

FOR SEMICONDUCTOR MANUFACTURERS, FABs & FOUNDRIES

Securing Silicon: Data Governance for an Industry Under Siege

Chip designs, technical data, and AI insight move constantly across fabs, foundries, suppliers, and borders. So does the risk that follows them.

IP Protection

Export Control Compliance

AI Governance

— THE PROBLEM

Growth and exposure are the same curve

Industry forecasts put the 2026 global semiconductor market between roughly \$1 trillion (Semiconductor Industry Association) and \$1.5 trillion (World Semiconductor Trade Statistics), driven by AI infrastructure and memory demand. The same currents, chip designs, technical data, and AI-driven insight moving constantly across fabs, foundries, suppliers, and borders, are exactly what attackers exploit. Cascading vendor breaches and a fracturing regulatory map compound the exposure.

6x

Rise in cyberattacks on
chipmakers since 2022
(CloudSEK)

78%

Enterprises unprepared for EU
AI Act obligations (Vision
Compliance)

51%

Enterprises now call data
sovereignty very important
(BARC)

THE STRUCTURAL FIX

Perimeter security and ad hoc policy cannot govern data that is required, by the nature of the business, to leave the perimeter constantly. The fix must be structural: protection and policy enforcement that travel with the data itself, across every fab, foundry, supplier, and AI system it touches.

— THE PROBLEM, CONTINUED

Three pressures, one exposure

Nation-state IP theft and supply chain attacks are accelerating

According to a 2026 CloudSEK analysis reported by Industrial Equipment News and CSO Online, cyberattacks on chipmakers have risen sixfold since 2022, contributing to over \$1 billion in industry-wide ransomware losses. Nation-state actors, including China's APT41 group, are actively targeting Taiwan's semiconductor and technology research ecosystem, treating chip designs and process data as strategic targets. Cascading vendor breaches carry their own cost: a 2023 ransomware attack on supplier MKS Instruments disrupted operations and cascaded into an estimated \$250 million impact on semiconductor equipment maker Applied Materials, a stark reminder that a single supplier compromise can propagate risk across an entire manufacturing chain.

The compliance map is bifurcating in real time

In January 2026, US export control policy shifted to case-by-case licensing for advanced AI chips, paired with a 25 percent tariff, according to the Bureau of Industry and Security. China simultaneously tightened its own IC design protections and is weighing new export restrictions of its own, per Reuters reporting. Semiconductor companies must now prove, to two increasingly divergent regulatory regimes, exactly who accessed which technical data, when, and under what authorization, or risk losing export privileges entirely.

AI governance and data sovereignty have outpaced most compliance programs

Vision Compliance's 2026 EU AI Act Readiness Report found 78 percent of enterprises still unprepared for their EU AI Act obligations. Separately, IBM's Cost of a Data Breach Report found shadow AI now factors into 43 percent of breaches and adds roughly \$670,000 to the average breach cost. Data sovereignty has become a boardroom issue, with BARC's Data Sovereignty 2026 survey finding 51 percent of enterprises now call it very important, up from 42 percent in 2025, while only 38 percent have mature governance in place and just 10 percent have a dedicated budget to close the gap.

— THE KITeworks SOLUTION

One policy, every channel

Kiteworks gives semiconductor manufacturers a single governed layer for every sensitive data exchange, so control does not stop at the network edge.

- 
Data Policy Engine: consistent protection across every channel
 The Data Policy Engine enforces role- and attribute-based access, including geolocation and data classification, uniformly across file sharing, email, SFTP, and MFT — one policy per chip design, regardless of channel, with a full audit trail of what was enforced and when.
- 
SafeEDIT: collaborate without ever handing over the file
 SafeEDIT lets external design partners and suppliers view and edit CAD, CAM, and other engineering files natively in-browser, while the file itself never leaves the Kiteworks secure enclave.
- 
Secure MFT and SFTP: automated, policy-enforced supply chain exchange
 Secure MFT and SFTP extend the same governance to high-volume automated transfers, requiring executive and legal sign-off before a Highly Restricted file moves, with every transfer captured in one audit log.
- 
Secure MCP Server: governed AI and agent data access
 The Secure MCP Server extends the same RBAC and ABAC governance to every AI operation. Every file an AI agent touches is authenticated, permissioned, and logged like a human user's, with credentials never exposed to the model, feeding directly into compliance reporting.

— OUTCOMES

Outcomes semiconductor clients can expect

- 
Provable compliance, on demand
 A complete, exportable audit trail across every channel means compliance leaders can answer any regulator's or auditor's question about who accessed what, when, and under what authorization.
- 
IP protection that survives the third boundary
 Because policy travels with the data, chip designs and firmware stay governed after they reach a supplier or an unmanaged device — not just while they sit inside the corporate network.
- 
Uninterrupted operations during rollout
 In a comparable deployment, a global manufacturer protecting IP at the edge of its supply chain went live on schedule with zero disruption and zero retraining.
- 
A defensible answer to the AI governance gap
 With most enterprises still unprepared for accelerating AI regulation, semiconductor companies gain a documented, policy-enforced answer well ahead of their next audit.

Kiteworks. Protecting the intellectual property that powers the chip industry, everywhere it must go.

www.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. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.