Découvrez comment un hôpital communautaire américain gagne des centaines d'heures chaque semaine en gérant les autorisations avec DataPrivilege

ÉTUDE DE CAS

« Varonis réduit la charge de travail du personnel informatique, dont le rôle n'est pas de gérer les droits d'accès des départements, et permet de redonner le contrôle aux parties prenantes. Nous pouvons enfin verrouiller nos données en toute confiance. »

À PROPOS DE CETTE ÉTUDE DE CAS :

Notre client est un hôpital communautaire américain. À sa demande, nous ne mentionnons aucun nom ni aucun lieu dans cette étude.

EN BREF

LE PROBLÈME

- Gagner du temps et de l'argent en réduisant la charge de travail du service informatique consistant à fournir des droits d'accès
- Améliorer l'efficacité en transférant les contrôles d'accès aux directeurs de départements
- Améliorer la visibilité des emplacements où sont protégées les données HIPAA, à caractère personnel (PII) et PHI et des les personnes qui y ont accès

LA SOLUTION

DatAdvantage :

- Connecte les personnes qui peuvent accéder et accèdent aux données, notamment aux données protégées PII, PHI et HIPAA
- Indique les emplacements où les utilisateurs disposent d'un accès excessif et où les données sont exposées à des risques
- Permet d'automatiser les modifications des listes de contrôle d'accès et des groupes de sécurité

DataPrivilege :

- Permet aux propriétaires de données de gérer les droits
- Réduit la charge de travail du personnel informatique et accélère l'accès aux fichiers
- Applique automatiquement les politiques de sécurité et le moindre privilège

RÉSULTATS

- Une diminution de 75 % des demandes de droit d'accès
- Ressources et heures de travail du service informatique allégées afin de permettre une concentration accrue sur la cybersécurité

Le Défi

Perte de temps et de ressources en raison du contrôle des droits d'accès

Avant que cet hôpital communautaire américain (dont le nom n'est pas mentionné à sa demande) ne fasse appel à Varonis, ses différents départements donnaient souvent l'impression d'être en conflit. Selon le directeur informatique :

> « Le service informatique était toujours fautif. Nous devions gérer les droits d'accès. Par conséquent, nous étions considérés comme des gardiens qui empêchaient les autres départements d'accéder aux informations dont ils avaient besoin. »

Même avec plus d'une douzaine de membres du service informatique affectés à la fourniture des droits d'accès, la tâche était longue et fastidieuse. **Cette équipe passait plus de *400 heures par semaine* à traiter les demandes d'accès.**

Le processus était décourageant pour tout le monde. Le personnel du service informatique passait tout son temps à courir après les gens et à leur poser des questions, car ils ne savaient pas quels employés avaient besoin d'accéder à des fichiers, dossiers et groupes spécifiques. Parallèlement, l'absence d'accès rapide affectait l'efficacité et la productivité des autres départements.

Pire encore, l'organisation commençait à commettre des erreurs en matière de traitement des données. Le DSI (directeur du service informatique) était préoccupé. Il leur manquait un moyen d'identifier clairement les emplacements des données sensibles (HIPAA, PII, PHI) sur leurs serveurs ou de retrouver les personnes qui y avaient accédé.

> « Nous nous posions beaucoup de questions sur l'intégrité des données HIPAA, PII et PHI, et nous n'avions pas la possibilité d'y répondre. Nous recherchions un moyen de protéger ces informations et de connaître leur destination. »

En cas de violation de données, qui représente la pire des situations, ils n'auraient pas été en mesure d'identifier les données dérobées ou les parties responsables.

> « Les hackers exploitent les données à caractère personnel exposées. Si ces données ne sont pas verrouillées, nous sommes exposés à de nombreux risques, en particulier au sein du réseau de santé. »

> « Nous devions gérer les droits d'accès. Par conséquent, nous étions considérés comme des gardiens qui empêchaient les autres départements d'accéder aux informations dont ils avaient besoin. »

La solution

Redonner le contrôle des droits d'accès aux directeurs de départements

Varonis DataPrivilege élimine les engorgements qui se produisent lorsque chaque demande d'accès doit passer par le service informatique. En permettant aux propriétaires de données de consulter et de gérer les droits d'accès des équipes, Varonis a permis à l'hôpital de rationaliser sa gouvernance de l'accès aux données (DAG) pour tous les fichiers, dossiers et groupes de sécurité.

> « Auparavant, une douzaine de personnes devait se concentrer sur la gestion des droits d'accès. Désormais, les parties prenantes bénéficient d'un contrôle direct de leurs données. Chaque département dispose de son propre disque avec des autorisations de partage et des contrôles de sécurité distincts », explique le DSI.

Le portail intuitif en libre-service permet aux directeurs de département de modifier facilement les droits d'accès, de surveiller l'utilisation des données et d'appliquer le « moindre privilège » sans solliciter l'aide du service informatique. Ainsi, seules les personnes qui ont besoin de consulter les données sensibles peuvent y accéder.

Selon le DSI, cela a permis à l'équipe informatique de se concentrer sur des tâches essentielles, comme le verrouillage des données sensibles.

> « Il y a tellement d'informations dans un hôpital. Si tout doit passer par le service informatique, celui-ci perd du temps et des ressources. Varonis me permet d'optimiser les performances de mon équipe et de la développer », explique le DSI.

DatAdvantage pour Windows permet à l'hôpital d'appliquer le principe du moindre privilège en cartographiant les droits d'accès actifs et en fournissant une piste d'audit claire qui permet de savoir quand les utilisateurs accèdent aux données et de connaître celles qu'ils ont manipulées.

Cette visibilité est essentielle pour garantir la sécurité des données, même si elles sont actuellement gérées par les différents services. Selon le DSI, ce niveau de contrôle était impossible avant que Varonis n'intervienne.

> « Nous pouvons exécuter des rapports sur tous nos disques et SharePoint pour localiser les données HIPAA, PHI et PII sur notre serveur et identifier les personnes qui peuvent y accéder. Sans Varonis, nous n'aurions pas la capacité ou les ressources nécessaires pour explorer ces informations et en examiner les détails. »

DatAdvantage avertit également le service informatique lorsqu'il détecte des utilisateurs bénéficiant d'un accès excessif. Cela a permis au DSI et à l'équipe informatique de verrouiller rapidement les données exposées en recherchant et en sécurisant un certain nombre de fichiers et de dossiers qui étaient accessibles à tous dans l'entreprise.

> « Il est très important de verrouiller les informations sensibles, surtout pour les hôpitaux. Il serait désastreux que des hackers parviennent à diffuser des informations sensibles sur les patients. »

> « Auparavant, une douzaine de personnes devait se concentrer sur la gestion des droits d'accès. Désormais, les parties prenantes bénéficient d'un contrôle direct de leurs données. Chaque service dispose de son propre disque avec des autorisations de partage et des contrôles de sécurité distincts. »

Résultats

Les demandes de droits d'accès ont chuté de plus de 75 %

Immédiatement après que l'hôpital ait donné à chaque service le contrôle de ses propres droits d'accès, **les demandes de droits d'accès ont chuté de 75 %**. Cela a permis un gain précieux de temps et de ressources au sein du service informatique.

Alors que la gestion des droits d'accès constituait auparavant un travail à temps plein pour plus d'une douzaine de membres du service informatique, **une seule personne** est désormais nécessaire pour contrôler DataPrivilege, et il ne s'agit plus d'un travail à temps plein.

Le résultat ? Des centaines d'heures de travail gagnées chaque semaine et une efficacité accrue à tous les niveaux.

> « Varonis réduit la charge de travail du personnel informatique, dont le rôle n'est pas de gérer les droits d'accès des départements, et permet de redonner le contrôle aux parties prenantes. Nous pouvons enfin verrouiller nos données en toute confiance. »

En ce qui concerne la sécurité des données, le DSI affirme que Varonis apporte aux hauts dirigeants une « vue panoramique » qui leur permet d'examiner l'ensemble de leurs données sensibles et d'évaluer les niveaux de risque actuels.

Cette visibilité accrue a aidé son équipe à prendre des mesures proactives afin de protéger les données HIPAA, PII et PHI contre les fuites.

> « Varonis nous a permis de passer d'une approche passive et réactive à une protection proactive de nos données sensibles. Nous disposons enfin de l'assurance et des capacités requises pour sécuriser nos dépôts de données. »

Cet hôpital s'efforce d'être toujours à la pointe de la cybersécurité, et son personnel est heureux d'avoir trouvé un partenaire comme Varonis qui innove, évolue et le soutien en permanence.

> « Aucun autre produit ne peut rivaliser avec ce que propose Varonis. De plus, leur service client est exceptionnellement efficace. Varonis répond à tous les besoins. »

« Varonis nous a permis de passer d'une approche passive et réactive à une protection proactive de nos données sensibles. Nous disposons enfin de l'assurance et des capacités requises pour sécuriser nos dépôts de données. »

Remettez les contrôles d’accès entre les mains des propriétaires de données sans sacrifier la cybersécurité.

DataPrivilege permet à votre équipe informatique de se concentrer sur ce qui compte le plus : protéger votre entreprise contre les fuites de données

DEMANDER UNE DÉMO