

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

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. Cascading vendor breaches and a fracturing regulatory map compound the exposure.

The structural fix

Perimeter security and ad hoc policy cannot govern data that must, by the nature of the business, 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.

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)

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. A 2023 ransomware attack on supplier MKS Instruments cascaded into an estimated \$250 million impact on Applied Materials, showing how one supplier compromise can propagate across a 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 has tightened its own IC design protections and is weighing new export restrictions of its own, per Reuters reporting. Semiconductor companies must now prove exactly who accessed which technical data, when, and under what authorization, and keep it from restricted geographies, 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. 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. BARC's Data Sovereignty 2026 survey found 51 percent of enterprises now call data sovereignty 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.

One Policy, Every Channel: A Single Governed Layer



Data Policy Engine

Role- and attribute-based access, including geolocation and data classification, applied 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.



Sovereign Edit

Partners edit files inside Kiteworks with no export, download, print, or copy-paste; Sovereign Edit – Streaming covers CAD.



Secure MFT and SFTP

The same governance for 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

RBAC and ABAC governance applies to people and AI agents alike. Every file an AI agent touches is authenticated, permissioned, and logged like a human's, with credentials never exposed to the model, feeding directly into compliance reporting.

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

A global manufacturer protecting supply chain IP 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.

Protecting the IP 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. 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.