Sécurité des conteneurs 101

COMPRÉHENSION DES BASES DE LA SÉCURISATION DES CONTENEURS

PRISMA
BY PALO ALTO NETWORKS

MediaOps

Toutes les équipes en charge de la cybersécurité ont désormais compris que la révolution des conteneurs est en marche. Les développeurs ont largement adopté les conteneurs, ces derniers facilitant en effet le développement et le déploiement d'applications natives dans le cloud. Les conteneurs suppriment une grande partie des problèmes généralement associés au déplacement du code d'application de la phase d'essai à la phase de production. De plus, le code d'application conditionné sous la forme de conteneurs peut être exécuté n'importe où. Toutes les dépendances associées à n'importe quelle application sont incluses dans l'application en conteneurs. Les applications en conteneurs sont donc particulièrement portables au niveau de machines virtuelles ou de serveurs sans système d'exploitation exécutés dans un centre de données local ou dans un cloud public.

Ce niveau de flexibilité permet aux développeurs de réaliser des gains de productivité si importants qu'ils ne peuvent être ignorés. Toutefois, comme c'est le cas avec le développement de n'importe quelle architecture informatique nouvelle, les applications natives dans le cloud doivent toujours être sécurisées. Les environnements de conteneurs s'accompagnent de toute une série de problèmes de cybersécurité impliquant les images, les conteneurs, les hôtes, les moteurs d'exécution, les registres et les plateformes d'orchestration qui doivent tous être sécurisés.

Le défi que les organisations doivent relever est d'abord de comprendre le nombre de couches d'un environnement informatique natif dans le cloud en interaction les unes avec les autres, puis de trouver les outils adaptés pour développer un ensemble de processus répétitif pour sécuriser chaque couche. Les problèmes de cybersécurité spécifiques aux conteneurs incluent les suivants :

IMAGES : les failles peuvent, comme n'importe quel autre élément du code, avoir un impact sur les images des conteneurs. Développer une nomenclature, identifier des secrets intégrés, classifier toutes les couches d'une image sont autant de tâches de cybersécurité fondamentales qui doivent toujours être traitées. Les choses se compliquent avec le nombre de conteneurs exécutés dans un environnement d'applications et la fréquence de leurs mises à jour. Grâce au développement de pratiques DevOps, les organisations peuvent désormais mettre les applications en conteneurs à jour plusieurs fois par semaine. Chaque mise à jour de ce qui peut rapidement représenter des milliers de conteneurs exécutés dans un environnement informatique constitue une opportunité pour l'infiltration de failles dans l'environnement en question.

REGISTRES DE CONTENEURS : les registres de conteneurs sont une source centralisée pratique pour le stockage et la distribution d'images d'applications. Les organisations d'aujourd'hui peuvent facilement avoir des dizaines de milliers d'images stockées dans leurs registres. Les registres sont essentiels au mode de fonctionnement de votre environnement en conteneurs, ils doivent donc impérativement être sécurisés. Les registres permettent d'apporter de l'ordre dans l'éventuel chaos des conteneurs. Ils constituent cependant également un chemin que les cybercriminels peuvent aisément emprunter pour compromettre l'ensemble de l'environnement. La surveillance continue des registres afin de détecter tout changement au niveau du statut de vulnérabilité est une exigence de sécurité de base qui doit inclure le confinement du serveur qui héberge le registre

MOTEURS D'EXÉCUTION DE CONTENEURS : les moteurs d'exécution de conteneurs sont l'un des éléments d'une pile de conteneurs les plus difficiles à sécuriser, les outils de sécurité traditionnels n'ont en effet pas été conçus pour la surveillance des conteneurs en cours d'exécution. Les outils patrimoniaux ne peuvent généralement pas analyser l'intérieur des conteneurs et encore moins établir une référence de ce à quoi un environnement de conteneurs sûr doit ressembler. Les problèmes de sécurité au niveau des moteurs d'exécution de conteneurs exigent des équipes en charge de la cybersécurité de se focaliser sur les problèmes de sécurité des applications qui ne sont pas traités par les pare-feu patrimoniaux.

ORCHESTRATION DES CONTENEURS : le contrôle des accès aux plateformes d'orchestration des conteneurs telles que Kubernetes afin d'éviter les risques générés par des comptes disposant de droits excessifs, des attaques via le réseau ou des mouvements latéraux indésirables doit être traité à l'aide de listes blanches, de manière similaire au traitement des accès aux environnements informatiques patrimoniaux. En cas de changements au niveau d'une plateforme d'orchestration de conteneurs, il est nécessaire de sécuriser également les communications entre les pods d'une grappe Kubernetes partagée par plusieurs applications.

SYSTÈMES D'EXPLOITATION DES HÔTES : le système d'exploitation qui héberge votre environnement de conteneurs est sans doute l'aspect le plus important et le plus souvent négligé de la sécurité d'un environnement de conteneurs. Le moindre compromis au niveau de l'environnement hôte offre aux cybercriminels un accès à l'ensemble de l'environnement d'applications. Chaque hôte doit disposer de son ensemble de contrôles des accès et doit également être surveillé en continu afin de détecter les failles qui apparaissent après le premier déploiement de l'hôte.

LES AVANTAGES DES CONTENEURS POUR LA CYBERSÉCURITÉ

Étant donné tous les défis associés à la sécurisation des applications en conteneurs, la réticence affichée par tant de professionnels de la cybersécurité lorsqu'il s'agit de déployer des conteneurs dans un environnement de production est compréhensible. Il existe des avantages manifestes en termes de productivité des développeurs, la plupart des organisations commencent cependant tout juste à découvrir les outils et processus à adopter pour sécuriser les applications en conteneurs. Aussi intimidant que le défi puisse paraître, les conteneurs présentent cependant un avantage inestimable que les équipes en charge de la cybersécurité n'évaluent pas à sa juste valeur. Les conteneurs étant très souvent supprimés et remplacés, les processus associés au traitement des failles sont bien plus simples. Au lieu d'avoir à patienter parfois des mois pour qu'une application monolithique bénéficie d'un correctif, il est possible d'ajouter de nouvelles fonctionnalités aux environnements d'applications en supprimant et en remplaçant des conteneurs. Ce processus est limité à un sous-ensemble de l'application, connu sous le nom de microservice, et peut généralement être effectué en l'espace de quelques minutes dans le cadre du processus de gestion du cycle de vie de l'application activé par une plateforme d'intégration continue/de déploiement continu telle que Jenkins. Il est ainsi possible de réduire considérablement la durée pendant laquelle une application fonctionne avec des failles connues dans un environnement de production.

Cette fonctionnalité est sans doute la force motrice derrière la montée en puissance des meilleurs processus DevSecOps par le biais desquels les développeurs prennent désormais davantage de responsabilités dans la mise en application des contrôles de cybersécurité. Les équipes en charge de la cybersécurité devront toujours définir ces contrôles et valider leur mise en application. Toutefois, les développeurs étant maintenant responsables de la mise en application de ces contrôles, le nombre d'applications pouvant être soumises à un audit de cybersécurité augmente au fil de la maturité des processus DevSecOps adoptés.

PRISMA BY PALO ALTO NETWORKS | MediaOps

PRISMA BY PALO ALTO NETWORKS | MediaOps

OUTILS POUR LA SÉCURITÉ DES CONTENEURS

Rien que l'an dernier, les outils que les organisations peuvent utiliser pour sécuriser les conteneurs se sont développés, que ce soit en termes de fonctionnalités ou de sophistication. Quel que soit le niveau de maturité DevSecOps atteint, les outils de sécurisation des conteneurs sont plus accessibles que jamais. Les outils pour la cybersécurité des conteneurs que les organisations doivent adopter et maîtriser incluent les suivants :

SURVEILLANCE DES CONTENEURS : pour assurer et préserver la sécurité des conteneurs, des outils de surveillance des conteneurs sont nécessaires : ils permettent de suivre les unités informatiques atomiques les plus éphémères conçues. Les développeurs suppriment et remplacent en permanence les conteneurs, des outils de surveillance qui permettent aux équipes informatiques et en charge de la cybersécurité d'appliquer un horodatage sur les conteneurs sont essentiels lorsqu'il est nécessaire de déterminer avec précision ce qui s'est passé et quand dans un environnement en conteneurs.

OUTILS D'ANALYSE DES CONTENEURS : il est nécessaire de surveiller en permanence les conteneurs afin de s'assurer de l'absence de failles à la fois avant le déploiement dans un environnement de production et après leur remplacement. Il est trop facile pour les développeurs d'inclure par erreur une bibliothèque dans un conteneur disposant de failles connues. Il est également important de rappeler que de nouvelles failles sont découvertes quasiment tous les jours. Cela signifie que ce qui semble être une image de conteneur totalement sûre aujourd'hui pourrait être le vecteur de distribution de toutes formes de malwares demain.

PARE-FEU DE CONTENEURS : un pare-feu de conteneurs inspecte et protège l'ensemble du trafic entrant et sortant des conteneurs, ainsi que le trafic entrant et sortant des réseaux externes et des applications patrimoniales. La plupart des pare-feu de conteneurs permettent de gérer un large spectre du trafic entrant et sortant de microservices constitués de plusieurs conteneurs.

MOTEURS DE STRATÉGIES : les outils de cybersécurité modernes permettent aux équipes en charge de la cybersécurité de définir des stratégies basées sur des listes blanches des personnes et des éléments autorisés à accéder à un microservice donné. Les organisations ont besoin d'un cadre pour définir ces stratégies et ensuite veiller à ce qu'elles soient mises à jour de manière cohérente dans un environnement d'applications de conteneurs particulièrement distribué.

DÉFENSE DE LA SURFACE D'ATTAQUE HYBRIDE

Maintenant que les conteneurs facilitent le transport des applications en conteneurs d'une plateforme à une autre, les organisations doivent être en mesure d'appliquer des stratégies de cybersécurité et de résoudre les problèmes qui surviennent au niveau de plusieurs plateformes. La plupart des conteneurs sont initialement déployés sur des machines virtuelles traditionnelles afin de veiller à ce qu'il y ait une couche d'isolation entre les charges de travail applicatives partageant la même plateforme.

Il est également possible rencontrer un cas où les organisations ne souhaitent pas déployer une machine virtuelle en raison des frais supplémentaires engendrés, ce qui peut avoir un impact négatif sur les performances des applications. Les développeurs préfèrent alors déployer les conteneurs sur des serveurs sans système d'exploitation ou sur une catégorie émergente de machines virtuelles plus légères. Cela est notamment le cas dans les environnements basés sur des processeurs graphiques qui ne se prêtent pas aux techniques de virtualisation traditionnelles autres que les conteneurs. Le refus de payer des frais de licence pour le logiciel d'une machine virtuelle est une autre raison pour laquelle une organisation peut décider de déployer des conteneurs sur un serveur sans système d'exploitation.

Quelle que soit la motivation, la seule chose dont les équipes en charge de la cybersécurité peuvent être sûres, c'est la présence des applications en conteneurs sur site ou dans des environnements informatiques dans le cloud public. Chaque environnement est constitué de plusieurs types de machines virtuelles et physiques exécutant des conteneurs qui doivent tous être sécurisés via un cadre commun.

Pour compliquer encore davantage les choses, les cadres informatiques sans serveur développés à l'aide de conteneurs constituent une autre surface d'attaque qui doit être sécurisée. Les cadres informatiques sans serveur, basés sur une architecture évènementielle, permettent aux développeurs d'appeler un processus enfant à partir de leurs applications à la demande. Il n'est ainsi plus nécessaire d'inclure un code dans une application pour exécuter une fonction qui n'est requise que de manière intermittente. Moins une application contient de code, plus elle est facile à sécuriser. Les équipes en charge de la cybersécurité ne doivent cependant pas négliger la nécessité de sécuriser le cadre informatique sans serveur.

LE GRAND PARADOXE DE LA CYBERSÉCURITÉ

Des millions de postes dans le domaine de la cybersécurité ne sont actuellement pas pourvus. Le volume de code d'application à sécuriser continue à augmenter de manière exponentielle, notamment grâce à la montée en puissance des conteneurs. La seule manière pour les équipes en charge de la cybersécurité et leurs collègues développeurs d'applications de suivre le rythme est de s'appuyer davantage sur l'automatisation.

Même s'il était possible de trouver des professionnels de la cybersécurité pour occuper tous ces postes, la plupart des organisations auraient toujours du mal à retenir l'expertise en matière de cybersécurité. Le seul moyen de limiter efficacement l'impact de la rotation du personnel en charge de la cybersécurité est d'automatiser autant de processus manuels que possible. Cette approche permet non seulement de développer des stratégies de cybersécurité à l'échelle, mais aussi que le personnel en charge de la cybersécurité puisse consacrer davantage de temps à des tâches telles que la recherche de malwares avant qu'ils ne soient activés.

La question n'est plus de savoir si les tâches de cybersécurité seront automatisées mais plutôt de déterminer leur niveau d'automatisation.

PLAIDOYER EN FAVEUR DE L'UNIFICATION

Le cloud computing natif, sous toutes ses formes, que les conteneurs ont permis de mettre en place est de plus en plus envahissant. La nécessité d'un cadre de cybersécurité pouvant être appliqué aux conteneurs et aux cadres informatiques sans serveur associés est donc évidente. Cet argument ne concerne cependant pas uniquement les applications de cloud computing natif. En effet, elles ne supprimeront pas l'ensemble du code d'application monolithique déployé dans les entreprises du jour au lendemain. Des organisations de toutes les tailles exécute ront un mélange d'applications natives dans le cloud patrimoniales et émergentes d'ici la fin de la prochaine décennie. Le prochain grand défi pour la cybersécurité sera de trouver un moyen de développer et de mettre à jour des stratégies de cybersécurité dans ces deux types d'environnements en utilisant le même cadre de gestion.

La réalisation de cet objectif est la principale raison pour laquelle Palo Alto Networks a fait l'acquisition il y a quelques mois de Twistlock, un fournisseur de plateformes de sécurité à conteneurs, et de PureSec, le fournisseur d'un cadre pour la sécurisation des cadres informatiques sans serveur. Palo Alto Networks a déjà investi des millions de dollars pour développer un cadre Prisma d'automatisation de la gestion de la cybersécurité dans les environnements d'applications monolithiques patrimoniaux. Prisma est actuellement en cours d'extension pour prendre en charge les applications de cloud computing natif basées sur des conteneurs et des cadres informatiques sans serveur.

Prisma est ainsi sur le point de devenir la plateforme de gestion du cycle de vie de la cybersécurité la plus complète disponible.

CONCLUSION

Comme toujours, c'est à la fois la meilleure et la pire des époques pour la cybersécurité. Par de nombreux aspects, préserver la cybersécurité est plus difficile que jamais, les environnements informatiques sont en effet plus hétérogènes qu'avant. Parallèlement, le rythme des innovations en matière de cybersécurité n'a jamais été aussi rapide.

La décision la plus importante que les organisations devront prendre dans les prochains mois concernant la cybersécurité sera d'identifier le fournisseur disposant des outils et de l'expertise nécessaires à la sécurisation des environnements existants mais également à la sécurisation des environnements d'applications émergents étant donné que les développeurs continuent d'adopter des plateformes novatrices quelles que soient les réserves que le reste de l'organisation peut émettre en matière de cybersécurité.

Pour en savoir plus au sujet de la sécurisation de ces environnements, veuillez consulter le site *www.paloaltonetworks.com/cloud-security*


PRISMA™
BY PALO ALTO NETWORKS