**APOLLO** Data Auditor

LIVRE BLANC · RISQUE PROTECTION

# Vos données survivraient-elles à une attaque ?

Pourquoi la surveillance n'est pas la protection — Et ce que l'audit de posture révèle avant la brèche

**Module Risque Protection — Avril 2026**

## RÉSUMÉ EXÉCUTIF

93% des attaques par ransomware ciblent maintenant les référentiels de sauvegarde avant de chiffrer les données de production. Si vos sauvegardes ne sont pas immuables, vous les perdez toutes les deux.

La plupart des PME investissent dans des outils réactifs — antivirus, EDR, pare-feux. Ces outils répondent à une question : « Une attaque se produit-elle en ce moment ? » Mais ils ne répondent pas à la question qui détermine si votre entreprise survit : « Si une attaque se produit demain, vos données sont-elles vraiment protégées ? »

Ce document examine pourquoi la surveillance réactive laisse des lacunes critiques dans la protection des données, ce que l'audit de posture proactive révèle que la surveillance ne peut pas, et pourquoi la différence entre les deux est la différence entre la récupération et la faillite.

## 1. LA PROTECTION QUE VOUS CROYEZ AVOIR

Une entreprise française de taille moyenne avait un EDR déployé, un pare-feu en place et une solution de sauvegarde en cours d'exécution chaque nuit. Lorsque le ransomware a frappé, la sauvegarde a été chiffrée avec la production — l'attaquant avait d'abord accédé au référentiel de sauvegarde. L'entreprise n'avait aucune copie immuable ou isolée. Coût de récupération : plus de 2 millions d'€. Temps pour reprendre les opérations : quatre mois.

Ce n'est pas un cas limite. C'est la nouvelle norme.

Selon Veeam, 93–96% des attaques par ransomware ciblent spécifiquement les référentiels de sauvegarde avant de toucher les systèmes de production. Les attaquants savent : détruisez la sauvegarde et la victime n'a d'autre choix que de payer ou de tout reconstruire à partir de zéro.

Le rapport State of Ransomware 2025 de Sophos confirme que la récupération via sauvegarde est à son plus bas niveau en six ans. 54% des organisations tentent la récupération par des sauvegardes, tandis que 49% paient la rançon — à un paiement moyen de 1 million de dollars. Coût total moyen de récupération : 2,57 millions de dollars. Temps moyen pour reprendre les opérations : plus de 130 jours.

Et pourtant, la plupart des organisations supposent que leur stratégie de sauvegarde est saine parce que les sauvegardes s'exécutent sans erreurs. Ils n'ont jamais testé si ces sauvegardes survivraient à une attaque ciblée. Ils n'ont jamais vérifié l'immuabilité. Ils n'ont jamais mesuré leur RPO réel par rapport à celui déclaré dans leur plan de reprise après sinistre.

La sauvegarde n'est que l'une des six lacunes. Les identifiants, les comptes dormants, les lacunes de chiffrement, les données obsolètes et les plans de réponse aux brèches non testés sont les autres. La section 3 examine chacun d'eux.

Mais d'abord, un chiffre qui encadre les enjeux : **une PME sur cinq qui subit une cyberattaque majeure dépose le bilan** (Mastercard 2025). Deux tiers des PME françaises ont subi une cyberattaque en 2025 (Orange Cyberdefense). La question n'est pas si vos outils détectent les menaces. La question est : **vos données survivraient-elles ? **

---

## APOLLO™ DATA AUDITOR EN ACTION — TROIS CAS RÉELS SCORÉS

Chaque cas ci-dessous illustre une dimension différente de défaillance de protection — sauvegarde, chiffrement, contrôle d'accès. Dans chaque cas, le problème était visible dans les données avant l'incident.

---

### Cas 1 — PME industrielle française, coût de récupération > 2 000 000 € (2025)

*Profil de scan : 24 000 fichiers sur 3 serveurs, 2 bases de données, sauvegarde quotidienne vers un partage réseau. Référentiel de sauvegarde accessible depuis le même segment réseau que la production. Pas de copie immuable ou isolée. 4 comptes administrateurs dormants. Pas de chiffrement au repos.*

| SCORE | VALEUR | STATUT |
|---|---|---|
| **Risque Privacy — S013 Global** | **17 / 100** | CRITIQUE |
| Protection des Données | 12 / 100 | CRITIQUE |
| Résilience Sauvegarde | 8 / 100 | CRITIQUE |
| **Exposition ransomware estimée** | **1 900 000 €** | — |

| DIMENSION | SCORE | CONSTAT |
|---|---|---|
| Résilience sauvegarde | 8 / 100 | Sauvegarde accessible depuis le réseau de production. Pas d'immuabilité. Pas d'isolation. |
| Couverture chiffrement | 14 / 100 | 0% de chiffrement sur les fichiers. 0% au repos sur les volumes DB. |
| Contrôle d'accès | 21 / 100 | 4 comptes admin dormants (90+ jours inactifs). Partage réseau ouvert à tous. |
| Données ROT | 35 / 100 | 38% des fichiers datent de plus de 5 ans sans politique de conservation |

| PRIORITÉ | ACTION | IMPACT ESTIMÉ |
|---|---|---|
| P1 | Isoler le référentiel de sauvegarde — migrer vers un stockage immuable ou isolé | Score sauvegarde : de 8 à 70+ |
| P1 | Désactiver immédiatement les 4 comptes admin dormants | Élimine la surface d'attaque à privilèges les plus élevés |
| P1 | Chiffrer les volumes DB de production | Référentiel Art. 32 — actuellement 0% de couverture |

> *Le coût de récupération a dépassé 2 M€. Délai de reprise d'activité : quatre mois. Le score de Résilience Sauvegarde APOLLO était de 8/100 — CRITIQUE. Le constat « sauvegarde accessible depuis le réseau de production » aurait été une action P1 dès le premier jour. À 2 999 €/an, le scan se serait rentabilisé 666 fois.*

---

### Cas 2 — Entreprise logistique britannique, compromission via compte Active Directory dormant (2024)

*Profil de scan : Active Directory — 340 comptes, 28 avec privilèges admin. 67 comptes inactifs depuis plus de 90 jours, dont 11 conservent un accès admin. Audit des mots de passe : 19% des comptes correspondent à des listes de compromission connues. Pas de MFA sur les comptes admin de domaine.*

| SCORE | VALEUR | STATUT |
|---|---|---|
| **Risque Privacy — S013 Global** | **23 / 100** | CRITIQUE |
| Protection des Données | 19 / 100 | CRITIQUE |
| Hygiène Contrôle d'Accès | 11 / 100 | CRITIQUE |
| **Exposition estimée** | **780 000 £** | — |

| DIMENSION | SCORE | CONSTAT |
|---|---|---|
| Comptes dormants | 4 / 100 | 67 comptes inactifs (19,7%). 11 conservent des privilèges admin. |
| Hygiène mots de passe | 18 / 100 | 65 comptes correspondent à des listes de compromission connues |
| Couverture MFA | 0 / 100 | MFA non appliqué sur aucun compte admin de domaine |
| Prolifération des privilèges | 12 / 100 | 28 comptes admin pour 340 utilisateurs — ratio 8,2% vs 2% recommandé |

| PRIORITÉ | ACTION | IMPACT ESTIMÉ |
|---|---|---|
| P1 | Désactiver tous les comptes inactifs depuis 90+ jours — 67 comptes signalés | Élimine le principal vecteur de mouvement latéral |
| P1 | Forcer la réinitialisation du mot de passe pour les 65 comptes dans les listes de compromission | Ferme le vecteur de credential stuffing |
| P1 | Appliquer le MFA sur tous les comptes admin de domaine | Standard industriel — actuellement 0% de couverture |

> *Palo Alto Unit 42 détecte des failles d'identité dans 90% des investigations d'incident. Le score de contrôle d'accès APOLLO était de 11/100. Les 11 comptes admin dormants auraient été des actions P1 avec impact financier quantifié. La compromission a été détectée 210 jours après l'intrusion initiale. APOLLO signale l'exposition avant que l'attaquant ne l'utilise.*

---

### Cas 3 — Prestataire de santé allemand, violation par données ROT (2024)

*Profil de scan : 47 000 fichiers. 38% signalés comme ROT (Redondants, Obsolètes, Triviaux) — fichiers de plus de 5 ans, sans utilisateur actif, sans balise métier. 1 400 fichiers ROT contiennent des données de santé, dont des formulaires d'admission de patients d'une clinique désaffectée. Pas de chiffrement. Classifiés RGPD Article 9.*

| SCORE | VALEUR | STATUT |
|---|---|---|
| **Risque Privacy — S013 Global** | **21 / 100** | CRITIQUE |
| Protection des Données | 16 / 100 | CRITIQUE |
| Conformité RGPD | 14 / 100 | Note F |
| **Exposition financière estimée** | **620 000 €** | — |

| DIMENSION | SCORE | CONSTAT |
|---|---|---|
| Données ROT | 9 / 100 | 17 860 fichiers ROT. 1 400 contiennent des données de santé Art. 9 d'une clinique fermée. |
| Couverture chiffrement | 0 / 100 | 0% des fichiers de santé chiffrés. Accès en lecture ouverts sur 4 partages. |
| Conformité conservation | 5 / 100 | Fichiers conservés 8+ ans. Base légale expirée. Pas de calendrier de suppression. |
| Simulation impact brèche | — | 4 200 patients concernés en cas d'exfiltration des données ROT |

| PRIORITÉ | ACTION | IMPACT ESTIMÉ |
|---|---|---|
| P1 | Supprimer les 1 400 fichiers de santé ROT de la clinique désaffectée — pas de base légale | – 420 000 € d'exposition (réduction du volume Art. 9) |
| P1 | Chiffrer les fichiers de santé restants en attente de révision juridique | Art. 32 : de 0 à conforme |
| P2 | Mettre en place une politique de conservation automatisée — signaler les fichiers ROT trimestriellement | Prévient la réaccumulation |

> *Les données de santé de la clinique désaffectée n'avaient aucune base de conservation — la clinique était fermée depuis 4 ans. Personne ne savait qu'elles étaient encore là. La détection ROT d'APOLLO a trouvé 1 400 fichiers contenant des données patients qui auraient dû être supprimées des années auparavant. La suppression seule aurait réduit l'exposition aux amendes RGPD d'environ 420 000 €.*

## 2. POURQUOI LA SURVEILLANCE NE SIGNIFIE PAS LA PROTECTION

Le marché de la cybersécurité pour les PME est dominé par trois catégories d'outils réactifs :

| CATÉGORIE | CE QU'IL FAIT | CE QU'IL NE FAIT PAS |
|---|---|---|
| **SIEM** (Gestion des informations et événements de sécurité) | Agrège les journaux, détecte les anomalies, génère des alertes | N'audite pas l'immuabilité de la sauvegarde, la couverture de chiffrement ou les comptes dormants |
| **EDR** (Détection et réaction aux menaces d'extrémité) | Détecte le comportement malveillant sur les points d'extrémité, isole les menaces | N'analyse pas le contenu des données, n'identifie pas les données d'identité, n'évalue pas la résilience des sauvegardes |
| **XDR** (Détection et réaction étendue) | Étend EDR sur le réseau, le cloud et l'e-mail | Mêmes lacunes que EDR — centrées sur l'infrastructure, pas sur les données |

Ces outils sont essentiels. Ils sont aussi insuffisants.

Ils répondent : « Une attaque se produit-elle en ce moment ? » Ils ne répondent pas : « Mes sauvegardes sont-elles immuables ? Mes données sensibles sont-elles chiffrées ? Combien de comptes dormants ont des privilèges d'administrateur ? Combien de données obsolètes contiennent des données d'identité ? Que coûterait une brèche — en euros, en personnes à notifier, en amendes réglementaires ? »

**Le fossé est structurel.** SIEM, EDR et XDR sont centrés sur l'infrastructure et réactifs. Ils surveillent ce qui arrive à vos systèmes. Ils n'auditent pas ce qui est vrai de vos données. Un audit de posture proactive pose une question fondamentalement différente : non « sommes-nous sous attaque ? » mais « survivrions-nous à une ? »

Aucun outil existant sous 50 000 €/an ne combine audit de résilience des sauvegardes + vérification de couverture de chiffrement + hygiène du contrôle d'accès + identification de données ROT + simulation d'impact de brèche basée sur données analysées réelles.

---

## 3. LES SIX DIMENSIONS DE LA PROTECTION DES DONNÉES

Un directeur informatique préparant un renouvellement d'assurance cyber lui est demandé : « Décrivez votre posture de protection des données. » Aujourd'hui, dans la plupart des PME, la réponse est un récit — « nous avons des sauvegardes, nous avons un EDR, nous avons un pare-feu. » Pas de chiffres. Pas de notes. Pas de preuve.

Un audit de posture remplace les récits par des mesures. Six dimensions, chacune notée :

**Résilience des sauvegardes.** Votre stratégie de sauvegarde est-elle conforme à la règle 3-2-1-1-0 — 3 copies, 2 types de supports, 1 site distant, 1 immuable ou isolé, 0 erreur de vérification ? Le RPO déclaré est-il cohérent avec la fréquence de sauvegarde et la rétention réelles ? Quand le dernier test de restauration réussi a-t-il eu lieu ?

**Couverture de chiffrement.** Quels volumes, bases de données et conteneurs cloud ont le chiffrement au repos activé ? Quels fichiers contenant des données d'identité sont stockés en clair ? La réponse n'est pas « nous chiffrons tout » — c'est « ces 340 fichiers avec données de santé sur le serveur X ne sont pas chiffrés. » Une entreprise française de logiciels de santé a été condamnée à une amende de 1,7 million d'euros pour exactement cette lacune — violations de l'article 32 sur des systèmes qui étaient censés être sécurisés.

**Préparation aux ransomwares.** Si 100% de vos données de production étaient chiffrées par un attaquant demain, combien de temps prendrait la récupération ? Combien de personnes devraient être notifiées ? Quelle serait l'amende réglementaire ? Ce n'est pas un exercice théorique — c'est un calcul basé sur les types et volumes de données d'identité réellement trouvés dans votre infrastructure.

**Hygiène du contrôle d'accès.** Les identifiants volés sont le vecteur d'attaque numéro un — 22% de toutes les brèches (Verizon DBIR 2025). 19% des comptes Active Directory ont déjà des mots de passe présents dans les listes de compromission connues (Enzoic 2025). Palo Alto Unit 42 a trouvé des faiblesses d'identité dans 90% de leurs enquêtes. Combien de vos comptes ne se sont pas connectés depuis 90 jours ? Combien ont des privilèges de niveau administrateur ? Chaque compte privé dormant est une porte que personne ne regarde.

**Hygiène des données (ROT).** Jusqu'à 70% des données d'entreprise sont redondantes, obsolètes ou triviales. Ces fichiers n'ont aucune valeur commerciale, mais ils contiennent souvent des données d'identité : anciennes exportations RH, listes de clients de 2019, bases de données de test avec des données réelles. L'intersection de ROT et des données d'identité est l'endroit où le risque se cache — des fichiers dont personne ne se souvient, contenant des données que les régulateurs poseront des questions.

**Simulation d'impact de brèche.** Que se passerait-il si les données de votre zone à plus haut risque étaient violées ? Combien de personnes affectées ? Quels types de données d'identité ? Quel coût de notification ? Quelle amende RGPD en vertu de l'article 83 ? Quelle exposition CCPA ? Modélisé à partir de résultats de scan réels, pas d'un scénario de table ronde hypothétique.

---

## 4. COMMENT APOLLO DATA AUDITOR MESURE VOTRE POSTURE

Les six dimensions décrites ci-dessus existent aujourd'hui dans un seul outil. Voici ce que le module Data Protection produit.

**Vos données restent les vôtres.** Un agent natif s'exécute localement sur Windows, Linux et macOS (arm64). Il analyse les fichiers, les bases de données, le stockage cloud, Active Directory et l'infrastructure. Seules les métadonnées et les compteurs transitent vers le tableau de bord cloud. L'agent est open source (BSL 1.1) — vérifiable sur GitHub.

**Six notes, pas un récit de sécurité.** Chacune des six dimensions est notée. La résilience des sauvegardes est mesurée par rapport à la norme 3-2-1-1-0. La couverture de chiffrement est cartographiée par volume et type de données. Les comptes dormants sont listés avec leurs niveaux de privilèges et leurs dernières dates de connexion. Les fichiers ROT sont croisés avec le scan des données d'identité — « ces 2 340 fichiers obsolètes contiennent toujours 847 enregistrements de données d'identité. »

**La brèche qui n'a pas encore eu lieu — quantifiée.** La simulation d'impact de brèche calcule ce qu'une brèche coûterait en fonction de votre profil de données réel — nombre de personnes affectées, types de données d'identité exposés, amende RGPD/CCPA estimée, coûts de notification. Ce n'est pas une simulation d'attaque d'infrastructure (c'est ce que les outils BAS font à 50 000 €+/an). C'est une projection d'impact centrée sur les données basée sur ce que votre scan a réellement trouvé.

**Corrigez d'abord la pire lacune.** Chaque action corrective (P1/P2/P3) montre quelle dimension elle améliore, quelle lacune spécifique elle ferme et quel impact sur votre note de posture globale. « Activer la sauvegarde immuable sur le serveur X → La résilience des sauvegardes passe de D à B, l'exposition aux ransomwares baisse de 40%. »

Chaque note est transparente, reproductible et publiée. Pas de boîte noire.

---

## LA COMPARAISON DES PRIX

| | SIEM/EDR/XDR | BAS (SIMULATION DE BRÈCHE ET D'ATTAQUE) | AUDIT DE CONSEIL | APOLLO DATA AUDITOR |
|---|---|---|---|---|
| **Coût annuel** | 50 000 $ – 500 000 $ | 50 000 $ – 200 000 $ | 10 000 € – 50 000 € par mission | **2 999 € / an** (Starter) |
| **Audite la posture de protection des données** | Non (surveille l'infrastructure) | Non (teste les chemins d'attaque) | Partiel (entretiens) | **Oui — 6 dimensions notées** |
| **Impact de brèche sur données réelles** | Non | Non (centré sur l'infrastructure) | Non (théorique) | **Oui — simulation centrée sur données** |
| **Corrélation ROT × données d'identité** | Non | Non | Non | **Oui** |
| **Déploiement** | Semaines à mois | Semaines | 4–8 semaines | **Moins de 48 heures** |

---

## 5. UN SCAN. UNE RÉPONSE. QUATRE DIMENSIONS.

La protection des données n'est pas une préoccupation isolée. Les données d'identité non chiffrées sont à la fois une lacune de protection et une violation de conformité. Un compte administrateur dormant est à la fois un risque de sécurité et une exposition financière. Une base de données obsolète remplie de données personnelles est à la fois un problème d'hygiène des données et un bloqueur de préparation à l'IA.

La plupart des PME traitent ces problèmes comme des problèmes séparés — un outil pour les sauvegardes, un autre pour la conformité, un tiers pour la surveillance de la sécurité, un consultant pour l'audit. Le coût combiné dépasse 100 000 €/an. Ce n'est pas réaliste pour une entreprise de 200 employés sans RSSI dédiée.

APOLLO a été construit pour répondre à toutes ces questions en un scan, à un prix qui reflète la réalité des PME.

→ **Risque Protection** — ce que ce document couvre. Résilience des sauvegardes, couverture de chiffrement, préparation aux ransomwares, hygiène du contrôle d'accès, identification des données ROT, simulation d'impact de brèche.

→ **Risque Privacy** — quantification financière en € et $, simulation d'impact de brèche, cartographie des données d'identité, combinaisons toxiques, zones à risque.

→ **Risque Conformité** — RGPD noté par article (Art. 5, 9, 30, 32), CCPA, NIS2, SOC2, DORA. Notes de A à F basées sur les données réelles. Plan de remédiation avec impact financier par action.

→ **Qualité & IA** — 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).

Aucun autre outil sous 5 000 €/an ne couvre tous les quatre. Le marché de la cybersécurité a été construit autour de la surveillance réactive pour les entreprises. **APOLLO™ Data Auditor** existe parce que les PME ont besoin de réponses proactives sur leurs données — avant l'attaque, pas après.

---

*Sources : Veeam Data Protection Trends 2024 & 2025 · Sophos State of Ransomware 2025 · Verizon DBIR 2025 · Palo Alto Unit 42 Incident Response Report 2026 · IBM Cost of a Data Breach 2025 · Enzoic AD Password Security Report 2025 · Orange Cyberdefense PME France 2025 · Mastercard SMB Study 2025 · CNIL Bilan sanctions 2025 · Fortune Business Insights BAS Market 2026*

---

**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