Silent Push Introduces Traffic Origin for Preemptive Cyber Defense Against Identity Obfuscation

Launch of Traffic Origin provides first dedicated defense layer against state-sponsored identity fraud and "laptop farm" infiltrations

RESTON, VA, UNITED STATES, January 22, 2026 /EINPresswire.com/ -- Silent Push, a leading preemptive cybersecurity vendor, today announced the debut of Traffic Origin, a unique cybersecurity solution that shifts an organization's security posture from reactive to proactive by exposing the true upstream origin of adversaries—whether they are hiding via residential proxy, laptop farm, virtual private network (VPN), or other obfuscation technique.

> Silent Push Traffic Origin empowers organizations to detect if seemingly legitimate web traffic is actually being routed from high-risk regions or adversary-controlled infrastructure."
>
> *Ken Bagnall*

Silent Push Traffic Origin continues the company's mission to give defenders the advantage by providing origin certainty where other defensive tools see nothing but obfuscation. Traffic Origin allows investigators to identify high-risk remote sessions before they escalate into attacks or credential theft.

Traffic Origin Key Capabilities and Detection:

Traffic Origin unmasks the "masking layer" of state-sponsored and cyber criminal actors through three core pillars:

-Upstream Traffic Discovery: Goes beyond the surface to reveal the true origin of web traffic. Traffic Origin identifies the "Countries Connected" to an IP, analyzing upstream routing sources, IP address reputation and density, as well as host diversity and categorization (VPN, proxy, Tor, or residential Proxy).

-High-Confidence Risk Indicators: Eliminate analyst guesswork. Traffic Origin provides a definitive indicator when a residential proxy is routing traffic from sanctioned or high-risk countries (such as DPRK/North Korea, Iran, or Russia).

-Total View Context: Visual correlation within the Silent Push platform. See the "UK" or "US" flag on an IP while simultaneously viewing the direct link to upstream traffic from high-risk zones.

“Silent Push Traffic Origin empowers organizations to detect if seemingly legitimate web traffic is actually being routed from high-risk regions or adversary-controlled infrastructure,” said Ken Bagnall, CEO at Silent Push. “This gives security teams the immediate capabilities to mitigate fraud, identify high-risk logins, vet remote workers, and improve processes of Know Your Customer (KYC) and Anti-Money Laundering (AML).

The "Invisible" Insider Threat that Organizations Face:

Traditional cyber defense is inherently reactive, detecting attacker infrastructure only after it is used in an attack. Today’s most sophisticated adversaries, especially DPRK (North Korea) IT workers, exploit this lag by "hiding in plain sight."

A significant example of this threat actor behavior is the use of fraudulent personas to gain legitimate employment, followed by the use of sophisticated obfuscation techniques to bypass geographic restrictions, which include:
-Laptop Farms: U.S.-based facilitators host company laptops accessed via hardware KVM switches.
-Residential Proxies: Masking true locations (often sanctioned jurisdictions) to appear as local, domestic residential traffic.
-Infrastructure Mimicry: Using valid credentials and domestic IPs to bypass standard Conditional Access and MFA policies.

The result is high-risk actors that appear as legitimate remote employees, creating a devastating insider threat that traditional defenses cannot detect.

To learn more, start a conversation with Silent Push preemptive cyber defense experts and Book a Demo to see how we can help you uncover attacker infrastructure by searching smarter, faster, and with greater confidence.

About Silent Push
Silent Push is a preemptive cyber defense company. It is the first and only solution to provide a complete view of emerging threat infrastructure in real-time, exposing malicious intent through its Indicators Of Future Attack™ (IOFA™) data to enable security teams to proactively block hidden threats and avoid loss. The Silent Push standalone platform is also available via API, integrating with various security tools, including SIEM & XDR, SOAR, TIP, and OSINT, providing automated enrichment and actionable intelligence. Customers include some of the world's largest enterprises within the Fortune 500 as well as government agencies. A free Community Edition is available. For more information, visit www.silentpush.com or follow on LinkedIn and X.

Michelle Kearney
Hi-Touch PR
+1 443-857-9468

email us here
Visit us on social media:
LinkedIn
