Orca Security fait passer Zip de 18 % de visibilité du risque à 100 % de couverture en moins d'une journée

INDUSTRIE
Services financiers

CHAMPION
Peter Robinson, Directeur de la cybersécurité et de l'informatique d'entreprise

ENVIRONNEMENT DU CLOUD
AWS, Azure

« Nous sommes passés d'années de souffrance à une visibilité totale en un seul après-midi. Venant d'un gars qui est dans les tranchées, c'est profond. »

Peter Robinson
Directeur de la cybersécurité et de l'informatique d'entreprise, Zip

Défis de la sécurité du cloud

- L'expansion rapide de l'entreprise entraîne une croissance rapide du patrimoine du cloud ;
- La nature éphémère de l'infrastructure rend difficile la recherche de vulnérabilités ;
- Différents environnements sont gérés par plusieurs personnes dans plusieurs pays.

Résultats de la sécurité du cloud

- Couverture à 100 % des comptes cloud avec une visibilité complète, un inventaire des actifs et une résolution prioritaire, le tout sans impact sur les environnements de production ;
- Dépendance réduite vis-à-vis du DevOps tout en obtenant leur soutien total pour les corrections prioritaires ;
- Économies de coûts massives car il n'y a pas de coûts d'intégration, pas besoin de six ETP pour trouver et hiérarchiser les risques, et le modèle de licence de paiement à l'utilisation d'Orca ne s'applique qu'aux actifs réellement utilisés.

Zip croit en l'innovation implacable

Zip Co est un acteur de premier plan dans la prochaine génération de l'industrie du financement et des paiements de détail. La société propose des services de crédit au point de vente et de paiement numérique aux secteurs de la vente au détail, de la maison, de la santé, de l'automobile et du voyage. Fondée en 2013 et basée à Sydney, en Australie, Zip a connu une croissance rapide et est désormais présente en Australie, en Nouvelle-Zélande, en Afrique du Sud, au Royaume-Uni et aux États-Unis. Une expansion supplémentaire en Amérique du Nord, en Europe et au Moyen-Orient est prévue.

La plateforme informatique de Zip est entièrement numérique et hébergée dans le cloud. La plate-forme exploite les données volumineuses dans sa technologie de prévention de fraude et de décision de crédit pour fournir des réponses en temps réel. Reflétant la croissance de l'entreprise, le domaine du cloud se développe également rapidement. Il y a un an, il y avait six comptes AWS. Aujourd'hui, il existe vingt-deux comptes AWS et neuf comptes Azure, et d'autres sont en cours.

> « Avant Orca, nous avions peut-être 18 % de couverture d'évaluation de vulnérabilité sur l'ensemble de notre périmètre. Orca nous a permis d'atteindre 100 % en moins d'une journée. »
>
> **Peter Robinson**
> Directeur de la cybersécurité et de l'informatique d'entreprise, Zip

Peter Robinson est le directeur de la cybersécurité et de l'informatique d'entreprise, responsable des postures de cyber-risque et de sécurité de l'entreprise. « Zip est né dans le cloud et c'est un environnement difficile pour sécuriser nos actifs, car les outils de sécurité traditionnels ne fonctionnent pas bien ici », dit-il. Il a passé la majeure partie de ses deux années chez Zip à rechercher la bonne combinaison d'outils qui offrira une bonne visibilité sur les vulnérabilités et les risques auxquels Zip est confronté et les moyens de les atténuer.

De peu de visibilité à 100 % en un après-midi

La plateforme de Zip est à la pointe des technologies cloud. « Nous avons fortement évolué vers l'informatique sans serveur et l'infrastructure en tant que code », déclare Robinson. « La nature éphémère de notre environnement nous met dans une position où nous ne pouvons pas obtenir d'agents sur ces appareils avant qu'ils ne soient partis. Nous ne pouvons pas les analyser en réseau au sens traditionnel du terme et il n'y a aucun moyen de se connecter à ces machines pour évaluer leur état de sécurité lorsqu'elles ne fonctionnent pas. »

« Nous avons également le problème d'avoir de nombreux environnements gérés par différents groupes. Nous avons six équipes DevOps qui travaillent sur différentes parties de l'infrastructure et d'autres choses. Amener ces équipes à déployer n'importe quoi pour faire une évaluation des risques est presque impossible », explique Robinson. « Orca a immédiatement résolu ce problème pour nous. »

Robinson a découvert Orca Security grâce à des articles sur LinkedIn. « Au début, nous étions sceptiques quant aux affirmations d'Orca, mais nous avons essayé. Nous sommes passés d'années de souffrance à une visibilité totale en un seul après-midi. Venant d'un gars qui est dans les tranchées, c'est profond. »

Orca surpasse de loin les outils concurrents

Robinson a passé deux ans à évaluer les outils d'analyse de vulnérabilité traditionnels et d'autres qui étaient spécifiques aux environnements de type conteneur. « Ils ont tous eu les mêmes problèmes. Premièrement, ils nécessitaient trop de ressources pour déployer des agents et des scanners. Deuxièmement, ils ont besoin d'informations d'identification pour s'authentifier, ce qui fait du modèle de licence un échec selon nous. Et troisièmement, aucun des outils ne priorise et ne suit automatiquement les corrections. »

Le problème des licences est également un gros point négatif pour ces outils. « Avec les autres fournisseurs, je devrais acheter une licence complète et infinie d'actifs. Dès qu'une licence est utilisée, bien qu'il s'agisse d'un actif éphémère, nous devons la payer. Un serveur n'a fonctionné que pendant six heures et il a maintenant consommé une licence. Faire le travail avec ces outils me coûterait cinq fois plus cher. » Robinson rapporte qu'une licence traditionnelle lui aurait coûté un quart de million de dollars par mois.

Le principal problème de tous ces outils est qu'il n'y a pas de hiérarchisation des risques. Par exemple, Robinson dit qu'il peut y avoir 129 règles qui échouent, qu'elles concernent 2000 actifs et que l'outil affiche 6 ou 8 pages répertoriant les échecs. « On peut vite se retrouver dépassé. Ce n'est pas faisable. Même le SIEM a fait face à 55 000 échecs ces sept derniers jours. Vous ne pouvez même pas tout évaluer. »

Orca surmonte tous ces inconvénients. Le déploiement est sans intervention et ne nécessite que la création d'un rôle, ne prenant que quelques minutes. Aucun agent n'a besoin d'être installé. L'octroi de licences est beaucoup plus gérable et est basé sur les actifs réellement utilisés.

Cependant, là où Orca se démarque vraiment, c'est dans ses capacités de hiérarchisation. « Orca me dit que j'ai 28 choses sur lesquelles je dois me concentrer aujourd'hui. Sur 25 comptes cloud avec environ 840 actifs de calcul, machines virtuelles et des milliers d'autres actifs, le risque réel se résume à 28 éléments à gérer aujourd'hui », explique Robinson. « C'est totalement gérable. »

L'équipe Zip de Robinson est petite, elle doit donc s'appuyer sur des outils pour l'aider à atteindre ses objectifs. « Avec Orca, toute l'automatisation, la hiérarchisation, la corrélation et le déploiement à impact zéro dans nos environnements de production sont tout simplement incroyables. C'est fantastique », déclare-t-il.

Orca améliore la sécurité informatique et la coopération et la productivité DevOps

Robinson affirme que les équipes DevOps agissent rapidement pour mettre leurs produits sur le marché. Il ne peut pas leur demander d'arrêter de créer un produit Zip pour déployer des agents et des scanneurs réseau. Orca enlève ce fardeau. En fait, les équipes DevOps sont celles qui l'ont le plus soutenu dans l'adoption de la plateforme Orca Security.

« L'essentiel est que nos équipes DevOps n'aient rien à faire. Ils créent un rôle et c'est fait, et ils n'auront plus rien à faire. Il n'y a pas de déploiement, pas de règles réseau, pas de groupes de sécurité à modifier, pas de déploiement d'application ou d'agent de point de terminaison, pas d'informations d'identification, rien. Cela a changé mon monde », explique Robinson.

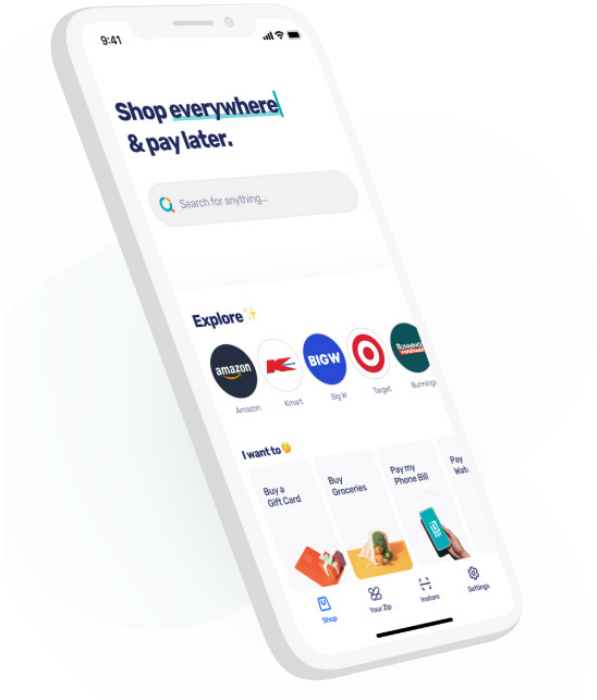
Les équipes de sécurité informatique et de DevOps travaillent désormais bien ensemble. « Je peux venir vers eux avec des mesures correctives prioritaires recommandées par Orca. Il y a des instructions très claires sur les problèmes qui sont très importants », explique Robinson. « Et ce n'est pas seulement une question d'actif de point de terminaison. Par exemple, supposons que nous ayons un problème avec le groupe de sécurité de cette ACL réseau, cet équilibreur de charge et ce point de terminaison. Orca fournit une carte. Nos employés disent : « Oh, Orca montre comment il est possible de contourner CloudFlare et les équilibreurs de charge internes. Elle montre le routage multi-chemins. » Nous savons que cela n'est pas censé se produire car cela signifie que quelqu'un contourne notre WAF. » Robinson dit que ce type d'information est inaccessible à partir d'autres sources. « Orca fournit un aperçu approfondi de leurs mauvaises configurations. Ils peuvent le voir visuellement. Ils savent qu'ils doivent le modifier ou renforcer les groupes de sécurité afin que vous ne puissiez passer que par l'équilibreur de charge. Et l'équilibreur de charge ne prend que les entrées de CloudFlare, et vous ne pouvez pas accéder à l'équilibreur de charge directement depuis Internet. Ce type d'informations est incroyablement utile pour réduire notre charge de travail », déclare Robinson.

« Nos équipes DevOps se concentrent sur notre produit et c'est ce qu'ils devraient faire. Je ne peux pas leur demander de détourner leurs efforts pour déployer des agents de point de terminaison partout et créer des informations d'identification de scanner. »

Peter Robinson
Directeur de la cybersécurité et de l'informatique d'entreprise Zip

Orca prend en charge des fonctionnalités de niveau entreprise telles que le contrôle d'accès basé sur les rôles. « Ce qui est vraiment bien, c'est que lorsque nous ajoutons des personnes, nous pouvons leur attribuer des comptes. Je peux le configurer de telle sorte que mes équipes Quadpay aux États-Unis ne puissent voir que les données Quadpay et travailler sur les comptes Quadpay, au lieu de voir l'ensemble de l'entreprise. Ils ne voient que ce dont ils ont besoin », dit Robinson.

Si Zip n'utilisait pas Orca dans toute l'entreprise, Robinson estime qu'ils auraient besoin d'au moins une personne à temps plein dans chacune de ses six juridictions. « Nous aurions probablement besoin de six ETP supplémentaires pour parcourir une longue liste de vulnérabilités non hiérarchisées, déterminer sur quoi travailler, créer des tickets pour les corrections, tout en essayant de gérer les agents et tout le reste. C'est donc plus qu'une simple question de gestion des risques. Il y a aussi une question de temps, de coût et d'effort », explique Robinson. « Orca fait d'une pierre deux coups : le risque est immédiatement pris en compte, du moins du point de vue de la visibilité, et les coûts sont pris en charge immédiatement. »



Orca s'intègre dans le processus de gestion des risques de Zip

Robinson a une méthode pour découvrir les problèmes - qu'il s'agisse d'un test d'intrusion, d'une analyse de vulnérabilité externe, d'une analyse interne, d'observations, d'incidents ou d'autres moyens - et de les conduire à travers un processus de gestion des risques dans Jira. « Nous avons un tableau des risques dans Jira où nous évaluons les risques inhérents. Nous attribuons ensuite un sous-ticket ou une tâche au propriétaire responsable et évaluons la correction nécessaire », explique Robinson. « L'intégration d'Orca avec Jira est parfaite, donc cela fonctionne vraiment pour nous. »

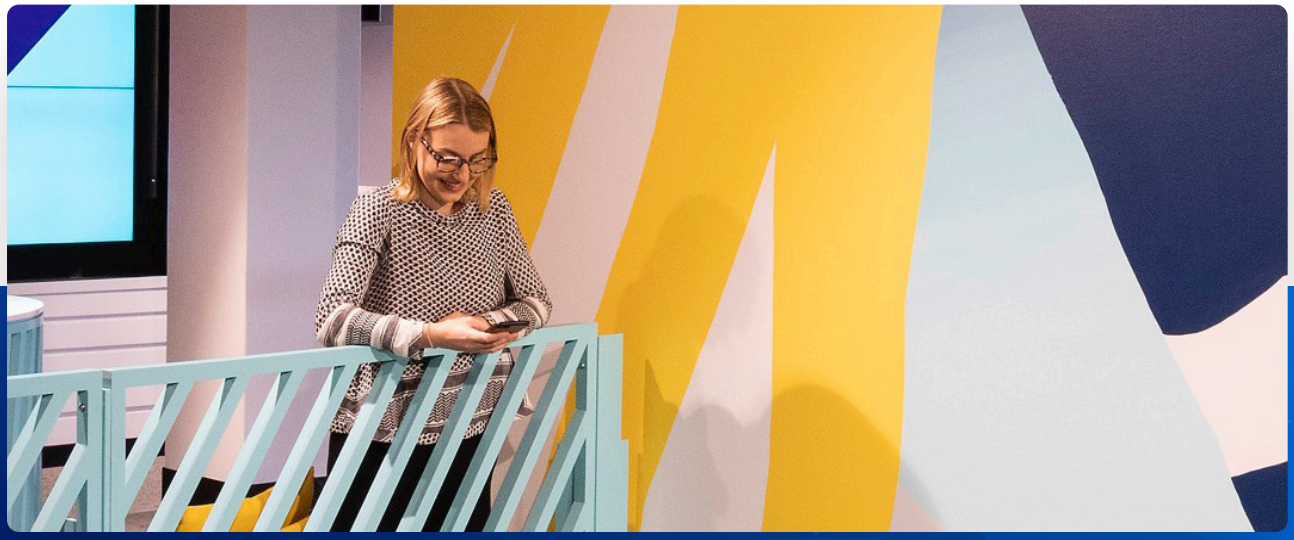
Une caractéristique unique d'Orca est sa résolution automatique. Si elle identifie un problème et qu'il est résolu, Orca note qu'il a été résolu. « Auparavant, les équipes devaient effectuer une évaluation manuelle et un test pour voir si ce problème avait été réellement corrigé ou non. Alors qu'Orca dit juste : « C'est fini. Merci. » Nous pouvons mettre notre risque résiduel à zéro et fermer le ticket », explique Robinson. « C'est un sacré gain de temps. »

Lorsque Zip a récemment acquis une entreprise, Robinson a été invité à mettre leurs actifs sous sa gestion. « Cela m'a pris littéralement quelques minutes et deux nouveaux comptes Amazon étaient entièrement sous mon champ d'application de la gestion des vulnérabilités, à 100 %. »

Orca remporte le retour sur investissement et l'analyse de rentabilisation

Zip dispose d'outils qui analysent leurs actifs de l'extérieur. « Nous lui lançons des noms de domaine, elle fait de la découverte et utilise des techniques de prime aux bogues pour évaluer nos vulnérabilités externes », explique Robinson. « Mais les évaluations internes étaient plus difficiles avant de trouver Orca. Je me suis battu pour obtenir les analyses internes dont nous avions besoin. Nous avons retravaillé les budgets et essayé de mettre un coût sur l'effort, la main-d'œuvre et la diminution de notre produit Zip. J'ai rédigé l'analyse de rentabilisation pour inclure ces actifs incorporels. J'ai parlé avec nos dirigeants du temps qu'il faut pour distraire les gens de leur travail habituel pour déployer des agents et configurer les choses, et de temps qu'il faut pour passer en revue les vulnérabilités pour trouver celles qui sont importantes et faire toute cette corrélation manuelle. Cela prend énormément de temps. De même, les coûts d'intégration sont énormes. »

Il déclare qu'avec Orca, le risque est considérablement réduit car la couverture est de 100 %. Et le gain de temps est à peu près de 100 % par rapport à tout autre produit. « Le déploiement prend 20 minutes et il est intégré à Jira sur le backend », explique Robinson. « Du point de vue de l'administration du système, de l'infrastructure ou du DevOps, il n'y a rien d'autre à faire, pour toujours. L'analyse de rentabilisation d'Orca est solide. »



À propos d'Orca Security

Grâce à sa technologie SideScanning™ unique (brevet en instance), Orca Security assure la sécurité et la conformité à l'échelle du cloud et des charges de travail de services comme AWS, Azure et GCP. Après une intégration instantanée, en lecture seule et sans impact, au fournisseur de cloud, il détecte les vulnérabilités, les logiciels malveillants, les mauvaises configurations, les risques de mouvement latéral, les risques d'authentification et les données non sécurisées à haut risque, puis hiérarchise les risques en fonction du problème sous-jacent, de son accessibilité et de son rayon d'action, sans déployer d'agents.

orca security

Connectez votre premier compte cloud en quelques minutes et voyez par vous-même : consultez orca.security

© Copyright Orca Security 2021. Toutes les marques déposées, les marques de service et les noms de commerce référencés dans ce support appartiennent à leurs propriétaires respectifs.