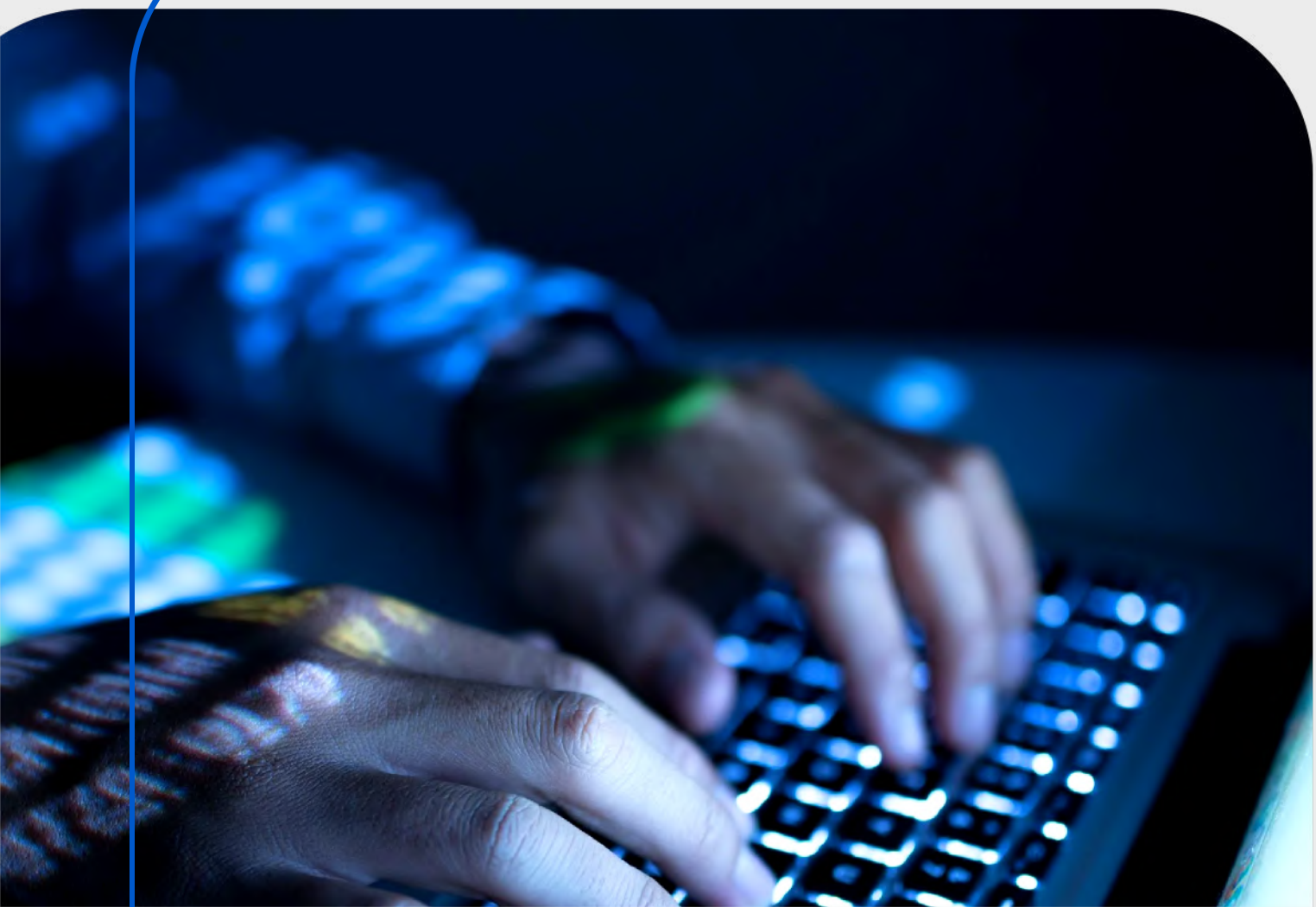
PRIVAL®

Checklist de préparation des données pour l'IA générative



PRIVAL

Contenu

La transition

Prêt à gérer la transition vers les données non structurées ?

Gartner prédit que d'ici fin 2026, 75 % des organisations réorienteront leurs dépenses de sécurité vers les données non structurées (fichiers, chats, médias) pour faire face aux risques posés par l'IA générative. Cette redéfinition des priorités découle de l'adoption rapide et souvent non réglementée des outils d'IA générative au sein des entreprises.

Pour aider les responsables TI à atténuer ces risques, nous avons élaboré une checklist que vous pouvez utiliser pour évaluer si votre organisation est prête à gérer la prolifération des données qui accompagne l'adoption de l'IA.

1. Visibilité

Trouver le Shadow AI

Vous ne pouvez pas protéger ce que vous ne pouvez pas voir. Les applications d'IA générative contournent souvent les contrôles périmétriques traditionnels et créent des référentiels de données inconnus.

- ☐ Identifiez les données inconnues

  Avez-vous un outil de gestion de posture de sécurité des données (DSPM) pour identifier les référentiels inconnus dans des environnements multicloud?

- ☐ Cartographier les flux de données de l'IA.

  Avez-vous identifié précisément quels types de données sensibles (informations personnelles, propriété intellectuelle) alimentent vos modèles d'IA ou vos agents d'IA tiers ?

- ☐ Établir les critères d'une utilisation acceptable

  Y a-t-il une politique claire limitant l'utilisation des chatbots publics d'IA générative tant que des contrôles de niveau entreprise ne sont pas en place ?

⚠ Les responsables de la sécurité croient souvent savoir où résident les données sensibles. Pourtant, sans vérification auprès des services concernés, ils risquent de mal identifier les actifs et de créer des failles de conformité.

2. Gouvernance

Simplifier les règles

La complexité est l'ennemie de la sécurité. Si les politiques sont trop difficiles à suivre, les utilisateurs les ignoreront, surtout lorsqu'ils utilisent des outils d'IA.

- [ ] Limiter les niveaux de classification

  Avez-vous simplifié votre schéma à seulement 3 ou 4 niveaux (par exemple, public, interne, confidentiel, secret) ? Les matrices complexes conduisent souvent à des erreurs.

- [ ] Découverte hybride

  Combinez-vous la découverte automatisée avec des entrevues pour comprendre le contexte de vos données, plutôt que de vous fier uniquement à l'automatisation ?

- [ ] Séparer la stratégie des tactiques

  Avez-vous une politique de classification des données de haut niveau (le Quoi) distincte d'une ligne directrice détaillée sur le traitement des données (le Comment)? Cela vous permet de mettre à jour les procédures techniques pour les nouveaux outils d'IA sans réécrire l'ensemble de la politique.

Selon le rapport Verizon Data Breach Investigations 2025, près de 50 % des pertes de données sont dues à des employés envoyant par erreur des données sensibles à la mauvaise personne.

3. Détection

Arrêter les fuites et réduire le bruit

Le DLP traditionnel bloque souvent le travail légitime ou noie les équipes dans de faux positifs. Le DLP moderne se concentre sur l'intention de l'utilisateur.

- [ ] Passer à la détection basée sur l'intention

  Utilisez-vous du User and Entity Behavior Analytics (UEBA) pour signaler les comportements risqués plutôt que d'utiliser des mots-clés ? Cela peut réduire les risques d'initiés d'un tiers.

- [ ] Consolider vos agents

- [ ] Êtes-vous passé au DLP intégré (dans vos plates-formes Endpoint ou Cloud existantes) pour réduire le coût et la complexité de la gestion d'agents séparés ?

- [ ] Surveiller les agents d'IA

  Vos outils actuels peuvent-ils détecter les anomalies spécifiquement dans la façon dont les agents d'IA interagissent avec vos données, et pas seulement les utilisateurs humains ?

4. Protection

Sécuriser les données pour l'IA

Le DLP est réactif. Vous devez également sécuriser les données elles-mêmes afin qu'elles restent sécurisées même si elles quittent votre réseau.

- [ ] Masquer les données dédiées à l'entraînement

  Utilisez-vous le masquage des données ou des données synthétiques pour désidentifier les informations sensibles avant qu'elles n'entrent dans des environnements utilisés par l'IA ?

- [ ] Crypter les données au repos

  Utilisez-vous un système Enterprise Key Management (EKM) pour sécuriser les données où qu'elles se trouvent ? Cela garantit que la protection suit le fichier, même lorsqu'il dépasse les limites du DLP.

5. Évaluation

0–3 : Risque élevé. Vos données non structurées sont probablement exposées.
4–7 : Place a l'amélioration. Vous avez des bases en place.
8–11 : Vous êtes presque prêt pour adopter l'IA.

PRIVAL

Conclusion

L'adoption de l'IA générative (GenAI) redéfinit les périmètres de sécurité traditionnels et engendre un réseau complexe de données non structurées et d'actifs invisibles.

Combler ces lacunes en matière de visibilité et de gouvernance devient une priorité incontournable.

En y parvenant, vous transformez la sécurité des données d'un frein bureaucratique en un atout stratégique, favorisant une innovation rapide et sécurisée.

Prêt à mettre à jour la sécurité de vos données ? Connectez avec nous

À propos de PRIVAL

Depuis plus de 20 ans, nous aidons les entreprises québécoises à maintenir leur informatique à jour grâce à des produits et services spécialisés.