Sécurisation des identités dans un environnement 100 % cloud : l'exemple d'AppsFlyer

ÉTUDE DE CAS

« Polyrize (désormais DatAdvantage Cloud) propose l'interface unique dont j'avais besoin pour sécuriser mes différentes applications cloud. »

Guy Flechter, CISO et DPD

Cette étude de cas a été publiée par Polyrize, une entreprise acquise par Varonis en 2020.

EN SAVOIR PLUS >

EN BREF

AppsFlyer, leader de l'attribution marketing, a installé son siège à San Francisco, mais l'entreprise dispose de 18 bureaux de par le monde, pour un total de plus de 1 000 collaborateurs. Sa mission ? Permettre à ses clients (spécialistes du marketing d'applications et développeurs) d'obtenir des métriques sur leurs campagnes.

DÉFIS

- Sécurisation de milliers d'identités et des droits associés sur plusieurs sites
- Visibilité et contrôle dans un environnement cloud complexe
- Application d'un modèle de moindre privilège

LA SOLUTION

- **DatAdvantage Cloud** (anciennement Polyrize) cartographie et analyse les relations entre les utilisateurs et les données sur l'ensemble des applications et services cloud.

RÉSULTATS

- Renforcement de la posture de sécurité sur le cloud tout en réduisant les coûts
- Capacité à identifier les utilisateurs au centre d'événements à haut risque
- Détection des événements à haut risque et mise en place des réponses appropriées

Défis

AppsFlyer se veut être une entreprise tournée vers le cloud et native du cloud. Conformément à cette vision, elle fait reposer son réseau d'entreprise sur le cloud : son infrastructure produit est ainsi basée sur AWS et l'ensemble des applications métier utilisées par ses collaborateurs et sous-traitants sont de type SaaS.

La principale difficulté de l'entreprise en matière de sécurité résidait donc dans la protection des milliers d'identités et multiples droits de son environnement cloud complexe, répartis sur de nombreux emplacements. Son équipe de sécurité ne disposait pas d'un niveau de visibilité et de contrôle équivalent à celui dont elle aurait pu bénéficier avec un réseau sur site.

Guy Flechter, CISO et DPD d'AppsFlyer, commente ainsi : « Le plus grand risque de sécurité pour notre environnement cloud, c'était avant tout la multiplication des identités humaines et non humaines sur de nombreux services cloud hétérogènes, ainsi que des droits complexes qui les accompagnaient. Ces différents éléments étendaient de manière importante notre surface d'attaque. Nous cherchions donc à appliquer un modèle de moindre privilège, supprimer les droits non utilisés et mal configurés, et éliminer les identités non utilisées, le tout en temps réel. »

> « Le plus grand risque de sécurité pour notre environnement cloud, c'était avant tout la multiplication des identités humaines et non humaines sur de nombreux services cloud hétérogènes, ainsi que des droits complexes qui les accompagnaient. Ces différents éléments étendaient de manière importante notre surface d'attaque. »

La solution

AppsFlyer a déjà pu tester diverses solutions de sécurité du cloud, comme une technologie périmétrique définie par logiciel permettant de fournir un accès Zero Trust aux services à l'intérieur de l'environnement de production, ainsi qu'un Cloud Access Security Broker (CASB). Ce dernier a été abandonné avant l'arrivée de Polyrize, car s'il était en mesure de détecter les fuites de données et d'autres incidents, il était incapable de fournir des informations sur les identités et privilèges, ce qui limitait son intérêt au niveau de la sécurité.

« Notre CASB nous a permis de repérer quelques activités risquées des utilisateurs, mais ne nous donnait aucune visibilité sur les actifs auxquels ces utilisateurs avaient accès, affirme Guy Flechter. Il nous manquait une grande partie du contexte, la mise au jour des identités et des privilèges à risque était très complexe. Avec Salesforce ou AWS, par exemple, il était loin de résoudre notre problème de visibilité. En mettant en corrélation les identités, droits et activités, Polyrize (désormais DatAdvantage Cloud) nous a permis de comprendre quels employés et sous-traitants auraient le plus fort impact sur notre entreprise en cas de fuites de données ou compromissions de comptes liées à des droits trop importants ou à un accès à de vastes quantités de données stratégiques. »

AppsFlyer a fait appel à Polyrize (entreprise acquise par Varonis en 2020) pour obtenir une visibilité et un contrôle sur les identités et accès. Dans un premier temps, cette mission a mis en difficulté l'équipe de Polyrize, car elle devait automatiser le suivi et la surveillance de l'ensemble des identités et privilèges en temps réel. De plus, ce processus jusque-là géré par le biais de feuilles de calcul complexes et statiques devait à terme être compatible avec plusieurs services SaaS et IaaS.

> « J'ai donné à l'équipe de Polyrize la priorité suivante : se connecter à Okta et me dire quels groupes ont accès à quelles applications pour que je puisse déterminer si ces accès sont appropriés, explique Guy Flechter. Ensuite, je voulais pouvoir localiser les attributions excessives ou incorrectement configurées pour que mon équipe soit en mesure d'isoler rapidement les problèmes et de révoquer les accès si nécessaire. »

Détection des événements de sécurité et mise en place des réponses appropriées

En plus de répondre aux besoins initiaux d'AppsFlyer, Polyrize (désormais DatAdvantage Cloud) a offert à l'entreprise un niveau stratégique de sécurité réactive en lui permettant de détecter les événements de sécurité et d'y répondre dès qu'ils se produisent. « Polyrize propose l'interface unique dont j'avais besoin pour sécuriser mes différentes applications cloud, s'enthousiasme Guy Flechter. La possibilité de détecter les identités à risque, d'attribuer les accès strictement nécessaires et de mettre au jour leur utilisation inappropriée depuis la même plateforme simplifie la gestion du processus de sécurité, mais fournit également une protection supplémentaire lorsque des incidents se produisent. »

Les équipes d'assistance et de service client de Polyrize ont travaillé en étroite collaboration avec les spécialistes de la sécurité d'AppsFlyer pour déployer la plateforme et l'intégrer à l'infrastructure et aux processus de sécurité du cloud de l'entreprise.

> « L'équipe de Polyrize a travaillé avec nous tout au long du déploiement initial et continue de faire le point avec nous pour résoudre les éventuels problèmes détectés lors de vérifications périodiques. Elle nous permet de contrôler notre sécurité et nous offre une visibilité sur notre conformité. Nous la considérons comme un partenaire de confiance et un maillon à part entière de notre stratégie de sécurité cloud. »

« La possibilité de détecter les identités à risque, d'attribuer les accès strictement nécessaires et de mettre au jour leur utilisation inappropriée depuis la même plateforme simplifie la gestion du processus de sécurité, mais fournit également une protection supplémentaire lorsque des incidents se produisent. »

Résultats

« Nous avons obtenu des résultats exceptionnels, se réjouit Guy Flechter. Aujourd'hui, Polyrize (désormais DatAdvantage Cloud) me permet de limiter l'impact potentiel d'une attaque en mettant au jour les identités inutilisées et les droits incorrectement configurés, en identifiant les utilisateurs au cœur d'événements à haut risque et en détectant, traitant et analysant ces événements une fois qu'ils se sont produits. De plus, Polyrize (désormais Varonis) a renforcé ma posture de sécurité dans le cloud tout en réduisant les coûts liés à l'équipe de sécurité et la gestion de la sécurité. »

« Polyrize (désormais DatAdvantage Cloud) a renforcé ma posture de sécurité dans le cloud tout en réduisant les coûts liés à l'équipe de sécurité et la gestion de la sécurité. »

Surveillez et détectez les menaces sur vos applications et dépôts de données cloud stratégiques.

DEMANDER UNE DÉMO