VARONIS

LIVRE BLANC

La conformité au GDPR avec Varonis

Table des matières

Présentation

Le 25 mai 2018, le Règlement général sur la protection des données (GDPR) de l'UE entrera en vigueur. Il s'agira du plus important changement apporté depuis plus de 20 ans à la législation européenne en matière de sécurité et de confidentialité des données. Basé sur l'actuelle Directive de protection des données, le GDPR renforcera les protections en place en matière de sécurité et de confidentialité des données et viendra y ajouter plusieurs exigences majeures inédites telles que le signalement des violations de données sous 72 heures et l'imposition d'amendes obligatoires.

Le GDPR n'est pas un modèle de sécurité des données totalement nouveau : il s'inspire du principe de Respect de la vie privée dès la conception (PbD) et d'autres concepts de sécurité des données. Dans l'ensemble, on pourrait dire que le GDPR se contente de transposer sous forme de loi certaines pratiques informatiques et certains concepts de sécurité des données. Dans la pratique, le GDPR (article 40) permettra en définitive aux entreprises (ou dans le jargon employé en UE, aux responsables du traitement) de prouver qu'elles sont en conformité avec le GDPR du fait qu'elles respectent des normes de données en place telles qu'ISO 27001 ou PCI-DSS.

Existe-t-il une approche de la sécurité des données qui engloberait de nombreuses normes et lois différentes, y compris le GDPR, et qui pourrait servir de base au programme de votre organisation ?

Les chercheurs en sécurité des données (par exemple, le CIS Framework du NIST) organisent généralement les normes de données en catégories plus larges. Voici trois catégories qui apparaissent habituellement dans ces listes.

1. **Détecter –** Identifier ou localiser les vulnérabilités en analysant les systèmes de fichiers, les services d'annuaire, l'activité des comptes et le comportement des utilisateurs. Améliorer la compréhension de l'organisation pour gérer le risque de cybersécurité auquel les systèmes, actifs, données et capacités sont exposés.

2. **Prévenir / Protéger –** Limiter les dommages potentiels des attaques futures en verrouillant les données sensibles et obsolètes, en limitant les accès généralisés et en simplifiant les droits.

3. **Maintenir –** Maintenir un état sécurisé en automatisant les workflows d'autorisation, les vérifications régulières des habilitations et la conservation et la mise au rebut des données. Surveiller les comportements inhabituels des utilisateurs et des systèmes.

Bien entendu, le GDPR n'est pas une norme de conformité des données explicite constituée de centaines de contrôles secondaires. Ses exigences sont définies sous forme d'articles définissant les objectifs généraux à atteindre, mais qui ne précisent pas comment y parvenir. Pour obtenir des informations plus détaillées sur le GDPR, nous vous conseillons de lire notre livre blanc, Règlement général sur la protection des données (GDPR) : nouvelles règles de sécurité des données dans l'UE.

Avec ce système de catégorisation, nous disposons à présent d'une formule qui nous permet d'organiser les principales exigences du GDPR et de mettre en place un plan d'attaque :

	Article du GDPR	Produit(s) Varonis
Détecter	Sécurité du traitement (Article 32)	DatAdvantage GDPR Patterns
	Analyse d'impact (Article 35)	
Protéger	Protection des données dès la conception et par défaut (Article 25)	DatAdvantage DataPrivilege Data Transport Engine DatAnswers
	Droit à l'effacement (Article 17)	
	Registres des activités de traitement (Article 30)	
Maintenir	Notification à l'autorité de contrôle d'une violation de données à caractère personnel (Article 33)	DatAlert
	Communication à la personne concernée d'une violation de données à caractère personnel (Article 34)	

Pour résumer, le plan de conformité au GDPR se décompose en trois étapes : identifier les actifs à risque, protéger ces actifs en maintenant des droits adéquats et en employant d'autres principes de confidentialité dès la conception, en enfin, surveiller ces actifs pour détecter les menaces.

En réalité, il existe une quatrième étape consistant à revenir à la première étape pour rapporter les informations obtenues au cours de la phase de détection/surveillance. Autrement dit, vous affinez les trois premières étapes en fonction de ce que vous avez appris en surveillant les menaces et autres vulnérabilités.

La stratégie de sécurité des données de Varonis est centrée sur les données elles-mêmes. Grâce à nos produits, en particulier à DatAdvantage, DataPrivilege, DatAlert et à notre Data Classification Engine, nous sommes en mesure de protéger et éliminer ou réduire le risque de vol à une partie du système informatique où il est le plus pertinent de cibler les efforts de sécurité – pas au niveau du périmètre, qui peut être franchi, mais des données elles-mêmes.

Passons maintenant le plan en revue.

Identification de base

Pour comprendre les vulnérabilités et risques potentiels auxquels vous êtes exposé, il est judicieux de procéder à un inventaire de votre système pour y rechercher les actifs et risques spécifiques. Pour Varonis, les utilisateurs, groupes et dossiers sont les composants de base utilisés dans tous nos rapports portant sur les risques.

Pour être en conformité avec le GDPR, vous ne manquerez pas d'examiner les informations sur les comptes et actifs du système de fichiers de base. Les rapports suivants générés par DatAdvantage peuvent être d'une aide précieuse.

Le rapport 4g de DatAdvantage de Varonis permet au personnel de sécurité de découvrir rapidement les dossiers contenant des données sensibles concernées par le GDPR, souvent disséminés sur les systèmes de fichiers de l'entreprise. C'est un moyen très efficace de commencer à réduire les risques.

En arrière-plan, le Moteur de classification des données de Varonis (Data Classification Engine), a déjà analysé les fichiers au moyen de filtres spéciaux capables d'identifier les schémas de données personnelles (numéro de téléphone, numéro de compte) et de noter les fichiers en fonction du nombre d'occurrences.

Classification Results (Selected Rules)	Hit Count	Risk%	Files with Hits	Scan Priority
GDPR UK (258/258), **GDPR Belgium** (120/120), **GDPR Poland** (120/120), **American Express** (122/122), **DE Personal Data Protection** (120/120), **MasterCard** (175/175), **PCI Data Security Standards** (PCI-DSS) (743/743), **DE Landline Phone Numbers** (120/120), **Visa** (322/322)	2100	5.69	6	252
GDPR UK (134/134), **GDPR Belgium** (100/100), **GDPR Poland** (100/100), **American Express** (102/102), **DE Personal Data Protection** (100/100), **MasterCard** (102/102), **PCI Data Security Standards** (PCI-DSS) (446/446), **DE Landline Phone Numbers** (100/100), **Visa** (322/322)	1394	3.77	2	254

▲ *Le rapport 4g de DatAdvantage montre les résultats de la classification des données*

Pour aider à identifier les données personnelles visées par le GDPR, Varonis propose des GDPR Patterns. Ceux-ci permettent de découvrir les données à caractère personnel auxquelles s'applique le GDPR : des numéros d'identification nationaux à l'IBAN jusqu'au groupe sanguin et aux informations de carte de crédit. Ainsi, vous serez en mesure de produire des rapports sur les données personnelles concernées par le GDPR : droits, accès ouverts, dernier accès ou degré « d'obsolescence ».

Quelles données GDPR ne sont plus nécessaires ?

Au niveau des dossiers, le rapport 4f indique les chemins d'accès, la taille, le nombre de sous-dossiers et le chemin de partage. En définissant un critère d'heure de dernier accès, il est aussi possible de produire une liste de dossiers rarement utilisés – « données obsolètes ». Comme nous le verrons dans la prochaine section, ces informations aident à limiter les risques auxquels les données sont exposées.

Où les données concernées par le GDPR sont-elles surexposées ?

Le rapport 4b est lui aussi très utile. Il montre les droits d'un répertoire donné, les décomposant éventuellement en groupes au niveau des LCA. Il fournit également des recommandations concernant les droits d'adhésion aux groupes. Si vous devez inspecter et ajuster rapidement les contrôles d'accès d'un ensemble de données critiques connu, le rapport 4b est celui qui est le plus utile.

Les rapports précédents apportent des informations d'identification essentielles qui peuvent alors servir à corriger les problèmes au cours de la phase Protéger. Pour rappel, le GDPR préconise d'adopter des pratiques de sécurité informatique courantes -- « mettre en œuvre les mesures techniques et organisationnelles appropriées ». Des rapports DatAdvantage sur les données sensibles largement exposées, sur des listes des véritables adhésions aux groupes et sur les comptes utilisateur et données obsolètes aideront le service informatique à mettre en œuvre ces mesures.

Identification et risque

Si les rapports de base constituent un bon point de départ, le personnel de sécurité informatique n'en devra pas moins explorer le système de fichiers plus en profondeur pour identifier les données sensibles ou critiques pouvant présenter un risque.

Généralement, il cherche des informations personnellement identifiables (PII) ou des données à caractère personnel, comme on les désigne dans le GDPR, telles que des adresses e-mail, numéros de téléphone, numéros de permis de conduire et numéros d'identification nationale.

Comme les fuites de données de grande ampleur des dernières années nous l'ont enseigné, ce sont les dossiers mal protégés — dossiers ou répertoires dotés de droits excessifs — qui sont visés par les hackers. Une fois qu'ils se sont infiltrés, les hackers n'ont plus qu'à utiliser les droits d'accès du compte dont ils ont pris le contrôle.

Pour aller au-delà des informations fournies par le rapport 4g, le rapport 4a de DatAdvantage est la source d'informations incontournable pour trouver les données concernées par le GDPR exposées à tous dans des fichiers spécifiques.

Access Path	User/Group	Current Permissions	Total Hit Count (Inc. subfolders)	Classification Results
rojects11.txt (1)	Abstract\ Everyone	FMRWX	10	**GDPR UK** (2/2), **MasterCard** (2/2), **DE Personal Data Protection** (5/5), **Visa** (1/1)
C:\share\84\ProjectData.txt (1)	Abstract\ Everyone	FMRWX	113	**GDPR Belgium** (16/16), **GDPR Poland** (16/16), **DE Personal Data Protection** (17/17), **Mastercard** (5/5), **PCI Data Security Standards (PCI-DSS)** (16/16), **DE Landine Phone Numbers** (16/16), **Visa** (11/11)

▲ *Figure 3 Le rapport DatAdvantage 4a montre les fichiers contenant des données sensibles qui disposent d'un accès global.*

Il est très risqué pour une organisation de conserver des données à caractère personnel visées par le GDPR dans des fichiers accessibles à tous. Le rapport 4a de DatAdvantage vous montre ces fichiers. Vous pouvez aussi configurer le rapport 4a de manière à afficher uniquement les dossiers à accès global qui contiennent des données GDPR à caractère personnel.

Vous pouvez l'utiliser à la place du rapport 4g (mentionné plus haut) pour disposer d'une vue d'ensemble initiale plus ciblée de votre environnement. Par ailleurs, lorsque vous connaîtrez mieux les filtres des rapports DataAdvantage, vous déterminerez probablement votre propre approche en fonction du programme de sécurité GDPR de votre organisation.

Nous avons identifié les dossiers qui présentent un risque pour la sécurité de nos données.

Que devons-nous identifier d'autre ?

Les utilisateurs qui ont accès à ce dossier sont un bon point de départ.

Il y a plusieurs façons de procéder avec DatAdvantage, mais contentez-vous d'utiliser les données brutes du journal d'audit d'accès de chaque événement de fichier d'un serveur, fourni par le rapport 2a. En ajoutant un filtre de chemin de répertoire, vous pouvez limiter les résultats à un dossier spécifique.

Date	User Name	File Server	Access Path	Event Type	Event Count
					46806
7/6/2015	corp.local\Alice Tanner	Corpfs02b	C:\Share\legal\Corporate\Finance	All event types	9
7/10/2015	corp.local\Alice Tanner	Corpfs02b	C:\Share\legal\Corporate\Finance	All event types	35
7/2/2015	corp.local\Alice Tanner	Corpfs02b	C:\Share\legal\Corporate\Finance	All event types	20
7/10/2015	corp.local\Alice Tanner	Corpfs02b	C:\Share\legal\Corporate\Distrobution Agreements\ DISTRIB (TEXIM EUROPE) V1 REVI.txt	All event types	1
1/7/2016	corp.local\Alice Tanner	Corpfs02b	C:\Share\legal\Corporate\CLA USES	File opened	1

▲ *Figure 4 Le rapport DatAdvantage 2a montre les dossiers qui contiennent les données à caractère personnel concernées par le GDPR.*

Les comptes utilisateur obsolètes constituent une autre source de risque négligée. Bien souvent, les comptes utilisateur ne sont pas désactivés ou supprimés lorsqu'un employé quitte l'entreprise ou lorsque la mission temporaire d'un contractuel est terminée.

Il n'est pas rare que d'anciens utilisateurs internes, les fameux employés mécontents, continuent d'accéder à leur compte même après avoir quitté l'entreprise. Ou que des hackers accèdent au compte inutilisé d'un ancien contractuel pour ensuite gagner accès à leur cible réelle. Au cours de la phase Protéger, nous découvrirons comment Varonis vous permet de désactiver rapidement ces comptes.

Pour être complet, un programme d'évaluation des risques devrait également identifier les menaces externes—nouveaux malwares et nouvelles techniques de piratage. Cette fonction est différente de l'identification des données. Grâce à ces nouveaux renseignements pratiques sur les menaces, vous réajustez les niveaux de risque que vous avez définis initialement et vous revoyez votre stratégie. Vous le faites de manière continue puisque le jeu du chat et de la souris avec les hackers ne s'arrête jamais.

Prévenir

La seconde phase de la méthodologie GDPR implique de restructurer les droits, de verrouiller ou réduire les données à caractère personnel surexposées et d'identifier les propriétaires de données pour faire en sorte de mettre en place des contrôles préventifs adaptés. Ceci élimine les domaines à haut risque, réduit la surface d'attaque potentielle, simplifie l'environnement et commence à impliquer les parties prenantes au-delà de l'équipe de sécurité informatique.

Au cours de cette phase, vous appliquerez aussi un principe clé du GDPR, la minimisation : à partir des informations sur les fichiers et les comptes, vous chercherez des moyens de limiter les personnes autorisées à accéder aux données à caractère personnel et de réduire les données sensibles.

Voyons comment y parvenir au cours de la phase Prévenir.

Dans ce domaine, l'un des principaux contrôles consiste à restreindre l'accès uniquement aux utilisateurs autorisés. Plus facile à dire qu'à faire, mais vous avez déjà préparé le terrain.

Les principes directeurs à appliquer sont des contrôles d'accès basés sur le moindre privilège et sur les rôles. En bref : accorder aux utilisateurs concernés uniquement les accès dont ils ont besoin pour faire leur travail et remplir leur mission.

Puisque nous nous apprêtons à rentrer dans le vif du sujet et à agir, nous devons passer de la section Rapports à la partie Vérification de DatAdvantage.

DataAdvantage fournit un support graphique pour vous aider à identifier les propriétaires de données.

Si vous voulez obtenir plus de précisions et ne pas savoir simplement qui accède à un dossier, vous pouvez consulter les statistiques d'accès réelles des principaux utilisateurs dans l'onglet Statistiques de DatAdvantage.

Ces informations sont très utiles pour savoir qui utilise réellement les dossiers. Le but final est de trouver les véritables utilisateurs et de retirer les groupes et utilisateurs superflus, qui ont peut-être eu besoin d'un accès occasionnel, mais pas dans le cadre du travail habituel associé à leur poste.

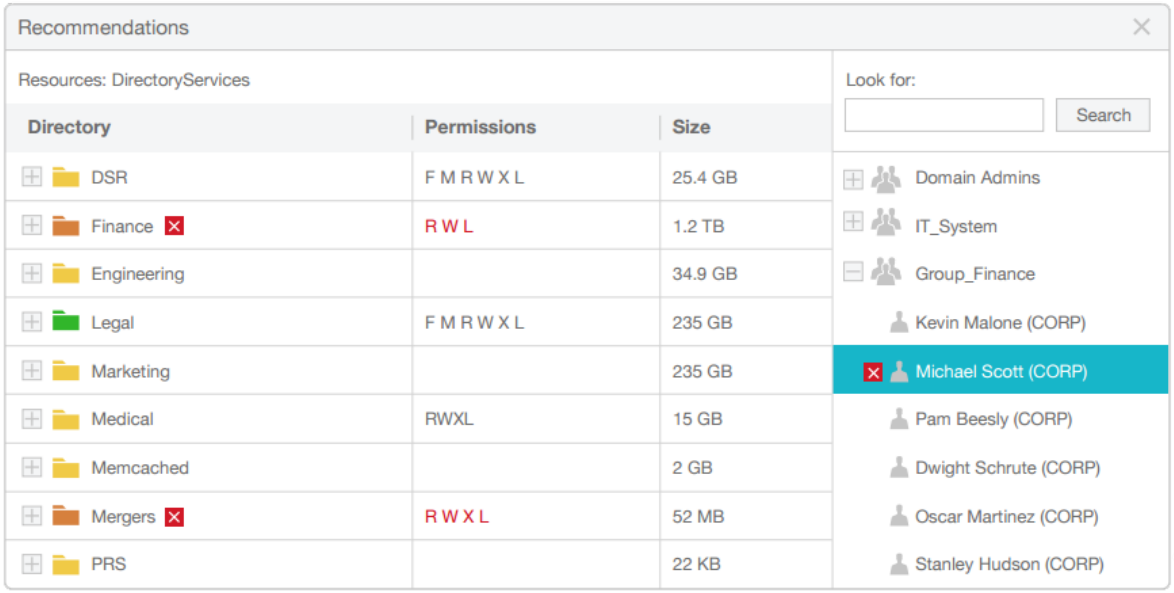
L'important est de commencer par déterminer qui est le propriétaire du dossier — la personne qui sait vraiment ce que contient le dossier et qui est le mieux à même à prendre les décisions le concernant. Pour cela, il est possible que l'équipe informatique soit amenée à échanger avec les utilisateurs, en s'appuyant sur des statistiques DatAdvantage, afin de comprendre la véritable chaîne de commande.

Une fois que vous utilisez DatAdvantage pour définir les propriétaires des dossiers, ces utilisateurs avancés peuvent gérer de manière indépendante qui a besoin de disposer d'un accès, et à qui il convient de le retirer. Le propriétaire du dossier recevra aussi automatiquement les rapports DatAdvantage qui l'aideront à opérer ses choix futurs au niveau de l'attribution des accès.

Abordons un point important avant de poursuivre. Depuis longtemps, le service informatique est responsable de la fourniture des accès, sans qu'il ne connaisse leur utilité métier. Varonis DatAdvantage aide l'équipe informatique à trouver les propriétaires, puis leur prête main-forte pour minimiser ou réduire les accès et gérer de manière formelle l'attribution des droits d'accès.

DatAdvantage aide aussi les propriétaires de données en leur fournissant son moteur de recommandations automatisé. Les propriétaires trouvent souvent ces recommandations utiles car elles les aident à identifier les utilisateurs qui ont changé de poste, n'ont plus besoin d'un accès, etc. Le rapport 4b de la section précédente est utile à ce stade puisqu'il fournit des recommandations en matière de LCA.

L'onglet Domaine de travail de DatAdvantage fournit aussi directement ce type d'informations.



▲ *Le rapport 4g de DatAdvantage montre les résultats de la classification des données*

Quoi qu'il en soit, une fois que le propriétaire de données a terminé de limiter et supprimer les utilisateurs et groupes inutiles, il veut mettre en place un processus de gestion des droits.

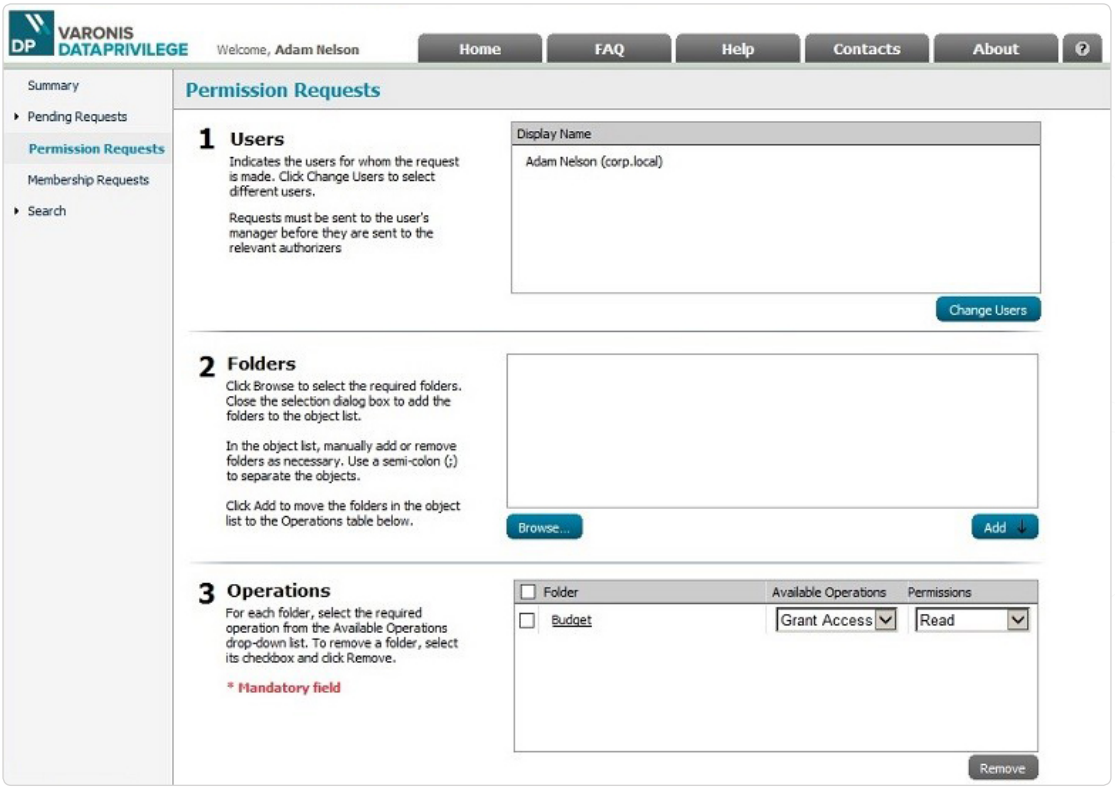
Les normes et lois de données, telles que le GDPR, reconnaissent l'importance de disposer de politiques et procédures de sécurité dans le cadre d'un programme permanent, c'est-à-dire une opération que le propriétaire ne fait pas une seule fois par an.

Ici aussi Varonis a un rôle important à jouer.

Maintenir un modèle de moindre privilège

Comment les utilisateurs ordinaires, dont le rôle évolue et exige à présent qu'ils accèdent à un dossier géré, demandent-ils au propriétaire de pouvoir y accéder ?

C'est là que Varonis DataPrivilege entre en scène. Les utilisateurs normaux interagiront avec DataPrivilege pour demander à accéder à un dossier géré, puis DataPrivilege gèrera le processus de workflow.



Le propriétaire du dossier possède une interface parallèle depuis laquelle il peut recevoir ces demandes puis accorder ou révoquer les droits. Ici, l'objectif est d'automatiser le workflow pour pouvoir limiter les droits d'accès aux personnes qui en ont vraiment besoin.

Une autre façon de maintenir un moindre privilège est de désactiver les comptes obsolètes ou inactifs. Ils peuvent présenter un risque. DatAdvantage vous permet de désactiver directement ces comptes via son interface en ligne, vous évitant ainsi d'avoir à passer par un service d'annuaire tel qu'Active Directory !

Minimiser les données sensibles

La minimisation est un thème important des normes et lois de sécurité. Elle est le mieux illustrée par les principes du Respect de la vie privée dès la conception (PbD) qui apporte un conseil de sécurité général pertinent : minimisez les données sensibles collectées, minimisez les personnes qui y accèdent et minimisez leur durée de conservation.

Dans le cas du GDPR, ces idées sont directement mentionnées dans la section « Protection des données dès la conception et par défaut » (Article 25).

Nous avons déjà vu comment DatAdvantage peut aider à restreindre les personnes qui accèdent aux données. Un autre principe de PbD consiste à réduire les risques en supprimant ou en archivant les données sensibles inutiles ou obsolètes contenues dans les fichiers.

C'est extrêmement judicieux, bien entendu. Les données personnelles obsolètes concernées par le GDPR peuvent, par exemple, être des données d'identification collectées dans le cadre de campagnes marketing à court terme mais figurant à présent dans des feuilles de calcul ou des présentations de gestion rarement utilisées.

Il est possible que votre organisation n'en ait plus besoin, mais c'est justement le type de données monétisables sur lesquelles les hackers adorent mettre la main.

DatAdvantage peut trouver et identifier les données de fichiers qui n'ont pas été utilisées après une certaine date. Le rapport 4f de DatAdvantage (mentionné dans la section précédente) peut-il être adapté de manière à trouver les données obsolètes qui se trouvent aussi être visées par le GDPR ?

Oui.

Vous devez ajouter le filtre « nombre d'accès » et définir de manière adéquate le nombre de correspondances de données sensibles souhaité.

L'étape suivante consiste à utiliser le Data Transport Engine (DTE) proposé dans DatAdvantage (menu Outils). Le DTE permet de créer une règle qui cherchera les fichiers à archiver et à supprimer si nécessaire.

Les critères de recherche de la règle reprennent les filtres utilisés dans la section précédente pour générer les rapports sur les données sensibles. La règle fait le gros du travail pour détecter et supprimer les données sensibles obsolètes.

Étant donné que la règle peut aussi être enregistrée, elle peut être exécutée de nouveau pour faire appliquer les limites de conservation. Mieux encore, DTE peut exécuter la règle automatiquement à intervalles réguliers afin que vous n'ayez pas à vous inquiéter des données à caractère personnel GDPR présentes dans votre système de fichiers.

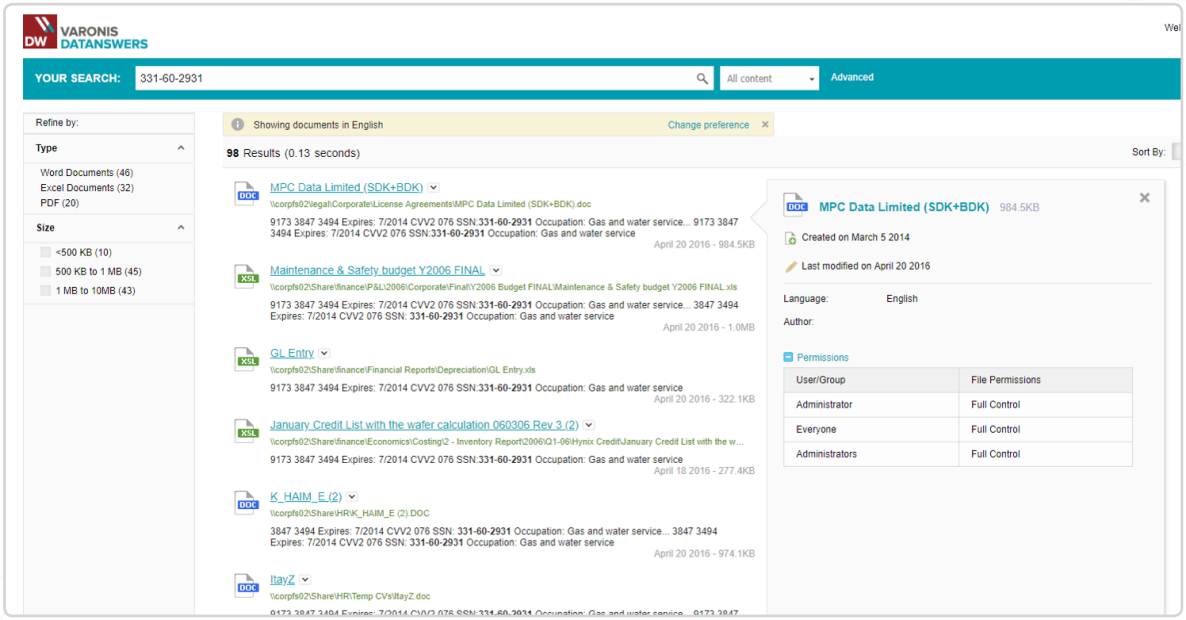
Droit à l'oubli

Varonis peut également aider à satisfaire une autre exigence du GDPR, le « droit à l'effacement ou droit à l'oubli » (Article 17).

Selon le GDPR, les consommateurs ont le droit de demander que les données à caractère personnel qui les concernent soient supprimées. Cette exigence s'applique non seulement à la suppression des données personnelles des bases de données structurées, mais aussi à celles qui figurent dans les systèmes de fichiers.

Bien qu'il soit possible d'ajouter de nouvelles règles de classification pour trouver un client *spécifique* — en utilisant par exemple un critère de recherche de nom ou de numéro de compte— et de demander ainsi la suppression, Varonis DatAnswers offre un moyen plus simple de faire appliquer le droit à l'effacement. DatAnswer est notre moteur de recherche intelligent qui sert à analyser les fichiers.

De la même façon que vous saisissez des mots clés dans Google, vous pouvez utiliser DatAnswers pour trouver les fichiers où sont conservées les données personnelles d'un client demandant qu'elles soient effacées. Ensuite, vous pouvez mettre en quarantaine le fichier et ajuster ses données.



Surveiller

Aucune stratégie de sécurité des données n'est infaillible. Par conséquent, vous devez mettre en place une défense secondaire basée sur des contrôles de détection et de surveillance : dans la pratique, vous examinez le système et vous recherchez toute activité inhabituelle trahissant un piratage.

Varonis DatAlert a un rôle unique à jouer dans la détection des violations car sa plate-forme de sécurité sous-jacente s'appuie sur la surveillance des activités du système de fichiers.

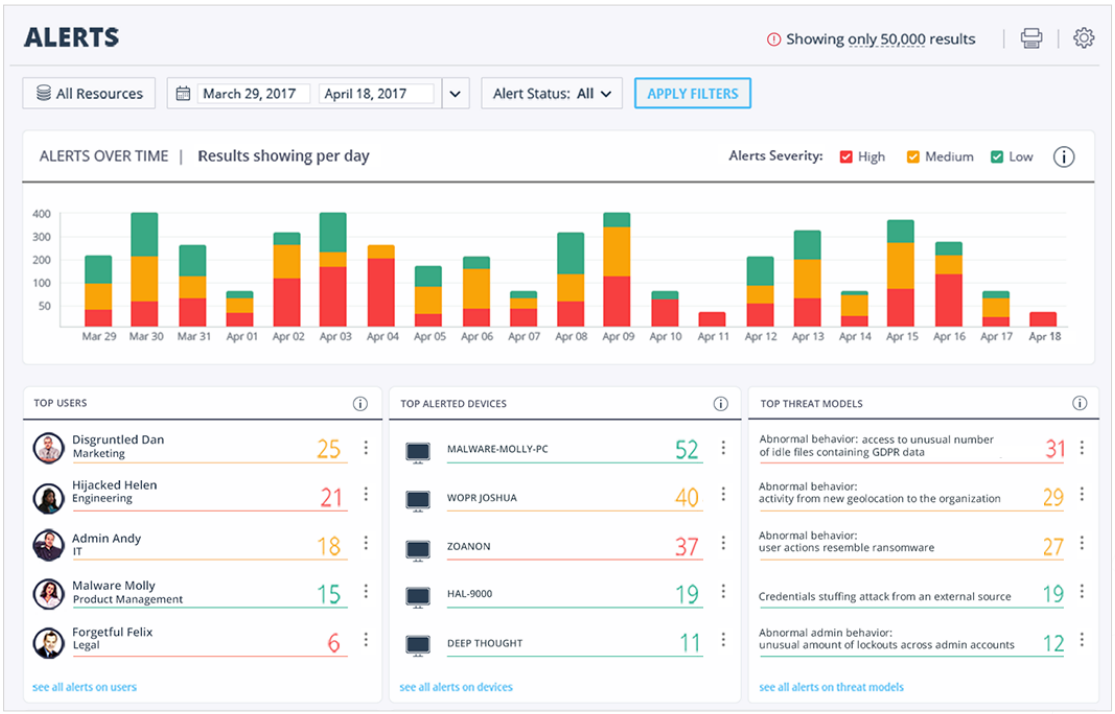
À ce stade, chacun sait (ou devrait savoir) que les attaques de phishing et par injection permettent aux hackers de contourner les défenses du réseau puisqu'elles empruntent les données d'identification des utilisateurs. De plus, des malwares parfaitement indétectables parviennent à agir totalement à l'insu des antivirus.

Comment faire pour détecter cette nouvelle génération de piratages furtifs ?

Aucun hacker ne peut se passer d'utiliser le système de fichiers pour charger son logiciel, copier des fichiers et explorer une hiérarchie de dossiers pour rechercher des données confidentielles à exfiltrer. Si vous identifiez les schémas d'activité uniques aux hackers au niveau des fichiers, vous pouvez les arrêter avant qu'ils ne suppriment ou n'exfiltrent les données, ou au moins, limiter l'exposition des données.

Nous ne pouvons pas détailler toutes les capacités de l'outil DatAlert, mais puisqu'il possède une vision approfondie des informations et événements du système de fichiers, et des historiques de comportement des utilisateurs, il est particulièrement bien positionné pour déterminer ce qui ne cadre pas avec les activités normales d'un compte utilisateur.

C'est ce que nous appelons l'Analyse du comportement des utilisateurs (UBA), et DatAlert est fourni avec une suite de modèles de menaces UBA. Libre à vous d'ajouter vos propres modèles, mais les modèles prédéfinis sont déjà fort efficaces. Ils incluent la détection dees intrusions de type Cryptolocker, des accès inhabituels des utilisateurs aux données sensibles, des accès inhabituels aux fichiers contenant des données d'identification, etc...



Toutes les alertes qui sont déclenchées peuvent faire l'objet d'un suivi depuis le tableau de bord DatAlert. Le personnel informatique peut soit intervenir et répondre manuellement, soit paramétrer des scripts qui s'exécuteront automatiquement — par exemple, pour désactiver automatiquement les comptes.

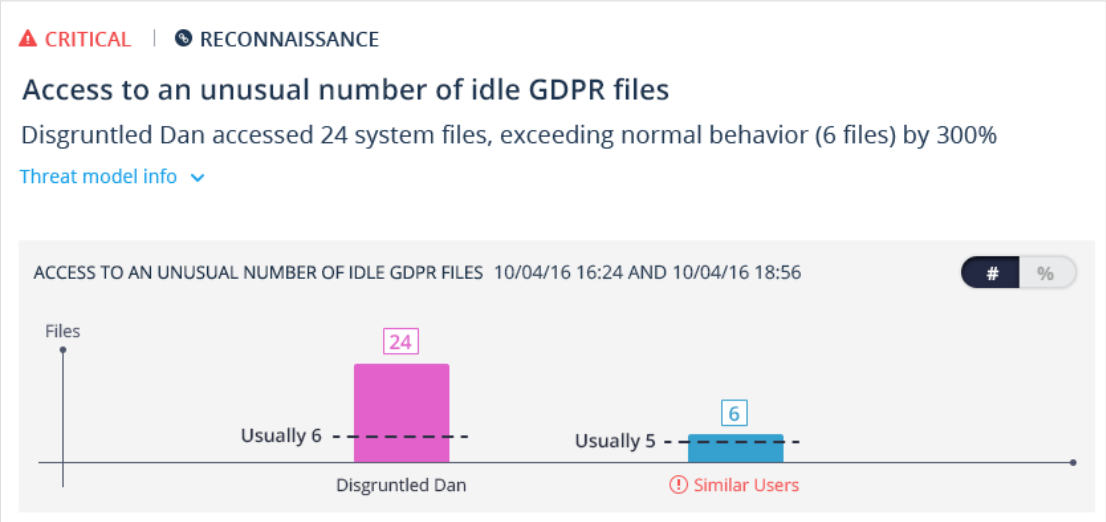
Pour ce qui est de la notification des fuites, le GDPR (Articles 33, 34) exige d'avertir le responsable du traitement de la nature de la violation, des catégories de données et du nombre d'enregistrements exposés ainsi que des mesures prises pour remédier au vol de données.

DatAlert peut fournir toutes ces informations et corriger la violation en lançant des scripts automatisés.

Voici quelques exemples de modèles de menaces pouvant être détectés et corrigés :

Modèle de menace	Description
Comportement anormal : **accès à un nombre inhabituel de fichiers GDPR inactifs**	Une augmentation statistique importante a été détectée au niveau du nombre de fichiers inactifs concernés par le GDPR ouverts par l'utilisateur, par rapport à son profil comportemental. Les fichiers inactifs sont des fichiers que l'utilisateur n'a ni créés ni modifiés dans le cadre de son accès, et auxquels il n'a pas accédé pendant une longue période avant cette alerte (bien que d'autres utilisateurs aient pu y accéder récemment). Ceci peut indiquer qu'un hacker recherche des données sensibles auxquelles il a accès pour les exfiltrer.
Comportement anormal : **nombre inhabituel de fichiers GDPR avec accès refusé**	Une augmentation statistique importante a été détectée dans le nombre de fichiers GDPR auxquels un utilisateur n'a pas pu accéder. Ceci peut indiquer qu'un hacker recherche différents ensembles de données pour tenter d'y accéder en vue d'exfiltrer des données.
Comportement anormal : **nombre inhabituel de fichiers GDPR supprimés ou modifiés**	Une augmentation statistique importante a été détectée dans des fichiers GDPR supprimés ou modifiés par l'utilisateur, par rapport à son profil comportemental. Ceci peut indiquer qu'un hacker tente d'endommager ou de détruire des données critiques dans le cadre d'une attaque par déni de service.
Comportement de service anormal : **accès à des dossiers inhabituels contenant des données concernées par le GDPR**	Un compte de service a accédé à des dossiers contenant des données GDPR auxquels il n'avait pas accédé auparavant. Généralement, les comptes de service effectuent toujours les mêmes actions ; par conséquent, tout changement de comportement est suspect. Des hackers peuvent se faire passer pour un compte de service et exploiter ses droits.

Pour aider à respecter le délai de 72 heures fixé par le GDPR pour fournir les informations aux autorités, DatAlert vous permet d'affiner les comportements des menaces afin de cibler uniquement les données à caractère personnel concernées par le GDPR. Autrement dit, vous pouvez recevoir des alertes concernant, par exemple, les accès inhabituels aux fichiers d'un dossier contenant des numéros de téléphone ou numéros nationaux d'identification.



▲ *Figure 9 - DatAlert peut être configuré pour se déclencher en cas de menaces visant les données à caractère personnel concernées par le GDPR.*

Autres considérations

Il est important de garder à l'esprit le fait que le GDPR n'est pas une norme de sécurité. Il fournit des directives – appliquées bien entendu par les régulateurs européens – pour aider à assurer la protection des données à caractère personnel.

Le GDPR vous demande de « mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » – voir Sécurité du traitement (Article 32). Le GDPR indique également que vous avez besoin « d'une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles ».

Par conséquent, la sécurité des données est une activité à mener en continu. Nous avons montré dans ce livre blanc comment le logiciel Varonis peut vous aider à mettre en place un programme de sécurité des données concernées par le GDPR. Nous n'avons pas abordé toutes les capacités Varonis. Si vous souhaitez obtenir des informations plus détaillées, vous pouvez consulter notre Plan opérationnel Varonis. Demandez-en une copie à nos commerciaux.

De nombreuses grandes organisations se sont probablement appuyées sur les normes de sécurité des données en vigueur, telles que PCI DSS ou ISO 27001, et ont déjà mis en œuvre un grand nombre des contrôles de sécurité préconisés par ces normes.

Si c'est votre cas, vous devrez faire en sorte que ces contrôles ciblent plus précisément la protection des données à caractère personnel concernées par le GDPR.

Grâce à son « code de conduite » approuvé (Article 40), le GDPR offre un moyen d'obtenir un « agrément » en cas de conformité aux normes en vigueur.

L'Article 40 dit que les associations de normalisation peuvent soumettre leurs contrôles de sécurité, par exemple PCI DSS, au comité européen de la protection des données (EDPB) pour approbation. Si une entreprise applique un « code de conduite » approuvé officiellement, cela peut dissuader les régulateurs d'intenter une action, comme d'infliger une amende, tant que l'organisme de normalisation — par exemple le PCI Security Standards Council — possède son propre mécanisme de surveillance pour vérifier la conformité au règlement.

Le GDPR va toutefois un peu plus loin. Il laisse la possibilité de certifier officiellement les opérations de données d'une entreprise, ou comme le désigne le GDPR, d'un responsable du traitement.

En pratique, les régulateurs ont le pouvoir (selon l'article 40) de certifier que les activités d'un responsable du traitement sont conformes au GDPR. Les régulateurs européens peuvent également homologuer d'autres organismes de normalisation, telles que PCI ou ISO, pour les autoriser à émettre directement ces certifications.

Délivrées pour trois ans, ces certifications devront être renouvelées passé ce délai.

Ces certifications sont totalement facultatives mais elles présentent des avantages indéniables pour de nombreuses entreprises. Le but est de tirer parti des normes de données déjà en place dans le secteur privé et de fournir aux entreprises une approche plus pratique de la conformité selon le GDPR, basée sur des exigences techniques et administratives.

L'EDPB devrait également proposer des logos et sceaux de certification pour mieux informer les consommateurs, ainsi qu'un registre des entreprises certifiées.

Nous devrons attendre de disposer d'informations complémentaires de la part des régulateurs concernant la certification du GDPR.

« Varonis est une solution fantastique »

Gartner peerinsights™

Bénéficiez d'une évaluation de l'état de préparation au GDPR

Évaluation des risques des données

Déterminez votre profil de risque, découvrez vos vulnérabilités et corrigez vos problèmes de sécurité réels.

varonis.com/gdpr-ra-fr

Démo en direct

Installez Varonis dans votre propre environnement et découvrez comment stopper le ransomware et protéger vos données.

info.varonis.com/trial-fr