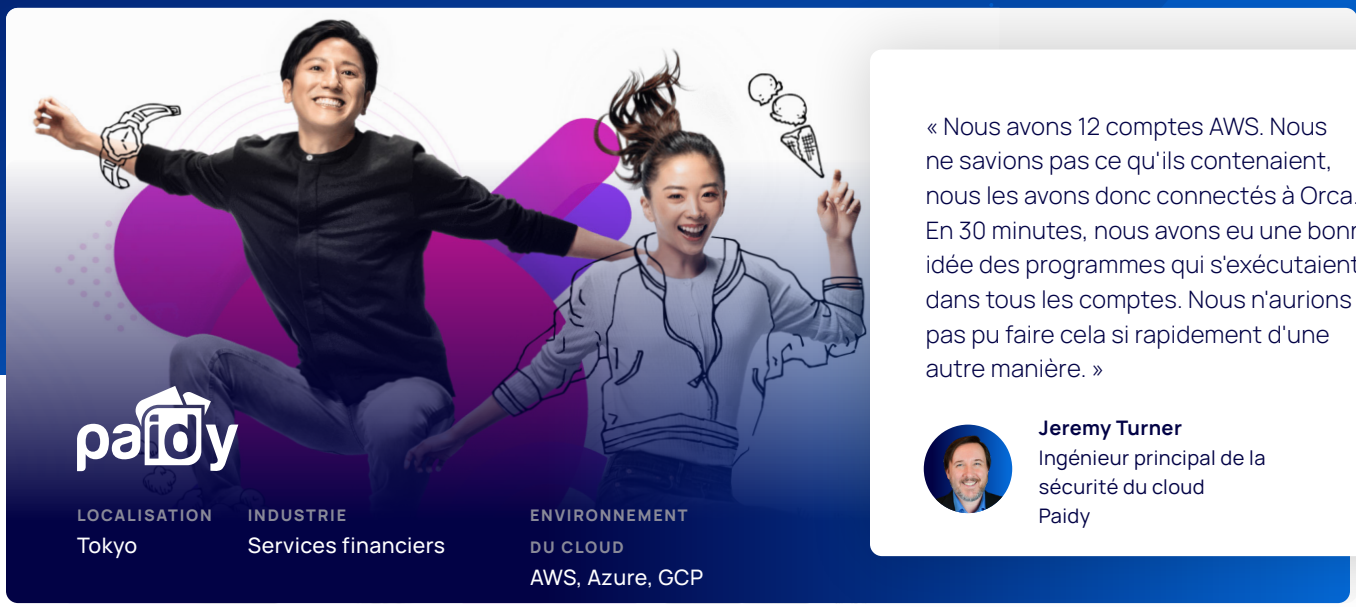
Paidy se tourne vers Orca Security pour une visibilité multi-cloud, économise deux ETP et 500 000 $/an en coûts de gestion de la sécurité du cloud



LOCALISATION
Tokyo

INDUSTRIE
Services financiers

ENVIRONNEMENT DU CLOUD
AWS, Azure, GCP

« Nous avons 12 comptes AWS. Nous ne savions pas ce qu'ils contenaient, nous les avons donc connectés à Orca. En 30 minutes, nous avons eu une bonne idée des programmes qui s'exécutaient dans tous les comptes. Nous n'aurions pas pu faire cela si rapidement d'une autre manière. »

Jeremy Turner
Ingénieur principal de la sécurité du cloud
Paidy

Défis de la sécurité du cloud

- Des centaines de développeurs poussant des microservices dans des dizaines de comptes sur plusieurs clouds rendent difficile le suivi et la sécurisation de chaque actif dans le patrimoine cloud de l'entreprise ;
- Le coût pour créer une solution par eux-mêmes serait d'au moins deux ETP pendant un an, puis 500 000 $ par an pour la maintenir ;
- Elle cherche à protéger de manière proactive les données personnelles d'identification et, à se conformer aux réglementations japonaises telles que le règlement sur la confidentialité transfrontalière et la loi sur la protection des données personnelles.

Résultats de la sécurité du cloud

- Il a fallu trente minutes pour commencer à gagner en visibilité sur son patrimoine cloud ; elle a connecté douze comptes AWS à Orca Security, qui a identifié un « compromis imminent » ;
- Elle économise 500 000 $ par an en travaux fastidieux de sécurité dans le cloud ;
- Elle peut prouver aux auditeurs qu'elle a la capacité d'identifier et de protéger les données personnelles d'identification ;
- L'intégration plus rapide des marchands entraîne une augmentation des revenus.

Paidy : une institution financière japonaise dans le cloud

Paidy est un leader de la technologie financière dans l'offre de paiements sans carte et d'autres services financiers au marché de masse et aux entreprises japonaises. Ses solutions sont à l'avant-garde pour révolutionner les paiements en ligne et mobiles, les transferts P2P, les finances personnelles et le règlement des commerçants. Paidy permet aux clients de payer en utilisant uniquement leur adresse e-mail et un numéro de téléphone portable. Aucune carte de crédit ou préinscription n'est nécessaire. Pour éviter la fraude, chaque transaction est authentifiée à l'aide d'un code PIN envoyé par SMS. Les clients peuvent acheter maintenant et payer une facture consolidée le mois suivant.

L'intégralité de la plate-forme de Paidy s'exécute dans le cloud, principalement sur plusieurs comptes AWS, mais également sur Azure et GCP. Elle dispose de plusieurs environnements de test et de développement. Avec une plate-forme traitant les transactions financières, la sécurité est de la plus haute importance. Le RSI, Felix Beatty, est responsable de l'optimisation de la posture de sécurité globale de Paidy.

« Nous sommes essentiellement une institution financière dans le cloud » explique Beatty. « Parce que nous avons connu une croissance si rapide (ayant gagné plus de trois millions de clients en moins d'un an) il y a des domaines de notre activité où nous pouvons nous améliorer et l'un d'eux est la sécurité du cloud. La plupart de nos services fonctionnent aujourd'hui dans le cloud, nous avons donc besoin de solutions de sécurité cloud qui mettent immédiatement en évidence les problèmes critiques afin que nous puissions les résoudre rapidement. »



« Un agent peut ou non fonctionner sur ce noyau Linux, et il en va de même pour les versions de Windows. Il y a tellement de variables qui entrent en jeu. Après des années passées à traiter avec des agents, puis à voir à quel point il est facile d'installer et d'utiliser Orca, je savais que son approche sans agent était à la fois une innovation majeure et un second souffle. »

Jeremy Turner
Ingénieur principal de la sécurité du cloud Paidy

L'environnement cloud à grande échelle de Paidy fait de la visibilité totale un défi

Gagner en visibilité sur tout ce qui se trouve sur la plateforme Paidy est l'un de ses principaux défis. « Nous avons un environnement cloud vaste et complexe ; il est difficile de gérer tous ces actifs dynamiques » déclare Beatty. « Nous avons des centaines de développeurs qui essaient de pousser les microservices aussi rapidement que possible dans le cloud, de démarrer ou d'arrêter des instances, de créer des sauvegardes, de créer des compartiments S3 et d'avancer si rapidement qu'il est très difficile de savoir à tout moment ce que nous avons. Nous devons nous poser la question : « Quelle est la posture de sécurité actuelle de tous nos actifs cloud ? » »

Jeremy Turner, ingénieur principal de la sécurité du cloud, est son bras droit dans la sécurisation de l'environnement cloud. Les deux font équipe depuis bien avant leur intégration à Paidy et savent comment aborder son défi de sécurité.

Les agents de sécurité sont excellents (Si et lorsqu'ils fonctionnent, ce qui est rarement le cas)

« Je fais ça depuis longtemps », déclare Turner. « J'ai appris que tout ce qui concerne la sécurité et la vulnérabilité nécessite généralement l'installation d'un certain type d'agent. Si vous travaillez dans infosec depuis un certain temps, vous savez que les agents tombent en panne, qu'ils doivent être mis à jour et qu'ils pourraient être des vecteurs d'autres failles de sécurité. »

Turner admet que les agents sont excellents (si et lorsqu'ils fonctionnent). « C'est rarement le cas. Il y a tellement de dépendances et d'autres choses auxquelles penser. Un agent peut ou non fonctionner sur ce noyau Linux, et il en va de même pour les versions de Windows. Il y a tellement de variables qui entrent en jeu. Après des années passées à traiter avec des agents, puis à voir à quel point il est facile d'installer et d'utiliser Orca, je savais que son approche sans agent était à la fois une innovation majeure et un second souffle. » déclare Turner.



Les anciens scanners de vulnérabilité et outils AWS n'étaient pas adaptés

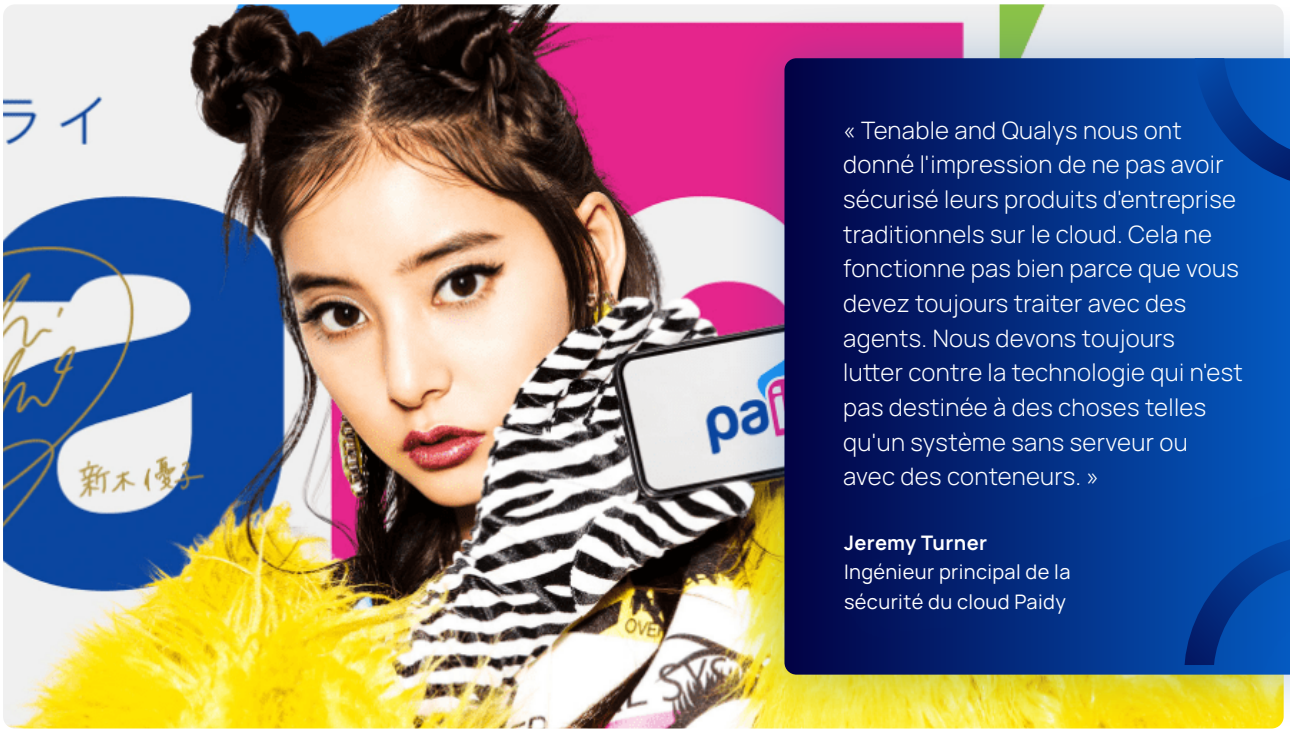
L'équipe de sécurité Paidy avait de l'expérience avec une variété d'outils hérités adaptés au cloud. Turner déclare : « J'ai utilisé Trend Micro, Qualys et Tenable, que ce soit dans un environnement d'entreprise ou pour des tests. Tenable and Qualys nous ont donné l'impression de ne pas avoir sécurisé leurs produits d'entreprise traditionnels sur le cloud. Cela ne fonctionne pas bien parce que vous devez toujours traiter avec des agents. Nous devons toujours lutter contre la technologie qui n'est pas destinée à des choses telles qu'un système sans serveur ou avec des conteneurs. »

Paidy a également exclu l'utilisation de scanners réseau. Selon Turner : « Ayant de l'expérience avec les scanners non authentifiés, je savais qu'ils avaient une visibilité limitée et pouvaient créer des temps d'arrêt.

« Les scanners authentifiés peuvent vous fournir plus de données de vulnérabilité, mais leur configuration nécessite encore beaucoup de travail, ainsi que des privilèges élevés. Cela expose votre entreprise à des risques car vous avez en fait un autre compte et mot de passe partagés. »

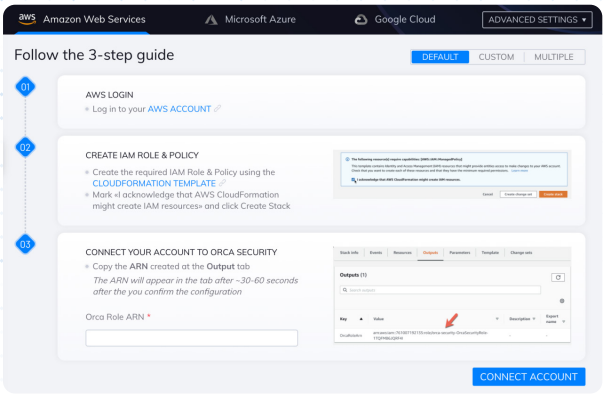
Les fournisseurs de cloud comme Amazon fournissent des outils d'analyse de sécurité. « L'AWS Inspector d'Amazon, scanner de vulnérabilité, nécessite un agent. Habituellement, il est intégré à l'AMI d'Amazon, mais cela ne fonctionne qu'avec certaines AMI », poursuit-il. « AWS GuardDuty coche la case pour une analyse des vulnérabilités et un contrôle de conformité. Mais le signalement est son plus gros problème ; l'utilisation des données peut être un défi. Il ne fait qu'afficher une liste de vulnérabilités, puis c'est à nous de trouver quoi faire à leur sujet. »

Beatty ajoute : « Parce que nous avons plusieurs comptes AWS et que nous sommes multi-cloud, il était difficile d'avoir une vue unique à partir de laquelle nous pourrions surveiller tout ce qui se passe. La visibilité multi-cloud était notre problème numéro un. Deuxièmement, nous n'avons ni le temps ni les ressources pour orchestrer un outil en utilisant, par exemple, les services AWS ou quelque



> « Tenable and Qualys nous ont donné l'impression de ne pas avoir sécurisé leurs produits d'entreprise traditionnels sur le cloud. Cela ne fonctionne pas bien parce que vous devez toujours traiter avec des agents. Nous devons toujours lutter contre la technologie qui n'est pas destinée à des choses telles qu'un système sans serveur ou avec des conteneurs. »
>
> **Jeremy Turner**
> Ingénieur principal de la sécurité du cloud Paidy

chose de similaire. Nous voulons utiliser un service qui ne nécessite aucun agent, où nous n'avons pas besoin de le mettre à jour régulièrement et qui fonctionne tout simplement. » Pour Paidy, Orca Security répond à tous ces besoins et plus encore.



Orca SideScanning™ offre une visibilité indispensable

La plate-forme Orca Security est largement différente des autres outils de sécurité. Livrée en tant que SaaS, elle lit le stockage en mode bloc cloud hors bande, d'où le terme SideScanning™. Aucun code ne s'exécute dans l'environnement cloud d'un client. Au lieu de cela, Orca crée un modèle en lecture seule de son environnement cloud, qu'elle analyse ensuite pour évaluer les problèmes de sécurité potentiels.

Avoir une visibilité complète est ce que Turner apprécie le plus. « La visibilité est un problème que chaque organisation rencontre. Orca nous a presque immédiatement donné une visibilité à la fois large et profonde sur notre paysage de menaces », explique Turner. « Lorsque nous prenons ces données et les montrons aux autres, ils n'en croient pas leurs yeux. Nous avons eu un cas où Orca a révélé un « compromis imminent » d'un système qui flotte dans un environnement de test depuis probablement deux ou trois ans.

Le système exécutait un système d'exploitation totalement obsolète. Une fois qu'Orca l'a identifié, nous avons créé un ticket permettant à un ingénieur de le résoudre. Nous avons eu la chance de capturer la vulnérabilité avant que le système ne passe au test d'acceptation de l'utilisateur et en production. »

Beatty est d'accord sur la valeur de la visibilité : « Il n'y a plus aucune excuse à ignorer les problèmes lorsqu'ils se présentent juste devant vous. Lorsque le tableau de bord Orca indique « compromis imminent », c'est très clair. »

Orca aide également Paidy à résoudre les problèmes d'étalement de compte. « Nous gérons 12 comptes AWS » explique Turner. « Nous ne savions pas ce qu'ils contenaient tous, alors nous les avons connectés à Orca. En 30 minutes, nous avons eu un aperçu de ce qui se passait dans tous les comptes. Nous n'aurions pas pu faire cela si rapidement d'une autre manière. »

La gestion des actifs est une autre fonction qu'Orca Security fournit à Paidy. Orca fournit un inventaire de l'emplacement de chaque élément, des métadonnées et une liste de vulnérabilités. « C'est plutôt sympa de pouvoir choisir une instance et voir qui s'y est connecté, combien de tentatives de connexion ont échoué ou quels packages y sont installés. J'apprécie de pouvoir le faire sans dépendre d'un agent pour chaque instance » déclare Turner.

Orca Security identifie et protège les données personnelles d'identification, facilitant les efforts de conformité de Paidy

Au fur et à mesure que Paidy acquiert de l'expérience avec la plate-forme Orca Security, son équipe trouve de nouvelles façons d'utiliser les données qu'elle génère. « En tant qu'entreprise Fintech, nous sommes très attentifs aux combinaisons toxiques de données. Orca nous y aide », déclare Turner. « Par exemple, les clients doivent fournir leur numéro de téléphone portable pour utiliser notre service. Mais si nous avons affaire à des adresses personnelles ou e-mail combinées à d'éventuelles informations de compte bancaire et à un historique d'achats, nous entrons alors dans les problèmes de données personnelles d'identification et de réglementations japonaises en matière de confidentialité des données. »

Turner explique comment Orca aide à protéger les données personnelles d'identification. » Une fonctionnalité nous permet de savoir si Orca soupçonne des problèmes au niveau des informations personnelles.C'est comme une balise qui nous dit : « Ce serveur contient des adresses e-mail qui n'appartiennent pas à paidy.com. Qu'est-ce qui se passe ? » Nous pouvons ensuite enquêter. À l'heure actuelle, l'outil ne dit pas :« Voici une combinaison toxique de données », mais il nous montre où creuser. Nous avons eu une situation où l'équipe de science des données a créé un nœud de base de données qui a conduit à une combinaison de données aussi toxique. Orca nous a aidés à nous en apercevoir à temps pour intervenir le plus tôt possible. »

Paidy doit se conformer à un certain nombre de lois sur la confidentialité des données. Le règlement sur la confidentialité transfrontalière du Japon est similaire au RGPD de l'UE et la loi sur la protection des données personnelles du pays a été promulguée en 2004. Orca aide à prouver aux auditeurs que Paidy est parfaitement capable d'identifier et de crypter les informations personnelles. Paidy peut être tranquille en sachant qu'Orca a la capacité de rechercher des informations personnelles vulnérables.

Turner utilise l'intégration d'Orca Security avec Jira pour ouvrir les tickets. À leur tour, ces derniers déclenchent les flux de travail afin que les personnes et les processus puissent prendre les mesures appropriées ; par exemple, pour chiffrer des données sensibles ou pour résoudre d'autres problèmes détectés par Orca.



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 services 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.

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.