# Sécurité du runtime dans le cloud : le pourquoi et le comment

Les containers et technologies sans serveur ne datent pas d'hier. Cela fait même presque une décennie qu'ils existent sous leur forme actuelle. La création de Docker remonte déjà à 2013, tandis que les premières fonctions sans serveur AWS Lambda sont apparues en 2014.

Ce qui a bien changé depuis, c'est le rythme avec lequel les technologies cloud-native investissent les environnements de production. D'après un rapport de mars 2020, dans 29 % des entreprises, plus de la moitié des applications de production seraient déjà containerisées, soit un bond de 31 % en seulement six mois. De son côté, Gartner prévoit que 70 % des entreprises exécuteront au moins trois applications dans des containers d'ici 2023. Dans la même veine, un rapport Forrester révèle que pour plus de 80 % des DSI, l'extension de l'usage des containers et autres technologies cloud-native fait partie des priorités.

L'adoption rapide de ces nouvelles technologies cloud a propulsé les outils et processus DevSecOps au cœur des pratiques de développement. C'est ainsi que les équipes superposent des couches de sécurité visant à protéger les workloads cloud-native à chaque étape du pipeline CI/CD.

Parmi ces nouvelles mesures de protection, la sécurité des environnements d'exécution, ou « sécurité du runtime », joue un rôle essentiel. En automatisant la sécurité des applications containerisées et de leurs environnements hyper-dynamiques, la sécurité du runtime fait coup double. D'une part, elle répond aux exigences uniques de sécurité et de conformité des environnements cloud-native. De l'autre, elle donne aux équipes les moyens d'appliquer les processus DevSecOps à leurs workloads cloud-native.

## Qu'est-ce que la sécurité du runtime ?

La sécurité du runtime fait référence à la surveillance et à la validation de bout-en-bout de toutes les activités au sein des containers, hôtes et fonctions sans serveur.

En pratique, elle recourt aux contrôles d'applications et listes d'autorisation pour établir une base de référence des comportements jugés normaux pour chaque hôte, container, fonction sans serveur et autres objets de l'environnement cloud-native. Ensuite, les outils de sécurité runtime observent en temps réel les systèmes de fichiers, processus et activités réseaux pour détecter les mouvements suspects et anormaux, puis alerter les équipes en conséquence.

En matière de sécurité, la surveillance en temps réel n'est évidemment pas une nouveauté. Cela fait même des années que les plateformes SIEM passent au crible les environnements applicatifs à la recherche de la moindre anomalie.

Ce qui change avec la sécurité du runtime dans les écosystèmes cloud-native, c'est la nature changeante de ces environnements et l'impossibilité d'établir une base de référence au sens traditionnel du terme. Entre les démarrages et arrêts incessants des instances de containers et de fonctions sans serveur d'une part, et les équilibreurs de charge qui redirigent continuellement le trafic entre différentes instances d'autre part, les sources de données traditionnelles (journaux, trafic réseau, etc.) ne suffisent pas à elles seules à détecter des anomalies symptomatiques d'une compromission de sécurité. La sécurité du runtime va plus loin en interprétant les variations des tendances comportementales au fil du temps, puis en établissant une base de référence dynamique reflétant ces changements. Dès lors, les outils de sécurité idoines peuvent détecter les changements dans les processus de containers internes, l'activité des systèmes de fichiers et tout autre comportement déviant de la norme, y compris dans les environnements à forte amplitude de charge.

En d'autres termes, la sécurité du runtime offre toutes les fonctionnalités essentielles pour une protection à la fois prédictive et basée sur les menaces effectives dans des environnements en perpétuelle évolution.

## Pourquoi la sécurité du runtime est-elle si importante ?

Par sa capacité à détecter les anomalies dans des environnements dynamiques, la sécurité du runtime offre toute une palette d'avantages avec lesquels les outils de surveillance traditionnels ne peuvent tout simplement pas rivaliser dans un écosystème cloud-native.

### Détection des menaces dans les environnements dynamiques

Tout d'abord, la sécurité du runtime est le seul moyen de sécuriser les applications cloud-native à grande échelle. C'est même là sa principale force. Comme nous l'évoquions plus haut, toute la difficulté consiste à établir la base d'un comportement « normal », puis d'identifier tout écart dans un environnement distribué en mutation constante. La tâche devient même particulièrement délicate lorsque cet environnement est constitué de centaines de containers/fonctions sans serveur et de dizaines de microservices.

Ensuite, la sécurité du runtime recourt à l'IA et au machine learning pour automatiser le processus de modélisation des activités normales et de détection des déviations de cet axe, notamment dans les environnements complexes où ce genre d'exercice dépasse les capacités du cerveau humain

### Prévention ou atténuation de l'impact d'une compromission

Dans un autre registre, la sécurité du runtime aide à réduire l'exposition des environnements aux vulnérabilités. Elle aide notamment à atténuer l'impact d'une compromission de sécurité par un meilleur contrôle sur les systèmes de fichiers, les processus et les activités réseau pour chaque container et fonction sans serveur.

Les outils de sécurité du runtime peuvent par ailleurs modéliser des comportements sûrs au niveau applicatif, puis faire appliquer des règles prévenant toute activité dangereuse sur le container et l'hôte. Ils parviennent ainsi à bloquer les containers compromis exécutant des processus qui visent à infecter d'autres containers, voire l'hôte.

### Réponse à incident

Les données collectées par les outils de sécurité du runtime jouent un rôle essentiel dans la réponse à incident. Plus précisément, ils capturent et stockent des données d'audit qui permettent aux équipes de sécurité de retracer le déroulement d'un incident, même si l'environnement cloud-native n'a plus la même configuration qu'au moment des faits.

## Défis de l'implémentation de la sécurité du runtime

La sécurité du runtime est un concept complexe et difficile à implémenter, pour différentes raisons que nous évoquons ci-dessous. Il existe des solutions à ces problématiques, à condition d'utiliser des outils de sécurité conçus pour les environnements modernes et hautement complexes que sont les écosystèmes cloud-native.

### Changements constants des environnements

Au risque de nous répéter, il est extrêmement difficile d'établir une base de référence des activités dites « normales » dans des environnements cloud-native où les configurations changent et où les charges varient constamment. De nombreuses variables entrent dans l'équation, notamment les variations de schémas de trafic entre différentes heures de la journée et différents jours de la semaine, ou encore la réaction des outils d'orchestration de containers en cas de changement des demandes d'applications ou de défaillance d'un pod.

### Diversité des technologies

Containers, fonctions sans serveur, machines virtuelles, services cloud... les environnements cloud-native sont composés d'une mosaïque de technologies. C'est pourquoi les outils de sécurité du runtime doivent être capables d'interpréter les caractéristiques architecturales et les schémas comportementaux de chacun de ces composants, de façon à modéliser les comportements normaux puis à éviter tout écart.

### Risques d'imprécision des alertes

Envoyer des alertes n'a rien de compliqué. Ce qui est plus difficile en revanche, c'est d'envoyer des alertes pertinentes et d'éviter qu'un décalage ne se crée à mesure que les environnements changent. Dans ce genre de scénario, des configurations manuelles qui ont déclenché des alertes précises pendant un certain temps peuvent vite finir par générer de nombreux faux positifs et faux négatifs.

## Avantages de la sécurité du runtime

Lorsqu'elle est implémentée dans les règles de l'art, une solution de sécurité du runtime apporte de nombreux avantages :

### Modélisation automatique du comportement des applications

Les outils de sécurité du runtime doivent systématiquement reconnaître les signes caractéristiques d'un comportement jugé sûr. Lorsque vous devez gérer des dizaines de services et des centaines de containers, de fonctions sans serveur et de VM qui les hébergent, vous n'avez pas le temps de configurer manuellement des modèles comportementaux, ni même de collecter vous-même les données associées. Il vous faut donc des outils capables d'effectuer toutes ces tâches automatiquement.

### Contrôle du comportement des applications

Hormis la modélisation des comportements normaux, une solution de sécurité du runtime doit pouvoir définir automatiquement les comportements autorisés et non autorisés pour chaque container, fonction sans serveur et tout autre objet de l'environnement. Un container doit ainsi savoir si, en présence d'un autre container, il peut communiquer avec lui, voire accéder à ses volumes de stockage de données. En cas de compromission de sécurité, ces règles permettent de limiter la propagation de l'attaque.

### Envoi d'alertes pertinentes

Même si les outils de sécurité du runtime sont capables de déployer automatiquement des mesures défensives, ils doivent aussi pouvoir alerter votre équipe lorsqu'une intervention s'impose. Il leur faut pour cela surveiller toutes sortes de ressources sur les infrastructures cloud-native (processus, connexions réseau, lectures/écritures sur les systèmes de fichiers, etc.), puis alerter les analystes sécurité en cas de changement suspect.

Pour éviter un trop-plein d'alertes, ces solutions doivent pouvoir se fier à des règles dynamiques pour décider par elles-mêmes quand déclencher l'alerte. Une activité jugée dangereuse un jour peut en effet être considérée comme bénigne le lendemain. Dans ces conditions, impossible pour des règles d'alerte statiques de tenir le rythme face aux menaces du cloud.

### Intégrations à d'autres solutions de sécurité

La sécurité du runtime ne représente que l'une des couches de défense actives dans votre écosystème de sécurité. Protection automatique des données, outils d'audit et de contrôle d'accès, scanners d'images de containers... tous ces autres éléments jouent également un rôle essentiel.

Les solutions de sécurité du runtime n'expriment leur plein potentiel que lorsqu'elles s'intègrent à d'autres outils de sécurité. Elles apportent ainsi des détails et du contexte en cas d'incident, tout en aidant à comprendre l'impact qu'une menace sur une couche de la stack technologique (sur l'environnement d'exécution, par exemple) peut avoir sur une autre couche (comme notamment les données au repos).

## Exploiter tout le potentiel de la sécurité du runtime

Les outils de sécurité du runtime offrent tout un éventail de fonctionnalités. Cependant, la valeur que vous en tirez dépend en grande partie de votre approche de la défense du runtime. Pour extraire le maximum de ces solutions, visez les objectifs suivants :

### Couverture de bout en bout

En ne surveillant qu'une partie de votre environnement, ou en vous limitant aux principaux services et infrastructures, vous risquez de laisser passer certaines menaces. Pour une protection réellement efficace, la sécurité du runtime doit couvrir toutes les couches de votre environnement, tant pour les environnements dev/test que pour les workloads de production.

### Détection des incidents en temps réel

Même si les solutions de sécurité du runtime sont capables d'atténuer l'impact d'une compromission a posteriori, leur vocation première est de détecter et neutraliser les menaces en temps réel, avant qu'elles n'aient la moindre chance de se propager.

### Traitez chaque ressource individuellement

Hôte, instance de container, fonction sans serveur... chaque ressource de votre environnement cloud-native a une configuration et un comportement qui lui sont propres. D'où l'importance de modéliser chacune séparément. Par exemple, n'imaginez pas que parce que les containers partagent la même image, ils se comporteront de la même manière. Ce faisant, vous vous enfermerez dans une approche compartimentée qui limitera votre visibilité sur les incidents de sécurité.

## La sécurité du runtime avec Prisma® Cloud

Lorsque vous migrez vers des technologies cloud-native, la sécurité du runtime devient l'un des piliers de votre stratégie défensive. Impossible de concrétiser tous les avantages des containers, fonctions sans serveur et services cloud sans une sécurité du runtime capable de protéger votre investissement.

C'est pourquoi Prisma Cloud propose une plateforme de sécurité cloud-native complète. Sa mission : assurer la défense du runtime tout en offrant d'autres fonctionnalités essentielles : protection des données, gestion des contrôles d'accès, gestion de la sécurité du cloud, etc. Les entreprises possèdent ainsi tout l'arsenal défensif pour protéger leurs environnements cloud, peu importe leur complexité et leur évolutivité. Pour en savoir plus, demandez votre démo.

paloalto NETWORKS

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam,
Pays-Bas

+31 20 888 1883

www.paloaltonetworks.fr


prisma_wp_add-runtime-defense-cloud-security_041921-fr