Kiteworks

FICHE SOLUTION

POUR LES RSSI, LES ÉQUIPES CONFORMITÉ ET SÉCURITÉ

Gouvernez chaque échange de données sensibles avec le Data Policy Engine

Politique définie une fois, appliquée à chaque échange de données sensibles, pour personnes et agents d'IA.

CMMC 2.0 | HIPAA / HITECH | RGPD / NIS 2 | ITAR / EAR | SOC 2 Type II | ISO 27001, 27017, 27018

FedRAMP Class D Agency Auth In Process (ex-High In Process) | FedRAMP Class C Certified (ex-Moderate Authorized)

Le défi

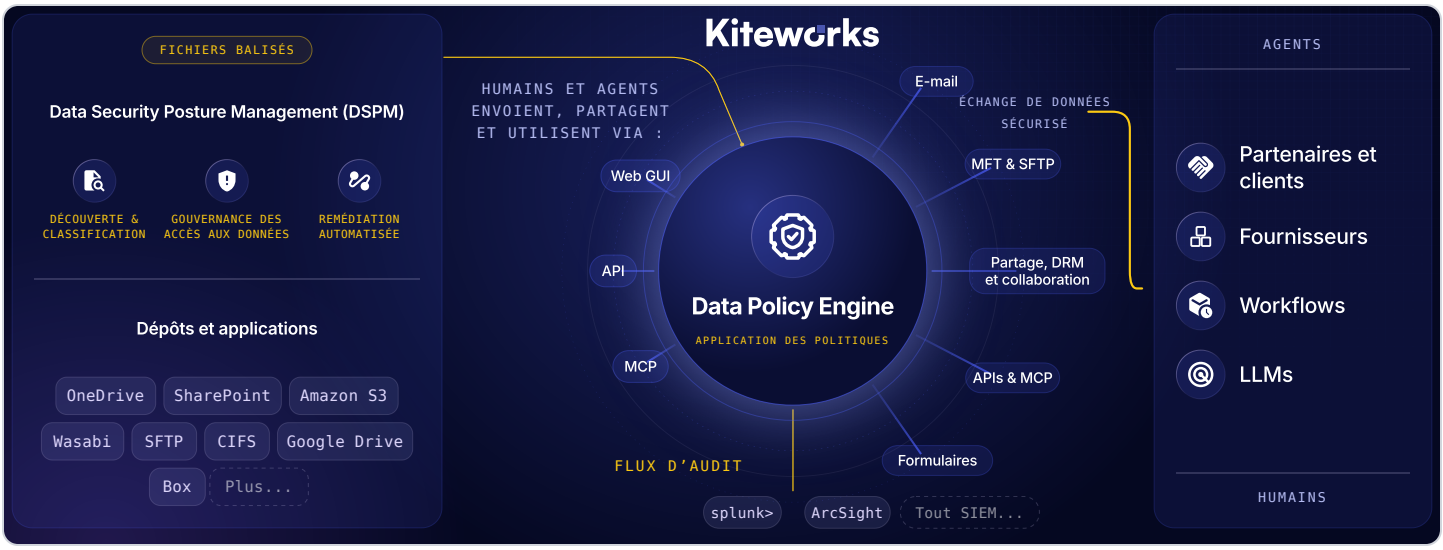
Agents d'IA, employés et parties externes demandent des données sensibles par les mêmes canaux : MCP, API, messagerie, formulaires, SFTP, partage de fichiers et MFT. Les outils traditionnels ont chacun leurs politiques et journaux. L'application des règles varie d'un canal à l'autre, des failles s'ouvrent entre eux, et prouver la conformité oblige à rassembler les preuves de chaque système avant un audit.

La solution

Avec le Data Policy Engine (DPE) de Kiteworks, les administrateurs définissent leurs politiques une fois ; elles s'appliquent à l'exécution sur chaque canal. Chaque décision pèse données, acteur (personne ou agent d'IA) et action : autoriser, bloquer, exiger une approbation ou limiter à une consultation ou édition protégée. Chaque action d'agent ou d'utilisateur va dans un seul journal d'audit.

Un seul plan de contrôle pour chaque échange de données sensibles

Que la demande vienne d'un employé, d'un partenaire ou d'un agent d'IA, le Data Policy Engine évalue les mêmes attributs de données, d'acteur et d'action, et applique les mêmes politiques sur les API, les agents d'IA, la messagerie, le partage de fichiers et les autres canaux.



Comment le Data Policy Engine décide

1 DONNÉES

Évaluer les données

Balises de classification, dossier et mots-clés des e-mails décrivent ce qui est échangé.

2 ACTEUR

Identifier l'acteur

Le contexte (e-mail, domaine, profil, géolocalisation) définit l'utilisateur ou l'agent demandeur.

3 ACTION

Évaluer l'action

Accéder, envoyer, partager ou téléverser : chaque action déclenche ses propres réponses.

4 APPLICATION

Appliquer la directive

La règle correspondante s'applique automatiquement, en temps réel, sans intervention manuelle.

Un contrôle des politiques sans complexité

Des règles SI-ALORS fondées sur les données, l'utilisateur ou l'agent, et l'action. Partez d'un modèle ou créez de zéro.

Règles ET/OU unifiées

Une seule logique de règles pour les utilisateurs, les données et les actions, appliquée à MCP, aux API, au web et à tous les autres canaux d'échange de données.

Modèles prêts à l'emploi

Partez de modèles, par exemple pour empêcher les données de quitter l'organisation ou exiger une approbation avant partage.

Basé sur la classification

Contrôlez l'accès des personnes et des agents d'IA via les balises Kiteworks et Cyera (IA) ou les étiquettes Microsoft Purview. Balisage possible au téléversement.

Sovereign Edit

La politique impose l'édition en ligne à certains utilisateurs et partenaires : le fichier reste sur Kiteworks, sans téléchargement ni envoi au cloud Microsoft.

Approbation et justification

Exigez une approbation avant un partage, ou un formulaire de justification avant un accès ou un téléversement.

RBAC granulaire et expiration

Rôles de moindre privilège, accès par dossier et expiration temporelle des fichiers et liens partagés.

Gouverner en temps réel chaque demande de données des agents et des personnes

Accès

Bloquer, SafeVIEW, Sovereign Edit, justification ou autoriser.

Partage ou envoi

Bloquer, exiger l'approbation d'un responsable ou autoriser.

Téléversement

Bloquer, balise Kiteworks, justification ou autoriser.

Appliquer automatiquement la conformité des agents et des personnes, et la prouver

Un journal d'audit immuable

Chaque action des agents et des personnes est consignée de façon centralisée et alimente les rapports de conformité et les intégrations SIEM.

Rapports et tableaux de bord des politiques

Évaluez une politique avant de l'activer, puis mesurez son impact en production.

Mappage des référentiels

Les règles DPE couvrent de façon large et granulaire des réglementations comme CMMC 2.0, HIPAA, RGPD, FedRAMP, ITAR, NIS 2, PCI DSS et PIPEDA.

Prêt à gouverner chaque échange de données sensibles ?

www.kiteworks.com sales@kiteworks.com

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.

Copyright © 2026 Kiteworks.