusters, des espaces de noms et des pods ;
- sont issues de données provenant de chacun des hôtes ;
- s'intègrent aux politiques réseau de Kubernetes pour comprendre comment les applications sont isolées.

Une stratégie de sécurité efficace n'est solide que si ses bases le sont. Il est également essentiel de disposer d'une visibilité complète sur le système pour assurer la bonne protection des applications cloud-native.

Détection des vulnérabilités critiques et des vecteurs de menace

À retenir : les solutions de sécurité native pour Kubernetes détectent les vulnérabilités, les vecteurs d'attaque et les erreurs de configuration dans Kubernetes, et en protègent.

Pour sécuriser les charges de travail qui s'exécutent sur Kubernetes, il faut bien comprendre les menaces propres aux environnements cloud et comment s'en protéger. Ces menaces ne se limitent pas aux conteneurs, mais s'étendent à la plateforme Kubernetes elle-même. La richesse et la complexité de Kubernetes génèrent un vaste ensemble de vecteurs d'attaque qui ne cessent d'évoluer à mesure que la Cloud Native Computing Foundation (CNCF), les communautés Open Source et les entreprises qui contribuent continuent de développer la plateforme. Voici deux exemples de menaces de sécurité propres à Kubernetes ayant eu une incidence auprès du grand public :

- Une configuration non sécurisée des consoles Kubernetes dans un environnement cloud Tesla[1] a permis à des cybercriminels d'accéder à des identifiants de compte et de miner de la cryptomonnaie.
- Un service Shopify vulnérable à une faille de type SSRF (falsification de requête côté serveur)[2] aurait pu permettre à un cybercriminel d'obtenir les informations d'identification du kubelet et de les répéter pour obtenir un accès root à tous les conteneurs.

La communauté cloud-native a également identifié ces menaces propres à Kubernetes. Un premier audit de sécurité[3] réalisé en 2020 a identifié des failles de sécurité au sein de Kubernetes, dont un modèle de menace touchant huit composants majeurs de Kubernetes. La solution Red Hat Advanced Cluster Security s'appuie sur ces événements et sur les recherches réalisées dans l'écosystème cloud-native pour offrir des fonctionnalités uniques d'identification des vulnérabilités, des erreurs de configuration et des exploits au sein de Kubernetes.

1 *Newman, Lily Hay, « Hack Brief: Hackers Enlisted Tesla's Public Cloud to Mine Cryptocurrency », Wired, 28 février 2018*

2 *Kerner, Sean Michael, « How Shopify Avoided a Data Breach, Thanks to a Bug Bounty », eWeek, 17 décembre 2018*

3 *« Kubernetes Final Report, » GitHub (kubernetes/community/wg-security-audit/findings), 6 août 2019*

Détection des vulnérabilités propres à Kubernetes

Parmi les nombreux composants de Kubernetes, le serveur de l'API est incontestablement celui qu'il faut protéger en priorité, étant donné son rôle essentiel dans l'orchestration et la gestion des applications conteneurisées. Par exemple, la vulnérabilité CVE-2018-1002100 affecte le serveur de l'API Kubernetes en donnant la possibilité à un acteur malveillant de compromettre un cluster entier en envoyant des requêtes autorisées, rendant sa détection encore plus difficile. Jusqu'à sa découverte plus de trois ans après le premier lancement de Kubernetes, cette vulnérabilité était présente dans chaque version.

La sécurité native pour Kubernetes détecte automatiquement les vulnérabilités de Kubernetes pour aider les administrateurs et les opérateurs de clusters à traiter certains des risques les plus importants pour leurs environnements.

Les solutions axées sur les conteneurs se concentrent quant à elles sur les vulnérabilités au sein des images de conteneurs. Si les conteneurs présentant moins de vulnérabilités sont plus sécurisés, une infrastructure Kubernetes vulnérable pourrait néanmoins les exposer aux risques. La solution Red Hat Advanced Cluster Security détecte de manière proactive les clusters présentant le plus de vulnérabilités propres à Kubernetes et permet aux utilisateurs de définir des politiques en fonction de chacune d'entre elles.

Détection des erreurs de configuration propres à Kubernetes

Outre les vulnérabilités, les mauvaises configurations des contrôles de base de Kubernetes peuvent donner lieu à des exploits et à l'exposition de données d'applications sensibles, en particulier en cas de propagation automatique d'une mauvaise configuration dans les clusters. Ces configurations incorrectes peuvent découler d'une erreur de l'utilisateur ou d'un manque de maîtrise de Kubernetes, comme l'octroi d'autorisations d'administration complètes du cluster à un utilisateur inexpérimenté ou à un compte de service par le biais du contrôle d'accès basé sur les rôles, ou l'exposition inutile de secrets Kubernetes en permettant aux déploiements d'en extraire même lorsqu'ils ne sont pas nécessaires.

La solution Red Hat Advanced Cluster Security intègre ces contrôles pour signaler rapidement toute configuration incorrecte aux entreprises, ce qui leur permet d'améliorer leur gestion des configurations dans son ensemble.

Les solutions axées sur les conteneurs se concentrent sur les configurations problématiques de l'environnement d'exécution des conteneurs et de chaque conteneur, rendant la protection incomplète et sujette aux failles. Même lorsqu'une erreur de configuration est corrigée, une mauvaise configuration de Kubernetes peut permettre à un attaquant de compromettre le nœud d'exécution du conteneur. Dans cet exemple, le conteneur est toujours compromis, même si la configuration du conteneur est correcte.

La solution Red Hat Advanced Cluster Security remédie à ce problème en recherchant les mauvaises configurations à la fois dans Kubernetes et dans les conteneurs.

Protection des communications réseau entrantes et sortantes

Kubernetes comprend également des options de mise en réseau extensibles, notamment pour contrôler la façon dont les pods communiquent entre eux à l'aide de spécifications de politiques réseau. Ces paramètres présentent toutefois des implications en matière de sécurité qui peuvent être facilement négligées. Par exemple, si aucune politique réseau Kubernetes n'est appliquée à un pod donné, alors tout le trafic réseau (entrant et sortant) est autorisé. Par défaut, Kubernetes n'applique aucune politique réseau.

La sécurité native pour Kubernetes comprend instantanément la topologie du réseau en fonction de la configuration des politiques réseau, souvent effectuée par les équipes DevOps ou d'exploitation.

Les solutions axées sur les conteneurs comprennent la configuration du trafic réseau en fonction des règles de leurs propres interfaces propriétaires, à l'extérieur de Kubernetes. La solution Red Hat Advanced Cluster Security assure l'utilisation de règles de trafic réseau cohérentes, ouvertes et standardisées au sein de Kubernetes.

Pour protéger efficacement les applications conteneurisées, il faut commencer par protéger l'infrastructure conteneurisée sur laquelle elles s'exécutent. Cette étape requiert de comprendre les vulnérabilités critiques, les vecteurs de menace et les erreurs de configuration propres à Kubernetes, ce qui n'est possible qu'avec une solution de sécurité native pour Kubernetes.

Réduction des délais et des coûts avec une solution de sécurité native pour Kubernetes

L'un des principaux atouts de Kubernetes est sa plateforme unifiée, qui permet de provisionner et d'exploiter les services d'infrastructure, que ce soit sur site ou dans le cloud. Celle-ci contribue à éliminer la complexité et les incohérences de l'exploitation et à rationaliser les workflows entre les équipes de développement, d'exploitation et de sécurité, avec à la clé un gain de temps et d'argent. Les entreprises doivent s'en inspirer pour sécuriser leurs environnements Kubernetes, et opter pour des solutions qui réduisent la quantité de travail requise.

Lors du choix d'une solution de sécurité, il faut se poser les questions suivantes :

- Cette solution peut-elle être prise en main rapidement par les équipes DevOps et de sécurité ?
- Cette solution peut-elle contribuer à accélérer l'analyse, l'étude et la correction des incidents ?
- Cette solution permet-elle d'automatiser les processus et de collecter des données pertinentes ?

Une architecture native pour Kubernetes répond à ces besoins de plusieurs manières.

Prise en main simplifiée pour les équipes

À retenir : les solutions de sécurité native pour Kubernetes facilitent la protection de Kubernetes en intégrant des abstractions et des outils ouverts et standard que les équipes DevOps utilisent déjà.

La complexité et la sécurité ne sont pas vraiment compatibles. Avec sa multitude de composants et d'outils associés, Kubernetes exige des équipes qu'elles acquièrent de nouvelles compétences et adoptent de nouveaux workflows de développement et d'exploitation. Celles-ci n'ont absolument pas besoin d'une solution de sécurité totalement distincte de ces nouveaux processus et chaînes d'outils, qui leur compliquerait encore plus la tâche.

Un framework unique et bien connu

Les architectures natives pour Kubernetes réduisent le nombre de nouvelles interfaces, de configurations et de modèles de ressources que les utilisateurs doivent maîtriser pour sécuriser leurs charges de travail cloud-native. Pour créer et distribuer des applications conteneurisées, les équipes de développement et d'exploitation utilisent déjà des abstractions standardisées telles que les manifestes Kubernetes. Les fonctions de sécurité de la solution Red Hat Advanced Cluster Security reposent sur les mêmes abstractions pour permettre aux équipes de développement, d'exploitation et de sécurité d'utiliser un seul et même framework pour créer, distribuer et exécuter des applications.

Par exemple, les utilisateurs peuvent consulter les métadonnées des fichiers des manifestes Kubernetes pour obtenir de précieux renseignements de sécurité concernant toute une application et sa fonction prévue. Les solutions axées sur les conteneurs se concentrent quant à elles sur les fichiers Dockerfile, qui comprennent uniquement les commandes à appeler pour créer une image.

La solution Red Hat Advanced Cluster Security tire également parti d'outils standardisés de gestion des paquets afin de déployer ces derniers de la même manière que les autres applications conteneurisées. La solution Red Hat Advanced Cluster Security est déployée à l'aide de charts Helm, tandis que les solutions

axées sur les conteneurs ne s'appuient que sur des options de gestion des paquets pas forcément adaptées à Kubernetes. Lorsque la sécurité s'appuie sur des abstractions et fonctions de mise en paquets ouvertes et standard, les équipes de sécurité et autres parties prenantes peuvent travailler de manière harmonisée, avec à la clé une meilleure collaboration et un gain de temps élevé.

Une seule configuration pour de multiples utilisations*, pour faciliter *une mise en œuvre précoce

Les solutions de sécurité native pour Kubernetes limitent le travail de sécurisation des configurations en utilisant Kubernetes pour orchestrer les configurations déclaratives dans l'environnement sur la base du modèle *une seule configuration pour de multiples utilisations*. Grâce à cette approche, les entreprises peuvent automatiser des centaines de contrôles pour appliquer les meilleures pratiques et politiques de sécurité.

La solution Red Hat Advanced Cluster Security permet aux utilisateurs de propager une configuration unique, telle qu'une politique réseau, qui doit s'appliquer à tous les pods d'un déploiement, plutôt que de configurer des contrôles au niveau du système sur chaque hôte d'un cluster, comme c'est le cas avec certaines solutions axées sur les conteneurs. Contrairement à ces dernières qui ne tirent pas pleinement parti de l'évolutivité et de la résilience inhérentes à Kubernetes, Red Hat Advanced Cluster Security exploite au mieux ces caractéristiques des contrôles au bénéfice des entreprises.

La sécurité des applications conteneurisées est influencée par les contrôles mis en œuvre tout au long de la chaîne d'approvisionnement des logiciels, avant l'exécution effective des conteneurs. Avec cette approche, les équipes DevOps et de développement peuvent utiliser leurs connaissances relatives à Kubernetes pour aider leur entreprise à mettre en œuvre la sécurité *dès le début du cycle* et à adopter la pratique de « sécurité en tant que code ». Ce concept est bien connu dans de nombreuses équipes, car il est similaire aux pratiques d'infrastructure en tant que code qui ont fait leurs preuves.

Les solutions de sécurité native pour Kubernetes complètent ces initiatives existantes avec des fonctionnalités telles que l'application des politiques lors du déploiement à l'aide de contrôles d'admission dynamiques intégrés à Kubernetes. Les solutions axées sur les conteneurs s'appuient sur des architectures propriétaires pour appliquer les politiques lors du déploiement. Les équipes DevOps et de développement n'ont donc pas la possibilité d'ancrer la sécurité dans les chaînes d'outils Kubernetes.

En alignant la sécurité sur les abstractions et les chaînes d'outils que les équipes DevOps et de développement connaissent déjà, la solution Red Hat Advanced Cluster Security aide les entreprises à économiser du temps et de l'argent lors de l'exécution des stratégies de sécurité cloud-native.

Accélération de l'analyse et de la correction

À retenir : les solutions de sécurité native pour Kubernetes facilitent l'analyse, la résolution des incidents et l'évaluation des risques grâce au contexte enrichi que fournit Kubernetes.

Aujourd'hui, les équipes de sécurité doivent chercher longtemps les réponses à leurs questions. Elles utilisent des outils nombreux et complexes et s'appuient sur des workflows manuels et des intégrations personnalisées pour les relier entre eux. Souvent, elles doivent faire le tri dans un flot ininterrompu d'alertes, les conteneurs rendant ce travail encore plus difficile. Les spécialistes de la sécurité font face à des défis de taille lorsqu'il s'agit de protéger les environnements cloud-native, notamment :

- Les incidents et leurs nouveaux schémas de menace non linéaires (c'est-à-dire les indicateurs d'attaque et de compromission) sont dispersés dans les composants d'applications et les environnements distribués, les conteneurs étant orchestrés de manière dynamique dans l'ensemble des machines.
- Les outils et les workflows existants n'ont pas les capacités de gérer les grands volumes de données produites par une multitude de conteneurs.

- De nombreuses approches classiques de la résolution des incidents reposent sur la conservation de données stateful permettant d'analyser les attaques et de comprendre les techniques et les procédés des attaquants. Or, elles s'avèrent inefficaces en raison de la nature éphémère des conteneurs.

Détection plus précise des menaces

Parce qu'elles fournissent un contexte détaillé, les solutions de sécurité native pour Kubernetes accélèrent l'analyse des incidents de sécurité et la correction des problèmes sous-jacents. Les applications conteneurisées, en particulier celles qui reposent sur des architectures de microservices, permettent une détection plus précise des menaces, car il est plus facile d'observer et d'identifier les anomalies sur des composants de plus petite taille dont l'activité est prévisible. En combinant ces renseignements au contexte fourni par Kubernetes, il est plus facile de distinguer les menaces réelles des faux positifs.

Le contexte fourni par Kubernetes comprend des informations sur l'ensemble du déploiement concernant :

- le processus qui sera exécuté ;
- l'existence de limites appliquées aux ressources pour éviter toute propagation entre les conteneurs ;
- les privilèges et capacités accordés à chaque conteneur ;
- l'accessibilité en écriture du système de fichiers root du conteneur ;
- le type d'appareils, de configurations et de secrets présents.

Il comprend également de précieuses métadonnées via les étiquettes qui permettent d'identifier l'application et les annotations, qui fournissent des descriptions de celle-ci.

La solution Red Hat Advanced Cluster Security utilise ce contexte pour rapprocher les données des charges de travail pertinentes (concernant les images de conteneurs et l'activité système de chaque conteneur durant l'exécution) des données de configuration fournies par Kubernetes. La sécurité de Kubernetes affecte la sécurité de chaque conteneur, et vice versa.

Parce qu'elle recueille des données sur chaque conteneur et sur la manière dont ils sont reliés les uns aux autres, la solution Red Hat Advanced Cluster Security est particulièrement efficace dans la résolution des problèmes de sécurité présents dans les environnements à grande échelle. Les solutions axées sur les conteneurs n'exploitent pas ces métadonnées issues de Kubernetes, et fournissent donc aux opérateurs de sécurité qu'une compréhension partielle de la cause profonde de l'incident.

Les solutions natives pour Kubernetes intègrent une multitude de données issues de l'ensemble des conteneurs, de Kubernetes et du cycle de vie des applications, depuis la création des images jusqu'à l'exécution des conteneurs. Grâce à ces informations, les équipes peuvent analyser l'activité d'exécution par rapport aux tâches pour lesquelles les conteneurs ont été configurés de manière déclarative en se basant sur les paramètres de Kubernetes. La solution Red Hat Advanced Cluster Security peut ainsi détecter plus précisément les activités d'exécution anormales et suspectes, tout en évitant les faux positifs et les alertes intempestives.

De leur côté, les solutions axées sur les conteneurs détectent les menaces en se basant sur les informations uniquement issues des conteneurs en cours d'exécution, ce qui entraîne un flux d'alertes que les opérateurs de sécurité sont contraints de gérer. La solution Red Hat Advanced Cluster Security regroupe les informations relatives aux menaces issues de l'ensemble du cycle de vie, des conteneurs et de Kubernetes, éliminant ainsi les silos de données que les spécialistes de la sécurité doivent assembler manuellement.

Définition des priorités de sécurité en fonction des risques

Avec la sécurité native pour Kubernetes, les données sur les vulnérabilités et la compréhension des configurations et des observations de l'activité d'exécution sont mises en corrélation afin d'évaluer la probabilité d'exploitation d'une vulnérabilité donnée.

Par exemple, l'exploitation d'une vulnérabilité qui nécessite des privilèges particuliers dépend de l'existence de ces privilèges pour les conteneurs d'un déploiement donné. Si un acteur malveillant exploite une vulnérabilité par l'écriture dans le système de fichiers d'un conteneur, il n'y a pas d'inquiétude à avoir s'il est en lecture seule. De même, il est possible de configurer un niveau élevé d'accès au réseau pour un déploiement donné s'il s'agit d'un cluster d'essai hors production ou d'une application web externe.

La solution Red Hat Advanced Cluster Security détermine un niveau de risque pour chaque déploiement de l'environnement et le classe pour les équipes de sécurité. Les solutions axées sur les conteneurs effectuent leur évaluation des risques en fonction des vulnérabilités des images et de systèmes standardisés tels que le CVSS (Common Vulnerability Scoring System), rendant tout type d'évaluation des risques inefficace. La compréhension globale des risques n'est possible qu'avec une vue d'ensemble sur Kubernetes.

L'efficacité de l'analyse et de la résolution des incidents dépend des données qu'une solution de sécurité recueille et présente à des fins d'étude. Parce qu'elles disposent de peu de temps et de ressources limitées, les équipes de sécurité doivent analyser et corriger les problèmes rapidement, ce que leur permettent les solutions de sécurité native pour Kubernetes.

Réduction des risques pour l'exploitation avec la sécurité native pour Kubernetes

Robuste et évolutive, la plateforme Kubernetes peut exécuter tous les types d'applications, y compris les charges de travail essentielles. Le développement de Kubernetes s'axe sur des fonctions qui renforcent la résilience opérationnelle, notamment :

- l'autoréparation, dont la capacité à gérer le redémarrage des conteneurs ;
- le réordonnancement ;
- la suppression de conteneurs en cas d'échec aux contrôles d'intégrité.

De plus, Kubernetes est une plateforme hautement évolutive qui s'appuie sur les mêmes principes qu'utilise Google pour exécuter des milliards de conteneurs chaque semaine. L'infrastructure de Kubernetes répond à des exigences d'exploitation élevées en matière de disponibilité, de fiabilité (temps moyen entre les pannes), de latence et d'autres indicateurs essentiels qui ont des répercussions directes sur l'activité, sans pour autant augmenter les risques pour l'exploitation concernant les applications, l'infrastructure ou l'entreprise.

Certains outils de sécurité appliquent des politiques de sécurité actives qui peuvent affecter directement l'environnement en supprimant des conteneurs ou des processus (ou en les empêchant de se lancer), en bloquant le trafic réseau ou en limitant les appels système qu'une application peut effectuer. Ces outils exposent les entreprises à davantage de risques, pour deux raisons principales :

1. Les actions entreprises par erreur peuvent engendrer une panne de l'application.
2. Les outils deviennent des dépendances supplémentaires dont les équipes d'exploitation doivent se préoccuper. En cas de défaillance, s'ils basculent en configuration fermée, ils peuvent alors perturber fortement les tâches d'exploitation, et s'ils basculent en configuration ouverte, l'entreprise est exposée.

Un outil de sécurité doit atténuer ces risques.

Application évolutive des politiques

À retenir : les contrôles de sécurité de Kubernetes permettent d'appliquer des politiques de sécurité de façon évolutive tout en limitant les perturbations des applications essentielles.

En utilisant l'outil d'orchestration pour exécuter les fonctions de sécurité, les entreprises réduisent les risques pour l'exploitation et renforcent l'évolutivité de leurs environnements Kubernetes. Il n'était pas possible d'adopter cette approche auparavant, car les plateformes d'infrastructure ne disposaient pas de fonctionnalités de sécurité native suffisantes. Aujourd'hui, Kubernetes comprend :

- des politiques réseau pour la segmentation du réseau ;
- des contrôleurs d'admission pour intercepter les requêtes adressées au serveur de l'API Kubernetes ;
- des secrets pour le stockage d'informations d'identification sensibles ;
- le contrôle d'accès basé sur les rôles pour accorder des autorisations aux utilisateurs et aux comptes de service ;
- et bien d'autres fonctionnalités.

Cette approche architecturale évite le recours à des outils de sécurité supplémentaires pour exécuter certaines fonctions de sécurité.

À l'opposé, certaines solutions axées sur les conteneurs exposent les entreprises à différents risques pour l'exploitation. Par exemple, ces solutions se trouvent souvent contraintes d'utiliser des proxies en ligne pour restreindre le trafic réseau entre les conteneurs, ou encore de prendre des mesures encore plus intrusives, comme écraser les règles IP des pare-feu.

De même, pour éviter de déployer des conteneurs qui présentent des vulnérabilités critiques ou qui contiennent des paquets non autorisés, les solutions axées sur les conteneurs peuvent avoir recours à des shims pour intercepter et remplacer des requêtes adressées au moteur de conteneurs. Cette approche introduit des points de défaillance unique dans l'environnement, car l'échec d'un proxy en ligne ou du moteur de conteneurs peut engendrer l'échec des applications.

La solution Red Hat Advanced Cluster Security stocke les politiques de segmentation du réseau, de contrôle d'admission et d'autres fonctions de sécurité dans Kubernetes, ce qui supprime les dépendances d'exploitation. Si pour une raison ou une autre Red Hat Advanced Cluster Security devient indisponible, les politiques de sécurité continuent d'être appliquées, ce qui n'est pas le cas avec les solutions axées sur les conteneurs.

Les solutions axées sur les conteneurs introduisent également des problèmes d'évolutivité, car dans certains cas, des fonctions de sécurité distinctes doivent s'exécuter sur chacun des hôtes du cluster. Cette approche affecte les performances ainsi que la disponibilité des ressources pour les conteneurs d'applications, et requiert une attention supplémentaire de la part des équipes d'exploitation, ce qui augmente la charge d'exploitation globale de l'entreprise.

L'outil d'orchestration de Red Hat Advanced Cluster Security joue un rôle clé dans l'application des politiques de sécurité, en exploitant les capacités de Kubernetes pour en assurer la fiabilité et l'évolutivité. Les équipes d'administration des clusters et de l'infrastructure peuvent ainsi se concentrer sur l'exploitation de Kubernetes sans se préoccuper des composants tiers. De plus, les entreprises bénéficient de nouveaux contrôles de sécurité ainsi que d'un système Kubernetes fiable et évolutif qui s'appuie sur un vaste écosystème de centaines d'entreprises et une communauté de milliers de développeurs.

Les solutions de sécurité native pour Kubernetes sont indépendantes des architectures communautaires, comme la spécification standard d'interfaces réseau CNI (Container Network Interface). Les fonctionnalités de segmentation du réseau de la solution Red Hat Advanced Cluster Security s'exécutent de manière cohérente avec tout plug-in CNI.

Les solutions axées sur les conteneurs peuvent dépendre de certains plug-ins ou être incompatibles avec d'autres, compliquant les problèmes d'exploitation auxquelles les entreprises sont déjà confrontées. Les contrôles de la solution Red Hat Advanced Cluster Security ne dépendent d'aucun outil ou plug-in, permettant ainsi aux équipes DevOps et d'exploitation d'utiliser ceux qui répondent à leurs besoins.

Élimination des conflits d'exploitation

À retenir : la sécurité native pour Kubernetes permet de réduire les problèmes d'exploitation qui découlent de configurations incohérentes, d'un manque de coordination et d'erreurs commises par les utilisateurs.

Afin de réduire les risques pour l'exploitation, les entreprises doivent également renforcer la cohérence des configurations de sécurité pour éviter tout comportement imprévisible des applications et la complexité qui conduit les utilisateurs à faire des erreurs. Avec une architecture native pour Kubernetes, la probabilité de ce type de problèmes d'exploitation est réduite.

Les équipes DevOps et de sécurité qui mettent en place plusieurs outils, contrôles et politiques peuvent créer des incohérences dans leurs configurations de sécurité. Des incohérences peuvent également survenir en cas de conflit entre les configurations effectuées aux différentes couches de la pile d'infrastructure. Par exemple, des paramètres configurés au niveau du conteneur peuvent être en conflit avec les paramètres configurés au niveau de Kubernetes.

Avec la sécurité native pour Kubernetes, les équipes de développement, d'exploitation et de sécurité peuvent consulter et gérer les politiques et leur application de manière centralisée au sein même de Kubernetes. Dans Red Hat Advanced Cluster Security, les politiques de segmentation du réseau et de contrôle d'admission sont conservées dans Kubernetes pour faciliter leur consultation.

Avec les solutions axées sur les conteneurs, les utilisateurs sont contraints de mettre en place les contrôles à l'aide de différents outils, ce qui entraîne un manque de coordination organisationnelle. Par exemple, un membre de l'équipe DevOps peut avoir recours à des politiques réseau Kubernetes pour restreindre le trafic réseau autorisé vers une application, tandis qu'un membre de l'équipe de sécurité utilise un pare-feu propriétaire. Cette situation peut engendrer des conflits entre les configurations et des failles dans la protection.

De même, des configurations incohérentes entre Kubernetes et les conteneurs peuvent avoir des effets inattendus sur les applications en cours d'exécution. Par exemple, les solutions axées sur les conteneurs peuvent restreindre un conteneur à certains types d'appels au système d'exploitation, même lorsqu'aucune restriction similaire n'est configurée dans Kubernetes à l'aide de politiques de sécurité des pods. En conséquence, un utilisateur qui vérifierait la configuration de Kubernetes pourrait ne pas identifier l'origine du problème d'exploitation, car la configuration recherchée se trouve dans une autre couche.

Et, en cas de conflit entre les restrictions, le trafic peut ne pas être autorisé ou restreint comme prévu. Par exemple, une politique réseau de Kubernetes autorise le trafic entre les conteneurs A et B, mais un proxy en ligne axé sur les conteneurs restreint le trafic entre ces derniers, ce qui peut entraîner de nombreux problèmes d'exploitation.

La sécurité native pour Kubernetes considère Kubernetes en tant que source fiable pour ses fonctions de sécurité, et réduit le nombre de changements de contexte nécessaires aux équipes d'exploitation et d'ingénierie de la fiabilité des sites. Les problèmes de sécurité sont immédiatement associés aux objets et aux ressources Kubernetes utilisés par ces équipes au quotidien pour assurer la disponibilité et la fiabilité de Kubernetes.

Cette approche permet de réduire la complexité de l'exploitation qui contribue aux erreurs des utilisateurs affectant les environnements Kubernetes. Avec les solutions axées sur les conteneurs, les équipes d'exploitation et d'ingénierie de la fiabilité des sites doivent intervenir pour mettre en corrélation les problèmes de sécurité avec les données du fournisseur et de Kubernetes. La solution Red Hat Advanced Cluster Security permet aux utilisateurs de consulter les données dans un format cohérent avec celui que propose Kubernetes. Les opérateurs de clusters peuvent ainsi identifier plus rapidement et simplement les problèmes, et les résoudre à l'aide des chaînes d'outils et des workflows de leur choix.

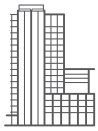
Conclusion

Les technologies cloud-native ont transformé (et continueront de transformer) la façon dont les entreprises exécutent leurs applications et, par conséquent, leur vision de la sécurité. Elles permettent l'adoption du DevSecOps et d'autres pratiques de collaboration, et font évoluer notre secteur vers le modèle de sécurité « en tant que code ». Leader sur le marché, le système d'orchestration de conteneurs Kubernetes se trouve au cœur de ce changement générationnel. S'il existe de nombreuses approches de protection des environnements de conteneurs, la sécurité native pour Kubernetes offre des informations approfondies, une analyse rapide et une exploitation simplifiée.

La solution de sécurité native pour Kubernetes de Red Hat apporte de nombreux avantages uniques aux entreprises qui développent et exécutent des applications conteneurisées :

- Protection renforcée des systèmes grâce à l'élimination des zones d'ombre et à la détection des vulnérabilités critiques et des erreurs de configuration propres à Kubernetes
- Réduction des coûts et des délais grâce à une prise en main facilitée pour les équipes et à l'accélération de l'analyse et de la correction des erreurs sur la base du contexte enrichi que fournit Kubernetes
- Diminution des risques pour l'exploitation grâce à l'application évolutive des politiques de sécurité et à l'élimination de la complexité de l'exploitation résultant de configurations incohérentes et d'erreurs commises par les utilisateurs
- Plateforme standardisée adaptée à différents cas d'utilisation du cycle de vie des applications cloud-native pour les équipes de développement, d'exploitation et de sécurité

Grâce à la solution Red Hat Advanced Cluster Security, les entreprises sont à même de sécuriser efficacement leurs environnements de production Kubernetes où qu'ils se trouvent, à grande échelle.



À propos de Red Hat

Premier éditeur mondial de solutions Open Source, Red Hat s'appuie sur une approche communautaire pour fournir des technologies Linux, de cloud hybride, de conteneurs et Kubernetes fiables et performantes. Red Hat aide ses clients à intégrer des applications nouvelles et existantes, à développer des applications cloud-native, à standardiser leur environnement sur son système d'exploitation leader sur le marché ainsi qu'à automatiser, sécuriser et gérer des environnements complexes. Red Hat propose également des services d'assistance, de formation et de consulting primés qui lui ont valu le titre de conseiller de confiance auprès des entreprises du classement Fortune 500. Partenaire stratégique des prestataires de cloud, intégrateurs système, fournisseurs d'applications, clients et communautés Open Source, Red Hat aide les entreprises à se préparer à un avenir toujours plus numérique.

facebook.com/redhatinc
@RedHatFrance
linkedin.com/company/red-hat

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)
00800 7334 2835
europe@redhat.com

FRANCE
00 33 1 41 91 23 23
fr.redhat.com

fr.redhat.com
#F28129_0421