SILENT PUSH

TRAFFIC ORIGIN: AMER ROI FOR CISOS AND EXECUTIVES

For a CIO, CISO, or Chief Risk Officer, the value of Traffic Origin lies in its ability to automate defense against high-stakes threats that bypass traditional Geo-IP and identity tools. By providing upstream origin certainty, the platform strengthens identity verification, KYC/KYB checks, and AML enforcement. This document outlines the ROI across cost avoidance, regulatory compliance, and operational efficiency.

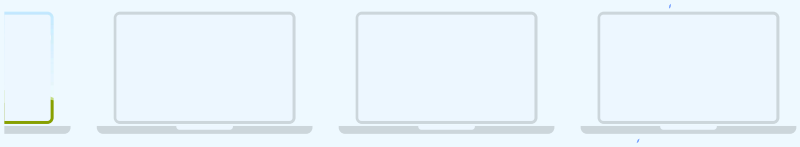
THE COST OF MISSING THE INSIDER THREAT

The most immediate financial return comes from preventing the hiring of fraudulent workers. Traditional background checks fail because these actors use stolen US identities and domestic laptop farms.

Traffic Origin helps prevent the catastrophic legal and security consequences of hiring a state sponsored operative or fraudulent remote contractors. Traditional background checks and video interviews are now bypassed by AI deepfakes and domestic laptop farms that present a clean local image to recruiters.

1 - OFAC SANCTIONS LIABILITY

Paying a DPRK operative is a direct violation of US Treasury and UN sanctions. Recent DOJ enforcement actions have resulted in over $15 million in civil forfeitures and potential prison sentences for facilitators. Traffic Origin provides a defensible layer by unmasking the upstream connection to sanctioned regions before the first payment is made.



2 - PREVENTION OF INSIDER ESPIONAGE

These workers are often high level cyber operatives. Once inside, they use legitimate access to install backdoors, steal export controlled technology, or exfiltrate proprietary source code. Traffic Origin identifies the technical signatures of residential proxy hops during the onboarding phase to neutralize the threat before they gain administrative rights.

3 - AVOIDING VICTIM LABELING

Being named in a DOJ indictment or an FBI announcement as a compromised organization carries massive reputational damage. Traffic Origin moves the organization from reactive victim status to proactive defense. This proves to the board and regulators that specific controls are in place to detect the sophisticated routing used by nation state actors

4 - WORKFORCE INTEGRITY

Beyond state actors like the DPRK, professional job milling groups use similar proxy tactics to place unqualified workers into high salary remote roles. These actors often hold multiple full time positions simultaneously, leading to payroll fraud and the introduction of unmanaged shadow access. Traffic Origin identifies these inconsistent connection patterns to protect the integrity of the remote workforce.

WHY EXISTING SOLUTIONS ARE FAILING

Legacy tools refer to GeoIP databases, 'IP reputation' feeds, SIEMs, and standard KYC/AML platforms.

- **Last-hop blindness:** They only see the entry point IP. Attackers use residential proxies and VPNs to look "clean" and local.
- **Easy evasion:** Reputation feeds miss threats using new or rotating ISP infrastructure with no prior history of abuse.
- **Compliance risk:** KYC systems validate the proxy location rather than the true upstream country, allowing sanctions evasion.
- **Lack of context:** Risk engines cannot distinguish between a local employee and an "invisible insider" routing traffic from a high-risk region.

ROI SUMMARY

Category	Status Quo	Traffic Origin Outcome
Insider threat	Identity theft and laptop farms bypass HR; organization risks OFAC sanctions.	Blocks hire: Unmasks upstream connections to sanctioned regions before payroll begins.
Espionage & threat	Operatives gain legitimate access to install backdoors or exfiltrate source code.	Neutralizes threat: Identifies proxy hop signatures to deny access to sensitive infrastructure.
High risk login	Analysts spend hours manually triaging vague travel alerts and VPN detections.	Automated response: High confidence risk labels trigger immediate MFA or blocks in Okta/Azure AD.
KYC and AML	Identify the source and destination of customers, money trails, and the conversion of crypto to fiat before traffic and money flows to sanctioned countries	Address compliance: Ensure business compliance with governmental regulations
Corporate standing	Organization is labeled a victim in federal indictments and FBI advisories.	Proactive defense: Demonstrates to the board and regulators that specific proxy detection is active.

REAL CASES: WHY YOU SHOULD CARE - AMER

- U.S. authorities launched a nationwide crackdown on North Korean remote IT worker schemes, finding fake laptop farms in 16 states and indictments tied to 100+ companies and over $3 million in damages. (justice.gov)
- In one DOJ case, co-conspirators used stolen and fake identities to land remote IT jobs at U.S. firms and steal sensitive, export-controlled data. (justice.gov)
- FBI searches of 21 "laptop farm" sites showed how fake remote profiles and U.S.-based IPs can bypass geolocation checks. (justice.gov)
- A North Korean IT worker scheme involved dozens of fake U.S. host identities and laptops, generating revenue funneled back to the DPRK and causing millions in legal and remediation costs for victim companies. (justice.gov)
- Earlier DOJ indictments charged North Korean nationals and U.S. facilitators with a multi-year fraudulent IT worker scheme, showing how identity obfuscation can bypass conventional controls. (justice.gov)
- Multiple individuals have pleaded guilty in related cases for helping North Korean IT workers infiltrate U.S. companies, highlighting the operational and legal risks when remote access is trusted based on IP alone. (The Hacker News)

REAL CASES: WHY YOU SHOULD CARE - EMEA

- The UK's OFSI issued a critical advisory warning that firms are being targeted by North Korean IT workers using laptop farms and residential proxies to fund illegal programs. (gov.uk)
- European authorities identified facilitators in the UK and Germany hosting corporate devices to make remote operatives in sanctioned regions appear as domestic residents. (therecord.media)
- In a 2025 enforcement action, a global firm with UK headquarters was penalized nearly £500,000 for sanctions violations, showing zero tolerance for unauthorized payments to sanctioned regions. (jerseyfsc.org)
- The PurpleBravo campaign targeted firms in Belgium, Italy, and the Netherlands using fake interviews and deepfake personas to infiltrate AI and financial sectors. (thehackernews.com)
- UK security agencies documented cases where fraudulent IT workers gained privileged access and then threatened organizations with extortion and proprietary code leaks. (therecord.media)
- Google's Threat Intelligence Group reported a single North Korean worker operating 12 different personas across Europe to target defense companies and government agencies. (staffingindustry.com)

REAL CASES: WHY YOU SHOULD CARE - APJ

- The governments of Japan, South Korea, and the U.S. issued a joint 2025 alert warning that North Korean IT workers are expanding global operations to fund sanctioned weapons programs. (state.gov)
- Australian authorities warned firms that DPRK actors use VPNs and residential proxies to appear domestic while operating from China or Russia to steal intellectual property. (dfat.gov.au)
- Japan updated its national "Alert for Companies" in late 2025, providing new evidence of state-sponsored operatives using AI voice changers and deepfakes to pass technical interviews. (mofa.go.jp)
- Cybersecurity reports confirmed that 60% of global crypto thefts in 2025 were linked to North Korean hacks, often initiated by workers embedded within APJ financial services. (onu.delegfrance.org)
- A major South Korean defense contractor faced an attempted state-sponsored intrusion by operators using fraudulent identities to bypass standard perimeter security in 2025. (industrialcyber.co)
- Authorities in Taiwan and the UAE identified facilitators who set up shell companies to funnel millions in illicit salary payments back to sanctioned entities in East Asia. (justice.gov)