

POUR LES FABRICANTS DE SEMI-CONDUCTEURS, FABS ET FONDERIES

SÉCURISER LE SILICIUM : LA GOUVERNANCE DES DONNÉES FACE À UNE INDUSTRIE SOUS PRESSION

Les conceptions de puces, les données techniques et les analyses d'IA circulent en permanence entre fabs, fonderies, fournisseurs et frontières. Le risque les accompagne.

Protection de la propriété intellectuelle

Conformité aux contrôles des exportations

Gouvernance de l'IA

Croissance et exposition suivent la même courbe

Selon les prévisions du secteur, le marché mondial des semi-conducteurs en 2026 se situerait entre 1 000 milliards de dollars (Semiconductor Industry Association) et 1 500 milliards (World Semiconductor Trade Statistics), porté par l'infrastructure d'IA et la demande de mémoire. Les compromissions en cascade chez les fournisseurs et une carte réglementaire morcelée aggravent l'exposition.

La réponse structurelle

La sécurité périmétrique et les politiques ponctuelles ne peuvent pas gouverner des données qui doivent, par nature, quitter sans cesse le périmètre. La réponse doit être structurelle : une protection et des politiques qui suivent les données elles-mêmes, à travers chaque fab, fonderie, fournisseur et système d'IA.

6x

Hausse des cyberattaques contre les fabricants de puces depuis 2022 (CloudSEK)

78%

Entreprises non préparées aux obligations de l'AI Act européen (Vision Compliance)

51%

Entreprises jugeant désormais la souveraineté des données très importante (BARC)

Trois pressions, une seule exposition



Le vol de propriété intellectuelle par des États et les attaques contre la chaîne d'approvisionnement s'accroissent

D'après CloudSEK (2026, relayé par Industrial Equipment News et CSO Online), les cyberattaques contre les fabricants de puces ont été multipliées par six depuis 2022 et ont contribué à plus d'un milliard de dollars de pertes liées aux rançongiciels. Des acteurs étatiques, comme le groupe chinois APT41, ciblent l'écosystème taïwanais des semi-conducteurs et visent les conceptions de puces et les données de procédé. L'attaque de 2023 contre MKS Instruments a coûté environ 250 millions de dollars à Applied Materials : un seul fournisseur compromis peut contaminer toute la chaîne.



La carte de la conformité se scinde en temps réel

En janvier 2026, les États-Unis sont passés à des licences au cas par cas pour les puces d'IA avancées, assorties d'une taxe de 25 % (Bureau of Industry and Security). La Chine renforce la protection de ses conceptions de circuits intégrés et envisage ses propres restrictions à l'exportation, selon Reuters. Les entreprises doivent prouver qu'elles ont accès à quelles données techniques, quand et avec quelle autorisation, et les tenir à l'écart des zones restreintes, sous peine de perdre leurs privilèges d'exportation.



La gouvernance de l'IA et la souveraineté des données ont pris de vitesse la plupart des programmes de conformité

Vision Compliance (2026) : 78 % des entreprises ne sont pas prêtes pour l'AI Act européen. Selon IBM, l'IA fantôme intervient dans 43 % des violations et ajoute environ 670 000 dollars au coût moyen. BARC : 51 % jugent la souveraineté des données très importante (42 % en 2025), mais seules 38 % ont une gouvernance mature et 10 % un budget dédié.

Une politique, tous les canaux : une couche unique et gouvernée



Data Policy Engine

Accès fondé sur les rôles et les attributs, avec géolocalisation et classification des données, appliqué de façon uniforme au partage de fichiers, à la messagerie, au SFTP et au MFT. Une politique par conception de puce, quel que soit le canal.



Sovereign Edit

Les partenaires modifient les fichiers dans Kiteworks sans export, téléchargement, impression ni copier-coller ; Sovereign Edit – Streaming prend en charge la CAO.



Secure MFT and SFTP

La même gouvernance pour les transferts automatisés à fort volume : accord de la direction et du service juridique avant tout transfert d'un fichier à restriction maximale, avec un journal d'audit unique.



Secure MCP Server

La gouvernance RBAC et ABAC s'applique aussi bien aux personnes qu'aux agents d'IA. Chaque fichier consulté par un agent est authentifié, autorisé et journalisé comme celui d'un humain, sans jamais exposer les identifiants au modèle.

Les résultats attendus par les clients du secteur des semi-conducteurs



Une conformité démontrable, à la demande

Une piste d'audit complète et exportable permet de répondre à toute question d'un régulateur ou d'un auditeur sur qui a accédé à quoi, quand et avec quelle autorisation.



Une protection de la propriété intellectuelle qui suit les données chez les tiers

Comme la politique accompagne les données, les conceptions de puces et les firmwares restent gouvernés chez un fournisseur ou sur un appareil non géré, pas seulement dans le réseau de l'entreprise.



Aucune interruption pendant le déploiement

Un fabricant mondial qui protège la propriété intellectuelle de sa chaîne d'approvisionnement a démarré dans les délais, sans perturbation ni reformation.



Une réponse défendable face au déficit de gouvernance de l'IA

Alors que la plupart des entreprises ne sont pas prêtes face à la réglementation de l'IA, les entreprises de semi-conducteurs disposent d'une réponse documentée et appliquée par des politiques, bien avant leur prochain audit.

Protéger la propriété intellectuelle qui fait tourner l'industrie des puces, partout où elle doit aller.

www.kiteworks.com

Kiteworks



La mission de Kiteworks est de permettre aux organisations de gérer efficacement les risques à chaque envoi, partage, réception et utilisation de données privées. La plateforme Kiteworks offre à ses clients un échange de données sécurisé qui assure la gouvernance, la conformité et la protection des données dans un plan de contrôle unifié. Kiteworks unifie, suit, contrôle et sécurise les données sensibles qui circulent au sein de l'organisation, vers l'extérieur et depuis l'extérieur, ce qui améliore nettement la gestion des risques et garantit la conformité réglementaire de tous les échanges de données privées. Basée dans la Silicon Valley, Kiteworks protège plus de 100 millions d'utilisateurs finaux ainsi que des milliers d'entreprises et d'administrations publiques dans le monde.