Comment une grande plateforme d'e-commerce a verrouillé 99,9 % de ses fichiers accessibles mondialement en moins de 3 semaines

+ de 791 000
dossiers en accès libre corrigés

4 à 5
heures gagnées par semaine sur le reporting

« Je connais aujourd'hui la taille et l'emplacement des données, je sais si elles sont sensibles ou non, qui a l'autorisation de les modifier et qui y a accès. Je n'aurais jamais pu trouver ces informations sans Varonis. »

À PROPOS DE CETTE ÉTUDE DE CAS :

Notre client est un site d'e-commerce mondial. À sa demande, nous ne mentionnons aucun nom ni aucun lieu dans cette étude.

EN BREF

LES PROBLÈMES

- Nettoyer plus de 800 000 dossiers en accès libre
- Verrouiller les données sensibles pour respecter le CCPA
- Localiser et corriger les erreurs, comme d'anciens sites et comptes utilisateur SharePoint

LA SOLUTION

La plateforme de sécurité des données la plus complète :

- **DatAdvantage** surveille l'accès aux données et les activités en ligne et sur site
- **Automation Engine** supprime en toute sécurité les groupes d'accès globaux
- **DatAlert** surveille et envoie des alertes sur les systèmes critiques
- **Data Classification Engine** recherche et classe les données sensibles
- **Policy Pack** améliore Data Classification Engine à l'aide de modèles qui tiennent compte du RGPD et du CCPA
- **DatAnswers** rationalise les réponses aux DSAR (demandes d'accès des personnes concernées)

RÉSULTATS

- Réduction des dossiers en accès libre, de 800 000 à 8 700 en 2 semaines et demie
- Entre 3 et 5 h gagnées par semaine sur le reporting et de nombreuses heures gagnées sur la remédiation
- La feuille de route vers la conformité au CCPA est clairement définie et réalisable

Le problème

Gérer près de 800 000 dossiers surexposés

Quand le responsable des systèmes d'informations (SI) d'un grand site d'e-commerce mondial (dont nous ne dévoilerons pas le nom à sa demande) a commencé le POC (proof of concept) avec Varonis, il ne savait pas vraiment à quoi s'attendre.

L'entreprise était consciente qu'elle devait verrouiller l'accès aux données sensibles. Elle savait aussi qu'elle avait besoin d'établir des rapports à ce sujet pour se conformer au CCPA américain. Enfin, elle savait qu'elle devait gagner en visibilité sur la structure des autorisations accordées.

Une chose est sûre, l'entreprise ne s'attendait pas à découvrir **près de 800 000 dossiers surexposés**. Ce qu'elle a appris grâce à une évaluation des risques sur ses données offerte par Varonis.

> « Nous avions pour ainsi dire des fichiers sur quasiment tous nos serveurs qui étaient grand ouverts et accessibles par n'importe qui dans l'entreprise, se souvient le responsable des SI. Ce fut un choc révélateur de découvrir tout ça. Je me suis rendu compte que les gens ne nettoient jamais leurs partages de fichiers. »

De nombreux dossiers surexposés contenaient des données sensibles, comme des données à caractère personnel et PCI, et des données protégées dans le cadre du CCPA et du RGPD. Une fuite de données aurait été catastrophique.

> « Nous avons découvert que l'un des grands problèmes venait du fait que les gens partageaient des fichiers sensibles via SharePoint à des personnes externes. Les gens envoyaient un lien de partage qui n'avait pas de date d'expiration. Ces liens étaient encore actifs et accessibles des années plus tard. »

Le POC a révélé d'autres problèmes, notamment 700 comptes utilisateur obsolètes et un grand volume de données obsolètes également. Ces problèmes augmentent le risque et font grimper le coût du stockage de données.

> « Nous avions plus de 600 sites SharePoint. J'étais sidéré. C'est difficile à détecter depuis la page Azure parce qu'une grande partie sont en réalité des sous-sites. Mais même si vous ne gérez pas activement ces dossiers dans Azure, ils vous sont tout de même facturés. »

Pour la première fois, l'ingénieur a obtenu de la visibilité sur les données de l'entreprise et a pu prioriser les tâches de remédiation.

> « Sans Varonis, je n'avais que des bouts d'information, sans vue d'ensemble. Je ne comprenais pas le risque. Avec le POC, j'ai recueilli beaucoup de données et j'ai pu montrer à la direction l'étendue des problèmes que j'essayais de résoudre. »

« Sans Varonis, je n'avais que des bouts d'information, sans vue d'ensemble. Je ne comprenais pas le risque. »

La solution

La remédiation des risques sur pilote automatique

Après avoir évalué les risques, l'ingénieur était préparé mentalement à un grand et laborieux nettoyage de fond. Il pensait qu'il faudrait passer en revue chaque dossier un par un pour en corriger les autorisations.

> « Je me suis dit que ça allait prendre un temps fou rien que d'écrire les scripts PowerShell et encore plus de temps par la suite pour les exécuter. »

Puis le représentant Varonis lui a expliqué que DatAdvantage et Automation Engine pouvaient accélérer ce processus laborieux et chronophage pour qu'il se fasse quasiment tout seul :

- **DatAdvantage** pour les directory services, Exchange, OneDrive, SharePoint et Azure Active Directory donne une visibilité totale sur les environnements cloud et sur site. Grâce à cette solution, l'ingénieur peut auditer chaque accès à un fichier et mettre de l'ordre dans les autorisations excessives en toute sécurité.

→ **Automation Engine** accélère le processus en corrigeant automatiquement des centaines, voire des milliers de dossiers en accès libre.

> « Varonis m'a annoncé que chaque serveur serait corrigé en un jour ou deux. Je me suis dit que c'était impossible, mais ils ont tenu parole. Tout a été réalisé par l'intermédiaire de l'application et je n'ai rien eu à faire. Nous avons simplement indiqué un dossier puis tout était terminé. »

L'ingénieur peut réaliser l'ensemble de cette remédiation à partir d'un point central et éviter de surcharger de travail des responsables de service déjà bien occupés.

> « Avant, c'était difficile de nettoyer des serveurs de départements entiers. Vous deviez tenter de convaincre les utilisateurs d'effacer leurs données obsolètes, mais ils n'avaient pas le temps. Aujourd'hui, je peux imprimer un rapport avec tous les dossiers qui contiennent des fichiers datant de 10 ans, leur demander s'ils ont besoin de ces vieux fichiers, puis les supprimer dans le back-end directement. »

L'entreprise d'e-commerce a également choisi la solution **DatAlert**, pour surveiller et envoyer des alertes sur ses systèmes critiques, ainsi que trois autres solutions de Varonis pour faciliter les efforts continus vers la conformité :

Data Classification Engine	Localise et classe les données sensibles, comme les données PCI ou données à caractère personnel sur tous les systèmes.
Policy Pack	Améliore Data Classification Engine en découvrant et en classant les données spécifiquement protégées par le RGPD et le CCPA.

DatAnswers	Permet de localiser facilement les fichiers contenant des données sensibles, pour que les DSAR (demandes d'accès des personnes concernées) puissent être remplies en quelques minutes.

L'ingénieur n'a pas eu besoin de développer sa propre solution de sécurité à l'aide de PowerShell. Varonis lui a fourni la visibilité et les capacités intégrées pour protéger les données, verrouiller les autorisations d'accès et générer des rapports sur la progression, tout cela rapidement et de manière efficace.

> « Je connais aujourd'hui la taille et l'emplacement des données, je sais si elles sont sensibles ou non, qui a l'autorisation de les modifier et qui y a accès. Je n'aurais jamais pu trouver ces informations sans Varonis.
>
> Aujourd'hui, j'adresse régulièrement un PowerPoint sur la cybersécurité à notre équipe dirigeante. Je peux rapidement illustrer une vue d'ensemble de notre progression, indiquant la suppression des anciens fichiers et des données sensibles obsolètes. »

« [La remédiation] a été réalisée par l'intermédiaire de l'application et je n'ai rien eu à faire. Nous avons simplement indiqué un dossier puis tout était terminé. »

Résultats

Diminution à 99,9 % du nombre de fichiers en accès libre

Grâce à Varonis, la plateforme d'e-commerce a réussi à réduire sa surexposition de 99,9 %, **en passant de 800 000 dossiers en accès libre à seulement 8 700 en tout juste deux semaines et demie.**

Grâce à Automation Engine, la remédiation s'est faite quasiment sans effort. Et pendant que notre solution travaillait en arrière-plan, l'ingénieur a pu se concentrer sur la protection des données sensibles et le nettoyage des fichiers obsolètes.

> « Nous avançons à grands pas. Le nombre de Microsoft Teams se réduit à mesure que nous supprimons les anciennes. Le nombre total de fichiers diminue à mesure que nous supprimons les anciennes données. La tendance est à l'allègement. »

Selon l'ingénieur, la fonction de reporting de Varonis à elle seule leur fait gagner « au moins quatre heures par semaine » et d'innombrables heures en ce qui concerne la correction des accès libres et la gestion des données.

> « Pouvoir localiser les problèmes prend énormément de temps. Et les corriger, c'est encore un autre challenge. Varonis vous permet de passer cette première étape automatiquement, vous montre une vue d'ensemble et vous aide à vous lancer. Cela vous fait gagner beaucoup de temps. »

En matière de conformité, l'ingénieur dispose aujourd'hui des outils pour prouver qu'ils prennent toutes les mesures nécessaires. La visibilité totale atténue le risque que des données sensibles passent entre les mailles et Varonis simplifie tout, des DSAR aux rapports de conformité.

> « Avec Varonis, nous avons la possibilité de consulter les classifications sur toutes les données. La plateforme nous permet de mieux cerner les éléments que nous avons besoin de conserver et la durée de stockage. Nous pouvons supprimer les données obsolètes et sensibles simultanément, ce qui nous aide grandement du point de vue de la conformité. »

À présent, l'ingénieur recommande Varonis à des collègues, mais les prévient : « Foncez, mais préparez-vous à être surpris. Personne d'autre ne vous donne autant d'informations d'ensemble sur un seul écran. »

« Personne d'autre ne vous donne autant d'informations d'ensemble sur un seul écran. »

Améliorez votre visibilité sur les risques de votre entreprise.

Localisez et corrigez les vulnérabilités avec Varonis.

DEMANDER UNE DÉMO