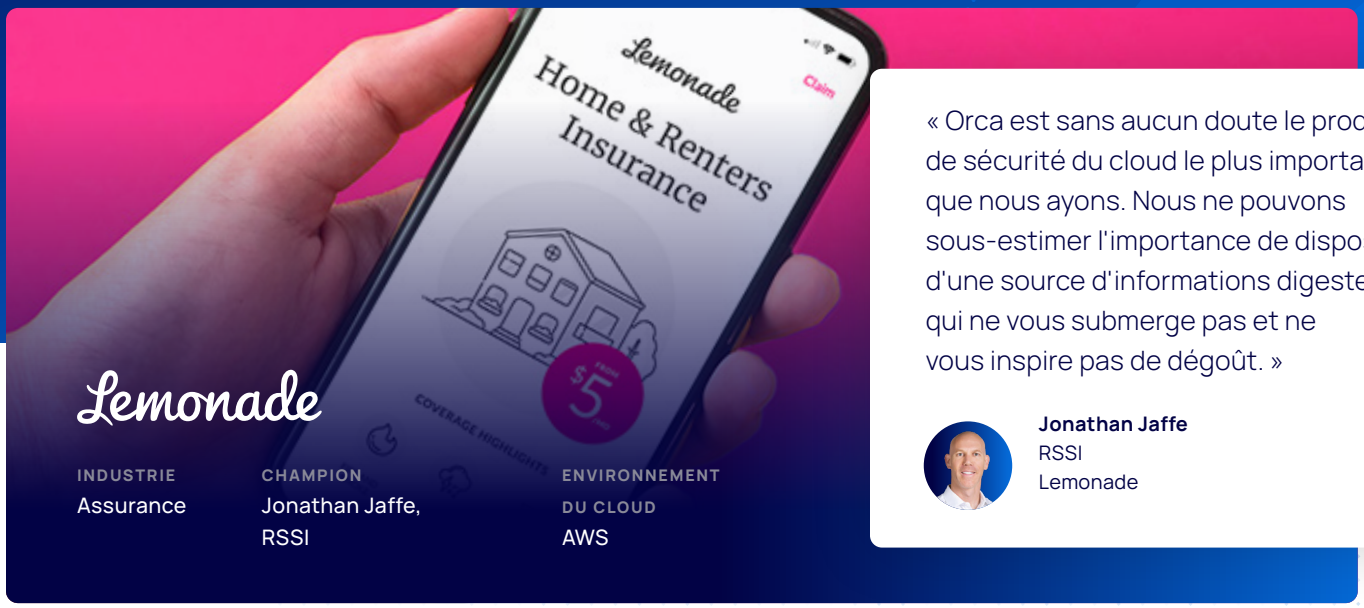
L'innovateur d'assurance Lemonade passe de 0 à 100 % de visibilité dans le cloud avec Orca Security



Lemonade

INDUSTRIE
Assurance

CHAMPION
Jonathan Jaffe, RSSI

ENVIRONNEMENT DU CLOUD
AWS

« Orca est sans aucun doute le produit de sécurité du cloud le plus important que nous ayons. Nous ne pouvons sous-estimer l'importance de disposer d'une source d'informations digeste qui ne vous submerge pas et ne vous inspire pas de dégoût. »

Jonathan Jaffe
RSSI
Lemonade

Défis de la sécurité du cloud

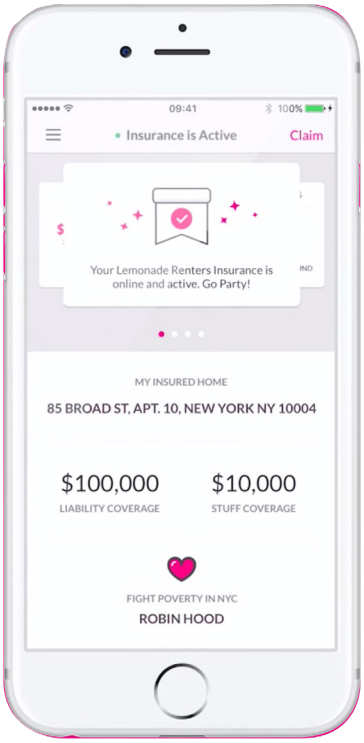
- Obtenir une visibilité complète de l'ensemble du domaine du cloud ;
- Classer rapidement les questions importantes par ordre de priorité en « bouchées digestibles » ;
- Réduire l'impact sur DevOps.

Résultats de la sécurité du cloud

- Couverture à 100 % des comptes cloud, avec une visibilité totale et des mesures correctives prioritaires, le tout sans impact sur DevOps et l'environnement de production ;
- Capacité de respecter les mandats de conformité et de prouver les contrôles aux auditeurs ;
- Le tableau de bord Orca montre les informations exploitables des problèmes prioritaires ;
- Tranquillité d'esprit, car il n'y a pas de lacunes dans la couverture.

Lemonade révolutionne le marché de l'assurance

Lemonade fournit des assurances aux États-Unis et en Europe. Elle fait partie du marché de l'« assurtech », où les fournisseurs d'assurance utilisent des technologies avancées pour offrir des produits et des services innovants que les entités traditionnelles ne peuvent pas égaler. En tant qu'entreprise relativement jeune, Lemonade dispose d'une pile technologique cloud native, qui lui permet de fonctionner 100 % en ligne. Cela fait de Lemonade un concurrent agile sur le marché de l'assurance. Par exemple, Lemonade fournit des devis de police à l'aide d'un bot d'intelligence artificielle sur le Web et via ses applications mobiles. Parallèlement, Lemonade est évalué A, entièrement réglementé et réassuré par les noms les plus fiables de l'assurance.



L'expérience antérieure d'Orca du responsable de la sécurité informatique ouvre la voie

L'infrastructure de Lemonade se trouve entièrement dans le cloud AWS, où il peut être difficile d'obtenir des informations en temps réel sur les vulnérabilités et les risques de sécurité. Même les outils natifs d'Amazon ne fournissent pas toutes les informations dont les praticiens de la sécurité et de DevOps ont besoin.

Jonathan Jaffe a rejoint Lemonade comme son RSSI en 2020. Il a immédiatement cherché à obtenir une visibilité complète de l'ensemble du domaine du cloud afin d'évaluer les risques de sécurité. « Lorsque je suis arrivée à bord, il n'y avait pas de solution adéquate en place pour m'informer de nos vulnérabilités », dit-il. « Je voulais une visibilité bien plus grande que celle que nous avions sur les problèmes de vulnérabilité du cloud. »

Orca bat ses concurrents basés sur les agents, Lacework et Palo Alto Prisma Cloud.

« Nous avons évalué Orca Security, ainsi que Palo Alto Prisma Cloud et Lacework », dit Jaffe. « Dans ma dernière entreprise, nous avons utilisé Lacework depuis plus d'un an. Au cours des quatre derniers mois dans cette entreprise, nous avons également utilisé Orca dans le cadre d'un POC, ce qui nous a permis d'effectuer facilement une comparaison côte à côte avec Orca. Et nous avons considérablement évalué Prisma Cloud. »

Chez Lemonade, l'équipe d'évaluation a dû compter sur des démos de produits pour Prisma Cloud et Lacework, même si Jaffe connaissait très bien Orca et Lacework. « Contrairement à Orca, les autres ont besoin d'agents. DevOps n'était pas enthousiaste à l'idée de mettre en place et de maintenir des agents. DevOps craignait également l'impact que les agents pouvaient avoir sur les performances de nos systèmes, notamment de production.

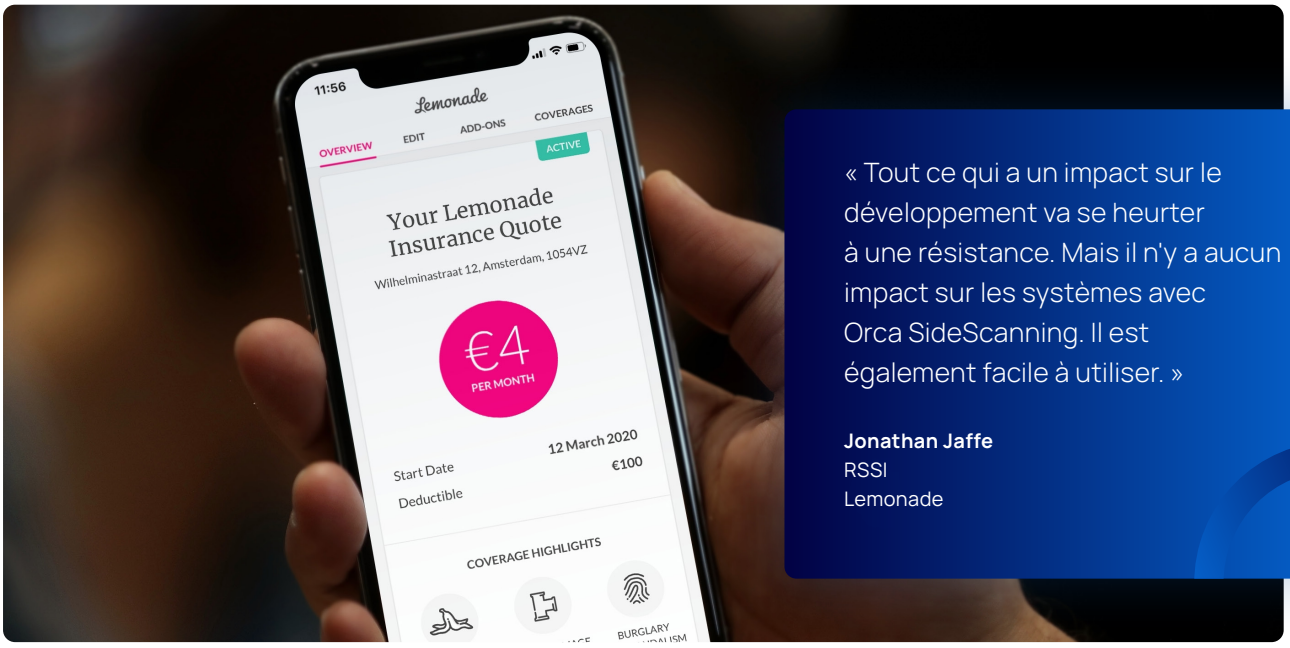
Et sur la base de mes expériences antérieures avec Laceworks, je savais que je me battrais avec une visibilité manquante à cause d'agents manquants. » Il aura fallu une demi-heure à Orca pour configurer et se déployer dans son intégralité pour le POC. « Nous l'avons fait fonctionner en un rien de temps. » dit Jaffe. « Nous avons vu des résultats immédiatement. En moins de 24 heures, nous avons pu voir toutes les ressources et l'environnement dans tous nos comptes AWS.
De plus, nous avons pu voir rapidement et facilement les problèmes qu'Orca a trouvés, qui, heureusement, étaient petits et gérables. »

Couverture à 100 % et priorisation des questions de sécurité

Jaffe a cherché plusieurs fonctionnalités importantes dans une solution de sécurité. « La première est une couverture à 100 %, c'est quelque chose que nous n'obtiendrons jamais si nous devons mettre en place des agents. Je dois être sûr que nous n'avons pas de lacunes dans la couverture. »

Une autre fonction indispensable est la possibilité de classer par ordre de priorité ce qui doit être réparé. « Lacework fournit des tas d'informations, mais nous ne les avons pas trouvées utiles ; au contraire, nous avons constaté qu'elles nuisaient à notre capacité à remédier aux problèmes. En avoir trop diluait la valeur des quelques joyaux qu'il aurait pu faire émerger.
De plus, il ne priorise pas les informations d'une manière utile. Lorsque nous utilisions Lacework, notre analyste de la sécurité passait le plus clair de son temps à essayer de comprendre quels problèmes il devait consacrer à la résolution. S'il parvenait à passer outre ce problème et à choisir un sujet à explorer, il se heurtait au problème suivant : y a-t-il vraiment eu une intrusion ou s'agit-il d'un autre faux positif ? Tout cela devait se produire avant qu'il ne puisse remédier à la situation.
Avant Orca, nous abandonnions souvent la résolution d'un problème parce que les informations étaient mal organisées. »

« Orca est le contraire. Grâce aux informations présentées dans une matrice, nous pouvons les examiner par type de menace, par vulnérabilité, par compte, par ressource affectée, etc. Nous pouvons afficher les cinq principaux éléments par catégories, tels que des actifs négligés ou des vulnérabilités.



« Tout ce qui a un impact sur le développement va se heurter à une résistance. Mais il n'y a aucun impact sur les systèmes avec Orca SideScanning. Il est également facile à utiliser. »

Jonathan Jaffe
RSSI
Lemonade

Les problèmes sont ainsi présentés en petites bouchées que nous pouvons mâcher, une à la fois, au lieu d'être submergés, comme c'est le cas avec de nombreux autres produits. Nous pouvons rapidement traiter des problèmes prioritaires, en supprimant ou en rejetant ceux qui ont une moindre importance. »

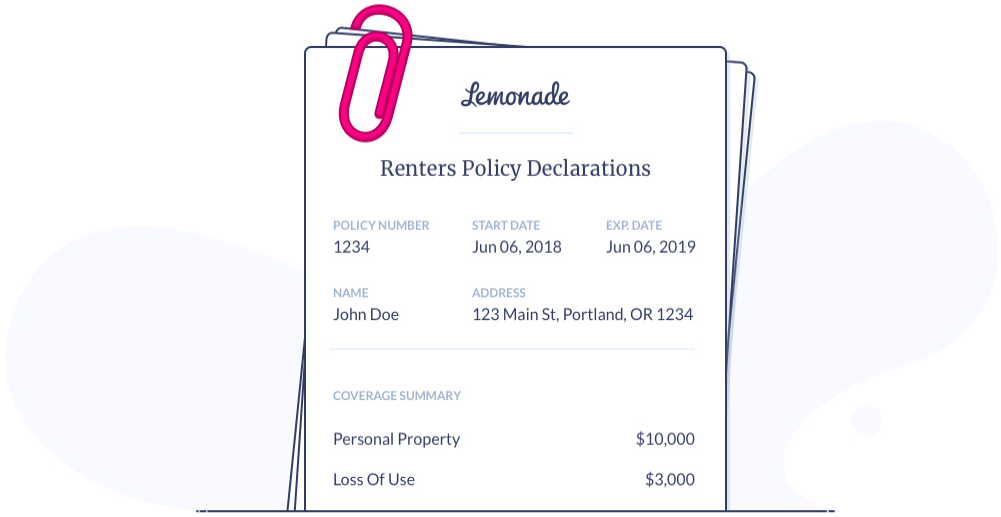
Pour Jaffe et son équipe, le tableau de bord Orca fournit un effet calmant, car il ne les submerge pas en leur fournissant trop d'informations. Selon lui, « la véritable valeur d'Orca réside dans le fait qu'elle couvre une grande partie de ma sécurité du cloud, en nous informant des vulnérabilités et, à un degré très réduit, des menaces réelles. »

Preuve de contrôles pour les audits

Avec son siège social à New York, le département des services financiers de cet État (NYDFS) régule les activités de Lemonade. De plus, l'entreprise est soumise à diverses réglementations de l'UE et dispose de ses propres audits SOC 2. Les rapports d'Orca aident Jaffe à fournir des preuves de contrôle pour les diverses réglementations et audits. « Orca a aidé à réduire mes activités de vérification. Par exemple, je peux exécuter des rapports qui montrent que nous maintenons moins de contrôles de privilège et que nous utilisons l'authentification à plusieurs facteurs. »

Orca alerte également Jaffe en cas de problèmes potentiels de perte de données ou si des données personnelles sont exposées dans des zones à risque. L'équipe de Lemonade peut remédier à ces problèmes bien avant qu'ils ne deviennent un problème qui apparaîtrait dans les rapports d'audit. « Orca est très efficace pour détecter l'exposition potentielle de données de cartes de crédit, d'adresses e-mail, de numéros de sécurité sociale ou d'autres identifiants nationaux », explique Jaffe. « Ce sont des questions prioritaires auxquelles nous pouvons rapidement remédier ».

> « Orca réduit notre principal problème : où sont nos risques de sécurité liés au cloud ? Avant Orca, nous n'avions tout simplement pas la visibilité dont j'avais besoin. »
>
> **Jonathan Jaffe**
> RSSI
> Lemonade

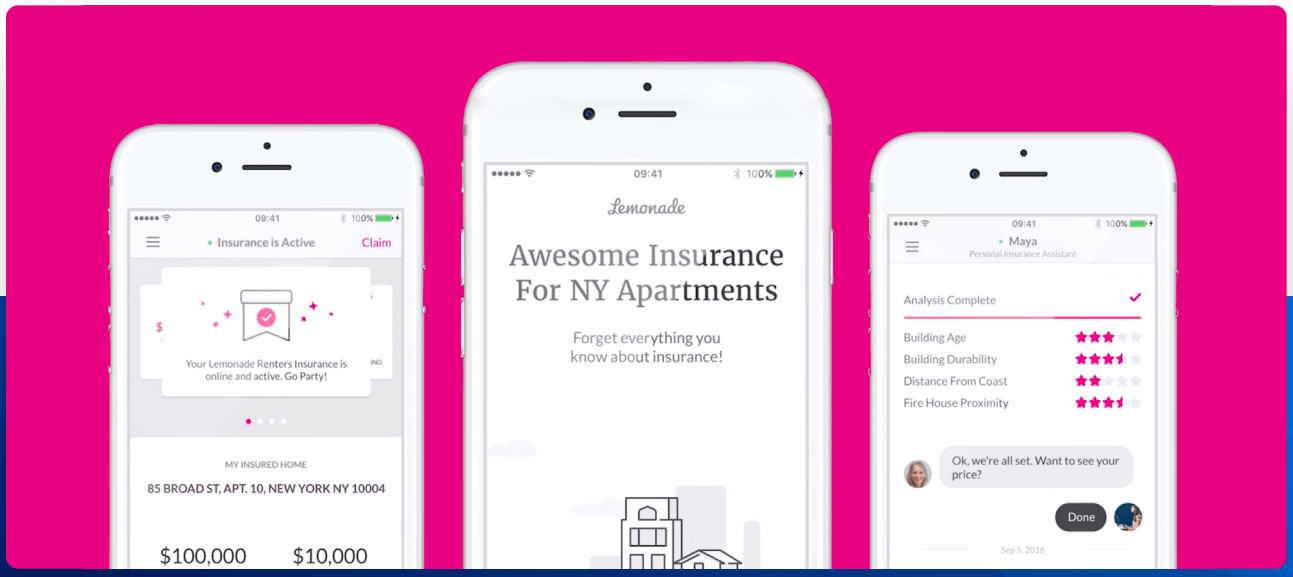


Les éléments à risque ont été largement réduits

Lemonade a considérablement réduit ses éléments à risque. « Nous les avons réduites à un sixième de ce qu'elles étaient, et maintenant nous pouvons les garder sous contrôle en les surveillant », dit Jaffe. « Orca nous permet d'éclairer les choses, nous savons ainsi ce qu'il faut réparer et ce dont nous n'avons pas à nous soucier. »

Ce que Jaffe aime le plus dans Orca est la façon dont elle répertorie les problèmes prioritaires. « Vous pouvez voir les cinq principaux éléments par catégories, tels que les actifs négligés ou les vulnérabilités. Les problèmes sont ainsi présentés en quantités digestes, ce qui nous permet de les traiter un par un, au lieu d'être submergés comme le font beaucoup d'autres produits. »

Il aime également l'interface, déclarant que le tableau de bord a un effet apaisant, car il ne le submerge pas en lui fournissant trop d'informations. Selon Jaffe : « La vraie valeur d'Orca est de couvrir une grande quantité de ma sécurité du cloud, en m'informant des vulnérabilités et, dans une moindre mesure, des menaces réelles. »



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.