Comment une société immobilière sécurise Salesforce grâce à Varonis

> Si vous utilisez Salesforce et que vous vous sentez concerné(e) par la sécurité des données, ne manquez pas d'essayer la solution Varonis. Sans elle, il est impossible de disposer d'une vision complète de toutes ces informations avec un point de vue centralisé.

À propos de cette étude de cas :

Notre client est une grande société immobilière américaine. À sa demande, nous avons préservé son anonymat.

En bref

Les problèmes

- Améliorer la visibilité des données pour plusieurs instances Salesforce
- Limiter l'accès dans un environnement Salesforce complexe
- Empêcher l'exfiltration de données et les menaces internes

La solution

Plateforme Varonis de sécurité des données :

- **DatAdvantage Cloud** empêche la surexposition des données dans les applications SaaS
- **Data Classification Cloud** recherche et classe les données sensibles dans les applications cloud
- **DatAdvantage** offre une visibilité et un contrôle sur vos données critiques et votre infrastructure informatique
- **Data Classification Engine** recherche et classe les données sensibles automatiquement
- **Policy Pack** améliore Data Classification Engine à l'aide de modèles qui tiennent compte du CCPA et du RGPD
- **DataPrivilege** rationalise la gouvernance de l'accès aux données
- **DatAlert** surveille les systèmes stratégiques et envoie des alertes en cas de comportement anormal
- **Edge** détecte et aide à prévenir les tentatives d'exfiltration DNS

Résultats

- Capacité à surveiller et détecter les menaces sur les applications cloud
- Diminution de la surexposition de toutes les instances Salesforce
- Tranquillité d'esprit à mesure qu'évolue l'utilisation de Salesforce

Le problème

Verrouiller les droits dans Salesforce

L'une des plus grandes sociétés immobilières d'Amérique du Nord (qui souhaite garder l'anonymat) a adopté **DatAdvantage Cloud** pour protéger les données sensibles dans ses applications SaaS les plus utilisées.

Son équipe savait que des données sensibles étaient potentiellement menacées dans Box, sans réaliser à quel point d'autres secteurs étaient devenus vulnérables. Des systèmes critiques comme Salesforce étaient surexposés en raison d'une augmentation progressive et généralisée des droits.

Tony Hamil, ingénieur principal en cybersécurité, explique :

> **« Nous avons réalisé une validation de concept (POC) pour DatAdvantage Cloud car nous souhaitions avoir une meilleure visibilité sur Box. Nous avons fait de même pour Salesforce, car j'ai pensé : pourquoi pas ?**
>
> **Nous avons ainsi découvert que nous avions bien plus besoin d'améliorer notre visibilité que nous ne l'avions réalisé, car nous en savions si peu sur nos instances Salesforce. »**

Comme beaucoup d'entreprises, la société immobilière était devenue très dépendante de Salesforce pour connecter ses canaux commerciaux, rationaliser son marketing et habiliter ses équipes commerciales. Mais si vous n'empêchez pas les accès excessifs et que vous ne désactivez pas correctement les utilisateurs, votre rayon d'exposition Salesforce (l'étendue des dommages que peuvent causer des hackers une fois qu'ils sont dans un réseau) augmente de façon exponentielle.

C'est ce qui s'était passé dans cette entreprise : plus de 150 utilisateurs disposaient de 64 ensembles de droits uniques, répartis sur huit instances. 55 % des profils utilisateur pouvaient communiquer avec toutes les autres API Salesforce, exporter des données et effectuer d'autres actions privilégiées. Et l'équipe de cybersécurité n'en avait aucune idée...

> **« Nous avions huit instances Salesforce et c'était un désastre. J'avais entendu des histoires horribles sur les problèmes de droits dans Salesforce et la façon dont des centaines d'entre eux, littéralement, peuvent être appliqués de toutes sortes de manières, mais je n'avais pas réalisé à quel point nos ensembles de droits s'étaient complexifiés », déclare Tony.**

Une évaluation gratuite des risques sur les données cloud a révélé un grand nombre d'utilisateurs de niveau administrateur effectuant des modifications fréquentes, notamment concernant les droits. Elle a également mis en lumière les données dont disposait l'entreprise et qui les utilisait.

> **« Je n'avais pas la moindre idée que tant de personnes disposaient d'un accès aussi large. Nous n'avions pas beaucoup de données sensibles dans Salesforce, mais nous devions verrouiller nos droits », dit Tony.**

« Nous avions bien plus besoin d'améliorer notre visibilité que nous ne l'avions réalisé, car nous en savions si peu sur nos instances Salesforce. »

La solution

Une vision holistique sur toutes les activités cloud d'un point de vue centralisé

DatAdvantage Cloud permet à la société immobilière de gérer facilement les droits, de surveiller les activités suspectes et de protéger les données stratégiques dans différentes applications SaaS.

Cette solution change la donne, en particulier pour les applications comme Salesforce, qui ne disposent pas d'un moyen natif de gérer les droits de toutes les instances ni d'une vue complète des accès.

> **« Je ne pense pas que Salesforce dispose d'un moyen intrinsèque de gérer toutes les instances ensemble. Il est impossible d'obtenir la vue globale nécessaire pour découvrir où les utilisateurs ont trop d'accès et gérer tous les droits », explique Tony.**
>
> **« Nous avons donc choisi DatAdvantage Cloud pour tout cela, et cette solution nous a beaucoup aidés, notamment du point de vue de la visibilité globale des droits. »**

Grâce à la visibilité et au contrôle de toutes les activités cloud, Tony peut :

- Cartographier et normaliser les droits dans toutes les applications SaaS, notamment Box et chaque instance Salesforce ;
- Visualiser les droits d'accès par utilisateur ou application cloud, puis désactiver les utilisateurs en toute sécurité pour minimiser le rayon d'exposition potentiel face à une attaque ;
- Détecter et signaler automatiquement les menaces, par exemple les accès inhabituels et l'élévation des privilèges.

Tony et son équipe ont enfin une visibilité totale leur permettant d'identifier **qui** partage des données, **quelles données** sont concernées, **où** ces données sont exposées et **comment** les utilisateurs les partagent. Avec Varonis, ils peuvent répondre à des questions cruciales sur leurs données Salesforce.

> **« Nous pouvons facilement exécuter des rapports et identifier qui a des droits de superadministrateur ou d'administrateur, ainsi que les points de chevauchement. DatAdvantage Cloud se révèle particulièrement pratique en ce qui concerne la visibilité sur l'ensemble des services cloud, car il est quasiment impossible de faire de même manuellement. Ce serait comme une gigantesque toile d'araignée, et il ne fait aucun doute que des informations passeraient au travers », explique Tony.**

Aujourd'hui, la société immobilière tire parti de la quasi-totalité de la suite Varonis de produits de cybersécurité.

Son équipe utilise **DatAlert** et **Edge** pour la détection avancée des menaces et la réponse ; **DatAdvantage**, **Data Classification Engine** et **Policy Pack** pour l'identification des données sensibles, le verrouillage des droits et l'application des règles de conformité ; et **DatAdvantage Cloud** et **Data Classification Cloud** pour l'obtention du même niveau élevé de sécurité et de gouvernance des données s'agissant des applications SaaS.

« DatAdvantage Cloud se révèle particulièrement pratique en ce qui concerne la visibilité sur l'ensemble des services cloud, car il est quasiment impossible de faire de même manuellement. »

Résultats

Minimisation du rayon d'exposition Salesforce

Les avantages pratiques de **DatAdvantage Cloud** et de **Data Classification Cloud** parlent déjà d'eux-mêmes.

Tony utilise ces solutions pour visualiser où les utilisateurs ont un accès excessif aux comptes, contacts, leads et opportunités dans Salesforce. Les données critiques de son entreprise sont ainsi protégées contre la surexposition et, potentiellement, l'utilisation abusive par des employés et des fournisseurs internes, ainsi que les attaques malveillantes externes et la compromission des identifiants.

> **« Du point de vue de la cybersécurité, il est bon de savoir que nous sommes couverts alors que notre utilisation de Salesforce continue de croître et d'évoluer. Je suis très confiant », indique Tony.**

Grâce à une meilleure visibilité et à des alertes fiables qui s'intègrent parfaitement aux solutions de sécurité existantes, l'entreprise a pu réduire les délais de confinement et de réponse.

En outre, le rayon d'exposition Salesforce de l'entreprise a considérablement diminué maintenant que l'équipe de sécurité peut désactiver correctement les utilisateurs et empêcher les accès excessifs de manière proactive.

> **« Si vous utilisez Salesforce et que vous vous sentez concerné(e) par la sécurité des données, ne manquez pas d'essayer la solution Varonis. Sans elle, il est impossible de disposer d'une vision complète de toutes ces données d'un point de vue centralisé », ajoute Tony.**

Alors que l'entreprise s'apprête à créer une autre instance Salesforce dans son environnement (une instance RH qui hébergera des données plus sensibles), Varonis garantit sa tranquillité d'esprit, en sachant que les données sont protégées.

> **« Si vous avez un environnement Salesforce, achetez la solution Varonis ou réalisez au moins la validation de concept, surtout si vous avez plusieurs instances ; c'est une évidence. »**

« Du point de vue de la cybersécurité, il est rassurant de savoir que nous sommes couverts alors que notre utilisation de Salesforce continue de croître et d'évoluer. »

VARONIS

Protégez les données critiques contre la surexposition, sur site et dans le cloud.

Verrouillez votre environnement et protégez les données sensibles dans Salesforce et d'autres services cloud.

Demander une démo