STRIDER FOR ENTERPRISE AI LEADERS

Protecting Global AI Programs, People, and Supply Chains From Nation-State Threats.

Overview

Enterprise AI leaders sit at the frontier of global competition. The models, research, and compute capacity they develop are prime targets for insider threats, IP theft, and supply chain exploitation by adversaries to bypass export controls and compromise critical compute resources. Strider equips CISOs and CSOs to protect innovation and ensure compliance while operating at global scale.

Enterprise AI leaders use Strider to:

- Continuously vet and monitor employees in sensitive positions.
- Identify and mitigate insider leaks of proprietary models and IP.
- Secure global chip and compute supply chains.
- Flag adversarial attempts to infiltrate via malicious communications or recruitment.

With Strider, Enterprise AI companies can innovate confidently while meeting the highest bar for security and compliance.

What's at Stake

Recent incidents show how quickly insider threats, IP theft, and supply chain manipulation can put even the most advanced AI programs at risk.

- **Ex-Google Engineer Charged with IP Theft (2024):** A former Google employee stole confidential AI trade secrets for PRC entities, exposing gaps in insider monitoring.[1]
- **DeepSeek Replication Fears (2025):** The rise of DeepSeek underscored how U.S. breakthroughs can be replicated abroad—sometimes aided by insider leaks.[2]
- **NVIDIA GPU Diversion to China (2024-2025):** Restricted AI chips were illegally acquired by PRC-linked firms, highlighting supply chain vulnerabilities.[3]

Enterprises must guard against insider leaks and geopolitical manipulation across vast, complex global operations.

[1] https://www.reuters.com/legal/ex-google-engineer-faces-new-us-charges-he-stole-ai-secrets-chinese-companies-2025-02-05/
https://finance.yahoo.com/news/ex-google-engineer-charged-ai-213843217.html
[2] https://www.theguardian.com/technology/2025/jan/29/openai-chatgpt-deepseek-china-us-ai-models
[3] https://www.businesstoday.in/technology/news/story/over-1billion-worth-of-nvidia-chips-smuggled-into-china-despite-us-export-ban-report-486292-2025-07-25

Failure to Act Can Lead to:

- **IP Loss or Theft:** Proprietary research or models exfiltrated through insider leaks.
- **Loss of Public Trust:** Customers, regulators, and partners can lose confidence in your ability to protect innovation.
- **Compliance Exposure:** Global export control and national security violations result in costly penalties.
- **Operational Disruption:** Compromised suppliers, contractors, or partners create cascading risks across global operations.

What Strider Does for AI Startups

CAPABILITY	HOW IT HELPS	STRIDER PRODUCTS IN ACTION
Continuous Employee Vetting	Vet employees in sensitive roles and rescreen regularly.	**Insights & People Search** Enhance insider threat monitoring with nation-state risk signals.
Safeguard IP & Research	Track risky affiliations, publications, and talent flows.	**Insights** Identify high-risk employees, targeted technologies, and potential leaks.
Secure Global Supply Chains	Map complex relationships across vendors, partners, and investors.	**Organizations Search** Map supplier and investor ties; prevent hidden affiliations.
Protect Communications	Identify and prevent malicious outreach from state-sponsored actors.	**Shield** Integrate with SIEM/DLP systems to identify and block adversarial emails communications.

Ready to Secure Your Innovation?

Schedule a demo to see how Strider's Strategic Intelligence Platform helps global AI leaders protect sensitive research, IP, and talent.

REQUEST A DEMO →