CROWDSTRIKE

# CrowdStrike Falcon Cloud Security sur AWS

aws PARTENAIRE

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



eBook CrowdStrike

# Sommaire

# Introduction

Partout dans le monde, la technologie cloud joue un rôle prépondérant dans le développement des entreprises, quelle que soit leur taille, et elles sont de plus en plus nombreuses à s'appuyer sur la plateforme AWS (Amazon Web Services) ou à migrer vers celle-ci. Les besoins métier tels que la flexibilité, l'innovation ou le coût total de possession incitent les directeurs des technologies ou des systèmes d'information à adopter les technologies AWS. Ces dirigeants font confiance à AWS pour les aider à réagir aux changements avec célérité et confiance, à organiser une montée en charge efficace des systèmes et à stimuler la croissance de leur entreprise.

Une telle évolution exige évidemment de revoir les stratégies de sécurité pour garder une longueur d'avance sur les menaces. Il est essentiel de mettre en place une stratégie de sécurité cloud à un stade précoce pour être bien préparé face à l'évolution technologique et à la sophistication croissante des cyberattaques.

Que vos activités s'appuient sur le cloud ou que vous soyez en train de migrer vers le cloud, il est essentiel de bien réfléchir à votre stratégie de sécurité cloud. À quelque stade que vous soyez, la sécurité de vos ressources de calcul doit être une priorité.

Dans un paysage des technologies cloud en constante évolution, il est une chose dont nous sommes sûrs : les cyberadversaires comprennent parfaitement les risques de sécurité posés par le cloud. Est-ce votre cas ?

**52 %**

**Pourcentage d'entreprises nord-américaines qui prévoient qu'au moins 41 % de leurs workloads fonctionneront dans le cloud au cours des 24 prochains mois.**

# Une migration vers le cloud en toute sécurité

La technologie cloud a permis d'accélérer le lancement des nouvelles entreprises. Elle a aidé les entreprises existantes à jeter les bases de l'innovation et a donné naissance à de nouveaux paramètres et menaces de sécurité. Mais l'innovation peut également comporter certains risques, notamment la décentralisation du développement et de l'implémentation de règles, le manque de visibilité entre les différentes technologies et les endpoints, et évidemment l'imprévisible facteur humain — en d'autres termes, le Shadow IT, les failles dans l'architecture, ainsi que le manque de connaissances et de compétences.

Pour les entreprises qui utilisent la technologie cloud pour développer des infrastructures évolutives, la sécurité revient à garantir leur protection dans un environnement en constante évolution. Les applications et solutions externalisées, développées par des tiers avec diverses normes de sécurité et d'architecture peuvent créer des failles de sécurité. Dès lors, l'implémentation d'une stratégie de sécurité à un stade précoce représente le meilleur moyen de bénéficier d'une visibilité centralisée sur les différents composants et services cloud.

Pour ceux qui migrent vers le cloud à partir de technologies d'ancienne génération, les risques de sécurité sont présents dans tous les systèmes, qu'ils soient anciens ou récents. Lors d'une migration, les solutions hybrides sont particulièrement vulnérables, tout comme les anciens systèmes et bases de données laissés en place, s'ils ne sont pas correctement éliminés. La plupart des migrations nécessitent également une requalification des collaborateurs ou l'embauche de nouvelles recrues, ainsi qu'un changement de la culture d'entreprise. Bien que cela constitue de bonnes bases pour gérer les changements technologiques futurs, cela peut aussi créer certains risques pour l'entreprise. Il est donc essentiel de préserver une visibilité complète sur la sécurité lors d'une transition technologique majeure.

# L'approche stratégique de CrowdStrike en matière de sécurité

Pour sécuriser les systèmes cloud, une solution possible consiste à faire appel à un partenaire de sécurité tel que CrowdStrike. Avec Falcon Cloud Security et l'assistance d'une équipe d'experts en cybersécurité, vous bénéficierez d'une protection de bout en bout, de l'hôte au cloud, en passant par tous les maillons intermédiaires, pour les workloads et les conteneurs hébergés sur la plateforme AWS.

## L'approche CrowdStrike :

- Se concentrer sur les cyberadversaires
- Réduire le risque d'exposition
- Surveiller la surface d'attaque
- Assurer la protection à l'exécution
- Faire partie du pipeline CI/CD

Les cyberadversaires ont adapté des attaques observées dans le paysage IT normal aux environnements cloud, notamment l'élévation des privilèges, les ransomwares et l'analyse des données et des paquets . De nouvelles techniques d'attaque cloud native sont également susceptibles d'émerger. Les solutions de sécurité cloud de CrowdStrike intègrent des alertes et des rapports en temps réel sur plus de 200 cyberadversaires. Ainsi, lors de l'émergence de nouvelles menaces, vous serez prêt à y répondre.

En matière de sécurité cloud, réduire l'exposition ainsi que la surface d'attaque revient à segmenter les workloads, à régler certains problèmes (en particulier pour ceux qui possèdent encore des anciens systèmes) et à s'assurer que la sécurité est la priorité absolue lors de l'utilisation du cloud, une approche également connue sous le nom de « Shift Left ». Une fois la surface d'attaque définie, une surveillance haute visibilité est le meilleur moyen de se défendre contre les cyberattaquants potentiels. Falcon Cloud Security propose une analyse automatisée, une protection à l'exécution et au repos, des indicateurs d'attaque cloud native et le Machine Learning pour accélérer les investigations.

### Falcon Cloud Security pour le DevSecOps et la surveillance

Pour ceux qui développent des applications et des services dans plusieurs environnements, Falcon Cloud Security rationalise la gestion de la sécurité grâce à une source unique d'informations fiables pour toutes les ressources et les configurations de sécurité du cloud. Tout ce que vous devez voir, dans une seule console. Grâce à la protection offerte par les indicateurs d'attaque et à une fonction de correction guidée, basée sur le Machine Learning et directement intégrée dans le plan de contrôle, Falcon Cloud Security aide les équipes à gérer la conformité et à déployer les intégrations AWS en toute sécurité et de façon plus efficace.

### Falcon Cloud Security pour une prévention complète des compromissions

Lorsque vous créez ou remplacez des systèmes par la technologie Cloud, Falcon Cloud Security offre une protection complète contre les compromissions dans les environnements cloud privés, publics, hybrides et multiclouds, permettant aux clients d'adopter et de sécuriser rapidement de nouvelles technologies indépendamment du type de workload. Falcon Cloud Security permet aux entreprises de développer, d'exécuter et de sécuriser des applications de manière rapide et en toute confiance.

# Sécurisation des conteneurs sur AWS

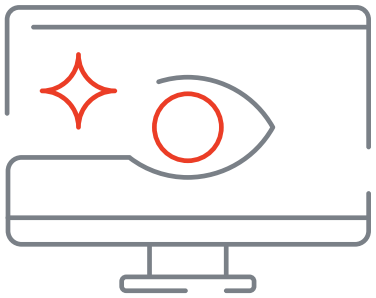
La sécurisation des conteneurs est l'un des autres éléments clés d'une stratégie de sécurité cloud efficace. Isolés et indépendants par nature, les conteneurs limitent la visibilité. Qui plus est, comme ils sont généralement développés selon une approche « set-and-forget » (configurer et oublier), la conformité à long terme de la sécurité est souvent reléguée au second plan. Quand bien même les entreprises respectent les meilleures pratiques en matière de surveillance, les conteneurs peuvent poser problème pour les analyses de la sécurité en raison du volume considérable de données qu'ils génèrent lors de l'évaluation des vulnérabilités.

Falcon Cloud Security relève facilement ces nouveaux défis. L'agent léger de CrowdStrike offre une visibilité complète sur les conteneurs, qu'ils soient déployés sur site ou dans le cloud. La surveillance continue et l'intégration du pipeline CI/CD permettent de vérifier facilement les conteneurs et, le cas échéant, de les réinitialiser. En outre, la surveillance et la détection automatisée et continue des menaces offertes par Falcon Cloud Security garantissent une analyse agile des données de vulnérabilité à grande échelle (via le Machine Learning et l'intelligence artificielle), ainsi qu'une protection à l'exécution avec des alertes en temps réel.

# Sécurisation des ressources de calcul sur AWS en toute simplicité avec Falcon

Les entreprises qui utilisent AWS connaissent la valeur de la technologie cloud pour migrer les systèmes obsolètes et créer des applications modernes. Elles connaissent également la valeur d'une collaboration avec des partenaires à la pointe de la technologie pour donner un coup de fouet à leurs systèmes et développer leurs activités.

L'architecture CrowdStrike Falcon Cloud Security s'intègre de manière transparente à AWS Security Hub : elle est pensée pour les services AWS tels qu'Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) et Amazon Linux 2, et son déploiement peut se faire via AWS Systems Manager. Les clients AWS qui choisissent CrowdStrike comme partenaire sont opérationnels en quelques minutes et ont instantanément accès à des informations utiles et aux analyses de tous leurs services par le biais d'une seule et unique console centralisée. En outre, CrowdStrike Falcon Cloud Security possède une empreinte de fonctionnement minime, sans aucun impact sur les performances à l'exécution — même lors des analyses, des recherches et des investigations.



## Points d'intégration entre AWS et CrowdStrike

### Services de traitement AWS et CrowdStrike

- Workloads de conteneurs
- Instances Amazon EC2 — y compris Graviton
- Amazon WorkSpaces
- Amazon Elastic Kubernetes Service
- Amazon Elastic Container Service
- AWS Fargate
- AWS Outposts

### Intégrations des services cloud AWS et CrowdStrike

- AWS Verified Access
- AWS Account Factory Customization
- AWS Control Tower
- AWS Security Hub
- AWS Systems Manager
- AWS PrivateLink
- Amazon GuardDuty
- AWS Network Firewall
- AWS CloudEndure Disaster Recovery

# Il est temps d'élaborer une stratégie de sécurité cloud

En matière de sécurité du cloud, s'associer à un expert qui comprend vos cyberadversaires, leurs cibles et les méthodes d'attaque est le meilleur moyen de s'en protéger. Leader du secteur de la cybersécurité, CrowdStrike a fait ses preuves en matière de prévention des compromissions.

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

- **CrowdStrike Falcon for AWS ›**
- **Événements à venir de CrowdStrike et AWS ›**
- **Page partenaire CrowdStrike et AWS ›**
- **CrowdStrike sur AWS Marketplace ›**