Kiteworks

SOLUTION BRIEF

Kiteworks Compliant AI

Gouvernance au niveau des données pour les agents IA
Accès aux données réglementées

Les agents IA deviennent les nouveaux collaborateurs numériques : ils accèdent à des données financières, médicales, CUI et secrets commerciaux à la vitesse de la machine. Contrairement aux collaborateurs humains, les agents ne font preuve d'aucun discernement et accèdent à toute donnée ou exécutent toute fonction, sauf si on leur interdit explicitement.

Des réglementations telles que HIPAA, CMMC/ITAR, PCI DSS, SEC et SOX imposent des contrôles stricts sur l'accès aux données, la traçabilité et le chiffrement. Ces exigences s'appliquent également aux agents IA qui accèdent à des données réglementées.

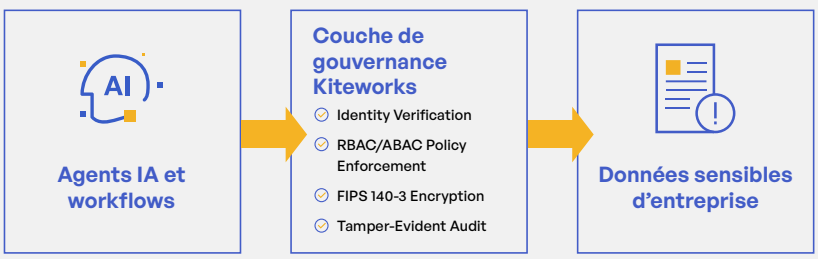
Gouvernance au niveau des données : le seul niveau que les agents IA ne peuvent pas contourner

Kiteworks Compliant AI régule les interactions des agents au niveau des données, et non au niveau du modèle. Les prompts et filtres de sécurité du modèle peuvent être contournés ; l'application des règles au niveau des données, non.

Chaque interaction d'agent passe par quatre points de contrôle :

- **Identité authentifiée :** Les agents sont vérifiés via OAuth 2.0 et reliés à la personne ayant délégué le workflow.
- **Accès soumis à des règles (ABAC) :** Les demandes sont évaluées en temps réel selon l'identité de l'agent, la classification des données et le contexte. L'accès minimum nécessaire est appliqué à chaque opération.
- **Chiffrement validé FIPS 140-3 :** Toutes les données auxquelles les agents accèdent sont chiffrées en transit et au repos avec des modules cryptographiques validés.
- **Traçabilité inviolable :** Chaque interaction est enregistrée avec attribution complète et transmise en temps réel au SIEM.

Là où l'IA devient conforme



La conformité est intégrée à l'architecture, pas ajoutée après le déploiement.

Solution

Gère l'accès des agents IA aux données sensibles au niveau des données, indépendamment du modèle, du prompt ou du framework agent

Chiffrement validé FIPS 140-3 pour toutes les données accédées par les agents, en transit et au repos

FedRAMP Moderate autorisé ; FedRAMP High en cours

Trois "Governed Assists" disponibles à l'achat via MCP pour les workflows réglementés

Compatible avec Claude, Copilot et tout LLM compatible MCP

Trois Governed Assists : workflows IA prêts pour la conformité

Kiteworks Compliant AI propose trois Governed Assists, des fonctions distinctes et disponibles à l'achat, propulsées par le Model Context Protocol (MCP) et régulées de bout en bout par le moteur de règles de données Kiteworks. Chaque opération est vérifiée par l'identité, évaluée par ABAC, chiffrée FIPS 140-3 et enregistrée de façon inviolable.

Governed Folder Operations Assist : Les agents IA naviguent, créent, renommant, déplacent et suppriment des arborescences de dossiers en langage naturel, chaque opération étant régulée par le moteur de règles. Les structures de dossiers héritent automatiquement des contrôles RBAC/ABAC, répondant aux exigences de séparation CUI (CMMC), de séparation des dossiers (HIPAA) et de provisionnement des espaces d'audit.

Cas d'usage : Structuration de portefeuilles clients · Séparation des dossiers CUI · Provisionnement d'espaces d'audit · Espaces de conservation pour contentieux · Documentation d'essais cliniques

Governed File Management Assist : Les agents IA gèrent tout le cycle de vie des données — téléversement, téléchargement, lecture, création, déplacement, renommage, suppression — avec chaque opération régulée par le moteur de règles. Cela répond aux exigences de conservation (NARA, SOX), d'accès minimum nécessaire (HIPAA) et d'élimination (PCI).

Cas d'usage : Contrôles de conservation SOX · Vérification du marquage CUI · Conditionnement de rapports d'événements indésirables · Génération de logs de privilèges · Application des calendriers de conservation

Governed Forms Creation Assist : Les agents IA génèrent des formulaires de collecte de données régulés à partir de descriptions en langage naturel, supprimant la charge manuelle de création tout en garantissant que toutes les soumissions sont stockées selon les règles, avec héritage des contrôles RBAC/ABAC.

Cas d'usage : Collecte KYC/CDD · Déclaration d'incidents FISMA · Formulaires d'autorisation HIPAA · Questionnaires de qualification fournisseurs · Signalement de lanceurs d'alerte

Respectez sereinement les exigences d'audit et de gouvernance

- Montrez votre maîtrise des flux de données réglementées (CUI, PCI, PHI, PII, contenus soumis à la SEC)
- Faites correspondre l'activité des agents IA aux référentiels de conformité : HIPAA, CMMC, PCI DSS, SEC/SOX, RGPD, NIST CSF, ISO 27001
- Exportez des journaux d'audit unifiés et des reportings dédiés à la conformité IA pour les audits et la gestion des incidents
- Générez rapidement des dossiers de preuves IA prêts pour le conseil d'administration

Intégration transparente avec toute plateforme IA

Kiteworks Compliant AI fonctionne avec toute plateforme IA compatible MCP — Claude, Copilot et tout futur LLM prenant en charge le Model Context Protocol. La passerelle de données IA fournit des API REST pour les pipelines RAG et les workflows IA programmatiques. Déployez dans n'importe quel environnement — cloud, sur site ou hybride — avec une prise en charge multiplateforme pour Windows, macOS et Linux. Gouvernance standardisée, indépendante des fournisseurs, protégeant votre investissement quel que soit le choix de plateformes IA de votre organisation.