

WATCHGUARD DATA CONTROL



Surveillez les données sensibles sur l'ensemble de vos postes de travail

SÉCURITÉ, VISIBILITÉ ET CONTRÔLE DES DONNÉES EN TEMPS RÉEL AU SEIN D'UN MÊME PRODUIT

L'accès non contrôlé aux données personnelles et sensibles de votre entreprise est une menace quotidienne pour la sécurité qui peut entraîner de graves pertes financières et nuire gravement à la réputation. Êtes-vous prêt à prendre ce risque ?

PROTÉGER VOS DONNÉES PERSONNELLES ET SENSIBLES

Les unités légales sont obligées de renforcer les mesures existantes ou d'en adopter de nouvelles pour protéger les données personnelles ou sensibles stockées par l'entreprise. Les facteurs les plus importants qui motivent cette transformation sont :

- **Augmentation exponentielle des cas d'exfiltration et des fuites de données.** Les vols de données sont généralement dus à des attaques externes, à des initiés malveillants qui cherchent à gagner de l'argent ou à se venger, ou simplement à la négligence, et les entreprises touchées n'ont souvent même pas conscience de ce qui se passe.
- **La conformité avec la réglementation avec des lois telles que le RGPD, dont la violation peut conduire au paiement d'amendes importantes ou d'un pourcentage du chiffre d'affaires mondial d'une unité légale.**
- **Les données non structurées augmentent massivement.** Les données non structurées représentent environ 80 % de l'ensemble des données d'une entreprise, et leur volume tend à doubler chaque année.

LA SOLUTION : WATCHGUARD DATA CONTROL

WatchGuard Data Control est un module de sécurité des données entièrement intégré dans WatchGuard EDR et WatchGuard EPDR. Il est conçu pour aider les entreprises à se conformer aux réglementations en matière de protection des données.

WatchGuard Data Control identifie, analyse et surveille les données personnelles non structurées¹ sur les endpoints, qu'il s'agisse des données résidentes ou des données utilisées, ou encore des données en transit. Son puissant moteur de recherche personnalisé permet aux administrateurs de rechercher n'importe quel fichier au sein de l'entreprise afin de vérifier les données qu'il contient (contenus protégés par le droit d'auteur, informations confidentielles, etc.).

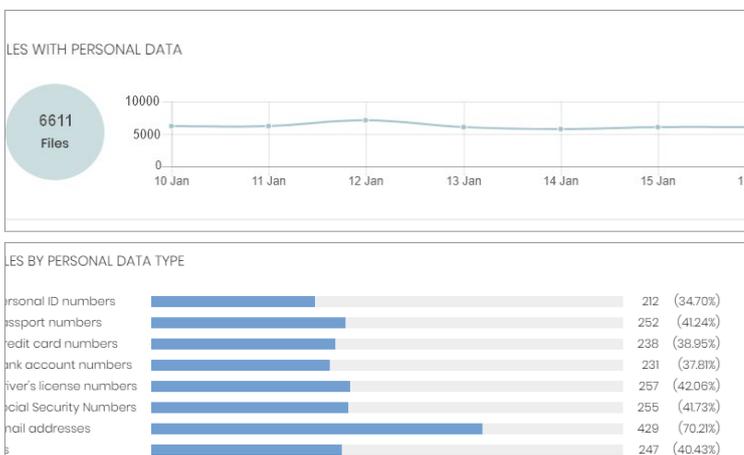


Figure 1 : Tableau de bord principal. Accédez à différents volets pour visualiser les fichiers contenant des données personnelles, les ordinateurs avec des données personnelles, et les fichiers par type de données personnelles.

PRINCIPAUX AVANTAGES

Découvrir et vérifier

Identifiez automatiquement les fichiers contenant des données personnelles ainsi que les utilisateurs, les employés, les collaborateurs, les postes de travail et les serveurs de votre entreprise qui accèdent aux informations permettant d'identifier les personnes (PII²).

Surveiller et détecter

Mettez en œuvre des mesures proactives pour empêcher l'accès aux PII à l'aide de rapports et d'alertes en temps réel sur l'utilisation, la transmission et l'exfiltration non autorisées ou suspectes de fichiers de données personnelles.

Démontrer la conformité

Montrez la conformité aux réglementations applicables à la direction, au Délégué à la Protection des Données (DPO pour Data Protection Officer),³ et à tous les autres employés de votre entreprise. Démontrez les mesures de sécurité strictes mises en place pour protéger les PII sur les postes de travail et les serveurs.

Trouver n'importe quel type de données à contrôler

Exécutez des recherches personnalisées pour trouver tout type de données dans les fichiers de votre réseau. Trouvez les fichiers personnels dupliqués et supprimez-les pour réduire le risque d'exfiltration de données.

Simplifier la gestion

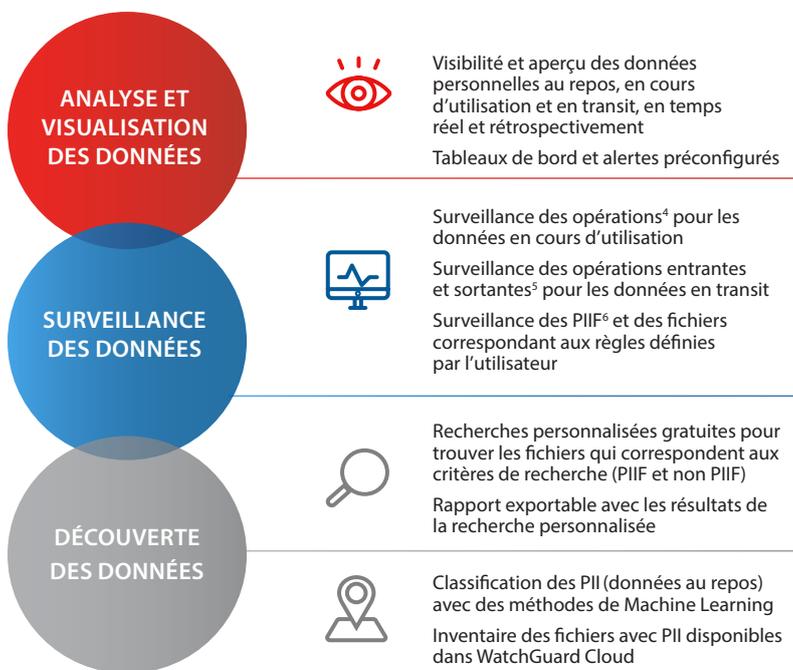
Les entreprises n'ont pas besoin de déployer de logiciel ou de matériel supplémentaire et il peut être activé facilement et immédiatement sans configurations fastidieuses. Une fois activé, le module est activé et géré depuis la plateforme Cloud.

GOVERNANCE DES DONNÉES DE L'ENTREPRISE

Une solide gouvernance des données permet aux entreprises de répondre à toutes les questions relatives aux données personnelles traitées par les employés : Quelles sont les données stockées sur les postes de travail des employés ? Qui peut accéder à ces données et quelles actions sont entreprises à leur sujet ? Ces actions sont-elles conformes à vos stratégies d'entreprise ?

- Découvrez et comprenez les données personnelles non structurées. Marquez, regroupez et classez ces données en fonction de leur importance.
- Établissez des stratégies de sécurité et d'accès pour contrôler l'accès aux données et leur utilisation par les utilisateurs autorisés.
- Formez votre personnel pour qu'il traite les données conformément aux réglementations externes et aux stratégies internes.
- Utilisez des tableaux de bord, des rapports et des alertes personnalisées et prédéfinies pour démontrer la gouvernance des données.
- Analysez les causes d'une violation de données personnelles et ajustez les stratégies d'entreprise. Établissez la séquence des actions effectuées lors d'une violation des informations personnelles.

FONCTIONNALITÉS PRINCIPALES DE WATCHGUARD DATA CONTROL



Pays pris en charge par WatchGuard Data Control

Disponible en Espagne, Allemagne, Royaume-Uni, Suède, France, Italie, Portugal, Pays-Bas, Finlande, Danemark, Suisse, Norvège, Autriche, Belgique, Hongrie et Irlande.

¹Les données non structurées désignent des données qui ne résident pas dans une base de données ou dans une autre structure de données.

Les données non structurées peuvent être textuelles ou non textuelles. WatchGuard Data Control est focalisé sur les données textuelles non structurées situées sur des endpoints et des serveurs.

²PII (informations personnellement identifiables) : Identifiant personnel, permis de conduire, passeport, numéro de sécurité sociale, email, identifiant fiscal, IP, prénoms, noms de famille, numéros de téléphone, comptes bancaires, cartes de crédit

³DPO (Data Protection Officer - Délégue à la Protection des Données) : La personne chargée de superviser la stratégie de protection des données dans une entreprise

⁴Données en cours d'utilisation. Surveillance des actions sur le PIIF : accès, ouverture, création, édition, suppression, changement de nom, copies et collages, etc.

⁵Données en mouvement avec risque de fuite par le biais d'Outlook, de navigateurs Web, de FTP, de clés USB

⁶Fichiers (PIIF) : Fichiers non structurés contenant des PII, tels que Office, OpenOffice, PDF, TXT, etc.

FONCTIONNALITÉS

Découverte de données

Classifie automatiquement et crée un inventaire indexé de tous les fichiers, y compris les doublons, qui stockent des données personnelles non structurées (données au repos), avec le nombre d'occurrences de chaque type de données. Ces fichiers peuvent être supprimés de l'inventaire. La fonctionnalité Planificateur détermine quand l'analyse du disque complet est lancée (nécessaire pour l'inventaire et les recherches).

Le processus de classification utilise une combinaison de règles, d'expressions régulières et de méthodes de Machine Learning, entre autres, ce qui permet d'optimiser les résultats de la classification tout en réduisant les faux positifs et la consommation de ressources sur les appareils.

Recherche de données

Exécutez des recherches personnalisées gratuites pour trouver des fichiers au contenu spécifique. WatchGuard Data Control générera une liste de tous les fichiers contenant les informations, avec la possibilité de les exporter pour faciliter la gestion.

Surveillance et contrôle des données

Surveillez les différents types d'opérations effectuées sur les fichiers non structurés (données en cours d'utilisation), tout en tenant à jour l'inventaire des fichiers de données personnelles. Toute tentative de copier ou de déplacer l'un de ces fichiers hors du réseau par le biais d'un email, d'un navigateur Web, d'un FTP ou d'un stockage amovible (données en mouvement) est enregistrée par le module. Contrôle des informations d'écriture sur des disques de stockage amovibles uniquement s'ils sont chiffrés.

Visualisation des données

Les résultats des tâches de surveillance et de découverte des données sont synchronisés en permanence sur la plateforme Endpoint Security et dans le module Advanced Visualization Tool. Ce module fournit des outils pour enquêter sur tous les événements affectant les données au repos, en cours d'utilisation et en mouvement, à la fois en temps réel et rétrospectivement tout au long de leur cycle de vie sur les appareils.

Les tableaux de bord et les rapports et alertes prédéfinis de WatchGuard Data Control permettent de couvrir de nombreux cas d'utilisation et d'assurer la gouvernance de la sécurité des données personnelles non structurées.

Plateformes prises en charge et configuration système requise pour WatchGuard Data Control

Compatible avec les solutions suivantes :
WatchGuard EPDR et WatchGuard EDR

Systèmes d'exploitation pris en charge : [Windows](#).

Liste des navigateurs compatibles : [Google Chrome](#) et [Mozilla Firefox](#) (d'autres peuvent être compatibles).