STRIDER FOR THE TELECOMMUNICATIONS SECTOR

Protecting Critical Networks from Insider Threats and Nation-State Risks

Overview

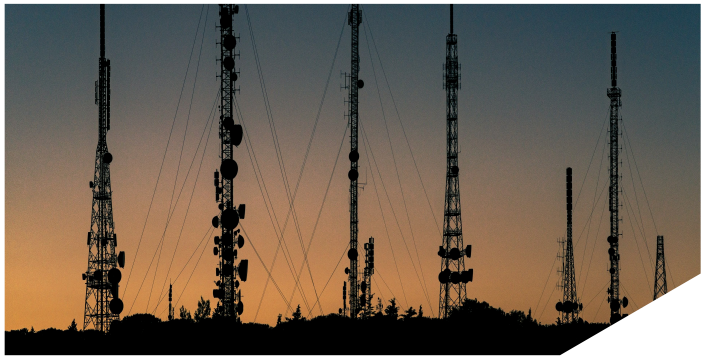
Telecommunications providers sit at the heart of national security and global connectivity, making their networks, supply chains, and engineering teams persistent targets for state-sponsored actors seeking to exploit routing systems, intercept communications, or insert compromised hardware.

Strider equips CISOs, CSOs, cyber defense teams, supply chain leaders, and insider threat programs with unified visibility into personnel risk, supply-chain exposure, and malicious communications empowering telecom operators to protect their networks, strengthen resilience, and meet regulatory expectations across distributed operations.

Telecom Security Leaders Use Strider to:

- Screen employees and contractors with privileged network access—reducing insider risk in engineering, 5G, fiber, and core-network operations.
- Vet hardware and software suppliers to detect hidden ownership, foreign control, or ties to restricted entities.
- Detect malicious outreach within cybersecurity, NOC, and network-engineering teams.
- Assess open-source contributors within routing, switching, and infrastructure software stacks.
- Protect against long-term infiltration campaigns by state-sponsored threat actors targeting infrastructure providers.

With Strider, telecom companies can secure their networks, protect customers, and maintain resilience across critical infrastructure operations.



What's at Stake

Recent incidents show how state-sponsored actors target telecom networks through personnel exploitation, supply-chain gaps, and persistent cyber intrusions.

- **Chinese State Hackers Compromise U.S. Telecom Providers (2024)**[1]: CNN revealed that PRC-linked actors infiltrated multiple American telecom networks, accessing sensitive routing systems and customer metadata highlighting the sector's systemic exposure.
- **Florida Telecommunications Worker Charged as PRC Agent (2023)**[2]: A telecom/IT contractor was charged with acting as an agent of the PRC's Ministry of State Security while maintaining system access demonstrating insider exploitation risk within major carriers.
- **Silk Typhoon Targeting IT & Telecom Supply Chains (2025)**[3]: Microsoft reported that PRC-linked Silk Typhoon actors targeted IT and telecom supply-chain providers to gain persistent access to managed infrastructure highlighting the risk of adversaries exploiting trusted vendor ecosystems.

Failure to Act Can Lead to:

- Operational Disruption: outages or manipulation of critical infrastructure affecting millions of customers.
- Regulatory & National-Security Exposure: including scrutiny from FCC, CISA, DHS, or congressional oversight.
- Nation-State Access to Core Network Infrastructure: enabling espionage, traffic interception, or systemic disruption.
- Compromised Subscriber Data: exposing law-enforcement requests, routing information, and customer communications.
- Supply-Chain Breaches: from foreign-controlled vendors supplying hardware or firmware.
- Insider Threat Incidents: contractors or employees maintaining access on behalf of foreign intelligence services.

What Strider Does for Telecommunications Providers

CAPABILITY	HOW IT HELPS	STRIDER PRODUCTS IN ACTION
Privileged-Access Vetting for Employees & Contractors	Identify hidden affiliations, falsified resumes, and state-sponsored ties before granting access to critical network systems.	**Insights, People Search, & Falsified Resume Screening:** Quickly vet internal and external personnel—especially engineers, contractors, OSS maintainers and IT staff.
Supply-Chain & Hardware Integrity	Illuminate upstream/downstream ties across device manufacturers, firmware suppliers, cloud partners, and integrators.	**Organizations Search** Surface hidden ownership, PRC or Russian affiliations, and multi-tier supplier dependencies for network hardware.
Detection of State-Sponsored Outreach	Flag adversarial recruitment attempts, malicious domains, or targeted phishing against engineering teams.	**Shield** Feed high-risk selectors into SIEM/DLP systems for identifying and monitoring risky correspondence through inbound/outbound activity.
Network Software & OSS Risk Mapping	Identify problematic contributors or dependencies in OSS used in routing, switching, or network-automation tools.	**OSS Search** Detect foreign-linked contributors and assess transitive software dependencies for APT exposure.
Continuous Insider Threat Visibility	Surface personnel with risky ties relevant to national-security threats or telecom-specific infiltration campaigns.	**Insights (My People & Network Tabs)** Identify employees with connections to strategic state-sponsored organizations.

Ready to Safeguard Your Networks & Critical Infrastructure?

Schedule a demo to see how the Strider Strategic Intelligence Platform helps telecom providers detect insider threats, secure supply chains, and prevent state-sponsored exploitation across their networks.

REQUEST A DEMO →