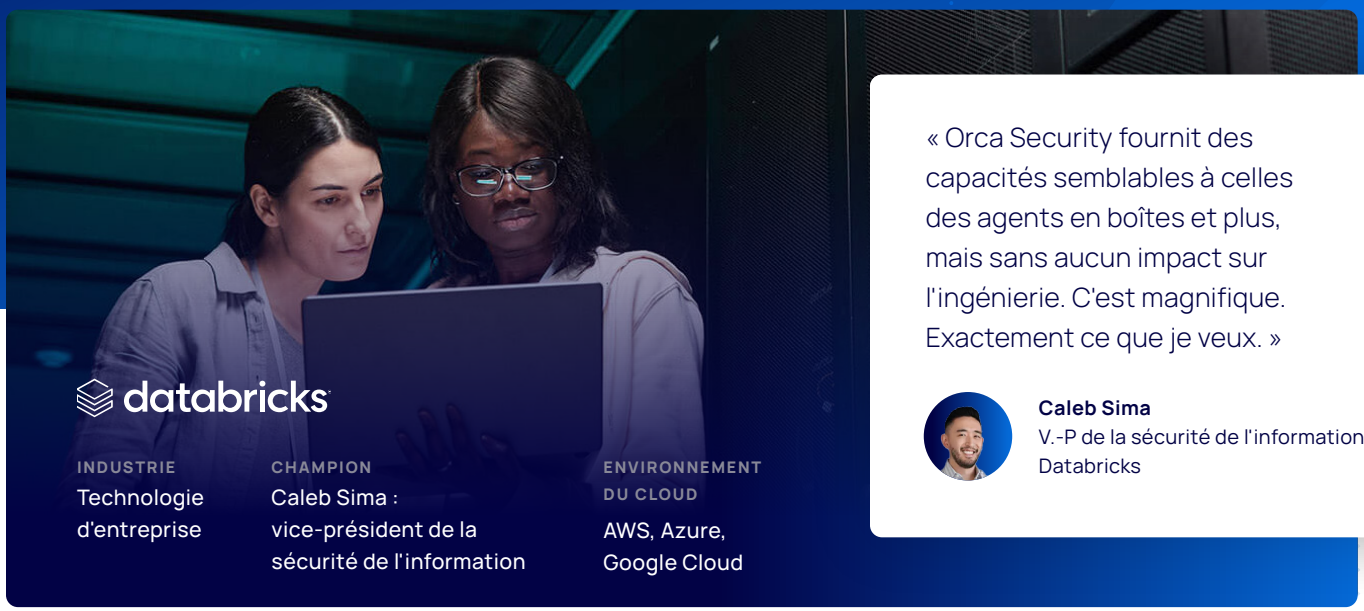
Orca Security est un choix évident pour Databricks



INDUSTRIE
Technologie d'entreprise

CHAMPION
Caleb Sima : vice-président de la sécurité de l'information

ENVIRONNEMENT DU CLOUD
AWS, Azure, Google Cloud

« Orca Security fournit des capacités semblables à celles des agents en boîtes et plus, mais sans aucun impact sur l'ingénierie. C'est magnifique. Exactement ce que je veux. »

Caleb Sima
V.-P de la sécurité de l'information
Databricks

Défis de la sécurité du cloud

- Gagner de la visibilité sur tout ce qui s'exécute sans avoir à déployer d'agents ;
- Évaluer précisément les vulnérabilités et les risques, en hiérarchisant leur résolution ;
- Prise en charge d'un patrimoine multicloud ;
- Éviter les frictions avec l'ingénierie logicielle.

Résultats de la sécurité du cloud

- Gain de visibilité grâce à des alertes hiérarchisées en fonction des risques qui sont précises, exploitables et dans le contexte ;
- Capable de traiter tous les principaux problèmes de sécurité ; surveiller maintenant les plus petits ;
- Un même outil hors bande permet d'identifier les vulnérabilités, fournit l'inventaire des actifs, la surveillance et la détection de ce qui se passe sur tous les systèmes cloud ;
- La technologie est totalement sous le contrôle de l'équipe de sécurité.

Databricks gère les risques pour aider les clients à réussir

Databricks est un leader de l'analytique des données et du machine learning. Aujourd'hui, plus de cinq mille organisations dans le monde, y compris plusieurs entreprises faisant partie du classement Fortune 500, dépendent de Databricks pour permettre l'ingénierie des données à grande échelle, la science des données collaborative, le cycle complet du machine learning et l'analyse commerciale. L'entreprise possède des centaines de partenaires dans le monde, dont de grandes marques comme Microsoft, Amazon, Informatica et Cap Gemini.

En tant qu'entreprise de technologie d'entreprise qui fait partie de la chaîne d'approvisionnement de ses clients et de ses partenaires, Databricks met l'accent sur la surveillance et la gestion de ses propres risques pour gagner et conserver leur confiance. Elle investit dans des produits et des fournisseurs de sécurité de premier ordre pour fournir cette assurance.

Databricks exploite un environnement multicloud à l'aide d'AWS, d'Azure et de GCP. L'emploi de ces trois plateformes rend difficile l'utilisation des outils natifs des opérateurs de cloud pour bénéficier d'une sécurité uniforme sur l'ensemble des systèmes. Il est donc essentiel de sélectionner de bons outils pour maintenir un environnement sécurisé.

Un entrepreneur spécialisé dans la sécurité qualifie Orca de « simple et brilliant »

Caleb Sima est le vice-président de la sécurité de l'information de l'entreprise. Il a été entrepreneur pendant une grande partie de sa carrière et a lancé, développé et vendu une série d'entreprises de cybersécurité. Il y a quelques années, Sima a décidé de prendre un tournant dans sa carrière de fondateur et d'entrepreneur pour devenir défenseur au sein des entreprises. Cela lui donne une perspective unique sur les meilleures technologies à déployer pour défendre et protéger les applications et les environnements cloud de Databricks.

« L'entrepreneur en moi a dit : "Eurêka !" C'est si évident et si simple, mais tout simplement brillant. Ça coule de source. »

Caleb Sima
V.-P de la sécurité de l'information
Databricks

« Lorsque j'ai rejoint Databricks, j'ai eu l'occasion de monter intégralement mon équipe de sécurité. Ensemble, nous avons évalué et choisi les outils de notre pile de sécurité » dit-il. Un critère important était de ne pas déranger l'équipe d'ingénierie logicielle de Databricks. « Nous sommes une entreprise dynamique et je ne voudrais surtout pas ralentir les progrès de nos ingénieurs. Notre pile technologique évolue si vite qu'il serait difficile et complexe d'installer des agents sur les ressources. »

« Dès que j'en ai entendu parler, j'ai vraiment voulu voir la démonstration Orca. Ce qui a piqué mon intérêt était d'apprendre comment cela fonctionnait en prenant essentiellement des instantanés de disque et en les analysant pour identifier les activités et les vulnérabilités. »

Les agents ajoutent de la complexité ; la complexité s'ajoute aux risques

Sima savait qu'il ne voulait pas d'un produit qui utilisait des agents sur les machines, notamment lorsqu'il s'agit d'infrastructures et d'hôtes critiques.

> « Orca hiérarchise les alertes de risque de façon très exploitable tant pour l'information qui est fournie, qu'au niveau de sécurité qui est donné. C'est parfait, de la magie pure. »
>
> **Caleb Sima**
> V.-P de la sécurité de l'information
> Databricks

« Ça demande beaucoup d'efforts inutiles, tant pour la sécurité que pour l'ingénierie, de faire fonctionner une solution basée sur des agents » dit-il. « Tous les fournisseurs qui utilisent des agents disent qu'ils sont légers. Le problème n'est pas la puissance du processeur, mais d'ajouter des risques. Plus vous ajoutez de choses à un système, plus vous accroissez sa complexité et plus les risques de problèmes sont élevés. »

La valeur d'Orca était immédiatement évidente

Databricks a demandé un POC et a rapidement mis Orca en service. Tout ce que l'entreprise a dû faire était de configurer certaines autorisations de compte cloud. En quelques heures, Orca montrait des résultats sur son tableau de bord. Sima et ses collègues de la sécurité ne pouvaient pas en croire leurs yeux. « Je me souviens d'avoir examiné les alertes avec étonnement » indique Sima. « Au début, nous pensions qu'il s'agissait de faux positifs. Nous avons alors vérifié par nous-mêmes et réalisé que chaque alerte était avérée. »

Databricks espérait résoudre plusieurs problèmes avec une solution comme Orca. La première intention était d'obtenir de la visibilité sur tout ce qui s'exécute sans avoir à installer des agents sur des boîtes. La société recherchait également un outil qui pourrait l'aider dans la surveillance du cloud, la détection et la réponse. Et elle voulait identifier les risques dans tous ses environnements cloud. « Orca réussissait à trouver un équilibre entre ces besoins et répondait à tous nos critères. La possibilité pour tous les environnements cloud de communiquer les uns avec les autres (et avec Orca) nous donne une image plus précise de notre risque global. »

« Notre principale difficulté concernait la visibilité sur nos charges de travail, instances et machines liées au cloud. » rapporte Sima. « Le POC nous a montré non seulement que nous pouvions voir ce qui se passait, mais aussi qu'Orca pouvait nous dire que quelque chose pouvait arriver. Autrement dit, « Voici les mouvements latéraux qui pourraient se produire et le type de ressources auxquelles un attaquant pourrait accéder potentiellement. »
Ces informations sont incroyables et nous avons donc tout de suite compris la valeur que nous apportait le produit. »

Sima apprécie tout particulièrement l'exactitude et la profondeur des conclusions d'Orca. « Vous pouvez faire des choses comme détecter qu'il y a un grand nombre d'échecs de connexions SSH sur cette boîte et qu'il se trouve que cette boîte contient des clés qui permettent d'accéder à ces boîtes, qui contiennent également un identifiant AWS qui permet d'accéder à cette infrastructure. Manifestement, cette boîte est attaquée et elle possède également trop de privilèges, ce qui est vrai. Et vous pouvez faire tout ça et le communiquer de manière assez compréhensible à toute personne de l'organisation », explique Sima. « C'est extrêmement utile. »

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.