Data Control

Monitor sensitive data across endpoints

Sécurité, visibilité et contrôle en temps réel des données personnelles. Simplifier la mise en conformité au RGPD.

Mai 2018 a vu l'entrée en vigueur du Règlement général européen sur la protection des données (RGPD). Ce nouveau règlement, destiné à améliorer la protection et le traitement des données, oblige toutes les organisations sans exception à **renforcer la sécurité des données à caractère personnel (DCP)** qu'elles conservent et/ou traitent, en particulier les données détenues, utilisées ou transmises sur les appareils des employés et des collaborateurs.

POURQUOI DEVEZ-VOUS PROTÉGER LES DONNÉES PERSONNELLES ET SENSIBLES DE VOTRE ORGANISATION ?

Depuis mai 2018, les entreprises qui ne se conformeraient pas aux exigences du RGPD peuvent s'exposer à de lourdes amendes pouvant atteindre 20 millions d'euros ou 4 pour cent du chiffre d'affaires annuel de l'entreprise en cas d'infraction.

Le RGPD concerne toutes les entreprises, tous les secteurs professionnels et toutes les zones géographiques, y compris celles situées en dehors de l'UE, qui collectent et stockent des données personnelles de citoyens européens.

La conformité aux dispositions du RGPD permet également aux entreprises d' éviter toute altération de leur réputation engendrée par une éventuelle fuite de données, avec ses effets négatifs sur la confiance des employés et celle des clients actuels ou potentiels.

Elles doivent notamment être en mesure de :

- **Réduire la prolifération incontrôlée de données non structurées.** Les données non structurées conservées sur des serveurs, des terminaux ou des ordinateurs portables d'employés ou de collaborateurs (partenaires, consultants, etc.) constituent environ 80 pour cent des données professionnelles d'une entreprise. Le volume de données non structurées doublant chaque année, le risque qu'elles font courir aux entreprises augmente également[1].

- **Lutter contre l'augmentation exponentielle du nombre de cas d'exfiltration.** Le nombre de cas où des données mal gérées ou mal sécurisées sont exfiltrées d'un système informatique augmente chaque jour. Et il arrive parfois que l'entreprise qui en est victime ne le sache même pas. Ces vols de données sont généralement le résultat d'attaques venues de l'extérieur ou d'actions de la part d'un personnel interne négligent ou bien motivé par des buts malveillants pécuniers ou encore de vengeance.

LA SOLUTION : PANDA DATA CONTROL

Data Control est un module de sécurité des données entièrement intégré à la plate-forme Panda Adaptive Defense. Il est conçu pour aider les organisations à se conformer aux règlements sur la protection des données, ainsi qu'à identifier et protéger les données personnelles et sensibles aussi bien en temps réel que tout au long de leur cycle de vie sur les postes clients et les serveurs.

Panda Data Control identifie, audite et surveille toutes les **données personnelles non structurées[2]** présentes sur les postes clients : Cela comprend aussi bien les données statiques que celles en circulation ou en exploitation.

Figure 1 – Vue générale des fichiers contenant des données personnelles et des utilisateurs y ayant accédé.

PRINCIPAUX AVANTAGES

Identifier et auditer

Identifier les fichiers de données personnelles (DCP) ainsi que les utilisateurs, employés, collaborateurs, postes clients et serveurs au sein de votre entreprise qui accèdent à ces données.

Surveiller et détecter

Mettre en place des mesures préventives pour empêcher l'accès aux données personnelles (DCP), à l'aide de rapports et d'alertes en temps réel sur toute utilisation, transmission ou exfiltration suspecte et non autorisée de fichiers contenant des données personnelles.

Simplifier la gestion

Le module Panda Data Control est un module natif de Panda Adaptive Defense et Panda Adaptive Defense 360. Il ne nécessite pas de la part des entreprises le déploiement d'une protection autre que la protection standard, et peut être activé facilement et immédiatement sans configurations complexes. Une fois activé, ce module se gère à partir de la plate-forme cloud dédiée.

Démontrer sa conformité avec les règlements applicables à l'équipe de direction, au DPO[3] et à tous les autres employés de votre organisation. Présenter les mesures strictes de sécurité en place pour protéger les données personnelles statiques, exploitées ou en circulation entre les postes.

SÉCURITÉ ET GOUVERNANCE DES DONNÉES PERSONNELLES (DCP)

Les organisations protégées par **Panda Adaptive Defense** peuvent être assurées que leurs postes clients et leurs serveurs ne seront pas compromis par des programmes malveillants en provenance de sources extérieures, et qu'elles ne seront donc pas victimes de tentatives d'exfiltration de données.

Panda Adaptive Defense **classifie la totalité des applications et processus** qui s'exécutent sur les postes clients et les serveurs protégés, en donnant un verdict sur leur fiabilité ou leur nature malveillante à l'aide de techniques **d'apprentissage machine** supervisées par les experts en cybermenaces de Panda Security. Ce système assure que **seules les applications classifiées comme légitimes** seront autorisées à s'exécuter.

Le **module Data Control** exploite les capacités EDR (Endpoint Detection and Response) de la solution afin de surveiller en continu les postes clients protégés dans l'organisation, en identifiant et en protégeant les données personnelles non structurées détenues et transmises sur le réseau.

Enfin, les **alertes et rapports** de Data Control peuvent être personnalisés et adaptés aux besoins propres à chaque entreprise.

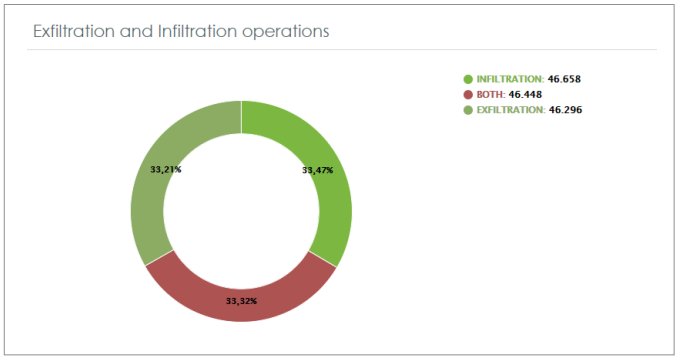


Figure 2 - Opérations sur des fichiers présentant des risques d'exfiltration et d'infiltration : Les graphiques vous permettent de surveiller et d'évaluer le risque des opérations effectuées par des utilisateurs et des machines sur des fichiers de données personnelles afin d'empêcher et de contrôler les exfiltrations de données.

PRINCIPALES FONCTIONNALITÉS

Découverte des données :

Crée un inventaire indexé de tous les fichiers contenant des données personnelles non structurées (données statiques), avec le nombre d'occurrences pour chaque type de données. Classifie automatiquement toutes les informations.

La classification combine plusieurs techniques et algorithmes d'apprentissage machine qui optimisent les résultats tout en réduisant les faux positifs et la consommation de ressources sur les appareils.

Surveillance des données :

Surveille les différents types d'opérations effectuées sur des fichiers non structurés (données exploitées), en gardant l'inventaire des fichiers de données personnelles à jour. Toute tentative de copie ou de déplacement d'un de ces fichiers hors du réseau, aussi bien par e-mail que via un navigateur Web ou un site FTP (données en circulation) est enregistrée par le module.

Visualisation des données :

Les résultats des tâches de découverte et de surveillance des données sont synchronisés en permanence sur la plate-forme Adaptive Defense et dans son module Advanced Visualization Tool. Ce module fournit des outils pour l'exploitation de tous les événements affectant les données statiques, exploitées ou en circulation, aussi bien en temps réel que de manière rétrospective, et ce tout au long de leur cycle de vie sur les terminaux.

Les tableaux de bord et les rapports et alertes prédéfinis de Data Control aident à couvrir les cas d'utilisation et à assurer la gouvernance de la sécurité des données personnelles non structurées détenues sur les appareils protégés de l'organisation.

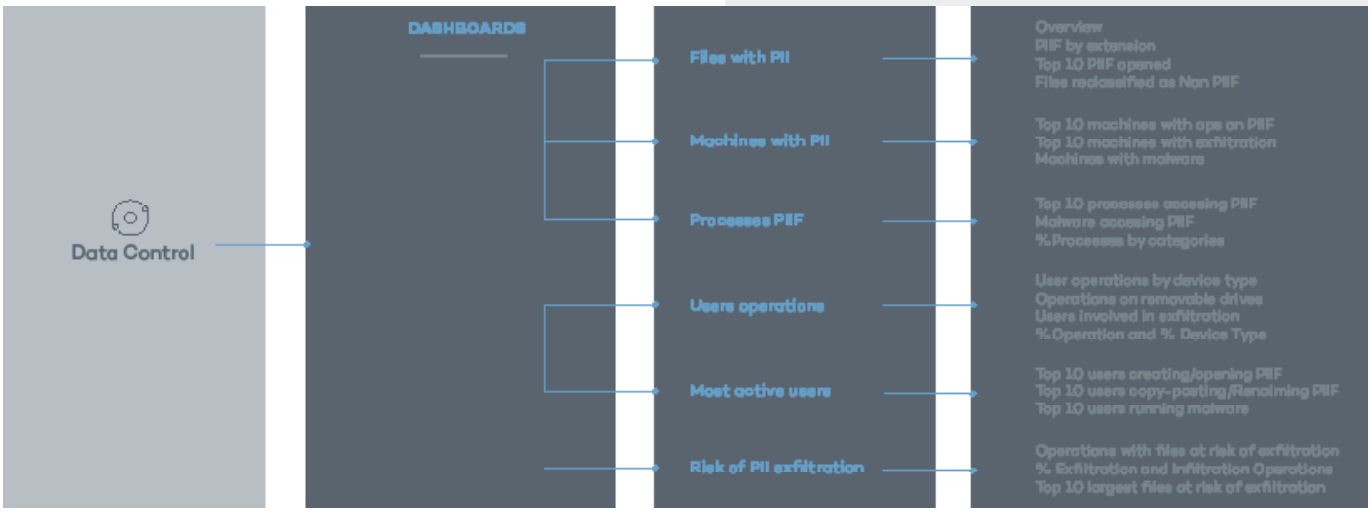


Figure 3 – Panda Data Control – Tableaux de bord, sections, graphiques et requêtes prédéfinies.

COMMENT PANDA DATA CONTROL FACILITE LA CONFORMITÉ RGPD

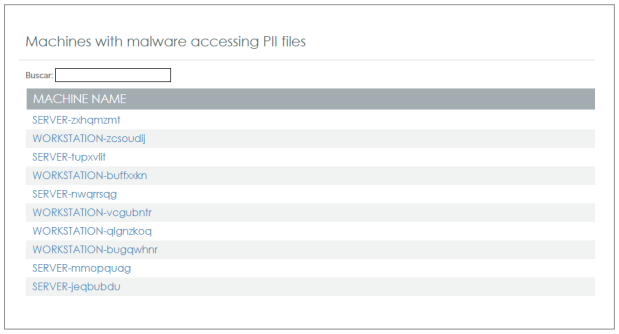
Article RGPD	Fonctionnalité de Panda Data Control
Art. 32: Sécurité du traitement. *«Le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.»*	Panda Data Control fournit aux entreprises des outils pour évaluer, en temps réel et de manière rétrospective, si les fichiers contenant des données personnelles stockés dans leur réseau sont uniquement accessibles par le personnel autorisé ou non et si les stratégies de sécurité en place sont adéquates ou pas. Les rapports disponibles comprennent : • Les machines avec des données personnelles (DCP), les fichiers de données personnelles, les machines effectuant le plus d'opérations sur des fichiers de données personnelles et les processus malveillants accédant à des fichiers de données personnelles, dans le tableau de bord Fichiers et machines avec des données personnelles. • La répartition des types d'opérations sur des données personnelles, les utilisateurs impliqués dans des opérations sur des données personnelles, et les utilisateurs exécutant des logiciels malveillants, dans le tableau de bord Opérations utilisateur sur des fichiers de données personnelles.
Art. 33: Notification à l'autorité de contrôle d'une violation de données à caractère personnel. *«En cas de violation de données à caractère personnel, le responsable du traitement notifie la violation en question à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Cette notification doit décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés.»*	Panda Data Control offre, en plus de tous les rapports détaillés pour l'article 32, une série d'informations particulièrement focalisées sur les exfiltrations de données personnelles : • Les opérations sur des fichiers avec des risques d'exfiltration et d'infiltration. • Les fichiers les plus gros présentant un risque d'exfiltration. • Les utilisateurs/machines impliqués dans des exfiltrations dans le panneau : Risque d'exfiltration de données personnelles.
Art. 35: Analyse d'impact relative à la protection des données. *«Lorsqu'un type de traitement en particulier est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.»*	Le module Data Control a pour but d'identifier les fichiers contenant des données personnelles, ainsi que de surveiller les actions effectuées sur ces fichiers et les utilisateurs impliqués. Ces informations permettent aux organisations d'identifier le volume, le type et l'utilisation des données personnelles conservées dans leur réseau, afin qu'elles puissent évaluer l'impact et le risque du traitement de ces données. Les tableaux de bord et rapports mentionnés plus haut s'appliquent également à cet article.

TABLEAUX DE BORD DE PANDA DATA CONTROL

Art. 32: Sécurité du traitement.

Tableau de bord **Fichiers et machines avec des données personnelles - Machines avec des logiciels malveillants accédant à des fichiers de données personnelles :**

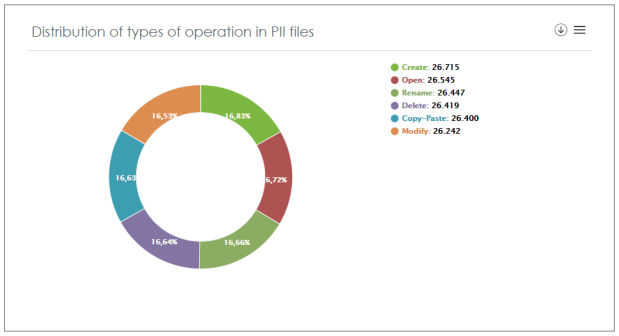
Ce tableau de bord affiche les 10 principaux ordinateurs au sein desquels des processus malveillants accédant à des données personnelles ont été détectés. Ces informations permettent aux administrateurs de sécurité de détecter les infections récurrentes de logiciels malveillants et les menaces persistantes sur certains ordinateurs, et d'évaluer l'impact de ces menaces sur les données personnelles détenues par l'entreprise, comme demandé par le RGPD.



Art. 33: Notification à l'autorité de contrôle d'une violation de données à caractère personnel.

Tableau de bord **Opérations utilisateur sur des fichiers de données personnelles – Répartition des types d'opérations sur des fichiers de données personnelles :**

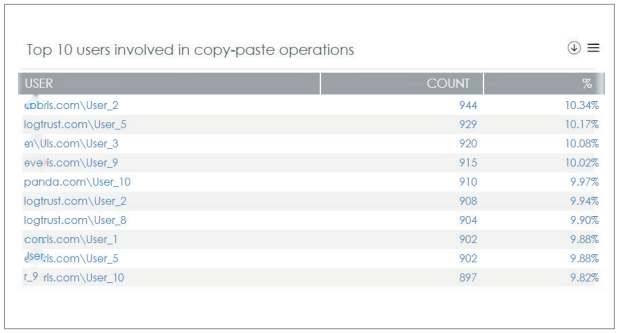
Ce tableau de bord présente les types d'opérations effectuées sur les fichiers de données personnelles et sensibles traités par votre entreprise. Une augmentation ou une diminution significative du nombre de ces opérations peut indiquer un incident ou un événement relatif à la sécurité des données.



Art. 35: Analyse d'impact relative à la protection des données.

Tableau de bord **Opérations utilisateur sur des fichiers de données personnelles – Top 10 des utilisateurs impliqués dans des opérations de copier-coller :**

Ce widget dresse la liste des principaux utilisateurs ayant effectué des opérations de copier-coller sur des fichiers contenant des données personnelles. Data Control surveille également d'autres types d'opérations telles que : l'accès, la création, l'ouverture, le changement de nom, la suppression, etc..

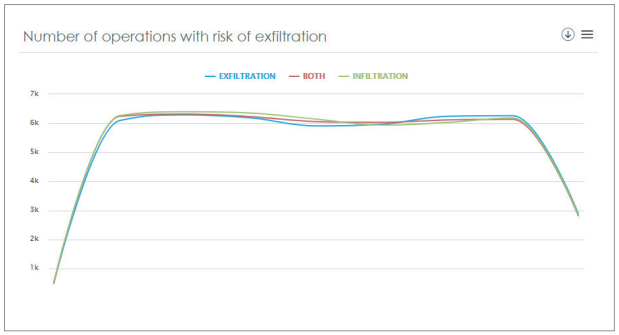


Art. 39: Missions du délégué à la protection des données (DPO).

Tableau de bord **Risque d'exfiltration de données personnelles - Nombre d'opérations sur des fichiers avec un risque d'exfiltration :**

Ce widget aide les entreprises à surveiller les flux de données personnelles en affichant le nombre d'exfiltrations effectuées sur des fichiers du réseau contenant des données sensibles.

Ces informations permettent au DPD de déterminer le nombre habituel d'exfiltrations, et de détecter les écarts engendrés par des incidents de sécurité.



[1] Carla Arend. IDC Opinion - Mars 2017.
[2] Les données non structurées sont des données ne résidant pas dans une base de données ou une autre structure de données. Les données non structurées peuvent être textuelles ou non textuelles. Panda Data Control se concentre sur les données non structurées textuelles détenues sur des postes clients et des serveurs.
[3] DPO/DPD (Data Protection Officer, délégué à la protection des données) : Personne responsable de superviser la stratégie de protection des données dans une organisation.