CROWDSTRIKE

FALCON CLOUD WORKLOAD PROTECTION

Prévention des intrusions pour les workloads cloud et les conteneurs

UNE PROTECTION DES WORKLOADS CLOUD QUI RÉVOLUTIONNE LES TÂCHES DEVOPS

Les entreprises numériques actuelles sont confrontées à un impératif de rapidité et d'agilité qui nécessite des modifications de l'infrastructure informatique, et plus particulièrement la migration vers des architectures natives au cloud et l'adoption de processus DevOps. Cette évolution a conduit de nombreuses entreprises à se tourner vers les conteneurs, les microservices et Kubernetes (K8s) pour améliorer l'efficacité et l'évolutivité des efforts de développement et mettre en place les fondements mêmes de leur infrastructure immuable de nouvelle génération.

Par ailleurs, les processus d'intégration/distribution continues (CI/CD) introduisent une automatisation et une surveillance continues tout au long du cycle de vie de l'application, de l'intégration et des tests à la distribution et au déploiement, permettant ainsi d'accélérer l'innovation. Cette évolution vers la CI/CD n'est pas sans risque, et les équipes chargées de l'infrastructure, des tâches DevOps et de la sécurité cherchent des solutions pour garantir la sécurité et la conformité des conteneurs et des microservices tout en éliminant les angles morts.

Comme Kubernetes et les conteneurs introduisent un nouvel environnement et une approche différente de la gestion, les équipes de sécurité peinent à suivre. Cette situation se traduit par une augmentation des risques en raison de la mauvaise visibilité, des approches fragmentées de la détection et de la prévention des menaces, des erreurs de configuration des workloads cloud, des conteneurs et des environnements sans serveurs, et de l'incapacité à assurer la conformité.

Voici quelques-uns des problèmes courants liés à la sécurisation des conteneurs auxquels les équipes sont confrontées :

- Manque de visibilité sur les workloads cloud, les conteneurs et les environnements Kubernetes
- Gestion inefficace des vulnérabilités pour les images de conteneurs, les registres, les bibliothèques et les hôtes
- Sécurisation de l'orchestration des conteneurs
- Protection des workloads natifs au cloud et des conteneurs lors de l'exécution
- Manque de compétences en sécurité du cloud et augmentation de la surface d'attaque
- Respect et maintien de la conformité, et application des règles de sécurité

Les processus manuels et les solutions traditionnelles ne sont pas en mesure de faire face à l'évolution rapide et aux défis uniques auxquels les entreprises sont confrontées avec les conteneurs. Les alternatives peuvent inclure des plateformes de sécurité cloud complexes ou des outils isolés, ce qui peut multiplier le nombre de fournisseurs et accroître la complexité de la sécurité globale de votre entreprise.

PRINCIPAUX AVANTAGES

Analyse et identification continues des vulnérabilités, des menaces, des secrets intégrés et des infractions à la conformité

Visibilité inégalée grâce aux événements de workloads cloud, aux événements de conteneurs et aux métadonnées détaillés

Identification des workloads cloud exécutés dans votre environnement, notamment ceux qui sont exécutés avec des configurations potentiellement à risque

Protection à l'exécution continue pour tous les workloads cloud et les conteneurs

Accélération du Threat Hunting et des investigations pour tous les workloads

Protection immédiate sans sacrifier les performances, à la vitesse exigée par les processus DevOps

Adaptation en temps réel à l'évolutivité dynamique des workloads cloud et des conteneurs

APPROCHE DE CROWDSTRIKE DE LA SÉCURISATION DES WORKLOADS CLOUD ET DES CONTENEURS

CrowdStrike sécurise son infrastructure cloud en s'attachant à garder une longueur d'avance sur les cyberadversaires, à réduire sans relâche sa surface d'attaque et à obtenir une visibilité totale sur les événements qui se produisent dans l'environnement. Pour bloquer les intrusions dans les workloads, les conteneurs et les environnements Kubernetes à l'aide de données et d'analyses cloud, une plateforme étroitement intégrée est indispensable. Chaque fonction joue un rôle crucial dans l'identification précoce des vulnérabilités, la détection des menaces, la protection à l'exécution et la mise en œuvre de la conformité, et chacune d'elles doit être conçue et développée dans un souci constant de vitesse, d'évolutivité et de fiabilité.

L'expérience de la gestion d'un des clouds de sécurité les plus vastes au monde fournit à CrowdStrike des informations uniques sur les cyberadversaires, lui permettant ainsi de proposer des solutions CrowdStrike® spécialement conçues pour réduire la charge de travail des équipes DevSecOps, assurer la protection contre les compromissions de données et optimiser les déploiements cloud.

PRINCIPAUX AVANTAGES

ÉVALUATION ET GESTION DES VULNÉRABILITÉS

Bénéficiez d'une visibilité complète sur les workloads, les conteneurs et les hôtes, sur site comme dans le cloud.

- **Prise de décisions améliorée :** Obtenez des informations et des détails sur vos workloads cloud et vos conteneurs, notamment les images, registres et bibliothèques ainsi que les conteneurs créés à partir de ces images.
- **Identification des menaces dissimulées :** Débusquez les logiciels malveillants dissimulés dans vos images, les secrets intégrés, les problèmes de configuration et bien plus encore, afin de réduire la surface d'attaque.
- **Visibilité sur les environnements de conteneurs :** Bénéficiez d'une visibilité complète sur les conteneurs en cours d'exécution afin d'obtenir des détails sur l'accès aux fichiers, les communications réseau et les activités des processus.
- **Identification précoce des vulnérabilités :** Gagnez un temps précieux grâce aux règles prédéfinies d'analyse des images, qui vous permettent de détecter rapidement les vulnérabilités, les erreurs de configuration, etc.
- **Identification des configurations de conteneur à risque :** Identifiez rapidement les conteneurs à risque et mal configurés, notamment les conteneurs présentant des points de montage ou des liens rares pouvant indiquer une compromission.
- **Élimination des menaces avant la mise en production :** Bloquez les vulnérabilités exploitables sur la base des indicateurs d'attaque avant l'exécution, et simplifiez ainsi la vie des équipes de sécurité.
- **Surveillance continue :** Identifiez les nouvelles vulnérabilités à l'exécution, envoyez des alertes et prenez des mesures correctives sans analyse supplémentaire des images.

SÉCURITÉ AUTOMATISÉE DU PIPELINE CI/CD

Intégrez la sécurité au pipeline CI/CD.

- **Distribution accélérée :** Créez des règles d'images vérifiées pour vous assurer que seules les images approuvées sont autorisées à progresser dans votre pipeline et à s'exécuter dans vos hôtes ou clusters Kubernetes.

PROTECTION DES WORKLOADS CLOUD OPTIMISÉE POUR LES TÂCHES DEVOPS

Plateforme unique pour l'ensemble des workloads et des conteneurs

Sécurisation des workloads cloud et des conteneurs, où qu'ils soient exécutés

Intégration directe au pipeline CI/CD pour l'analyse des images et des registres

Efficace dès le jour du déploiement : déploiement et mise en fonction en quelques minutes seulement, sans nécessiter de redémarrage, de paramétrage subtil ni de configuration complexe

Hiérarchisation intelligente des incidents en fonction de leur gravité et de leur criticité

Optimisation du processus de tri et automatisation de la réponse

- **Identification précoce des menaces :** Analysez en permanence les images de conteneurs pour détecter les vulnérabilités connues, les problèmes de configuration, les secrets/clés et les problèmes de licence OSS.
- **Évaluation du niveau de vulnérabilité de votre pipeline :** Identifiez les logiciels malveillants qui échappent aux analyses statiques avant le déploiement des conteneurs.
- **Amélioration des opérations de sécurité :** Optimisez la visibilité sur les opérations de sécurité en fournissant des informations et du contexte pour les erreurs de configuration et les infractions à la conformité.
- **Intégration aux chaînes d'outils de développement :** Assurez l'intégration transparente de vos outils avec Jenkins, Bamboo, GitLab et bien d'autres pour corriger et intervenir plus rapidement au sein des outils DevOps que vous utilisez déjà.
- **Processus DevSecOps :** Les rapports et les tableaux de bord favorisent l'alignement et une compréhension commune de la part des équipes chargées des opérations de sécurité, des tâches DevOps et de l'infrastructure.

PROTECTION À L'EXÉCUTION

Protégez les workloads cloud et les conteneurs où qu'ils se trouvent.

- **Sécurisation des hôtes et des conteneurs :** La protection à l'exécution de CrowdStrike Falcon® protège les conteneurs contre les attaques actives.
- **Prise en charge étendue des conteneurs :** Falcon prend en charge les conteneurs exécutés sous Linux et peut être déployé dans des environnements Kubernetes tels qu'EKS. Il prend également en charge les solutions CaaS (Container-as-a-Service) telles que Fargate, tout en offrant le même niveau de protection. Des aperçus technologiques sont disponibles pour AKS, GKE et Red Hat OpenShift.
- **Exploitation de technologies de protection de pointe :** L'apprentissage automatique, l'intelligence artificielle, les indicateurs d'attaque et le blocage du hachage personnalisé assurent une protection automatisée contre les logiciels malveillants et les menaces sophistiquées ciblant les conteneurs :
  - **Apprentissage automatique et intelligence artificielle :** Falcon s'appuie sur l'apprentissage automatique et l'intelligence artificielle pour détecter les logiciels malveillants connus et inconnus au sein des conteneurs sans analyse ni signatures.
  - **Indicateurs d'attaque :** Falcon utilise les indicateurs d'attaque pour identifier les menaces en se basant sur le comportement. La compréhension du déroulement des séquences d'actions permet à Falcon de bloquer toutes les attaques, au-delà de celles qui utilisent des logiciels malveillants, y compris les attaques sans fichiers.
- **Blocage des comportements malveillants :** Le profilage comportemental vous permet de bloquer les activités qui enfreignent les règles en vigueur, sans impact sur le fonctionnement légitime du conteneur.
- **Investigation accélérée des incidents liés aux conteneurs :** Analysez facilement les incidents grâce à des détections associées à un conteneur spécifique plutôt que regroupées avec les événements de l'hôte.
- **Visibilité complète :** Capturez les informations relatives au démarrage, à l'arrêt, à l'image et à l'exécution du conteneur, ainsi que tous les événements générés au sein du conteneur, même si celui-ci ne s'exécute que pendant quelques secondes.
- **Déploiement transparent avec Kubernetes :** Déployez en toute facilité votre solution à grande échelle en intégrant Falcon dans un cluster Kubernetes.
- **Amélioration de l'orchestration des conteneurs :** Capturez l'espace de noms et les métadonnées des pods, ainsi que les événements réseau, de processus et de fichier Kubernetes.

MOTEUR DE PRÉVENTION DES INTRUSIONS THREAT GRAPH

Anticipez et prévenez les menaces modernes en temps réel grâce à l'ensemble de données télémétriques le plus complet du secteur, regroupant des données sur les endpoints, les workloads cloud et les conteneurs ainsi que des renseignements sur les cybermenaces et des analyses reposant sur l'intelligence artificielle.

- **Renseignements intégrés de pointe sur les cybermenaces :** Falcon tire parti de renseignements sur les cybermenaces enrichis pour fournir une représentation visuelle des relations entre les rôles des comptes, les workloads et les API afin d'offrir un contexte approfondi propice à une réponse plus rapide et efficace.
- **Prévention automatisée des menaces :** L'intelligence artificielle et l'analyse comportementale approfondies identifient les menaces nouvelles et inhabituelles en temps réel et prennent les mesures appropriées, faisant ainsi gagner un temps précieux aux équipes de sécurité.
- **Réponse accélérée :** CrowdStrike Threat Graph® met cette mine de connaissances à la disposition des équipes de réponse à incidents en temps réel, leur permettant ainsi de comprendre immédiatement les menaces et d'agir de manière décisive.

- **Réduction de la lassitude face aux alertes répétées :** L'approche ciblée de l'identification et de la gestion des menaces permet de faire le tri dans les alertes de sécurité des environnements multiclouds et de réduire la lassitude face aux alertes répétées.
- **Décodage des attaques et amélioration de la réponse :** L'outil CrowdScore™ Incident Workbench de CrowdStrike permet de décortiquer les attaques et de réduire les délais de réponse en mettant en corrélation les alertes de sécurité sous forme d'incidents, et en triant, hiérarchisant et mettant automatiquement en évidence celles qui méritent une attention urgente.

SOURCE D'INFORMATIONS FIABLES UNIQUE AVEC API PUISSANTES

Une source de données unique permet aux équipes de sécurité d'accéder rapidement à tout ce dont elles ont besoin pour répondre aux incidents et mener des investigations.

- **Automatisation compatible avec les processus DevOps :** De puissantes API permettent d'automatiser les fonctionnalités de CrowdStrike Falcon, notamment la détection, la gestion, la réponse et les renseignements sur les cybermenaces.
- **Optimisation des performances métier :** Exploitez l'orchestration de la sécurité, l'automatisation et d'autres flux de travail avancés pour optimiser les performances métier.
- **Intégration avec les pipelines CI/CD :** Les intégrations Chef, Puppet et AWS Terraform prennent en charge les flux de travail CI/CD.
- **Protection évolutive adaptée à la vitesse des processus DevOps :** Falcon offre une protection immédiate, ainsi que la vitesse exigée par les processus DevOps. Il s'adapte à l'évolutivité dynamique des conteneurs en temps réel grâce à une intégration CI/CD via les scripts d'appel d'API et de prédémarrage.

SIMPLICITÉ ET PERFORMANCES

Utilisez une plateforme unique pour tous les workloads et conteneurs. Cette plateforme fonctionne dans tous les environnements de cloud : privés, publics et hybrides.

- **Adoption simplifiée des processus DevSecOps :** Réduisez la charge administrative, les frictions et la complexité associées à la protection des workloads cloud, des conteneurs et des environnements sans serveurs.
- **Console centralisée :** Une console unique offre une visibilité centralisée sur le niveau de sécurité du cloud, les workloads et les conteneurs, quel que soit leur emplacement.
- **Flexibilité totale des règles :** Appliquez les règles au niveau du workload individuel, du conteneur, du groupe ou à un niveau supérieur, et unifiez-les pour les déploiements sur site et multiclouds.
- **Évolutivité infinie :** Aucune modification de l'architecture ni infrastructure supplémentaire n'est nécessaire.
- **Prise en charge étendue des plateformes :** La plateforme Falcon prend en charge les conteneurs OCI (Open Container Initiative), tels que Docker et Kubernetes, ainsi que les plateformes d'orchestration autogérées et hébergées telles que GKE (Google Kubernetes Engine), EKS (Amazon Elastic Kubernetes Service), ECS (Amazon Elastic Container Service), AKS (Azure Kubernetes Service) et OpenShift.

À PROPOS DE CROWDSTRIKE

CrowdStrike, leader mondial de la cybersécurité, redéfinit la sécurité pour l'ère du cloud en proposant une plateforme de protection des endpoints conçue spécifiquement pour empêcher les compromissions. L'architecture à agent léger unique de la plateforme CrowdStrike Falcon® s'appuie sur l'intelligence artificielle à l'échelle du cloud pour offrir une visibilité et une protection en temps réel au sein de l'entreprise et prévenir les attaques sur les endpoints, qu'ils soient connectés ou non au réseau. Optimisé par la base de données propriétaire CrowdStrike Threat Graph®, CrowdStrike Falcon met en corrélation en temps réel plus de quatre billions d'événements liés aux endpoints identifiés chaque semaine dans le monde, qui viennent enrichir l'une des plateformes de données les plus avancées au monde en matière de sécurité.