

SILIZIUM SCHÜTZEN: DATA GOVERNANCE FÜR EINE BRANCHE UNTER BESCHUSS

Chipdesigns, technische Daten und KI-Erkenntnisse wandern ständig zwischen Fabs, Foundries, Zulieferern und Ländergrenzen. Das Risiko wandert mit.

Schutz geistigen Eigentums

Compliance bei Exportkontrollen

KI-Governance

Wachstum und Angriffsfläche steigen im Gleichschritt

Branchenprognosen sehen den Halbleitermarkt 2026 zwischen rund 1 Billion US-Dollar (Semiconductor Industry Association) und 1,5 Billionen US-Dollar (World Semiconductor Trade Statistics), getrieben von KI-Infrastruktur und Speichernachfrage. Kaskadierende Lieferantenvorfälle und eine zerfallende Regulierungslandschaft vergrößern die Angriffsfläche.

Die strukturelle Lösung

Perimeterschutz und Ad-hoc-Richtlinien können Daten nicht kontrollieren, die das Unternehmen geschäftsbedingt ständig verlassen müssen. Nötig ist ein struktureller Ansatz: Schutz und Richtliniendurchsetzung, die den Daten selbst folgen, durch jede Fab, Foundry, jeden Zulieferer und jedes KI-System.

6x

Anstieg der Cyberangriffe auf Chiphersteller seit 2022 (CloudSEK)

78%

Unternehmen, die auf die Pflichten des EU-KI-Gesetzes nicht vorbereitet sind (Vision Compliance)

51%

Unternehmen, die Datensouveränität inzwischen als sehr wichtig einstufen (BARC)

Drei Belastungen, eine Angriffsfläche



IP-Diebstahl durch Staaten und Angriffe auf die Lieferkette nehmen zu

Laut einer CloudSEK-Analyse von 2026 (Industrial Equipment News, CSO Online) haben sich Cyberangriffe auf Chiphersteller seit 2022 versechsfacht und zu Ransomware-Schäden von über 1 Milliarde US-Dollar beigetragen. Staatliche Akteure wie Chinas Gruppe APT41 nehmen das taiwanische Halbleiter-Ökosystem ins Visier und behandeln Chipdesigns und Prozessdaten als strategische Ziele. Der Angriff auf MKS Instruments 2023 kostete Applied Materials geschätzt 250 Millionen US-Dollar: Ein kompromittierter Zulieferer kann die ganze Kette anstecken.



Die Compliance-Landkarte spaltet sich in Echtzeit

Im Januar 2026 stellten die USA bei fortgeschrittenen KI-Chips auf Einzelfalllizenzen um, verbunden mit einem Zoll von 25 Prozent (Bureau of Industry and Security). China verschärft den Schutz seiner IC-Designs und erwägt laut Reuters eigene Exportbeschränkungen. Unternehmen müssen belegen, wer wann mit welcher Berechtigung auf welche technischen Daten zugegriffen hat, und sie von eingeschränkten Regionen fernhalten, sonst droht der Verlust der Exportprivilegien.



KI-Governance und Datensouveränität sind den meisten Compliance-Programmen davongeeilt

Vision Compliance (2026): 78 Prozent der Unternehmen sind auf das EU-KI-Gesetz nicht vorbereitet. Laut IBM spielt Schatten-KI bei 43 Prozent der Datenpannen eine Rolle und erhöht die Kosten um rund 670.000 US-Dollar. BARC: 51 Prozent halten Datensouveränität für sehr wichtig (2025: 42 Prozent), nur 38 Prozent haben ausgereifte Governance, 10 Prozent ein eigenes Budget.

Eine Richtlinie, jeder Kanal: eine einheitlich gesteuerte Ebene



Data Policy Engine

Rollen- und attributbasierter Zugriff samt Geolokalisierung und Datenklassifizierung, einheitlich für Filesharing, E-Mail, SFTP und MFT. Eine Richtlinie pro Chipdesign, egal über welchen Kanal, mit lückenlosem Audit-Trail.



Sovereign Edit

Partner bearbeiten Dateien innerhalb von Kiteworks ohne Export, Download, Druck oder Kopieren und Einfügen; Sovereign Edit – Streaming deckt CAD ab.



Secure MFT and SFTP

Dieselbe Governance für automatisierte Hochvolumen-Transfers: Hochsensible Dateien werden erst nach Freigabe durch Geschäftsleitung und Rechtsabteilung übertragen, jeder Transfer landet in einem Audit-Log.



Secure MCP Server

RBAC- und ABAC-Governance gilt für Menschen und KI-Agenten gleichermaßen. Jede Datei, die ein Agent berührt, wird wie bei einem Menschen authentifiziert, berechtigt und protokolliert; Zugangsdaten gelangen nie zum Modell.

Ergebnisse, die Halbleiterkunden erwarten können



Nachweisbare Compliance auf Abruf

Ein vollständiger, exportierbarer Audit-Trail beantwortet jede Frage von Aufsichtsbehörden oder Prüfern: wer wann mit welcher Berechtigung auf welche Daten zugegriffen hat.



IP-Schutz, der bis zum Zulieferer reicht

Weil die Richtlinie den Daten folgt, bleiben Chipdesigns und Firmware auch beim Zulieferer oder auf nicht verwalteten Geräten geschützt, nicht nur im Unternehmensnetzwerk.



Unterbrechungsfreier Betrieb beim Rollout

Ein globaler Hersteller, der das geistige Eigentum seiner Lieferkette schützt, ging termingerecht live, ohne Betriebsunterbrechung und ohne Nachschulung.



Eine belastbare Antwort auf die KI-Governance-Lücke

Da die meisten Unternehmen auf die KI-Regulierung nicht vorbereitet sind, erhalten Halbleiterunternehmen eine dokumentierte, durch Richtlinien durchgesetzte Antwort, lange vor dem nächsten Audit.

Wir schützen das geistige Eigentum der Chipindustrie, überall dort, wo es hin muss.

www.kiteworks.com

Kiteworks



Die Mission von Kiteworks ist es, Organisationen dabei zu unterstützen, Risiken bei jedem Senden, Teilen, Empfangen und Verwenden privater Daten wirksam zu steuern. Die Kiteworks-Plattform bietet Kunden einen sicheren Datenaustausch, der Data Governance, Compliance und Schutz in einer einheitlichen Kontrollebene vereint. Kiteworks vereinheitlicht, verfolgt, kontrolliert und sichert sensible Daten, die innerhalb der Organisation, in sie hinein und aus ihr heraus bewegt werden, verbessert das Risikomanagement erheblich und stellt die Einhaltung regulatorischer Vorgaben bei allen Austauschvorgängen privater Daten sicher. Kiteworks hat seinen Hauptsitz im Silicon Valley und schützt über 100 Millionen Endnutzer sowie Tausende globale Unternehmen und Behörden.