Livre blanc

L'IA : accélérateur d'un problème de confiance numérique

Pourquoi l'identité connectée, les transactions fiables et les données vérifiables sont les fondements d'une IA responsable

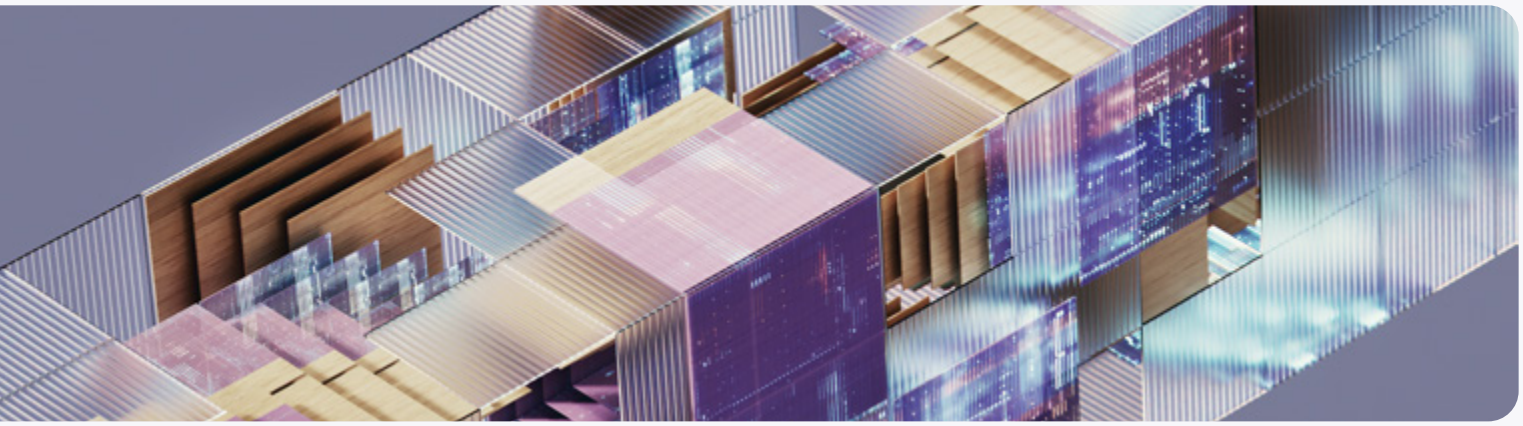
PORTAGE cybertech

portagecybertech.com

info@portagecybertech.com

Résumé

L’IA ne résoudra pas la fragmentation de la confiance. Elle risque plutôt de l’amplifier.



Qu’il s’agisse de rédiger un courriel rapide, de choisir un nouveau restaurant ou de planifier un voyage dans plusieurs pays, nous sommes nombreux à consulter un assistant d’IA avant même de nous tourner vers une autre personne. Que ce soit par l’entremise de ChatGPT, Claude, Gemini ou Copilot, l’IA est passée du statut de nouveauté à celui de nécessité en un temps remarquablement court.

Les gouvernements et les organisations réglementées ressentent la même pression. Les citoyens, les clients et les employés s’attendent à des services numériques plus rapides et plus personnalisés, tandis que les dirigeants doivent gagner en efficacité, maîtriser les risques et faire plus avec des ressources limitées. L’IA peut aider à acheminer les dossiers, à résumer des éléments de preuve, à déceler des tendances, à accélérer les transactions et à appuyer la prise de décision d’une manière qu’aucune équipe humaine ne pourrait égaler. Ce potentiel est bien réel. La pression d’agir rapidement l’est tout autant. Le danger réside dans la confusion entre vitesse et préparation.

L’IA amplifie les capacités existantes; elle ne corrige pas les problèmes sous-jacents. Elle ne peut corriger, à elle seule, une identité fragmentée, des flux de travail déconnectés, des preuves insuffisantes ou des données non vérifiées. En réalité, elle risque de rendre ces failles plus difficiles à détecter tout en en aggravant les effets.

L’intégration réussie de l’IA repose sur un contexte cohérent. Or, de nombreuses organisations ne disposent pas de ce contexte. Les utilisateurs doivent prouver leur identité à maintes reprises. Les transactions critiques demeurent manuelles, fortement tributaires du papier ou juridiquement peu fiables. Les données restent cloisonnées entre systèmes, programmes et administrations. Ces défaillances de l’expérience utilisateur, des processus et de l’infrastructure érodent la confiance numérique et augmentent considérablement les risques associés au déploiement de l’IA à grande échelle.

Une IA responsable commence avant même le modèle. Elle repose d’abord sur la confiance numérique : la capacité d’établir quel acteur intervient, d’appliquer le niveau d’assurance approprié, d’autoriser l’action, de protéger la transaction, de vérifier le document ou le résultat, de préserver les preuves et de favoriser une prise de décision éclairée.

L’objectif est de créer une chaîne continue qui relie la vérification de l’identité à l’action, puis au résultat. Une fois cette chaîne en place, l’IA peut améliorer la prestation des services tout en préservant la responsabilité, la fiabilité juridique et la confiance du public. Sans cette chaîne, l’IA ne fera qu’automatiser l’incertitude.

#1 Le problème de la confiance numérique existait déjà

Des systèmes fragmentés engendrent une fragmentation de la confiance.

La transformation numérique a donné naissance à des outils impressionnants, mais pas toujours à une expérience cohérente. Derrière un formulaire Web soigné peuvent encore se cacher plusieurs comptes, des saisies répétitives, des pièces jointes transmises par courriel et une bonne dose de connaissance institutionnelle pour mener à bien une seule transaction.

Les citoyens, les clients, les entreprises et les professionnels ne voient pas ces systèmes en arrière-plan. Ils vivent un parcours unique. Lorsqu'ils doivent prouver à nouveau leur identité, soumettre deux fois les mêmes renseignements, passer d'un service à l'autre ou perdre la trace de ce qu'est devenu un document signé, les cloisonnements internes deviennent perceptibles sous forme de frictions. Si cela se répète suffisamment souvent, les utilisateurs commencent à se demander si quelqu'un est aux commandes.

C'est pourquoi la confiance numérique va au-delà de la simple technologie. Elle repose sur l'attente que les personnes, les processus, les systèmes et les éléments de preuve fonctionnent de manière harmonieuse et conforme aux attentes. Les principaux cadres de confiance considèrent la confiance numérique comme une capacité de l'écosystème fondée sur l'interopérabilité, la protection de la vie privée, la sécurité, la gouvernance et des preuves fiables.

Trois types de défaillances se renforcent mutuellement :

- **Défaillance de l'expérience utilisateur :** les utilisateurs perdent confiance lorsque les services sont incohérents et difficiles à utiliser.
- **Défaillance des processus :** des flux de travail lourds, inefficaces ou opaques affaiblissent la responsabilisation.
- **Défaillance de l'infrastructure :** des systèmes déconnectés et des données cloisonnées empêchent d'obtenir des résultats fiables d'une organisation ou d'une administration à l'autre.

À mesure que la confiance s'effrite, les frictions augmentent et le doute s'installe.

#2 L'IA amplifie le problème

L'IA accélère la fragmentation de la confiance sans la corriger.

L'IA peut améliorer l'expérience d'un service donné, mais elle ne peut pas, à elle seule, assurer la continuité de l'identité entre des services fragmentés. Un assistant conversationnel peut répondre parfaitement à une question, alors que l'utilisateur doit toujours jongler avec trois comptes pour accomplir la même démarche.

L'IA peut également accélérer une transaction, mais la rapidité ne permet pas de vérifier si la personne qui agit est autorisée à le faire ou si l'action requiert un niveau d'assurance plus élevé. Ces questions doivent être intégrées dès la conception du flux de travail.

L'IA peut générer des recommandations, acheminer des dossiers et signaler des risques. Mais lorsque les données sous-jacentes sont incomplètes, non vérifiées ou déconnectées, le résultat obtenu peut être difficile à expliquer, à contester ou à vérifier.

Le plus grand risque n'est pas simplement que l'IA commette une erreur. C'est que la fragmentation existante s'automatise, s'amplifie et devienne encore plus difficile à corriger. Une mauvaise décision prise une seule fois est un problème. La même décision, appliquée à des milliers de cas sans le niveau d'assurance requis et sans les garanties de confiance nécessaires, avant même que quiconque puisse reconstituer les raisons qui la sous-tendent, en est un bien plus grave. C'est ainsi que des fondations fragiles produisent de moins bons résultats, plus rapidement.

L'automatisation est merveilleusement impartiale : elle reproduit un mauvais processus avec exactement le même enthousiasme qu'un bon.

#3 L'IA rehausse les exigences en matière de preuve

La confiance ne peut plus reposer sur les apparences, la facilité ou des pistes de vérification isolées.

L'IA a considérablement réduit le coût de création de documents, de rapports, de contrats, de dessins, de sceaux et même d'usurpations d'identité numériques crédibles. Une mise en page soignée, un logo familier ou une image de signature réaliste peuvent sembler rassurants. Malheureusement, il n'a jamais été aussi facile de créer une apparence de crédibilité.

À l'ère de l'IA, la crédibilité visuelle ne constitue plus une preuve d'authenticité. Les processus de signature à haut risque doivent établir trois éléments :

1. **Identité vérifiée :** Qui a signé, approuvé, soumis ou produit le document ?
2. **Intégrité du document :** Le contenu a-t-il été modifié depuis l'action validée ou autorisée ?
3. **Preuve durable :** La preuve demeure-t-elle vérifiable au fil des années ?

Les directives publiques sur l'IA générative et les médias synthétiques soulignent l'importance de contrôles plus rigoureux en matière d'identité, de provenance et de preuve.

Les normes de provenance du contenu, comme la C2PA, permettent d'établir l'origine d'un contenu numérique et de retracer ses modifications. Les programmes de confiance en matière de signature numérique et les normes de validation à long terme, comme la liste Adobe Approved Trust et la norme ETSI PAdES, peuvent contribuer à protéger l'intégrité, à établir un lien entre l'action de signature et le signataire, et à préserver des preuves vérifiables au fil du temps. Chacun de ces mécanismes répond à une partie du problème, mais l'intégrité de la chaîne de confiance repose toujours sur l'identité, l'autorisation, l'enregistrement de la transaction et la conservation de preuves durables, qui doivent fonctionner de concert.

Le processus de signature est tout aussi important que le fichier final. Une signature électronique de base peut parfaitement convenir à un consentement à faible risque. Une approbation réglementée, un dessin technique, un document officiel ou une transaction de grande valeur peut nécessiter une identité vérifiée, une authentification plus forte, une signature fondée sur un certificat numérique, une protection contre la falsification et une validation à long terme. Le niveau d'assurance doit être proportionnel à l'importance des enjeux.

La question n'est plus « Peut-on faire cela en ligne ? », mais plutôt : « Peut-on prouver qui l'a fait, ce qui s'est passé et si cette preuve demeure valide ? »

4 L’identité au fondement de la confiance numérique

Avant que l’IA puisse agir de manière responsable, les organisations doivent savoir qui agit et à quel titre.

L’identité est le point de départ d’un environnement de confiance. Elle devrait guider les décisions d’accès, les autorisations de transaction, les droits de signature, l’utilisation des données et le niveau d’assurance associé aux résultats qui en découlent.

Cela ne signifie pas pour autant qu’il faille imposer un maximum de frictions partout. Les lignes directrices du NIST sur l’identité numérique font la distinction entre la vérification de l’identité, l’authentification et la fédération, et appuient des choix d’assurance qui tiennent compte du risque. Les interactions à faible risque devraient rester simples. Les actions à risque plus élevé devraient déclencher des contrôles plus rigoureux en matière de vérification, d’authentification, d’autorisation ou de signature. Toutes les portes n’ont pas besoin du niveau de protection d’un coffre-fort bancaire. L’important est de savoir quelles portes mènent à un tel coffre-fort.

Le modèle de données des identifiants vérifiables du W3C offre aux émetteurs, aux détenteurs et aux vérificateurs un moyen normalisé d’échanger des déclarations inviolables. Les identifiants réutilisables permettent de transmettre des renseignements vérifiés d’un service à l’autre sans obliger les utilisateurs à recommencer le processus. Cela permet un parcours plus fluide tout en maintenant l’assurance liée à la politique et au risque.

Voici une démarche pratique axée sur l’identité :

1. Vérifier et établir l’identité
2. Émettre et associer les identifiants
3. Établir, fédérer et échanger la confiance
4. Appliquer le niveau d’assurance approprié
5. Évaluer le risque et la fiabilité
6. Orchestrer les interactions de confiance
7. Fournir les éléments probants nécessaires à des décisions fiables

L’identité ne résume pas à elle seule le modèle de confiance numérique, mais elle en constitue le fondement. Une fois l’identité et le niveau d’assurance établis, ce contexte peut s’étendre à l’accès, aux transactions, aux documents, aux éléments probants et à la prise de décision.

Lorsque l’IA agit au sein du flux de travail

À mesure que l’IA passe de la génération de contenu à l’exécution d’actions, certains agents pourraient avoir besoin de leur propre identité non humaine (NHI), encadrée par des mécanismes de gouvernance. Contrairement aux utilisateurs humains, dont l’accès est généralement lié à une personne et à un rôle connus, les agents d’IA peuvent interagir avec de multiples systèmes, API et entrepôts de données tout en agissant sous une autorité déléguée. Cela crée un périmètre d’identité plus vaste et plus complexe, qui exige des droits d’accès soigneusement définis et une chaîne de délégation claire.

Cela ne fait pas de l’IA une personne et ne décharge pas les humains de leur responsabilité. Cela permet à l’organisation d’identifier l’agent, de définir ses autorisations, de limiter sa portée, de consigner l’origine de cette délégation, de vérifier les actions effectuées et de révoquer l’accès au besoin.

Dans les flux de travail à haut risque, un agent d’IA ne devrait pas être invisible ni impossible à distinguer de la personne ou de l’organisation qu’il soutient. L’agent peut disposer de sa propre identité et de droits d’accès, mais la responsabilité doit toujours incomber à la personne et à l’organisation qui l’ont mandaté.

#5 Le modèle de confiance numérique connecté

L'identité, les transactions et les données fiables doivent évoluer de concert.

La confiance numérique connectée réunit ces composantes au sein d'un modèle opérationnel unique plutôt que de les considérer comme des outils distincts. Une identité continue, des transactions fiables et l'échange de données de confiance constituent trois capacités qui se renforcent mutuellement et favorisent une IA responsable ainsi qu'une prise de décision plus éclairée.

Identité continue

Les utilisateurs passent d'un service à l'autre grâce à une identité et à des identifiants fiables et réutilisables.

Transactions fiables

Les flux de travail deviennent sensibles au risque, autorisés, vérifiables et juridiquement fiables lorsque nécessaire.

Échange de données fiables

Les renseignements vérifiés circulent entre systèmes, organisations et administrations, tout en conservant leur provenance, le consentement et les règles qui leur sont associées.

IA responsable et meilleures décisions

Un contexte fiable favorise une automatisation plus sûre, des résultats vérifiables et une prise de décision responsable.

À mesure que ces capacités s'intègrent davantage, l'IA peut améliorer l'expérience utilisateur, évaluer les risques, automatiser les services, produire des résultats fiables et favoriser une prise de décision mieux éclairée. Elle s'appuie sur un contexte fiable, sous supervision humaine, avec les mécanismes de traçabilité et les éléments probants nécessaires à la vérification des résultats.

Un paysage de confiance numérique en pleine convergence

Différents secteurs se retrouvent à la même croisée des chemins en matière de confiance numérique.

Les fournisseurs d'identité étendent leurs activités à l'autorisation des agents d'IA. Les plateformes de signature numérique intègrent désormais la vérification d'identité et l'intelligence des flux de travail. Les plateformes d'entreprise intègrent des agents d'IA dans les processus d'affaires et les environnements de données. Les fournisseurs de services de confiance, de traçabilité et de gouvernance renforcent les mécanismes permettant de démontrer l'intégrité et l'authenticité des systèmes, du contenu et des données.

Cette convergence montre que la confiance devient une couche de contrôle essentielle autour des flux de travail alimentés par l'IA. Elle met également en évidence une lacune : de nombreuses approches commencent et se terminent encore par la partie de la pile technologique dont elles disposent déjà.

Les gouvernements et les organisations réglementées fonctionnent rarement au sein d'une seule plateforme. Leurs services chevauchent les ministères, les fournisseurs, les professions, les organisations et les juridictions. La confiance doit donc accompagner la personne ou l'agent, la transaction, le document, les données et les preuves.

La gouvernance des modèles et l'automatisation des flux de travail sont essentielles, mais ni l'une ni l'autre ne peuvent créer des preuves que le processus sous-jacent n'a jamais produites. L'identité, les transactions, les documents et les données fiables doivent fonctionner ensemble au sein d'un modèle de confiance cohérent.

#6 Une IA responsable repose sur l'imputabilité humaine

L'IA recommande ou agit. Les humains demeurent responsables. La chaîne de preuve demeure intacte.

On aborde souvent l'IA responsable sous l'angle du modèle : équité, sécurité, explicabilité et robustesse. Ces qualités sont importantes, mais elles ne régissent pas l'ensemble du flux de travail. Elles n'indiquent pas qui a autorisé l'action et/ou qui l'a exécutée, quelles données l'ont influencée, quelle transaction en a découlé ni si le document produit est demeuré intact.

La Directive canadienne sur la prise de décision automatisée s'applique non seulement aux décisions entièrement automatisées, mais aussi aux recommandations, aux cotes, aux résumés et aux autres résultats qui contribuent aux décisions administratives. Les Principes de l'OCDE sur l'IA mettent également l'accent sur la transparence, la traçabilité, la robustesse et la responsabilité. Dans le cas des systèmes agentiques, le Forum économique mondial présente la gouvernance comme un ensemble de droits décisionnels délégués assortis de limites clairement applicables. La responsabilité doit s'étendre au-delà du modèle pour englober le flux de travail qui l'entoure.

La présence d'un « humain dans la boucle » ne constitue pas une stratégie de gouvernance. Si une personne reçoit une recommandation opaque, n'a aucun moyen réel de la remettre en question et ne laisse aucune trace liée à sa décision, cette intervention humaine risque de n'être qu'une simple formalité.

Les flux de travail responsables devraient préserver une chaîne traçable :

- qui est à l'origine de l'action;
- qui a autorisé l'action;
- quelles données et quelle politique ont été utilisées;
- quelle transaction, recommandation ou quel document en a résulté;
- quel examen humain a été effectué;
- quelles preuves subsistent.

Dans un cadre clair et bien défini, l'IA peut formuler des recommandations ou agir. Les personnes et les institutions demeurent responsables du service, des politiques appliquées et des conséquences qui en découlent. Les éléments de preuve permettent de rendre cette responsabilité visible et démontrable.

La fiabilité d'une IA responsable dépend de celle de l'identité, des transactions, des données et des éléments de preuve sur lesquels elle repose.

#7 Des services fragmentés à des résultats vérifiables et à de meilleures décisions

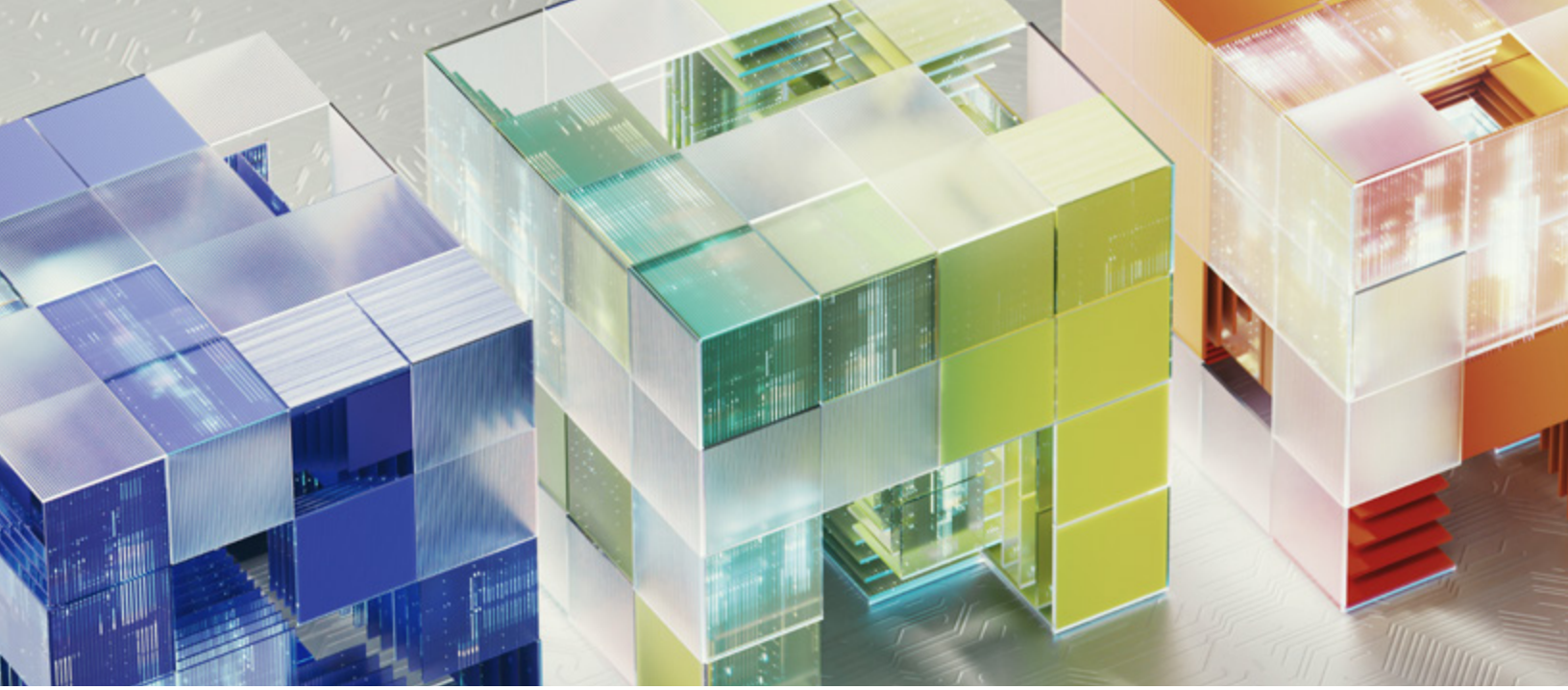
Un parcours de maturité vers une transformation numérique et une prise de décision dignes de confiance.

La confiance numérique connectée s'acquiert par étapes. Les organisations n'ont pas besoin de tout reconstruire d'un seul coup, mais chaque étape devrait rendre la suivante plus sûre, plus efficace, plus utile et plus facile à régir.

Étape	Capacité de confiance	Valeur de l'IA libérée
Consolider l'accès	Une identité unique pour tous les services	L'IA peut contribuer à un parcours utilisateur plus fluide.
Numériser les transactions	Flux de travail fiables et traçables	L'IA peut apporter son aide sans compromettre la responsabilité.
Mettre en place des identifiants de confiance	Preuves d'identité et identifiants réutilisables	L'IA peut personnaliser ou acheminer les services en s'appuyant sur un contexte plus riche.
Personnaliser les services	Consentement, préférences, admissibilité et contexte d'identité	L'IA peut proposer des recommandations pertinentes sans se fonder uniquement sur des hypothèses fragmentées.
Appliquer une assurance fondée sur le risque	Assurance adaptée au risque	L'IA peut aider à évaluer le contexte et à déclencher les contrôles appropriés.
Automatiser les services en ligne	Règles claires, autorisation et traçabilité	L'IA peut réduire les frictions tout en préservant la responsabilisation.
Permettre l'échange de données fiables	Des données vérifiées entre les systèmes	L'IA peut agir en s'appuyant sur des renseignements de meilleure qualité.
Prendre de meilleures décisions	**Une identité de confiance, des données fiables, des transactions vérifiables et des preuves durables intégrées à chaque étape du parcours de service**	**L'IA peut appuyer les recommandations et les décisions en s'appuyant sur un contexte plus solide, tandis que les humains conservent la responsabilité**

Les résultats vérifiables ne constituent pas la ligne d'arrivée. Ils constituent le fondement probant de décisions plus éclairées. Lorsqu'une organisation peut avoir confiance dans l'identité des personnes concernées, dans les autorisations qui leur sont accordées, dans les données utilisées, dans ce qui a été signé ou approuvé, ainsi que dans les preuves qui subsistent, tant les humains que les systèmes d'IA peuvent agir avec davantage de clarté et de contexte.

La qualité d'une décision ne repose pas uniquement sur la performance d'un modèle. Elle dépend de données d'entrée fiables, de règles claires, de transactions dignes de confiance et de preuves pouvant résister à un examen minutieux.



#8 Le point de vue de Portage CyberTech

Une base de confiance numérique connectée pour les gouvernements et les organisations réglementées.

Portage CyberTech aide les gouvernements et les organisations réglementées à intégrer la confiance numérique à l'ensemble du parcours de service.

Cette base peut s'appuyer sur CitizenOne, une plateforme de gestion des identités et des accès client (CIAM) de calibre gouvernemental qui prend en charge l'identité de confiance et l'accès sécurisé à travers tous les services et canaux. CertifiO ID ajoute une vérification d'identité à haut niveau de garantie, adaptée au risque lié à la transaction. CertifiO associe une personne vérifiée et, le cas échéant, son affiliation professionnelle à une signature numérique hautement sécurisée. ConsignO Cloud prend en charge les flux de travail de signature sécurisés, l'assurance configurable, l'intégrité des documents et les preuves d'audit.

La valeur ne réside pas dans la séquence des produits. Elle réside dans la continuité dela confiance :

Identité vérifiée → Niveau d'assurance approprié → Action autorisée → Document fiable → Preuve durable → Décision défendable

Portage rassemble ces exigences de confiance au sein d'un modèle opérationnel unique : vérifier l'identité et l'associer à une personne ou à un agent; relier cette identité à ce à quoi elle peut accéder, signer, approuver ou initier; définir les preuves qu'un flux de travail réglementé doit conserver; et permettre à la confiance de s'étendre d'une organisation à l'autre et d'une juridiction à l'autre.

Pour le secteur public et les services réglementés, ce lien transforme l'automatisation en prestation de services responsable et les résultats fiables en décisions défendables.

#9 Les prochaines étapes pour les dirigeants

Évaluer où l'IA pourrait accentuer les lacunes existantes en matière de confiance.

Avant de déployer l'IA à grande échelle, cartographiez la chaîne de confiance associée aux flux de travail qu'elle touchera. Posez-vous les questions suivantes :

1. Pouvez-vous vérifier avec certitude que chaque utilisateur correspond à une personne dont l'identité a été dûment vérifiée ?
2. Dans quels cas les utilisateurs doivent-ils encore gérer des comptes distincts, se soumettre à des vérifications d'identité répétées ou utiliser des identifiants non reliés ?
3. Quelles transactions nécessitent une assurance plus solide en raison du risque, de la valeur, de la sensibilité ou des conséquences juridiques ?
4. Quels flux documentaires reposent encore sur l'apparence, des fichiers PDF ou des pistes de vérification limitées plutôt que sur des preuves cryptographiques ?
5. Où les données sont-elles fragmentées entre les systèmes, les organisations ou les juridictions ?
6. Où l'IA risque-t-elle d'automatiser un processus défaillant plutôt que d'en améliorer les résultats ?
7. Quelles décisions, recommandations, signatures ou approbations nécessitent des preuves durables ?
8. Quel niveau d'assurance devrait s'appliquer à chaque service ou flux de travail majeur ?
9. Dans quels cas les agents d'IA pourraient-ils nécessiter leur propre identité, leur propre champ d'application, leur propre mécanisme de délégation, leur propre traçabilité ou leur propre processus de révocation ?
10. Quelles décisions gagneraient à ce que l'identité, les transactions, les données, les documents et les éléments de preuve soient reliés tout au long du flux de travail ?

Accordez ensuite la priorité aux services où l'identité, les transactions, les documents, les données et l'IA se croisent. Renforcez la chaîne de confiance avant d'accélérer le processus.

L'IA transformera la prestation des services numériques. Les organisations qui en tireront le plus grand bénéfice seront celles qui sauront vérifier l'identité de l'acteur, confirmer l'autorité à l'origine de l'action, retracer les données et les transactions, préserver les documents et les éléments de preuve, puis mettre ce contexte au service de décisions plus éclairées.

Appendix: References and Source Notes

1. Institut national des normes et de la technologie (NIST). Cadre de gestion des risques liés à l'IA (AI RMF 1.0). Cadre principal de gestion des risques.
2. Forum économique mondial. Mesurer la confiance numérique : appuyer la prise de décision en faveur de technologies dignes de confiance. Cadre de référence sur la confiance numérique.
3. Conseil canadien de l'identification numérique et de l'authentification (DIACC). Cadre pancanadien de confiance.
4. Institut national des normes et de la technologie (NIST). Cadre de gestion des risques liés à l'intelligence artificielle : profil pour l'intelligence artificielle générative (NIST AI 600-1). Lignes directrices relatives aux risques associés à l'IA générative.
5. NSA, FBI, et CISA. Mise en contexte des menaces liées aux hypertrucages pour les organisations. Lignes directrices relatives aux menaces associées aux médias synthétiques.
6. Coalition for Content Provenance and Authenticity (C2PA). Spécification technique de la C2PA. Norme relative à la provenance du contenu.
7. Liste de confiance approuvée par Adobe. Infrastructure de confiance fondée sur les certificats pour les signatures numériques.
8. Institut européen des normes de télécommunication (ETSI). Profil PAdES de validation à long terme (ETSI TS 102 778-4). Norme de validation des signatures numériques.
9. Institut national des normes et de la technologie (NIST). Lignes directrices sur l'identité numérique, SP 800-63-4. Lignes directrices sur la vérification de l'identité, l'authentification et la fédération.
10. World Wide Web Consortium (W3C). Modèle de données des identifiants vérifiables v2.0. Norme technique relative aux attestations vérifiables.
11. Gouvernement du Canada. Guide sur la portée de la Directive sur la prise de décision automatisée. Lignes directrices relatives à la prise de décision et à l'imputabilité dans le secteur public.
12. Organisation de la coopération et du développement économiques (OCDE). Principes de l'OCDE en matière d'IA. Principes internationaux pour une IA digne de confiance.
13. Forum économique mondial. Des systèmes d'enregistrement aux systèmes de confiance : Guide à l'intention des conseils d'administration pour la gouvernance de l'IA agentique. Lignes directrices destinées aux dirigeants sur les droits décisionnels délégués et les limites de la gouvernance.

Établissez la confiance numérique à l'échelle de votre organisation

Portage CyberTech peut évaluer où l'IA risque d'amplifier les lacunes liées à l'identité, aux transactions, aux documents, aux données et aux éléments de preuve.

À titre de fournisseur de solutions de confiance numérique connectée destinées aux gouvernements et aux organisations réglementées, nous contribuons à renforcer les fondements d'une automatisation responsable, de résultats vérifiables et d'une prise de décision éclairée.

Communiquez avec Portage CyberTech pour obtenir une évaluation de votre chaîne de confiance numérique à l'ère de l'IA.
https://www.portagecybertech.com/fr/nous-joindre

Pronchaines étapes ?
Des questions ?

Découvrez les solutions de Portage CyberTech.

Ou réservez une consultation avec l'un des nos experts pour explorer comment nos solutions peuvent bénéficier à votre municipalité.