

# STRIDER FOR AI STARTUPS

## Safeguarding Innovation and Growth From Insider and Nation-State Threats.



### Overview

AI startups are scaling at unprecedented speed. However, with rapid growth comes risk including rushed hiring pipelines, fragile supply chains, and relentless targeting by state-sponsored actors to further the interests of nation-states. The Strider Strategic Intelligence Platform delivers the visibility founders and CISOs need to protect their people, IP, and investors' trust without slowing momentum.

AI startups use Strider to:

- Screen applicants at scale through ATS integration to prevent insider risks.
- Detect falsified resumes and hidden affiliations with state-sponsored programs.
- Protect proprietary research and models from exfiltration.
- Monitor suppliers of chips, GPUs, and compute infrastructure for adversarial ties.

With Strider, fast-growing AI firms can scale securely and build innovation without sacrificing resilience.

### What's at Stake

Nation-states see AI breakthroughs as a strategic prize. Unfortunately, startups with world-leading models and talent are prime targets.

- **Ex-Google Engineer Charged with IP Theft (2024):** A former Google engineer was indicted for stealing confidential AI model files to benefit Chinese firms.<sup>1</sup>
- **DeepSeek Controversy (2025):** Chinese AI firm DeepSeek rattled the sector amid allegations it replicated techniques from U.S. companies, raising fears of technology leakage.<sup>2</sup>
- **NVIDIA GPU Diversion to China (2024-2025):** Despite U.S. export controls, restricted H100 GPUs were acquired by PRC-linked firms through intermediaries.<sup>3</sup>

Even one compromised hire or supplier can undo years of innovation.

### Failure to Act Can Lead to:

- **IP Loss or Theft:** Insider-driven IP loss that derails product roadmaps
- **Investor Distrust:** Trust from investors can erode if compliance and security gaps surface.
- **Regulatory Penalties:** Regulatory penalties can be enforced tied to export control or sanctions violations.
- **Competitive Disadvantage:** Talent and tech leaks to adversarial firms can weaken your position in the market.

<sup>1</sup> <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>





<sup>2</sup> <https://www.theguardian.com/technology/2025/jan/29/openai-chatgpt-deepseek-china-us-ai-models>

<sup>3</sup> <https://www.businessinsider.com/news/story/over-1-billion-worth-of-nvidia-chips-smuggled-into-china-despite-us-export-ban-report-486292-2025-07-25>





## What Strider Does for AI Startups

CAPABILITY	HOW IT HELPS	STRIDER PRODUCTS IN ACTION
<b>Applicant &amp; Insider Screening</b>	Vet candidates at scale for falsified resumes and hidden nation-state ties.	 <b>People Search &amp; Falsified Resume Screening</b> Integrate with ATS to prescreen applicants and flag risky hires before they enter sensitive roles.
<b>Protect Proprietary Models</b>	Detect talent movements and risky affiliations before they become leaks.	 <b>Insights</b> Monitor talent flows and risky associations linked to PRC, Russia, and Iran.
<b>Secure Compute Supply Chains</b>	Ensure vendors for chips, GPUs, and cloud services are free of adversarial links.	 <b>Organizations Search</b> Map supplier and investor ties; prevent hidden PRC affiliations.
<b>Protect Communications</b>	Reduce noise and protect employees from high-risk outreach.	 <b>Shield</b> Integrate with SIEM/DLP systems to identify and block adversarial email communications.

**Ready to Secure  
Your Operations & IP?**

Schedule a demo to see how Strider's platform can protect your IP, talent, and investors while scaling at speed.

[REQUEST A DEMO](#) →

