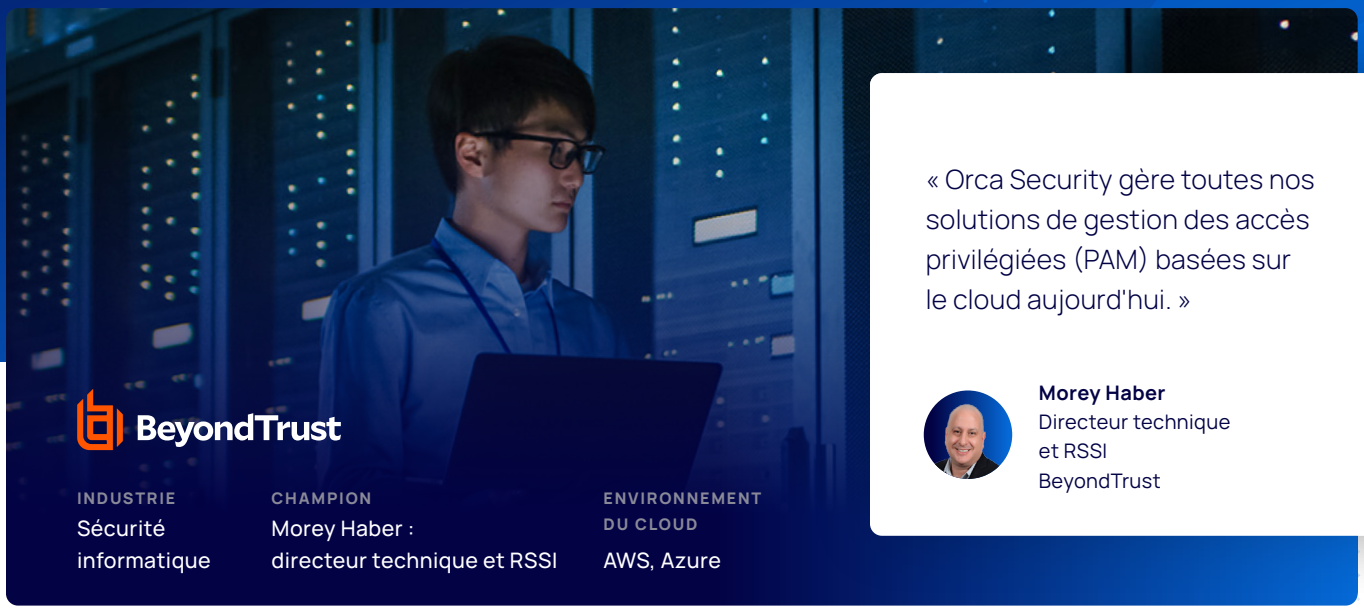
Orca Security aide les services sécurisés dans le cloud de BeyondTrust qui sont utilisés par des milliers de clients



BeyondTrust

INDUSTRIE
Sécurité informatique

CHAMPION
Morey Haber : directeur technique et RSSI

ENVIRONNEMENT DU CLOUD
AWS, Azure

« Orca Security gère toutes nos solutions de gestion des accès privilégiées (PAM) basées sur le cloud aujourd'hui. »

Morey Haber
Directeur technique et RSSI
BeyondTrust

Difficultés de la sécurité du cloud

- L'utilisation d'un outil de sécurité s'appuyant sur des agents était devenue trop complexe et coûteuse à gérer ; elle n'avait pas non plus fourni une visibilité suffisante ;
- Les agents ne peuvent pas se charger sur les images d'appareils personnalisées de l'entreprise ;
- Des rapports étaient nécessaires pour aider à assurer la conformité aux normes ISO, SOC, CIS, et PCI.

Résultats de la sécurité du cloud

- La solution était en production complète dans les deux mois ; entièrement intégrée par le centre de sécurité d'Azure Sentinel (comprend la génération de tickets avec ServiceNow, Jira et d'autres intégrations ;
- Capable de sécuriser et de surveiller les solutions cloud vendues aux clients sans ajouter de risque aux environnements de production ;
- Elle a réduit les délais de développement et d'AQ de 1,5 ETP tout en fournissant une visibilité plus étendue et des résultats d'évaluation plus exploitables ;
- Les rapports Orca montrent des preuves de conformité concernant les mots de passe, la configuration des pare-feu, les vulnérabilités et plus encore.

BeyondTrust fournit une gestion des accès privilégiés basée sur le cloud à plus de 70 % des entreprises du classement Fortune 500

BeyondTrust est le leader mondial de la gestion des accès privilégiées, permettant aux organisations de sécuriser et de gérer l'ensemble de leur univers de privilèges. Plus de 20 000 clients, dont plus de 70 % sont des entreprises du classement Fortune 500, utilisent les trois solutions principales de BeyondTrust pour sécuriser leurs environnements et acquérir le contrôle dont ils ont besoin pour réduire les risques, atteindre la conformité et accroître les performances opérationnelles.

Morey Haber remplit plusieurs rôles chez BeyondTrust. En tant que directeur technique, il supervise la stratégie des produits. Il est également le RSSI de l'entreprise, ce qui le rend responsable de la sécurité interne et du cloud pour plus de 4 000 déploiements cloud utilisés par les clients. Il supervise également tous les efforts liés à la gouvernance, aux risques et à la conformité.

Sur ses 20 ans de carrière dans l'informatique, Haber en a consacré 20 à différents aspects de la cybersécurité. Il a écrit plusieurs livres sur les vecteurs d'attaque et la stratégie de gestion des vulnérabilités et a été directeur de l'ingénierie de sécurité pour une entreprise acquise par BeyondTrust. Il comprend ce qui est nécessaire pour détecter les lacunes techniques qui mettent les entreprises en danger.

Orca adopte une nouvelle approche de la sécurité du cloud

Suite à une démonstration d'Orca Security, Haber était intrigué. « J'étais abasourdi. De toutes mes années spécialisées dans les stratégies et les produits de gestion des vulnérabilités, il s'agit d'une approche complètement nouvelle qui possède tellement de potentiel. »

Haber et son équipe des opérations cloud ont réalisé un essai de la plateforme Orca. « Nous l'avons faite installer et elle a fonctionné en quelques jours. Elle a produit de meilleurs résultats et davantage de visibilité que les agents concurrents nous ont jamais fournis. Avant Orca, les agents nous donnaient seulement de la visibilité sur l'exécution des instances, mais ils ne nous montraient pas le reste de l'environnement » explique Haber. « Ça nous avait beaucoup impressionnés. Orca est maintenant entièrement déployée et gère toutes les solutions cloud que nous vendons aujourd'hui. »

Orca sécurise les charges de travail des clients de BeyondTrust

BeyondTrust représente un cas d'utilisation unique pour Orca Security. Alors que la plupart des clients d'Orca l'utilisent pour évaluer leurs propres charges de travail cloud, en tant que fournisseur de sécurité, BeyondTrust surveille les charges de travail exécutées sur les solutions cloud utilisées par ses clients. Aujourd'hui, l'entreprise prend en charge plus de 4 000 déploiements cloud, beaucoup d'autres étant planifiés alors que BeyondTrust poursuit sa croissance rapide.

> « Je travaille sur des solutions d'évaluation des vulnérabilités depuis plus de 20 ans. J'ai même écrit un livre sur l'élaboration d'une stratégie de gestion des vulnérabilités. Je n'ai jamais rien vu de tel que la plateforme d'Orca Security. Ce produit est un véritable petit bijou. »
>
> **Morey Haber**
> Directeur technique et RSSI
> BeyondTrust

Haber cite un exemple de la manière dont il utilise Orca aujourd'hui. « L'accès à distance privilégié de BeyondTrust permet à des tiers d'accéder à l'environnement d'un client pour vérifier des éléments comme un système CVCA, s'assurer que les imprimantes fonctionnent ou quel que soit le besoin. Notre solution injecte des informations d'identification dans les systèmes cibles, de sorte que les tiers ne connaissent pas ou ne voient pas du tout les mots de passe. Une fois qu'ils se sont connectés, le produit enregistre les activités qui s'affichent à l'écran et documente tout ce qu'ils font, ce qui permet d'établir une véritable architecture à vérification systématique pour l'accès à distance. »

« Orca nous aide à nous assurer que rien n'est ouvert ou mal configuré, qu'aucune instance ne manque de correctifs et qu'aucune vulnérabilité n'existe dans l'environnement cloud de notre client » explique Haber. « Voici un autre exemple dans lequel Orca a démontré une valeur considérable. Nous avons installé un nouveau pare-feu pour un de nos produits. Orca a rapidement signalé que les paramètres par défaut étaient mal configurés et nous avons pu les corriger immédiatement. Comment aurions-nous pu le voir autrement ? Un agent n'aurait pas aidé, car il se trouvait à l'extérieur, mais Orca l'a identifié. Pour moi, c'est inestimable. »

« Orca nous aide à nous assurer que rien n'est ouvert ou mal configuré, qu'aucune instance ne manque de correctifs et qu'aucune vulnérabilité n'existe dans l'environnement cloud de notre client. »

Morey Haber
Directeur technique et RSSI
BeyondTrust

Problèmes avec les solutions basées sur des agents

BeyondTrust utilise une solution concurrente de l'industrie dans le cadre de la gestion des vulnérabilités traditionnelle de ses ressources internes et de ses ordinateurs portables. Avant de trouver Orca, l'entreprise avait tenté d'utiliser sa technologie basée sur des agents dans ses solutions basées sur le cloud, mais s'était heurtée à de nombreux problèmes. « Grâce à l'infrastructure et à la connaissance de cet outil, nous avons décidé d'utiliser leurs agents dans nos produits. L'idée était de déployer un agent avec chacune de nos machines virtuelles » explique Haber.

« Il faut plusieurs machines virtuelles pour constituer une instance pour un client, plus toute la plomberie de backend. Les coûts étaient raisonnables, mais l'implémentation de la chaîne DevOps, le pipeline d'obtention d'une certification, de construction, de connexion, d'exécution, de mise à jour et tout le reste, a pris environ six mois. Et il était très difficile de garder tous ces agents en fonctionnement alors que nous nous efforcions d'intégrer des centaines de clients pendant notre croissance exceptionnelle. Il est devenu très vite évident que cela serait difficile à gérer. »

Haber explique que lorsqu'il s'agit du cloud, si on lui donne un ensemble d'agents à inclure dans une de ses offres de produit, il doit être inclus dès les premiers stades de développement, dans l'AQ et dans la production. « Nous devons configurer les environnements pour gérer l'agent à chaque stade afin de nous assurer qu'il fonctionne, obtenir la sortie des données, puis nous assurer qu'il ne tombe pas en panne. Lorsque vous avez des milliers d'agents, un ou plusieurs d'entre eux finiront par tomber en panne ou échoueront à obtenir des mises à jour. Nous devons ensuite résoudre puis mettre à jour l'environnement de production du client. En matière de contrôle des changements et de conformité, c'est un cauchemar qu'il vaut mieux éviter complètement. »

Orca permet à BeyondTrust d'éviter ces problèmes. « Orca me libère du temps et de l'investissement que nécessitent les agents. Je ne paie pas pour l'exécution d'un agent qui touche un CPU et je n'ai aucun risque de contrôle des changements lorsque je mets un membre de l'équipe des opérations dans un environnement de production. » En ce qui concerne les économies de coûts, Haber indique : « Le coût d'un agent par client s'élève à environ 20 ou 30 dollars par an. Lorsqu'il s'étend sur des centaines et des milliers de clients, le coût de l'utilisation des agents devient considérable. Avec Orca, rien de tout cela. J'estime que nous économisons environ 2 % des coûts d'exécution par client et que nous avons réduit de 1,5 ETP le temps de DevOps et d'AQ. »

Une autre raison critique pour laquelle les agents ne fonctionnent pas pour BeyondTrust est qu'un de ses produits utilise un noyau durci personnalisé. Les agents ne se chargent tout simplement pas sur ce système. La technologie SideScanning™ d'Orca n'éprouve aucune difficulté à le voir.

> « Orca offre une approche rationalisée à toute entreprise envisageant de se développer dans différentes régions. Elle prend moins de temps à mettre en place, offre un délai de rentabilisation plus rapide et fonctionne avec beaucoup moins de risques. »
>
> **Morey Haber**
> Directeur technique et RSSI
> BeyondTrust

Les modules de conformité et les intégrations d'Orca sont inestimables

Plusieurs aspects liés à la conformité avec l'industrie ou la réglementation sont essentiels pour BeyondTrust. Pour gagner la confiance des clients et faire affaire avec eux, BeyondTrust maintient la conformité aux normes SOC et ISO, qui sont toutes les deux entièrement certifiées sur ses plateformes AWS et Azure. Et bien que BeyondTrust ne nécessite pas de conformité PCI dans le cadre de ses activités, il est possible qu'un client obtienne une licence pour sa technologie et l'utilise dans une zone PCI. Il est donc essentiel de posséder une certification PCI. Orca possède des modules de conformité intégrés qui aident Haber à documenter les exigences de conformité (par exemple, concernant les mots de passe, les configurations de pare-feu, l'exposition des informations d'identification, etc.).

L'intégration d'Orca avec le centre de sécurité d'Azure Sentinel et ServiceNow rend la solution beaucoup plus précieuse pour BeyondTrust. Elle utilise le centre de sécurité comme un SIEM et les conclusions d'Orca sont transmises directement dans le centre de sécurité d'Azure Sentinel. Orca Security peut générer un ticket dans ServiceNow si une enquête ou une résolution est nécessaire.

Un tableau de bord du centre de sécurité d'Azure Sentinel est surveillé en permanence afin que les problèmes puissent être traités rapidement. « Nous avons mis en place ces intégrations en moins d'une semaine et cela fonctionne parfaitement. » explique Haber. « Le diagramme d'un tableau de bord m'indique le délai de triage depuis le moment où Orca détecte quelque chose. Notre délai de résolution moyen a été réduit de moitié pour tout ce qui est essentiel » dit-il. « Une fois qu'un ticket est fermé et qu'Orca ne voit plus le problème, nous avons une boucle fermée, ce qui est important pour notre équipe de gouvernance et les personnes qui doivent s'assurer que nous respectons nos ANS » explique Haber.

Impact sur l'ingénierie de la sécurité

Grâce à son intégration avec ServiceNow, Orca peut générer des tickets contenant des détails spécifiques que l'ingénierie de sécurité doit traiter. Cela permet de gagner un temps considérable par rapport à un outil basé sur des agents. « Nous déployons dans plusieurs régions du monde : l'Amérique du Nord, l'Europe et l'Amérique du Sud » raconte Haber. « Par région, lorsque vous examinez le nombre de composants que nous devrions déployer en utilisant une technologie basée sur des agents par rapport à une simple connexion Orca, vous comprenez pourquoi mes équipes de l'ingénierie et des opérations sont beaucoup plus heureuses avec Orca. »

Quant à la vitesse de déploiement et la précision d'Orca, Haber déclare : « C'est un moyen efficace d'obtenir des données complexes pour obtenir des directives exploitables. Elle nous aide dans la gestion des vulnérabilités, la conformité et les configurations sécurisées. Après seulement quelques mois d'utilisation, Orca est devenue une solution très précieuse pour nous. »

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.

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