STRIDER FOR SEMICONDUCTOR COMPANIES

Safeguarding Innovation, Compliance, and the Global Chip Supply Chain from Nation-State Threats

Overview

Semiconductor companies operate at the center of technological and economic power. From equipment and materials to design and fabrication, every layer of the chip ecosystem is targeted by state-sponsored actors seeking to accelerate domestic capabilities and evade export controls.

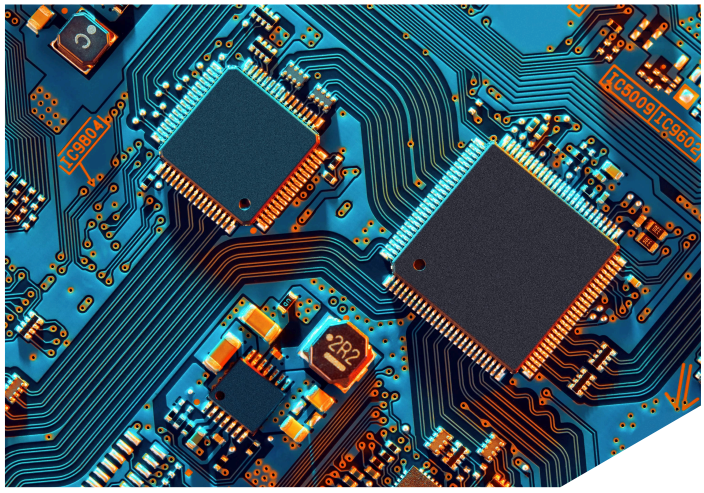
Amid rising geopolitical pressure, semiconductor leaders must protect critical R&D, talent, and supplier networks while meeting the rigorous compliance standards of the CHIPS and Science Act, Bureau of Industry and Security (BIS) export rules, and Foreign Ownership, Control, or Influence (FOCI) regulations.

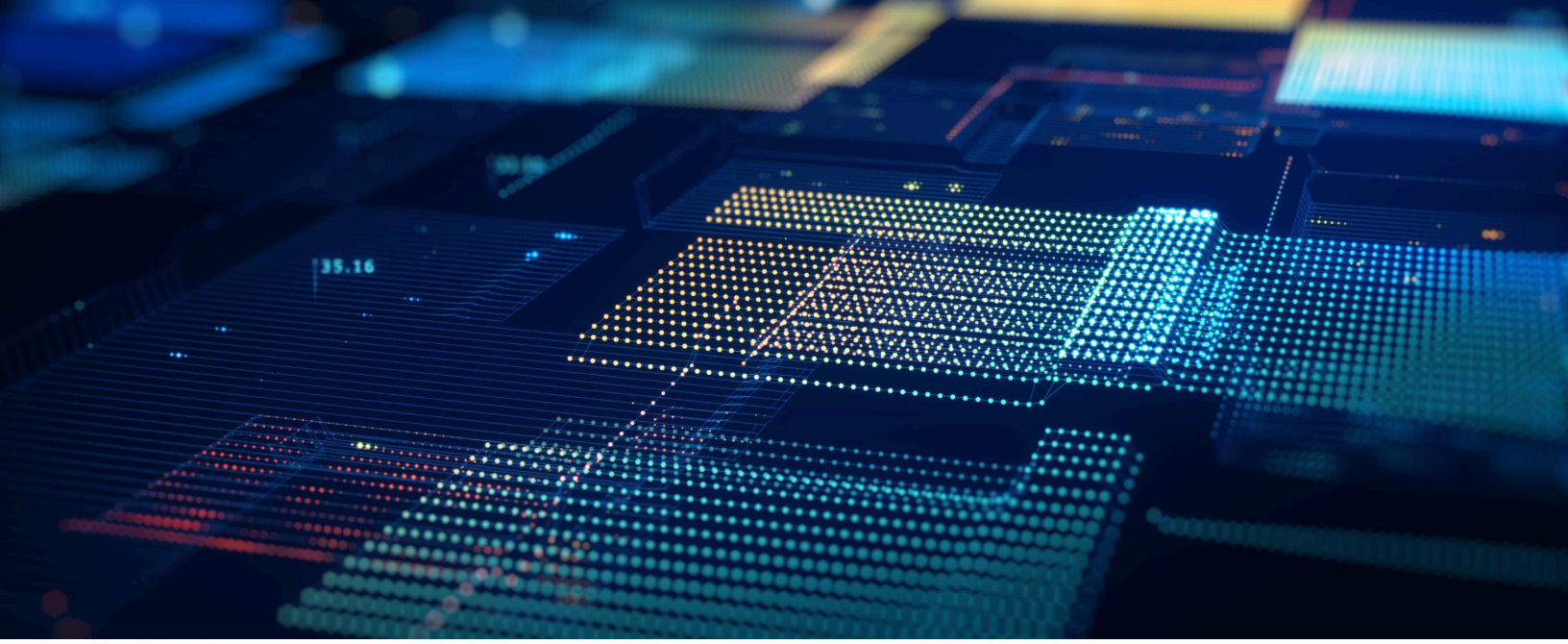
Strider's Strategic Intelligence Platform delivers visibility into the nation-state risks affecting people, organizations, and technologies—empowering semiconductor companies to protect IP, maintain compliance, and strengthen supply-chain resilience.

Semiconductor leaders use Strider to:

- Screen and continuously vet employees and contractors for hidden affiliations, falsified resumes, or insider risk.
- Map and monitor global supplier networks for hidden ownership, front companies, and FOCI exposure.
- Identify and protect high-value technologies and experts targeted by foreign talent programs.
- Detect and block adversarial outreach or malicious communications before they infiltrate sensitive programs.
- Demonstrate proactive due diligence to regulators and investors through auditable intelligence.

With Strider, semiconductor companies can safeguard mission-critical programs, comply with national-security regulations, and innovate confidently while maintaining the highest standard of operational security.





What's at Stake

Recent incidents underscore how insider threats, IP theft, and export-control violations can jeopardize semiconductor innovation and national-security objectives.

- **TSMC Export-Control Investigation (2025)[1,2,3]:** Taiwan Semiconductor Manufacturing Company is under U.S. investigation for allegedly producing chips that ended up in Huawei's AI processors—potentially facing fines exceeding US $1 billion.
- **NVIDIA GPU Diversion to China (2025)[4,5]:** Restricted NVIDIA AI chips were illegally rerouted to China through intermediaries in Singapore and Malaysia, exposing vulnerabilities in global distribution networks.
- **Micron Espionage Case (DOJ, 2018)[6,7]:** The U.S. Department of Justice charged a PRC state-owned enterprise and Taiwanese firm with conspiring to steal Micron's trade secrets for DRAM manufacturing, highlighting ongoing risks to semiconductor IP.

The semiconductor supply chain's complexity—from fabs to design firms and equipment manufacturers—creates numerous entry points for exploitation. One weak link can compromise compliance, intellectual property, and long-term competitiveness.

Failure to Act Can Lead to:

- **IP Theft and R&D Loss:** Proprietary chip designs, process technologies, or EDA software exfiltrated through insider access or espionage.
- **Regulatory & Legal Exposure:** Violations of CHIPS Act guardrails, BIS export controls, or ITAR restrictions, resulting in fines, contract loss, or disqualification.
- **Supply-Chain Compromise:** Hidden ownership or third-tier supplier ties to restricted entities creating cascading compliance risk.
- **Operational Disruption:** Loss of trusted suppliers or restricted component access undermining manufacturing continuity.
- **Erosion of Trust:** Damaged credibility with customers, partners, and regulators who expect secure, compliant operations.

[1] https://jeffnewmanlaw.com/tsmc-faces-potential-fine-over-1-billion-for-violating-export-control-regs-for-selling-chips-to-chinese-companies/
[2] https://www.investopedia.com/tsmc-could-face-usd1b-us-fine-for-violating-export-control-rules-report-says-11711445
[3] https://techcrunch.com/2025/04/09/us-may-fine-tsmc-1b-over-chip-allegedly-used-in-huawei-ai-processor/
[4] https://techwireasia.com/2025/03/nvidia-chip-crackdown-malaysia-under-us-pressure-to-stop-ai-reaching-china/
[5] https://www.channelnewsasia.com/singapore/nvidia-chips-probe-singapore-malaysia-export-restrictions-shanmugam-4972321
[6] https://www.crowell.com/en/insights/client-alerts/u-s-charges-chinese-and-taiwanese-companies-with-trade-secret-theft-continues-vigilant-prosecution-of-chinese-economic-espionage
[7] https://www.justice.gov/usao-ndca/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage

What Strider Does for Seminconductor Companies

CAPABILITY	HOW IT HELPS	STRIDER PRODUCTS IN ACTION
Continuous Employee & Contractor Vetting	Verify credentials and uncover hidden affiliations to prevent insider risk and compliance violations.	**People Search & Falsified Resume Screening** Integrate with ATS or HR systems to detect falsified identities and high-risk connections before hire.
Supply-Chain Integrity & Export Compliance	Reveal hidden ownership, front companies, and sanction risks across multi-tier suppliers and investors.	**Organizations Search** Map global economic and personnel ties to strengthen due diligence and ensure CHIPS Act and BIS compliance.
Protection of Critical Technologies & Expertise	Identify which technologies and SMEs are being targeted by foreign programs.	**Insights (Technologies Tab):** Pinpoint targeted technologies and experts to prioritize protective measures and defensive briefings.
Secure Communications & Threat Monitoring	Detect and monitor adversarial outreach from state-linked collectors and recruiters.	**Shield** Integrate curated threat-intelligence data into SIEM/DLP tools to flag and monitor malicious communications.
AI-Driven Risk Analysis	Accelerate investigations and unify intelligence across people, organizations, and technologies.	**Spark** Use Strider's AI engine to rapidly surface insights across your workforce, suppliers, and R&D ecosystem.

Ready to Secure Your Supply Chain and Innovation?

Schedule a demo to see how Strider's Strategic Intelligence Platform helps semiconductor companies protect intellectual property, maintain export-control compliance, and ensure resilience across the global chip ecosystem.

REQUEST A DEMO →