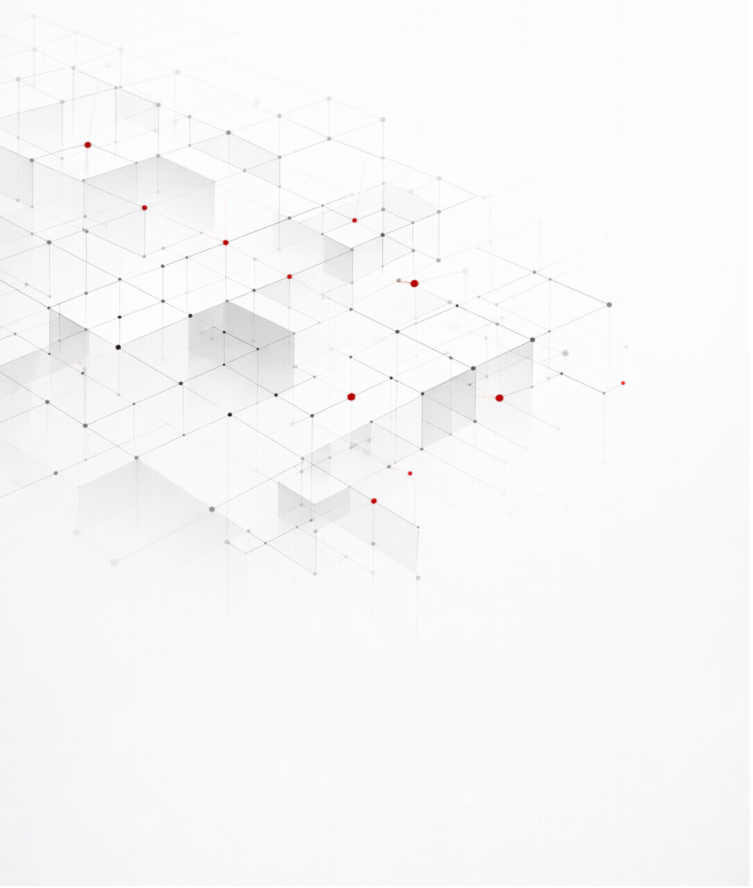

APOLLO Data Auditor

LIVRE BLANC · EXPOSITION AU RISQUE

Combien vous coûtent vraiment vos données ?

Mesurer l'exposition financière avant la brèche

Quel est vraiment le coût de vos données ?

MESURER L'EXPOSITION FINANCIÈRE AVANT LA BRÈCHE

Module Risk Exposure — Avril 2026

RÉSUMÉ EXÉCUTIF

443 notifications de brèche de données par jour. C'est le rythme actuel en Europe — une augmentation de 22% en un an.

La plupart de ces organisations ont découvert l'ampleur du problème après l'incident, pas avant. Elles n'avaient aucune cartographie de leurs données sensibles. Aucune estimation financière de leur exposition réglementaire. Aucun moyen de répondre à la seule question qui importe pour un conseil d'administration, un assureur ou un régulateur : combien ?

Ce document examine pourquoi cette question reste sans réponse dans la plupart des PME, pourquoi les outils qui pourraient y répondre sont hors de portée, et à quoi ressemble une approche différente.

1. VOUS NE SAVEZ PAS CE QUE VOUS STOCKEZ

Un cabinet juridique de taille moyenne au Royaume-Uni a été violé par l'intermédiaire d'un compte de service hérité. Le mot de passe était inconnu de l'équipe IT. Aucune authentification multifacteur. L'attaquant s'est déplacé latéralement sur le réseau et a exfiltré 32,4 Go de dossiers de cas judiciaires — documents judiciaires, photographies, données personnelles de 791 individus. Tous publiés sur le dark web.

Le cabinet n'a pas identifié l'incident comme une brèche à déclarer pendant 43 jours. L'obligation RGPD est de 72 heures.

L'autorité de contrôle leur a infligé une amende de 60 000 £.

Le compte compromis avait des privilèges excessifs et n'avait jamais été audité. Personne ne savait qu'il existait. C'est à quoi ressemble l'accès fantôme en pratique :

des identifiants et des données qui se trouvent en dehors de la visibilité de tout le monde, jusqu'à ce qu'un attaquant les trouve en premier.

Ce schéma se répète dans tous les secteurs et zones géographiques.

À New York, un cabinet comptable a connu deux incidents successifs exposant les numéros de sécurité sociale, les comptes financiers et les données d'avantages médicaux de 4 700 individus. Le cabinet a pris plus d'un an pour notifier les victimes. Accord avec le procureur général : 60 000 $, plus une refonte obligatoire de la sécurité.

En Estonie, un programme de fidélité de pharmacie avait accumulé six ans d'historique d'achat — tests de grossesse, tensiomètres, produits d'hygiène intime — pour 750 000 individus. Pas d'AMF, pas de journaux d'accès, pas de rôles définis. Les données n'avaient jamais été auditées. Amende : 3 000 000 €, la plus grande jamais imposée en Estonie.

Aucune de celles-ci n'était une entreprise Fortune 500. C'étaient des organisations de 50 à 500 employés qui n'avaient aucun inventaire de leurs données sensibles.

Les données confirment que ce n'est pas anecdotique :

- 35% de toutes les brèches de données impliquent des données fantômes — des données que les organisations ne savent pas qu'elles ont. Ces brèches coûtent 16% plus cher et prennent 26% plus de temps à détecter (IBM 2024).
- 59% des responsables de la sécurité admettent qu'ils ne peuvent pas maintenir un inventaire détaillé des données (Forrester/Cyera 2024).
- 48% des victimes de ransomware en France sont des PME (ANSSI 2025). 88% des brèches affectant les PME impliquent des ransomwares (Verizon DBIR 2025).
- Le temps moyen de détection d'une brèche est de 241 jours. Brèches de chaîne d'approvisionnement : environ 9 mois (IBM 2025).
- Les amendes RGPD ont atteint 7,1 milliards d'€ cumulés. En Espagne, 70% des actions d'exécution en 2024 visaient les PME (AEPD).

APOLLO™ DATA AUDITOR EN ACTION — TROIS CAS RÉELS SCORÉS

Chacun des incidents décrits ci-dessus suit le même schéma : personne ne savait quelles données il détenait, où elles se trouvaient, ni dans quelle mesure il était exposé — jusqu'à ce qu'un attaquant ou un régulateur le découvre en premier. Voici ce qu'un scan APOLLO™ Data Auditor aurait détecté pour chaque organisation, réalisé avant l'incident.

Cas 1 — Cabinet d'avocats britannique, 791 personnes, amende de 60 000 £

Profil de scan : 8 400 fichiers — dossiers judiciaires, photos de tribunal, correspondances personnelles. Compte de service legacy avec accès réseau complet, inconnu du service IT. Pas de MFA. Pas de registre des traitements.

Score	Valeur	Statut
Exposition au Risque — S013 Global	**19 / 100**	CRITIQUE
Conformité RGPD	11 / 100	Note F
Protection des Données	14 / 100	CRITIQUE
Exposition financière estimée	**340 000 €**	—

Article RGPD	Score	Constat
Art. 9 — Données sensibles	2 / 100	Dossiers judiciaires classés catégorie spéciale — 100% non protégés
Art. 32 — Sécurité	0 / 100	Pas de MFA. Compte fantôme avec accès lecture total. Pas de chiffrement.
Art. 30 — Documentation	10 / 100	Pas de registre des traitements. Compte fantôme non référencé.
Art. 5 — Conservation	40 / 100	Fichiers datant de plus de 8 ans. Pas de politique de conservation.

Priorité	Action	Impact estimé
P1	Auditer et supprimer tous les comptes de service absents de l'annuaire LDAP	– 190 000 € d'exposition
P1	Activer le MFA sur tous les points d'accès (fichiers + partages réseau)	Art. 32 : de 0 à conformité partielle
P1	Créer un registre des traitements couvrant les types de dossiers judiciaires	Obligatoire — Art. 30 actuellement manquant

L'amende ICO était de 60 000 £. APOLLO estimait 340 000 € d'exposition potentielle. L'écart : l'ICO a appliqué une remise significative pour coopération. Si le registre des traitements avait existé, la violation de l'article 30 — et une partie de l'amende — n'aurait pas été applicable.

Cas 2 — Programme de fidélité d'une pharmacie estonienne, 750 000 personnes, amende de 3 000 000 €

Profil de scan : base de données fidélité, 2,1 millions d'enregistrements, 6 ans d'historique d'achats. Catégories de produits : tests de grossesse, tensiomètres, hygiène intime — classés données de santé adjacentes sous le RGPD article 9. Pas de MFA. Pas de journaux d'accès. Pas de rôles définis. Pas de politique de conservation.

Score	Valeur	Statut
Exposition au Risque — S013 Global	**8 / 100**	CRITIQUE
Conformité RGPD	0 / 100	Note F
Protection des Données	7 / 100	CRITIQUE
Exposition financière estimée	**4 100 000 €**	—

Article RGPD	Score	Constat
Art. 9 — Données sensibles	0 / 100	100% des enregistrements contiennent des données de santé adjacentes
Art. 32 — Sécurité	0 / 100	Pas de MFA. Pas de journaux d'accès. Pas de contrôle d'accès par rôle.
Art. 30 — Documentation	0 / 100	Pas de registre. Pas de documentation du responsable de traitement.
Art. 5 — Conservation	0 / 100	6 ans de conservation sans base légale identifiée au-delà de 12 mois.

Priorité	Action	Impact estimé
P1	Purger tous les enregistrements de plus de 12 mois — aucune base légale identifiée	– 2 400 000 € d'exposition
P1	Définir les accès par rôle — accès lecture total pour tout le personnel actuellement	Art. 32 : de 0 à partiel
P1	Documenter la base légale du programme fidélité sous l'Art. 6	Obligatoire — aucun registre n'existe

L'amende était de 3 000 000 € — la plus élevée jamais prononcée en Estonie. Le modèle APOLLO : 4 100 000 €. La différence : l'autorité de contrôle a appliqué le plafond de 4% du chiffre d'affaires. Les données n'avaient jamais été auditées. Si APOLLO avait été utilisé un an plus tôt, la purge seule aurait réduit l'exposition financière d'environ 58%.

Cas 3 — Cabinet comptable de New York, 4 700 personnes, accord à 60 000 $

Profil de scan : patrimoine mixte fichiers et bases de données. Types de PII détectés : numéros de Sécurité Sociale, numéros de comptes financiers, données de prestations médicales. Deux incidents successifs en 24 mois. Pas de contrôle d'accès structuré. Notification retardée de plus de 12 mois.

Score	Valeur	Statut
Exposition au Risque — S013 Global	**24 / 100**	CRITIQUE
Conformité CCPA	Note F	CRITIQUE
Protection des Données	21 / 100	CRITIQUE
Exposition financière estimée	**420 000 $**	—

Combinaison Toxique	Classification	Multiplicateur appliqué
Numéro de Sécurité Sociale + Données médicales	Tier 1 — Sensibilité maximale	× 3,0
Numéro de compte financier + NSS	Tier 1 — Sensibilité maximale	× 2,5

Priorité	Action	Impact estimé
P1	Séparer les fichiers NSS des fichiers financiers — colocalisés dans 3 répertoires	Élimine la combinaison toxique Tier 1
P1	Supprimer les fichiers de prestations médicales dépassant 3 ans de conservation	– 180 000 $ d'exposition CCPA
P2	Mettre en place la journalisation d'accès sur tous les répertoires contenant des NSS	Permet la détection des brèches (délai moyen actuel : 241 jours)

L'accord avec le Procureur Général était de 60 000 $. Le modèle d'exposition APOLLO : 420 000 $. L'écart reflète une résolution négociée — et exclut le coût des deux incidents, des notifications obligatoires à 4 700 personnes, et de la refonte de sécurité imposée. Les trois auraient pu être évités par un scan à 2 999 €/an, qui aurait signalé la combinaison toxique dès le premier jour.

2. POURQUOI LES SOLUTIONS EXISTANTES NE RÉPONDENT PAS À LA QUESTION

Si vous êtes un directeur financier préparant une réunion du conseil d'administration et que vous posez la question « combien sommes-nous exposés en vertu du RGPD ? », aujourd'hui personne dans votre organisation ne peut répondre avec un chiffre. Votre DPD a un registre des traitements construit à partir de déclarations. Votre équipe IT sait quelles bases de données existent mais pas ce qu'elles contiennent. Votre RSSI a des contrôles de sécurité en place mais aucun modèle d'impact financier.

Le marché propose plusieurs catégories d'outils. Aucun d'eux ne répond à la question.

Ce dont vous avez besoin	Plateformes de sécurité des données d'entreprise	Automatisation de la conformité	Outils de gouvernance de la vie privée	Découverte de données PME	Cabinets de conseil
Analyse les données réelles	✅ Oui	❌ Déclarations	❌ Questionnaires	⚠️ Fichiers Windows uniquement	❌ Entretiens
Calcule l'exposition en € / $	❌ Scores de risque, pas de montants	⚠️ Modèles génériques	❌ Élevé/moyen/faible	❌ Non	⚠️ Estimation ponctuelle
Simule l'impact de la brèche	❌ Posture, pas d'impact	❌ Rare	❌ Non	❌ Non	⚠️ Manuel, facturé séparément
Prix typique	50 000 $ – 500 000 $/an	10 000 $ – 200 000 $/an	5 000 € – 50 000 €/an	1 000 € – 15 000 €/an	5 000 € – 50 000 € par mission
Délai de déploiement	Semaines à mois	Semaines	Jours	Minutes	4–8 semaines

Les plateformes d'entreprise analysent les données mais ne traduisent pas les conclusions en montants d'amendes réglementaires. Les outils de conformité modélisent le risque de manière abstraite mais ne regardent jamais les données réelles. Les outils de gouvernance de la vie privée gèrent les processus de manière déclarative. Les cabinets de conseil fournissent un instantané ponctuel basé sur des entretiens — pas répétable, pas évolutif, pas abordable pour la plupart des PME.

Pour couvrir toutes les dimensions du problème — analyse, quantification et simulation — une PME aurait besoin de combiner trois ou quatre de ces catégories. Plusieurs fournisseurs, plusieurs contrats, plusieurs interfaces, à un coût combiné dépassant 100 000 € par an. Ce n'est pas réaliste pour une organisation de 50 à 500 employés.

Le gap : aucune catégorie existante sous 50 000 €/an ne combine analyse de données réelles + calcul automatisé de l'exposition financière + simulation d'impact de brèche dans un seul outil.

3. QUE COÛTERAIT UNE BRÈCHE DEMAIN ?

Imaginez que votre assureur cyber vous demande de quantifier votre exposition aux données d'identité personnelle. Vous avez 47 000 fichiers sur des serveurs locaux, deux bases de données, une instance SharePoint et un Active Directory avec 230 comptes. Aujourd'hui, vous ne pouvez pas répondre.

Ce dont vous avez besoin n'est pas une autre liste de contrôle de conformité. Vous avez besoin de cinq choses :

Une cartographie des données d'identité. Un inventaire complet des fichiers, tables et documents cloud qui contiennent quels types de données personnelles. Sans cela, tout le reste est une supposition.

Exposition financière en € et $. Calculée à partir des données d'identité réellement détectées, des types de source impliqués et des formules de pénalité réglementaire — Article 83 du RGPD (jusqu'à 4% du chiffre d'affaires ou 20 M€) et CCPA (2 663 $ par violation standard, 7 988 $ par violation intentionnelle). Pas un score abstrait. Un chiffre que votre directeur financier peut présenter au conseil d'administration et que votre assureur peut utiliser pour tarifier une police.

Simulation d'impact de brèche. Que se passerait-il si ces données étaient violées demain ? Quelle amende, quel coût de notification, quel coût de remédiation, quelle interruption d'activité ? Modélisé à partir des types et volumes de données d'identité réellement trouvés dans votre infrastructure — pas un scénario théorique.

Détection de combinaisons toxiques. Un IBAN seul est sensible. Un numéro de sécurité sociale seul est sensible. Les deux dans le même fichier constituent une catastrophe réglementaire. Ces co-localisations multiplient l'exposition et doivent être identifiées avant qu'un incident ne les révèle.

Identification des zones à risque. Quels répertoires, bases de données ou conteneurs cloud ont la plus forte concentration de données d'identité non protégées ? Cela vous dit où vous concentrer en premier — et où les dégâts seraient les plus importants.

---

4. COMMENT APOLLO DATA AUDITOR RÉPOND À LA QUESTION

Les cinq capacités décrites ci-dessus existent aujourd'hui, dans un seul outil, à un prix adapté aux PME. Voici comment cela fonctionne.

Vos données restent les vôtres. Un agent natif s'exécute localement sur votre infrastructure — Windows, Linux et macOS (arm64). Il analyse 11 types de sources : PostgreSQL, MySQL, MongoDB, SQL Server, OneDrive, SharePoint, Active Directory/LDAP, ERP (Pennylane), fichiers locaux, partages NFS/SMB et infrastructure. Seules les métadonnées et les compteurs transitent vers le tableau de bord cloud. Les données brutes ne quittent jamais votre périmètre. L'agent est open source (BSL 1.1) — chaque ligne de code est vérifiable sur GitHub. Ce n'est pas une affirmation. C'est auditable.

Vous obtenez une réponse financière. Le tableau de bord affiche votre exposition RGPD et CCPA en euros et en dollars — article par article, source par source. Il cartographie chaque type de données d'identité détecté, marque les combinaisons toxiques, identifie vos zones à plus haut risque et simule l'impact financier d'un scénario de brèche basé sur votre profil de données réel.

Vous obtenez un plan de remédiation. Actions priorisées (P1/P2/P3) avec impact financier estimé pour chacune. Pas une liste générique de meilleures pratiques — des actions liées aux risques spécifiques trouvés dans votre scan.

À quoi cela ressemble en pratique : un souscripteur d'assurance cyber demande à un fabricant de taille moyenne une évaluation du risque de données. Le fabricant dispose de 47 000 fichiers, de deux bases de données PostgreSQL, d'une instance SharePoint et de 230 comptes Active Directory. Le scan s'exécute en moins de 48 heures. Résultat : 2,3 M€ d'exposition RGPD potentielle concentrée dans trois répertoires, 12 combinaisons toxiques de données d'identité, et 1 400 fichiers contenant des données de santé que personne n'avait classées. Le fabricant dispose maintenant d'un chiffre pour l'assureur, d'une liste de priorités de remédiation et d'une base de référence pour mesurer l'amélioration.

44 types de données d'identité détectés dans les réglementations de l'UE et des États-Unis — IBAN, SSN, NIR, PESEL, BSN, NIE, NISS, codice fiscale, passeport, email, téléphone, données de santé et 32 autres. **129 scores auditables avec formules publiées.** Chaque score est transparent, reproductible et vérifiable. Pas de boîte noire. Jusqu'à **1,16 million de lignes par seconde.**

LA COMPARAISON DES PRIX

	Plateformes d'entreprise	Cabinets de conseil	APOLLO Data Auditor
Coût annuel	50 000 $ – 500 000 $	5 000 € – 15 000 € par audit	**2 999 € / an** (Starter)
Déploiement	Semaines à mois	4–8 semaines	**Moins de 48 heures**
Répétable	Oui	Non (ponctuel)	**Oui — à chaque scan**
Calcule l'exposition en €/$	Non	Partiel (manuel)	**Oui — automatisé**
Simulation d'impact de brèche	Non	Manuel (facturé séparément)	**Oui — inclus**

5. UN SCAN. UNE RÉPONSE. QUATRE DIMENSIONS.

La plupart des PME auraient besoin de combiner trois ou quatre fournisseurs pour couvrir ce qu'un audit de données unique devrait livrer : savoir quelles données vous avez, combien elles vous coûtent, si elles sont protégées et si elles sont prêtes pour ce qui vient ensuite. Ce n'est pas une stratégie viable pour une entreprise de 200 employés sans équipe de sécurité dédiée.

APOLLO Data Auditor a été construit pour résoudre exactement cela. Un scan, un outil, quatre dimensions de votre risque de données — à un prix qui reflète la réalité des budgets des PME, pas les cycles d'approvisionnement des entreprises.

→ **Risk Exposure** — ce que ce document couvre. Quantification financière en € et $, simulation d'impact de brèche, cartographie des données d'identité, combinaisons toxiques, zones à risque.

→ **Compliance** — RGPD noté par article (Art. 5, 9, 30, 32), CCPA, NIS2, SOC2, DORA. Notes de A à F basées sur vos données réelles — pas des déclarations. Plan de remédiation priorisé (P1/P2/P3).

→ **Data Protection** — couverture de chiffrement, résilience des sauvegardes, simulation de préparation aux ransomwares, hygiène du contrôle d'accès, détection des comptes dormants. La posture technique qui détermine si une brèche reste contenue ou devient catastrophique.

→ **Intelligence** — Score de préparation à l'IA, métriques de qualité des données, pré-conformité à la loi sur l'IA (gouvernance des données article 10, posture cybersécurité article 15). Si vos données sont prêtes pour l'IA — ou si elles bloqueront le déploiement.

Aucun autre outil sous 5 000 €/an ne couvre tous les quatre. Ce n'est pas un argument marketing — c'est le résultat d'un marché où les plateformes DSPM d'entreprise commencent à 50 000 €, les outils GRC n'analysent pas les données et les cabinets de conseil fournissent des rapports ponctuels basés sur des entretiens qui sont obsolètes avant que la facture ne soit payée.

APOLLO™ Data Auditor existe parce que les PME méritent la même visibilité sur leur risque de données qu'une entreprise Fortune 500 — sans le budget Fortune 500.

Sources : IBM Cost of a Data Breach Report 2024 & 2025 · Verizon 2025 DBIR SMB Snapshot · DLA Piper GDPR Fines & Data Breach Survey 2026 · ANSSI Panorama de la cybermenace 2025 · CMS GDPR Enforcement Tracker 2024/2025 · CPPA CCPA Fines 2025 · ICO UK Enforcement Actions · Linklaters AEPD FY24 · Forrester/Cyera Data Security Study 2024 · FBI IC3 Annual Report 2024

APOLLO™ Data Auditor Tout fichier est un risque. Mesurez-le.

→ https://apollo.aiia-tech.com → GitHub : https://ggabrie2025.github.io/apollo_data_auditor/ → contact@aiia-tech.com