# STRIDER FOR ENTERPRISE FINANCIAL INSTITUTIONS

## Safeguarding Financial Innovation, Operations, and Global Exposure from Nation-State Risk.

### Overview

Enterprise financial institutions sit at the center of global innovation and capital flows, making their AI, quantum, cybersecurity, and data-driven systems prime targets for state-sponsored actors seeking to infiltrate hiring pipelines, exploit third-party relationships, or influence strategic deals.

Strider equips CISOs, counterintelligence teams, insider threat programs, and compliance leaders with visibility into personnel risk, supply-chain exposure, and malicious communications enabling financial institutions to safeguard sensitive technologies, protect employees globally, and maintain regulatory and operational resilience across complex, distributed environments.

Enterprise Financial Institutions Use Strider to:

- Screen applicants and employees for falsified resumes, hidden affiliations, or ties to risky foreign entities.
- Continuously vet high-trust personnel in innovation units working on AI, quantum, and other strategic programs.
- Protect global dealmaking by revealing hidden ownership, foreign control, or sanction-linked exposure in counterparties, investors, and board members.
- Monitor risky outreach and malicious communications.
- Assess open-source contributors or external collaborators for hidden nation-state ties when reviewing software dependencies.
- Safeguard employees traveling abroad by identifying geopolitical risks tied to overseas partners, clients, or state-controlled institutions.

With Strider, financial institutions can protect their innovation pipelines, safeguard their global operations, and stay ahead of geopolitical, insider, and compliance risks

### What's at Stake

Recent incidents reveal how insider threats, geopolitical pressures, and opaque global partnerships can place even the most sophisticated financial institutions at risk.

- **U.S. House Subpoenas JPMorgan & Bank of America (2025)**[1]: A House committee subpoenaed both banks over their role in CATL's IPO, underscoring rising scrutiny of U.S. financial institutions' exposure to high-risk foreign entities and the need for stronger due diligence.
- **Wells Fargo Employee Barred from Leaving China (2025)**[2]: A Wells Fargo employee was temporarily prevented from leaving China over a past business dispute, showing how geopolitical pressures can directly affect personnel and why foreign legal and political risk matters.
- **North Korean IT Worker Scheme in U.S. Companies (2023)**[3]: The DOJ charged North Korean operatives for infiltrating U.S. companies using false identities to secure remote IT roles, highlighting the scale and sophistication of DPRK efforts to access corporate systems.

## Failure to Act Can Lead to:

- **Exposure to Regulatory & Geopolitical Scrutiny:** including Congressional inquiries, sanctions reviews (OFAC), and cross-border legal challenges.
- **Insider-Driven IP Loss:** especially in AI, quant models, cybersecurity R&D, and proprietary risk systems.
- **Compromised Hiring Pipelines:** fraudulent or high-risk employees gaining access to sensitive systems or funds.
- **Blocked Deals or Reputational Damage:** resulting from hidden ties to restricted entities or foreign influence.
- **Operational & Personnel Risk Abroad:** including nation-state talent recruitment tactics or geopolitical retaliation targeting key staff.

## What Strider Does for Enterprise Financial Institutions

| CAPABILITY | HOW IT HELPS | STRIDER PRODUCTS IN ACTION |
|---|---|---|
| **Continuous Employee & Candidate Vetting** | Verify identities, detect falsified resumes, and uncover risky affiliations before hire; especially for remote IT, cybersecurity, and R&D roles. | **People Search & Falsified Resume Screening** Automate screening through ATS integrations; identify DPRK or PRC-linked applicants attempting to impersonate Western talent. |
| **Protection of AI, Quantum, and Cyber R&D Programs** | Identify employees working on targeted technologies and provide tailored briefings to reduce recruitment risk. | **Insights (Technologies Tab):** Surface targeted technologies and associated employees most at risk from state-sponsored actors. |
| **Strategic Deal & Partner Due Diligence** | Protect M&A, investment banking, and strategic transactions by identifying foreign ownership, sanctions exposure, and hidden affiliations. | **Organizations Search** Map multi-tier ownership and personnel ties for deal counterparties, investors, and joint-venture partners. |
| **Threat Intelligence for High-Risk Outreach** | Detect malicious emails, domains, and multilingual terms tied to state-sponsored cyber or recruitment activity. | **Shield** Feed curated selectors into SIEM/DLP tools to identify, flag, and monitor geopolitical threats targeting employees. |
| **Open-Source Software & Contributor Risk** | Assess contributors and dependencies in open-source tooling used in internal platforms or quantitative systems. | **OSS Search** Detect state-linked contributors across open-source repos; prevent supply-chain compromise. |

**Ready to Protect Your People, Technology, & Global Operations?**

Schedule a demo to see how Strider helps enterprise financial institutions safeguard innovation, mitigate insider and geopolitical risk, and strengthen compliance across global operations.

REQUEST A DEMO →