CROWDSTRIKE

Principales techniques d'attaque du cloud

Et comment vous en prémunir

Le cloud est une surface d'attaque en constante expansion et évolution. Pour le protéger contre le nombre croissant d'attaques qui le ciblent, vous avez besoin d'une compréhension approfondie des activités des cybercriminels. Voici les trois principales tendances en matière d'attaque du cloud observées par CrowdStrike et comment vous en prémunir.

Les cybercriminels ciblent de plus en plus le cloud

Les environnements cloud continuent de se développer :

41,4 % des responsables du cloud déclarent intensifier leur utilisation des services et produits basés dans le cloud¹

33,4 % prévoient d'abandonner les logiciels d'entreprise d'ancienne génération au profit d'outils cloud¹

32,8 % sont en train de migrer leurs workloads sur site vers le cloud¹

Cela n'a pas échappé aux cybercriminels.

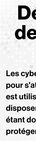
Observations de CrowdStrike en 2022 :

95 % Augmentation des cas d'exploitation du cloud

x3 Augmentation des cas impliquant des cybercriminels ciblant le cloud

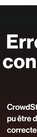
71 % des attaques n'utilisaient pas de logiciel malveillant

Pourquoi cibler les environnements cloud ?



Les environnements multicloud sont complexes et donc plus difficiles à protéger

Les processus de distribution rapide de logiciels exposent les applications cloud native à des vulnérabilités et à des erreurs de configuration



Les environnements cloud non approuvés et fantômes ne disposent pas de contrôles de sécurité ni de capacités de surveillance

Les produits de sécurité isolés et cloisonnés offrent aux cyberadversaires des portes dérobées par lesquelles s'introduire en toute discrétion

Les cybercriminels maîtrisent parfaitement le cloud et perfectionnent leurs tactiques pour exploiter les services cloud et les vulnérabilités de cet environnement. Voici les trois principales techniques d'attaque du cloud observées par l'équipe CrowdStrike Threat Intelligence au cours de l'année écoulée dans le cadre du suivi de plus de 200 cybercriminels.

Déplacements latéraux au sein de l'infrastructure informatique

Les cybercriminels exploitent de plus en plus les endpoints traditionnels pour s'attaquer à l'infrastructure cloud. À l'inverse, l'infrastructure cloud est utilisée comme passerelle pour accéder aux endpoints. Les entreprises disposent rarement de la visibilité nécessaire pour bloquer cette activité, étant donné qu'elles ont acquis une multitude de solutions isolées pour protéger l'environnement sur site et, plus récemment, les environnements cloud.

Pour bloquer les déplacements latéraux, les entreprises ont besoin d'une visibilité totale sur l'ensemble de l'infrastructure informatique, tant sur site que dans le cloud.

Erreurs de configuration du cloud conduisant à des compromissions

CrowdStrike enquête régulièrement sur des compromissions du cloud qui auraient pu être détectées plus tôt ou évitées si les paramètres de sécurité du cloud avaient été correctement configurés. Les erreurs de configuration augmentent non seulement le risque de compromission, mais deviennent en outre de plus en plus fréquentes et problématiques à mesure que l'infrastructure cloud de l'entreprise s'étend.

N° 1 Principale vulnérabilité des environnements cloud

60 % des conteneurs observés par CrowdStrike ne disposaient pas de protection correctement configurée

36 % des environnements cloud présentaient des paramètres par défaut non sécurisés du fournisseur de services cloud

Les identités cloud qui forment le nouveau périmètre

En tant que nouveau périmètre, les identités constituent désormais les clés du royaume. Les cybercriminels ont moins recours à la désactivation des antivirus et des pare-feux et se concentrent davantage sur la modification des processus d'authentification et l'attaque des identités. L'adoption généralisée d'applications et de services cloud augmente le nombre d'identités susceptibles d'être ciblées et utilisées par des cybercriminels.

Des comptes utilisateur légitimes ont été utilisés pour obtenir un accès initial dans **43 %** des intrusions cloud

47 % des erreurs de configuration critiques dans le cloud **sont dues à de mauvaises pratiques en matière de gestion des identités et des droits**

Dans **67 %** des incidents de sécurité dans le cloud, **CrowdStrike a mis en évidence des rôles IAM (gestion des identités et des accès) dotés de privilèges excessivement élevés, signe qu'un cyberadversaire avait sans doute détourné le rôle pour compromettre l'environnement et se déplacer latéralement**

CrowdStrike pour assurer la sécurité du cloud

Étant donné que les environnements cloud continuent de se développer, les attaques qui les ciblent vont également évoluer. Il est devenu impossible d'identifier toutes les vulnérabilités du cloud, les erreurs de configuration et les erreurs humaines, ou encore de suivre l'évolution des tactiques, techniques et procédures utilisées par les cybercriminels. Les entreprises ne peuvent pas s'en sortir seules — elles ont besoin d'un partenaire qui connaît sur le bout des doigts les comportements cybercriminels et le cloud.

En tant que principal fournisseur mondial de services de détection et réponse à incident basés sur un agent, CrowdStrike a adopté une approche visionnaire pour concevoir une solution de sécurité du cloud évolutive et performante, qui peut être déployée et gérée facilement au sein d'une seule plateforme. CrowdStrike Falcon® Cloud Security a été conçu spécifiquement pour offrir une protection avec et sans agent. Il suffit aux entreprises de l'activer pour étendre la protection de leurs endpoints au cloud, et protéger ainsi l'ensemble de leur infrastructure informatique à l'aide d'une solution transparente et unifiée. Falcon Cloud Security réunit gestion du niveau de sécurité du cloud, protection des workloads cloud et gestion des droits des identités dans le cloud au sein d'une plateforme de protection des applications cloud native (CNAPP) entièrement intégrée.

Téléchargez le livre blanc « Guide de la protection du cloud pour les initiés ».

En savoir plus →

À propos de CrowdStrike

CrowdStrike (Nasdaq : CRWD), leader mondial de la cybersécurité, redéfinit la sécurité avec sa plateforme cloud native la plus avancée au monde, conçue pour protéger les ressources critiques des entreprises, à savoir les endpoints, les workloads cloud, les identités et les données.

Optimisée par l'architecture de sécurité cloud de CrowdStrike et une intelligence artificielle de pointe, la plateforme CrowdStrike Falcon® s'appuie sur des indicateurs d'attaque en temps réel, le renseignement sur les cybermenaces, l'évolution des techniques des cybercriminels et des données télémétriques enrichies récoltées à l'échelle de l'entreprise pour assurer une détection ultraprécise, une protection et une correction automatisées, un Threat Hunting de pointe et une observation prioritaire des vulnérabilités.

Spécialement conçue dans le cloud au moyen d'une architecture à agent léger unique, la plateforme Falcon offre un déploiement rapide et évolutif, une protection et des performances de haut niveau, une complexité réduite et une rentabilité immédiate.

CrowdStrike : We stop breaches.

CROWDSTRIKE

Suivez-nous

https://cloud.google.com/blog/transform/top-cloud-computing-trends-facts-statistics-2023