通信産業を支援するStrider

基幹ネットワークを内部脅威と国民国家のリスクから守ります

概要

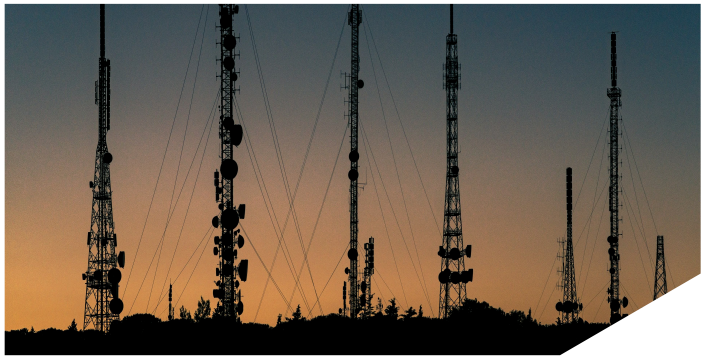
通信事業者は、国家安全保障とグローバル接続の中心におり、そのネットワーク、サプライチェーン、エンジニアリング・チームは、ルーティング・システムの悪用、通信の傍受、改ざんされたハードウェアの混入などをもくろむ国家支援型アクターによって絶えず標的にされています。

Striderは、人的リスク、サプライチェーンに起因するリスク、悪意のある通信に対する統合的な可視化を実現し、CISO、CSO、サイバー防御チーム、サプライチェーン・リーダー、内部脅威プログラムを支援します。これにより通信事業者は、ネットワークの保護とレジリエンスの強化が可能になり、また、分散した業務全体で規制当局が求める水準を満たすことができます。

通信業界のセキュリティ・リーダーはStriderで次のことが可能になります。

- ネットワークへの特権的なアクセス権を持つ従業員および請負業者をスクリーニングし、エンジニアリング、5G、光、コアネットワーク事業における内部リスクを軽減します。
- ハードウェアおよびソフトウェアのサプライヤーを精査して、隠れた所有関係、外国支配、規制対象組織とのつながりを検出します。
- サイバーセキュリティ、NOC、ネットワーク・エンジニアリングの各チーム内で悪意のある接触を検出します。
- ルーティング、スイッチング、インフラ関連の各ソフトエア・スタック内でオープンソースのコントリビューターを評価します。
- インフラ事業者を狙う国家支援型の脅威をもたらす行為者による長期的な侵入行為から保護します。

Striderを使用すると、通信会社は保有するネットワークの安全性を確保し、顧客を守り、基幹インフラ運用全体でレジリエンスを維持できます。



危険にさらされているもの

最近のインシデントから、国家支援型の行為者がどのようにして、従業員の搾取、サプライチェーンの欠陥、持続的なサイバー侵入を通じて通信ネットワークを狙っているかが分かります。

- **中国政府系ハッカーが米国通信会社に不正侵入（2024年）[1]:** CNNは、中国とつながりのあるアクターが米国の複数の通信ネットワークに侵入し、機密性の高いルーティング・システムや顧客メタデータにアクセスしていることを明らかにしました。このケースは、この産業に構造的に内在するリスクを浮き彫りにしています。
- **フロリダの通信会社社員、中国工作員として活動した疑いで起訴（2023年）[2]:** 通信/ITの契約社員が、中国国家安全部の工作員として活動した容疑で起訴されました。システムへのアクセス権を保持した状態で行われたこのスパイ行為は、大手キャリア内に存在する内部からの悪用リスクを露呈しました。
- **Silk TyphoonがIT・通信サプライチェーンを標的に（2025年）[3]:** マイクロソフトの報告によると、中国とつながりがあるSilk Typhoonの行為者が、管理インフラへの持続的なアクセスを確保するために、IT・通信のサプライチェーン・プロバイダーを標的にしていました。このケースは、信頼されているベンダー・エコシステムが攻撃者によって悪用された際のリスクを際立たせています。

対応を怠った場合には次のことが起こる可能性があります。

- 業務の混乱：基幹インフラの停止や不正操作で何百万もの顧客に影響が及びます。
- 規制および国家安全保障上のリスク：FCC、CISA、DHS、議会監督による厳しい審査などがあります。
- 国家主体によるコア・ネットワーク・インフラへのアクセス：スパイ行為、通信遮断、システム全体に及ぶ障害を引き起こすことが可能になります。
- 利用者データの侵害：法執行機関からの要請、ルーティング情報、顧客とのやり取りなどが漏えいします。
- サプライチェーンへの不正侵入：ハードウェアまたはファームウェアを提供する外国の支配下にあるベンダーに起因します。
- 内部脅威によるインシデント：請負業者または従業員が外国の諜報機関の利益のためにアクセス権を保持します。

通信事業者を支援するためのStriderの機能

機能	どのように役立つか	Strider製品の活用例
従業員および請負業者の特権アクセス権の精査	隠れた関係性、虚偽の経歴、国家支援型行為者とのつながりを、基幹ネットワーク・システムへのアクセス権を付与する前に特定します。	**Insights、People Search、履歴書詐称スクリーニング：** 内部および外部の人員、特に、エンジニア、請負業者、OSS保守担当者、ITスタッフを迅速に精査します。
サプライチェーンおよびハードウェアの整合性	デバイス・メーカー、ファームウェア・サプライヤー、クラウド・パートナー、インテグレーター全体にわたって、上流/下流の関係性を明らかにします。	**Organizations Search** 隠れた所有関係、中国またはロシアとの関係性、ネットワーク・ハードウェアにおけるサプライヤー各層の依存関係を可視化します。
国家支援型行為者による接触の検出	敵対勢力による勧誘の試み、悪意のあるドメイン、エンジニア・チームを標的としたフィッシングに警告を出します。	**Shield** 高リスクのセレクターをSIEM/DLPシステムに入力して、インバウンド/アウトバウンド通信の挙動に基づいてリスクのある通信を特定、監視します。
ネットワーク・ソフトウェアおよびOSSのリスク・マッピング	ルーティング、スイッチング、ネットワーク自動化の各ツールに使用されているOSSの、問題のあるコントリビューターや依存関係を特定します。	**OSS Search** 外国勢力とつながりのあるコントリビューターを検出し、ソフトウェアの推移的依存関係のAPTリスクを評価します。
内部脅威の継続的な可視化	国家安全保障上の脅威や通信事業者に特化した侵入行為に関してリスクのあるつながりを持つ人員を明らかにします。	**Insights（「My People」タブおよび「Network」タブ）** 戦略的な国家支援型組織との接点を持つ従業員を特定します。

貴社のネットワークと基幹インフラを保全する準備はできましたか？

是非デモをご予約ください。Striderの戦略的インテリジェンス・プラットフォームが、通信事業者による内部脅威の検出、サプライチェーンの保護、ネットワーク全体における国家支援型アクターによる悪用の阻止をどのように支援するかをご紹介します。

デモを申し込む →