TRAFFIC ORIGIN: THE GOLD STANDARD FOR FRAUD, AML, AND KYC

ELIMINATING THE "GEOGRAPHIC BLIND SPOT" IN FINANCIAL COMPLIANCE

THE INVISIBLE RISK: SOPHISTICATED FINANCIAL EVASION

Modern money launderers and fraud syndicates no longer use "dirty" IP addresses. They use **Residential Proxy-as-a-Service (RPaaS)** and **multi-hop VPNs** to appear as legitimate domestic customers. This allows sanctioned actors and professional fraudsters to bypass geo-fencing and pass initial KYC checks undetected.

For banks and FinTechs, this creates three critical vulnerabilities:

- **The Attribution Gap:** A customer appears to be in London, but their session is being controlled by a sanctioned actor in Russia or Iran.
- **The Crypto-Fiat Gateway:** Illicit funds are "washed" through mixers and then cashed out into fiat currency via banks that cannot see the transaction's true geographic origin.
- **Synthetic Identity Fraud:** Fraudsters use stolen or synthetic IDs paired with domestic IPs to bypass automated onboarding systems.

OPERATIONAL IMPACT & COMPLIANCE OBJECTIVES

OBJECTIVE	TRAFFIC ORIGIN DELIVERY
Prevent Sanctions Breaches	Real-Time Sanctions Guardrails: Block connections from sanctioned regimes (Russia, Iran, North Korea) that attempt to bypass filters by masquerading as local domestic users.
Enhance KYC & KYE	Geographic Truth: Strengthen "Know Your Customer" and "Know Your Employee" protocols by verifying that a user's physical location matches their digital footprint, exposing synthetic identities and "laptop farms."
Uplift Cyber Investigations	True Attribution: Reveal the actual origin behind VPNs and residential proxies. This provides a much higher-confidence indicator by proving a connection is not where it claims to be, allowing IR teams to link activity to known state-sponsored TTPs.
Real-Time Fraud Prevention	High-Confidence Orchestration: Feed "Very High Risk" indicators into SIEM/SOAR/Risk Engines to trigger immediate MFA challenges, account lockouts, or transaction holds before funds leave the system.

KEY USE CASES FOR FINANCIAL INSTITUTIONS

1. UNMASKING THE "TRUE" UPSTREAM ORIGIN

Adversaries use VPNs and proxies to hide their traces. Traffic Origin identifies the Countries Connected to an IP, exposing sessions that appear to originate in London or New York but are actually routed from high-risk or sanctioned jurisdictions.

2. HARDENING THE FIAT-TO-CRYPTO BRIDGE

Traffic Origin provides the missing link between digital assets and traditional banking. By analyzing the true origin of entities interacting with exchanges, defenders can identify when a "clean" domestic withdrawal is actually backhauled from a sanctioned region or a high-risk crypto mixer.

3. TRANSITIONING FROM REACTIVE TO PREDICTIVE

Traditional risk engines create "alert fatigue" by flagging all proxies. Traffic Origin utilizes enriched Silent Push datasets to provide a definitive risk indicator. This allows AML teams to move away from manual review and toward automated, predictive blocking of high-risk traffic.

Traffic Origin delivers the precise intelligence needed to dismantle identity obfuscation.

By exposing the hidden origins of a connection, you investigate the infrastructure with absolute certainty, cutting through layers of deception to identify the real-world source of risk.

ABOUT US

Silent Push is a pre-emptive cyber defense platform that exposes threat actor infrastructure before attacks are launched. Using **Indicators of Future Attack (IOFA™)**, Silent Push maps the internet from an attacker's perspective, revealing malicious infrastructure as it is being established. This enables security teams to disrupt threats early, reduce organizational risk, and move beyond reactive cybersecurity.

Neutralize before compromise.

SILENT **PUSH**

PREEMPTIVE CYBER DEFENSE WITH INDICATORS OF FUTURE ATTACK™

REQUEST A DEMO

silentpush.com