Kiteworks

OPLOSSINGSOVERZICHT

VOOR HALFGELEIDERFABRIKANTEN, FABS EN FOUNDRY'S

SILICIUM BEVEILIGEN: DATAGOVERNANCE VOOR EEN SECTOR ONDER VUUR

Chipontwerpen, technische data en AI-inzichten bewegen voortdurend tussen fabs, foundry's, leveranciers en landsgrenzen. Het risico beweegt met ze mee.

Bescherming van intellectueel eigendom | Naleving van exportcontrole | AI-governance

Groei en blootstelling gaan hand in hand

Sectorprognoses plaatsen de wereldwijde halfgeleidermarkt in 2026 tussen ruwweg 1 biljoen dollar (Semiconductor Industry Association) en 1,5 biljoen dollar (World Semiconductor Trade Statistics), aangejaagd door AI-infrastructuur en vraag naar geheugen. Kettingreacties van leveranciersincidenten en een versplinterende regelgevingskaart vergroten de blootstelling verder.

De structurele oplossing

Perimeterbeveiliging en ad-hocbeleid kunnen data niet beheersen die het bedrijf door de aard van het werk voortdurend moet verlaten. De oplossing moet structureel zijn: bescherming en beleidshandhaving die met de data zelf meereizen, langs elke fab, foundry, leverancier en elk AI-systeem dat ze raken.

6x

Toename van cyberaanvallen op chipmakers sinds 2022 (CloudSEK)

78%

Bedrijven die niet klaar zijn voor de verplichtingen van de EU-AI-verordening (Vision Compliance)

51%

Bedrijven die datasoevereiniteit inmiddels zeer belangrijk vinden (BARC)

Drie drukpunten, één blootstelling

IP-diefstal door staten en aanvallen op de toeleveringsketen nemen toe

Volgens een CloudSEK-analyse uit 2026, waarover Industrial Equipment News en CSO Online berichtten, zijn cyberaanvallen op chipmakers sinds 2022 verzesvoudigd en hebben ze bijgedragen aan meer dan 1 miljard dollar aan ransomwareschade. Statelijke actoren, zoals de Chinese groep APT41, richten zich op het Taiwanese halfgeleiderecosysteem en zien chipontwerpen en procesdata als strategische doelwitten. De aanval op MKS Instruments in 2023 kostte Applied Materials naar schatting 250 miljoen dollar: één gecompromitteerde leverancier kan de hele keten besmetten.

De compliancekaart splitst zich in realtime

In januari 2026 stapten de VS over op vergunningverlening per geval voor geavanceerde AI-chips, met een tarief van 25 procent, aldus het Bureau of Industry and Security. China heeft de bescherming van zijn IC-ontwerpen aangescherpt en overweegt volgens Reuters eigen exportbeperkingen. Bedrijven moeten kunnen aantonen wie wanneer en met welke autorisatie toegang had tot welke technische data, en die weghouden uit beperkte regio's, anders verliezen ze hun exportprivileges.

AI-governance en datasoevereiniteit zijn de meeste compliance-programma's voorbijgestreefd

Vision Compliance (2026) vond dat 78 procent van de bedrijven niet klaar is voor de EU-AI-verordening. Volgens IBM speelt shadow-AI een rol bij 43 procent van de datalekken en kost het gemiddeld ongeveer 670.000 dollar extra. BARC meldt dat 51 procent datasoevereiniteit zeer belangrijk vindt (42 procent in 2025), maar slechts 38 procent volwassen governance heeft en 10 procent een eigen budget.

Eén beleid, elk kanaal: één beheerde laag

Data Policy Engine
Toegang op basis van rollen en attributen, met geolocatie en dataclassificatie, uniform toegepast op bestandsdeling, e-mail, SFTP en MFT. Eén beleid per chipontwerp, ongeacht het kanaal, met een volledig auditspoor.

Sovereign Edit
Partners bewerken bestanden binnen Kiteworks zonder exporteren, downloaden, printen of kopiëren en plakken; Sovereign Edit – Streaming dekt CAD.

Secure MFT and SFTP
Dezelfde governance voor geautomatiseerde transfers met hoge volumen: goedkeuring van directie en juridische zaken vóór een streng beperkt bestand wordt verplaatst, met één auditlog.

Secure MCP Server
RBAC- en ABAC-governance geldt voor mensen en AI-agenten. Elk bestand dat een agent aanraakt, wordt net als bij een mens geauthenticeerd, geautoriseerd en gelogd, zonder dat inloggegevens ooit aan het model worden blootgesteld.

Wat klanten uit de halfgeleidersector mogen verwachten

Aantoonbare compliance, op afroep
Een volledig, exporteerbaar auditspoor beantwoordt elke vraag van een toezichthouder of auditor over wie wanneer en met welke autorisatie toegang had tot wat.

IP-bescherming die ook bij derden standhoudt
Omdat het beleid met de data meereist, blijven chipontwerpen en firmware beheerd bij een leverancier of op een onbeheerd apparaat, niet alleen binnen het bedrijfsnetwerk.

Ononderbroken bedrijfsvoering tijdens de uitrol
Een wereldwijde fabrikant die het IP in zijn toeleveringsketen beschermt, ging op schema live, zonder verstoring en zonder omscholing.

Een verdedigbaar antwoord op de AI-governancekloof
Nu de meeste bedrijven niet klaar zijn voor AI-regelgeving, krijgen halfgeleiderbedrijven een gedocumenteerd, door beleid afgedwongen antwoord ruim voor hun volgende audit.

Wij beschermen het IP dat de chipindustrie aandrijft, overal waar het naartoe moet.

www.kiteworks.com

Kiteworks

De missie van Kiteworks is organisaties in staat te stellen risico's effectief te beheersen bij elke verzending, elke deling, elke ontvangst en elk gebruik van privédata. Het Kiteworks-platform biedt klanten een veilige data-uitwisseling die datagovernance, compliance en bescherming levert in één uniform controlevlak. Kiteworks verenigt, volgt, controleert en beveiligt gevoelige data die binnen, naar en uit de organisatie stromen, verbetert het risicomanagement aanzienlijk en waarborgt naleving van regelgeving bij alle uitwisselingen van privédata. Kiteworks heeft zijn hoofdkantoor in Silicon Valley en beschermt meer dan 100 miljoen eindgebruikers en duizenden wereldwijde ondernemingen en overheidsinstellingen.

Copyright © 2026 Kiteworks.