CROWDSTRIKE

Plans stratégiques pour sécuriser les workloads AWS

L'alliance de CrowdStrike Falcon Cloud Security, pour la protection et la visibilité totales des workloads et conteneurs, et d'AWS Security Hub, pour la vision complète des alertes, est le moyen le plus efficace de concevoir des architectures cloud sécurisées

aws PARTENAIRE

- Secteur public
- Prise en charge d'Amazon Linux
- Disponibilité sur les places de marché
- Compétences en logiciels de sécurité

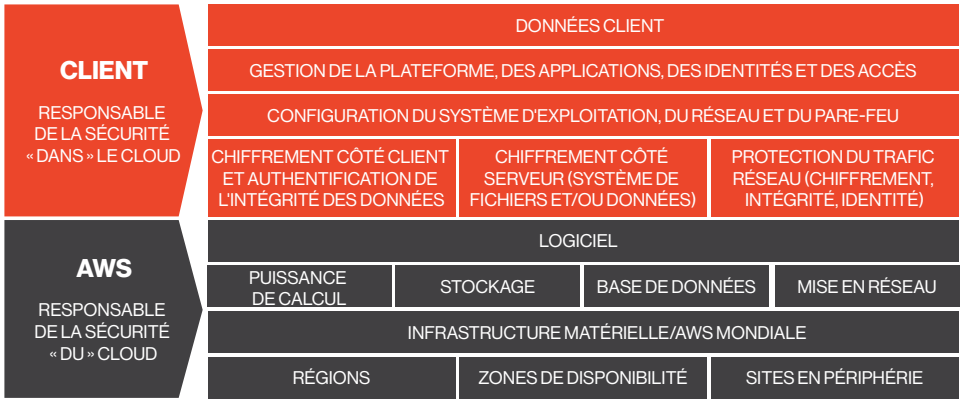
eBook CrowdStrike

Sommaire

Les stratégies obsolètes rendent les architectures cloud modernes vulnérables aux attaques

Alors que l'adoption du cloud explose, de nombreuses approches de sécurité restent figées dans le passé. Étendre au cloud les outils de sécurité sur site d'ancienne génération s'avère une méthode inadaptée, qui laisse les architectes cloud et les équipes DevOps sans stratégie claire pour sécuriser les applications, les workloads et les infrastructures.

Avec Amazon Web Services (AWS) et CrowdStrike, l'un des leaders de la protection des endpoints et des workloads cloud, vous pouvez créer un socle de sécurité solide. L'alliance de CrowdStrike Falcon et d'AWS Security Hub permet une gestion centralisée et automatisée des alertes sur les cybermenaces provenant des services AWS, notamment Amazon GuardDuty. CrowdStrike Falcon Cloud Security renforce la sécurité des workloads AWS tout en vous permettant d'adopter le modèle de responsabilité partagée.



CrowdStrike Falcon Cloud Security protège vos workloads AWS

AWS protège votre infrastructure cloud

AWS Security Hub vous offre une visibilité totale sur les alertes de sécurité et la conformité

- Agrégation des données d'alerte provenant de Falcon et des services AWS natifs comme Amazon GuardDuty
- Surveillance de l'état de votre infrastructure AWS grâce à des visuels intuitifs
- Réalisation de contrôles de conformité

CrowdStrike Falcon Cloud Security protège vos workloads AWS par le biais d'un seul agent léger

- Sécurité avancée des applications cloud native, avec prévention des compromissions, protection des workloads et gestion du niveau de sécurité du cloud
- Simplification de l'infrastructure de sécurité grâce à un agent unique à faible empreinte sur les ressources AWS, pour des performances optimisées
- Réduction de l'architecture nécessaire pour une visibilité totale sur la sécurité et simplification pour tirer davantage de valeur des investissements AWS

L'alliance de Falcon et d'AWS, gage d'une sécurité fluide pour vos flux de travail

L'intégration de CrowdStrike à AWS Security Hub offre une visibilité en temps réel complète sur les alertes de sécurité ultraprioritaires. L'approche orientée API de CrowdStrike associe Falcon Cloud Security à AWS Security Hub pour faciliter l'automatisation des tâches de sécurité et améliorer la protection globale pour l'ensemble de vos effectifs (RSSI, équipes DevOps et en charge des opérations, architectes cloud, etc.).

SURVEILLER — AVEC UNE VISIBILITÉ TOTALE

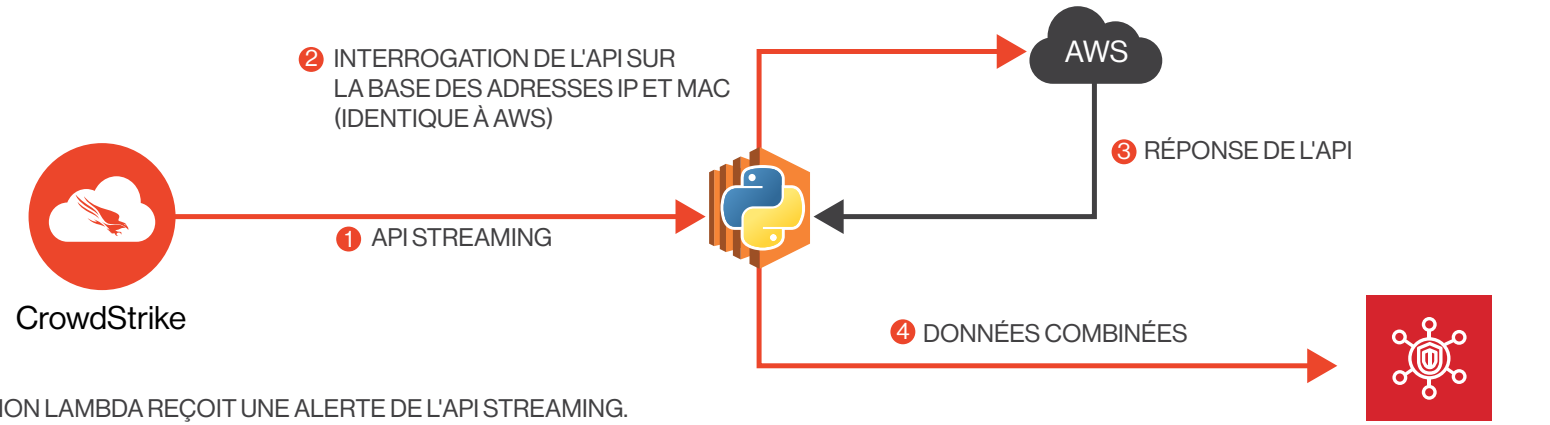
Falcon Cloud Security protège vos workloads AWS tout au long du cycle de vie des cybermenaces en réunissant Machine Learning, intelligence artificielle, analyse comportementale et Threat Hunting proactif au sein d'une seule et même solution.

PROTÉGER — AVEC DES PERFORMANCES OPTIMALES

Falcon Cloud Security fonctionne de manière polyvalente — avec les instances Amazon Elastic Cloud Compute (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) sur Amazon EC2 et Amazon Elastic Kubernetes Service (Amazon EKS) sur Amazon EC2 — de façon à assurer la sécurité des endpoints et des workloads même lorsqu'ils sont hors ligne.

DÉFENDRE — AVEC UNE ARCHITECTURE SIMPLIFIÉE

Falcon Cloud Security simplifie les pipelines DevSecOps complexes et renforce la fiabilité opérationnelle en simplifiant les architectures cloud. Falcon consolide vos agents d'endpoint et de workload par le biais d'une plateforme extensible qui évolue et s'adapte à vos besoins sans introduire de complexité supplémentaire.



1. LA FONCTION LAMBDA REÇOIT UNE ALERTE DE L'API STREAMING.
2. LA FONCTION LAMBDA INTERROGE L'API AWS POUR OBTENIR DES INFORMATIONS.
3. EN CAS DE CORRESPONDANCE AVEC UNE INSTANCE EC2, LES DONNÉES SONT RENVOYÉES.
4. LES DONNÉES EC2 ET CROWDSTRIKE SONT COMBINÉES, MISES EN FORME ET ENVOYÉES À AWS SECURITY HUB.

Surveiller — avec une visibilité totale

Grâce à l'agrégation par AWS Security Hub des alertes d'Amazon GuardDuty et de Falcon Cloud Security, votre équipe dispose d'une vue d'ensemble unique qui lui procure la connaissance situationnelle nécessaire pour prendre des décisions stratégiques en matière de sécurité et de ressources. L'automatisation de l'analyse de routine de la sécurité accélère votre capacité à détecter et à traiter les incidents les plus critiques.

Exploiter la recherche de menaces du Threat Graph
Identifiez les cybermenaces potentielles rapidement et avec précision grâce à la recherche de menaces du Threat Graph optimisée par l'IA, et atteignez un niveau de protection de vos workloads AWS jusque-là inédit.

Automatiser les tâches de sécurité
Sans Threat Graph, les analystes devraient collecter manuellement la télémétrie des endpoints et des workloads, intégrer des flux de recherche de menaces, écrire des règles de corrélation et croiser les données pour identifier les éventuels liens entre les événements de sécurité. Avec Falcon Cloud Security, tous les renseignements, les événements et les relations qui existent entre eux sont capturés au même endroit, ce qui permet aux administrateurs sécurité d'automatiser l'analyse, et de bénéficier d'une visibilité stratégique et détaillée lorsqu'ils enquêtent sur des brèches potentielles.

Intégrer la sécurité aux pipelines CI/CD
Falcon Cloud Security permet aux équipes de sécurité du cloud de s'adapter à la nature dynamique et flexible des workloads AWS. En effet, la prise en charge fluide des flux de travail de déploiement CI/CD repose sur de puissantes API et sur l'intégration simplifiée d'AWS Security Hub.

Automatisation accrue pour les équipes DevOps

- Automatisation de la distribution des pipelines de développement
- Simplification du déploiement et de la gestion
- Sécurité qui s'adapte à la vitesse de distribution des applications

Informations détaillées pour les équipes de sécurité

- Contextualisation des alertes de sécurité AWS
- Compréhension de l'impact des événements de sécurité
- Simplification de la réponse à incident
- Identification de l'intention en fonction des indicateurs d'attaque
- Réduction des faux positifs et renforcement de la sécurité

> 7 billions
d'événements par semaine

200 000
nouveaux IOC publiés chaque jour

> 200
cyberadversaires traqués

> 1,2 million
d'échantillons de logiciels malveillants traités chaque jour

Protéger — avec des performances optimales

Avec CrowdStrike, un seul capteur suffit à protéger tous vos endpoints et workloads — des terminaux IoT aux instances de calcul dans le cloud, en passant par les ordinateurs portables. En utilisant AWS Security Hub en tant que tableau de bord, vous pouvez agréger et prioriser les alertes de sécurité provenant de Falcon Cloud Security et d'Amazon GuardDuty, et donc protéger les instances Amazon EC2 ou les conteneurs qui s'exécutent sur Amazon ECS et Amazon EKS.

Maintenir la sécurité et les performances des instances Amazon EC2

Falcon Cloud Security s'appuie sur une évolutivité cloud native pour sécuriser les instances Amazon EC2 avec un impact minime sur les performances d'exécution, et sans analyse intempestive ni mise à jour invasive des signatures. Il offre une protection contre toutes les attaques avancées qui contournent les approches traditionnelles basées sur le périmètre et les signatures.

Protéger les conteneurs qui s'exécutent sur Amazon ECS et Amazon EKS

Falcon Cloud Security s'exécute sur le nœud d'instance Amazon EC2, protégeant ainsi tous ses conteneurs, y compris ceux gérés par Amazon ECS et Amazon EKS. Depuis les logiciels malveillants connus jusqu'aux attaques les plus sophistiquées, Falcon protège les conteneurs en surveillant et en découvrant les workloads, et en examinant des paramètres tels que l'identifiant unique et le type de configuration des conteneurs, avant de transmettre les alertes à AWS Security Hub.

Anticiper la sécurité des conteneurs dans les pipelines CI/CD

En réalisant les tâches de sécurité plus tôt dans le cycle de développement logiciel, les équipes peuvent identifier les failles avant qu'elles ne fassent des ravages. Ajouter Falcon Cloud Security à votre flux de déploiement CI/CD vous permet de gagner en sécurité d'exécution pour les workloads Amazon ECS et Amazon EKS, mais également en visibilité sur les applications conteneurisées. Vous pouvez également visualiser et gérer les événements tels que les images de conteneurs à risque grâce au tableau de bord AWS Security Hub.

1
agent léger

0
redémarrage nécessaire

Simplification du codage pour les équipes DevOps

- Protection antimalware sans intégrer d'appliance d'ancienne génération
- Simplification du code et des scripts grâce à un agent unique facile à déployer

Une meilleure compréhension pour les équipes de sécurité

- Mise en corrélation des alertes AWS et de la fonction de détection de Falcon Cloud Security pour un tri et une correction accélérés
- Mise à disposition d'une plateforme de Threat Hunting pour les équipes chargées des opérations

Défendre — avec une architecture simplifiée

L'efficacité accrue offerte par l'association de Falcon Cloud Security et d'AWS Security Hub contribue à réduire les délais de détection, d'investigation et de correction, de façon à bloquer davantage de compromissions. Disposer d'un service intégré gage d'une sécurité totale augmente l'efficacité des équipes qui, par conséquent, passent moins de temps à gérer des flux de travail distincts. Maximisez les performances d'AWS Security Hub pour agréger les événements en tirant parti de la recherche de menaces et de l'architecture simplifiée de CrowdStrike.

Simplifier les architectures AWS

Les autres fournisseurs de solutions de sécurité requièrent souvent un routage complexe pour les applications d'ancienne génération qui doivent être intégrées au flux de paquets, ainsi que de nombreux agents de workload pour assurer des fonctionnalités d'antivirus, d'EDR et de sécurité des conteneurs installées et gérées séparément. Ces exigences contribuent à complexifier les environnements AWS et à allonger les temps d'arrêt. Étant un agent unique, Falcon offre quant à lui le même niveau de sécurité moyennant une charge de travail réduite.

Accélérer les délais de réponse

Le classement des incidents par ordre de priorité dans AWS Security Hub contribue à rationaliser le processus de tri, ce qui permet à votre équipe de s'attaquer d'abord aux cybermenaces les plus critiques.

Renforcer l'efficacité pour plus d'économies

La possibilité de se procurer Falcon Cloud Security sur AWS Marketplace permet de profiter de systèmes de comptage et de facturation intégrés, tout en optimisant les dépenses induites par les workloads flexibles.

Démarrage rapide des équipes DevOps

- Intégration de la sécurité et de la correction via un seul capteur d'endpoint
- Aucune installation requise — CrowdStrike s'exécute à partir d'une console SaaS
- Un seul service de sécurité pour une protection totale

Rationalisation de la conception pour les architectes cloud

- Consolidation de l'architecture pour gagner en simplicité
- Évolutivité en fonction de l'augmentation des workloads cloud — pas besoin d'infrastructure supplémentaire
- Puissantes API permettant d'automatiser tous les domaines fonctionnels pour une défense en profondeur

100 000 nœuds
par jour pour un déploiement immédiat

75 %
d'efficacité en plus

Viser l'excellence

La cybersécurité n'est pas qu'une question de technologies — protéger les workloads AWS nécessite également de pouvoir s'appuyer sur des effectifs et des processus efficaces. Ignorer les opérations de sécurité peut entraîner des dommages et des efforts de correction qui génèrent des ralentissements pour les équipes DevOps et diminuent la disponibilité des applications critiques. Les conséquences de cette situation peuvent être évitées si les technologies de sécurité sont configurées correctement et tenues à jour, et si les alertes de sécurité précédant un incident sont triées, analysées et suivies d'actions de correction dans les plus brefs délais.

De nombreuses entreprises ont du mal à gérer cet aspect opérationnel de la sécurité dans la mesure où le personnel qualifié nécessaire pour assurer la cybersécurité en continu peut être difficile à embaucher et coûteux.

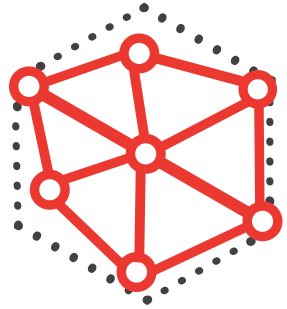
Renforcer les équipes grâce à la détection et l'intervention managées
En tant que service MDR, CrowdStrike Falcon Complete renforce les performances de la plateforme Falcon avec l'efficacité d'une équipe dédiée de professionnels de la sécurité. Falcon Complete se concentre sans relâche sur la gestion et la surveillance de la sécurité des endpoints et des workloads, pour intervenir rapidement, automatiquement et précisément en cas de cybermenace.

Moindres perturbations pour les équipes DevOps

- Surveillance 24 heures sur 24 et 7 jours sur 7 avec correction ultraprécise pour éliminer rapidement les cybermenaces, sans répercussions sur le workload sous-jacent

Expertise accrue et gain d'efficacité immédiats pour les équipes de sécurité

- Règles de sécurité ajustées en permanence pour un maximum d'efficacité
- Identification et correction des cybermenaces en quelques minutes
- Garantie de prévention des compromissions gage de tranquillité d'esprit



La règle 1-10-60 correspond au délai idéal que nous recommandons aux entreprises de respecter pour être plus rapides que les cyberadversaires :

< 1 minute
pour détecter les menaces

< 10 minutes
pour comprendre les menaces

60 minutes
pour corriger

Démarrer avec CrowdStrike sur AWS dès aujourd'hui

Pour en savoir plus sur les solutions CrowdStrike et AWS, suivez les liens ci-dessous :

- **CrowdStrike Falcon Cloud Security**
- **Page CrowdStrike dans AWS Marketplace**
- **Déterminer votre niveau de sécurité grâce à une évaluation des risques liés au cloud**