Silent Push Product Messaging Source Document (MSD)

Last edited: February 9, 2026

This document provides approved messaging for Silent Push – please use the messaging within this document and the associated PowerPoint (SALES DECK UNDER REVIEW BY KEN) to ensure consistency in the marketplace. This is meant to be a living document and will be updated regularly.

Must read:

1. **THIS IS NOT A CUSTOMER FACING DOCUMENT** – it's for Marketing and Sales teams to *create consistent* collateral, campaigns, webinars, website copy etc.
2. Remember that product messaging is storytelling and is told in a pyramid structure with a small amount of information at first, then building the story piece by piece, adding more detail each time.
3. Lastly, consistency is critical to effective messaging so rather than going off script, help us keep this document up to date.

Language Style

Always use American spelling, grammar, and data format. Use US Eastern Time as the key reference time (our HQ location is Reston). If possible, use date formats that are un-ambiguous such as "02 Feb 23". Avoid use of seasonal references such as "Fall Summit" as this is confusing to people in the southern hemisphere, and UK uses "autumn". Instead say something like "Q3 Summit".

Brand Usage

Product Brand	**Silent Push**
Company Brand	Silent Push, Inc. — *DO NOT USE IN MARKETING MATERIALS*
Brand Usage	Avoid possessive usage. For example, use "the Silent Push value…" instead of "Silent Push's value…"
Abbreviation	DO NOT EVER ABBREVIATE COMPANY NAME TO "SP" DO NOT ABBREVIATE FEATURES e.g., NO "TIM"
Our Industry	Preemptive Cyber Defense
Gartner Categories	Primary: Preemptive Cyber Defense

About Silent Push

25 words

Silent Push provides a Preemptive Cyber Defense platform that continuously discovers and tracks adversary infrastructure, enabling teams to detect and disrupt emerging threats before attacks launch.

50 words

Silent Push provides a Preemptive Cyber Defense platform that gives real-time visibility into previously unknown adversary infrastructure. By continuously tracking the infrastructure attackers rely on to stage operations, Silent Push allows security teams to detect emerging threats earlier, investigate activity in context, and disrupt attacks before they escalate.

100 words –

Silent Push provides a Preemptive Cyber Defense platform that gives real-time visibility into previously unknown adversary infrastructure. Instead of waiting for an alert to trigger, the platform continuously tracks the staging grounds attackers rely on to launch operations. By using our **Context Graph** to map the "Internet's DNA," Silent Push identifies malicious management patterns to generate **Indicators of Future Attack™ (IOFA™)**.

Our API-first solution integrates seamlessly with SIEM and SOAR tools, allowing teams to automate the enrichment and blocking of threats weeks or months before weaponization. This allows organizations to move from reactive alerts to a truly proactive defense.

150 words

Silent Push provides a Preemptive Cyber Defense platform that delivers real-time visibility into previously unknown adversary infrastructure. Powered by the Context Graph, the platform continuously discovers and tracks the domains, IPs, and hosting providers attackers rely on to stage and execute operations.

By focusing on infrastructure rather than waiting for known indicators, Silent Push reveals threat activity earlier in the attack lifecycle. This often occurs well before weaponization. Security teams use **Indicators of Future Attack™ (IOFA™)** to investigate activity in context, track changes over time, and understand how adversaries operate across the global internet.

Silent Push combines this automated discovery with analyst-driven investigation, offering the flexibility to work within a dedicated console or via seamless integration with SIEM and SOAR platforms. The result is earlier detection and more confident response decisions that help

organizations stay ahead of evolving threats by identifying the "Internet's DNA" of an attack before it launches.

200 words

Silent Push provides a Preemptive Cyber Defense platform that delivers real-time visibility into previously unknown adversary infrastructure. Powered by the Context Graph, the platform continuously discovers and tracks the domains, IPs, and hosting providers attackers rely on to stage and execute operations.

This infrastructure-first approach allows security teams to identify emerging campaigns earlier in the attack lifecycle. This is frequently accomplished before payloads or phishing pages are even deployed. By leveraging the Context Graph to generate **Indicators of Future Attack™ (IOFA™)**, defenders can investigate activity in context and understand adversary behavior as it evolves across the internet.

Built with an API-first architecture, the platform allows analysts to pivot across infrastructure relationships via the native console or ingest data directly into existing SIEM, SOAR, and TIP stacks for automated enrichment and blocking. This supports both automated discovery and deep, analyst-driven workflows, enabling teams to move faster without sacrificing accuracy.

Used by security operations and threat hunting teams, Silent Push shifts the balance from reactive defense to proactive disruption. By making previously unknown infrastructure visible and actionable, the platform enables defenders to neutralize threats weeks or months before weaponization. This ensures organizations stay one step ahead of the adversary's next move.

Market Storyline

For years, security teams have built their defenses around what they can already see: alerts, malware, known indicators, and activity that has already crossed into their environment. While these approaches are necessary, they are inherently reactive. By the time most tools surface a threat, the adversary has already established infrastructure, launched campaigns, or begun targeting victims.

At the same time, attackers have adapted. Modern adversaries operate across a constantly changing internet footprint—registering domains, shifting hosting providers, rotating IPs, and standing up short-lived infrastructure designed to stay ahead of detection. Much of this infrastructure exists long before an attack occurs, but remains invisible to traditional security tools.

The gap in the market is visibility. Security teams lack a reliable way to see adversary-controlled infrastructure while it is being built and operated, not just after it is used.

Silent Push addresses this gap by providing a Preemptive Cyber Defense platform real-time visibility into adversary-controlled internet infrastructure that was previously unknown. Instead of waiting for alerts or known indicators, the platform continuously discovers and tracks the infrastructure attackers rely on to stage and execute operations. This allows defenders to detect emerging threats earlier in the attack lifecycle, investigate activity in context, and understand how adversaries operate across the internet.

By making previously unseen infrastructure visible, Silent Push enables a shift from reactive defense to proactive threat discovery and disruption—giving security teams time, context, and control before attacks reach their environment.

Mission

Everyone deserves to be able to defend themselves. Our mission is to replace reactive security with preemptive defense by providing the definitive Context Graph of the internet; exposing hidden infrastructure management patterns to enable the earliest possible detection of adversary intent

Vision Statement

To empower the world's defenders to see earlier, act faster, and disrupt adversary infrastructure before it becomes an attack

Business Value – Why Silent Push

Silent Push delivers business value by reducing the cost and impact of cyber risk through earlier detection and disruption of attacker infrastructure at a point when it is cheaper and easier to contain. IBM's 2025 *Cost of a Data Breach Report* estimates the global average cost of a data breach at around **$4.44 million**, with some industries and regions far higher, illustrating the significant financial exposure organizations face when incidents occur.

By identifying threats before campaigns are launched, Silent Push helps organizations avoid these downstream costs of incidents, including response, recovery, downtime, regulatory fines, and reputational damage, and reduces analyst effort by shortening investigation and response timelines.

Because Silent Push integrates directly into SIEM, SOAR, and threat intelligence workflows, it increases the return on existing security investments without adding operational overhead, lowering breach likelihood and making security operations costs more predictable while strengthening overall risk posture.

Key Terms (to use and repeat)

Product Brand	Silent Push
Neutralize Before Compromise	What is it: Company tagline and core value proposition Silent Push enables defenders to neutralize before compromise by identifying attacker infrastructure and Indicators of Future Attack (IOFA)™ before threats are operationalized.
Indicators of Future Attack (IOFA™)	What is it: Proprietary early-warning system Indicators of Future Attack (IOFA)™ identify adversary infrastructure during the setup and staging phases, before an actual attack is launched. Unlike traditional Indicators of Compromise (IOCs) that focus on past events, IOFAs enable security teams to preemptively detect and block threats by analyzing pre-weaponized patterns in domains and hosting environments. MSD Rule: Always capitalize. Use ™ on first reference. Pluralize as IOFAs.
Behavioral Fingerprints	What is it: Behavioral fingerprints refer to pattern-based infrastructure attributes. These are used to produce IOFAs, enabling security teams to preemptively detect and block threats by analyzing pre-weaponized patterns in domains and hosting environments. By creating behavioral fingerprints of adversary infrastructure, Silent Push provides a persistent series of searchable, advanced infrastructure and behavioral attributes used to identify, correlate, and surface Indicators of Future Attack (IOFA)™ across the Silent Push dataset.
Indicators of Compromise (IOCs)	What is it: Retrospective, post-compromise indicators Indicators that identify activity after compromise. IOCs are often stale, easily evaded, and do not provide insight into emerging or developing threats. MSD Rule: Use *only* in contrast to IOFAs.
Emerging Threats	What is it: Developing, pre-weaponized threats and infrastructure Adversary activity and infrastructure that has not yet been widely detected, operationalized, or weaponized. Common phrases to refer to: “pre-weaponized infrastructure”, “infrastructure in staging”, “infrastructure being set up for an attack”
Adversary Infrastructure	What is it: The core object of analysis Internet-facing assets controlled or leveraged by threat actors, including domains, IPs, certificates, hosting, and DNS infrastructure.
Adversary Infrastructure	What is it: Primary product output Infrastructure derived from discovering, correlating, and tracking attacker-controlled infrastructure rather than victim-side artifacts.

Legacy Threat Intelligence	What is it: Competitive positioning term Traditional, retrospective, IOC-driven threat intelligence that relies on aggregated third-party feeds and provides limited early warning. MSD Rule: Use for competitive framing and analyst discussions. Do not position Silent Push as Threat Intelligence. The Silent Push platform enables Preemptive Cyber Defense.
Preemptive Threat Intelligence	What is it: Industry and analyst-aligned use this term in some cases. Most threat intelligence focuses on activity after compromise. Silent Push is a Preemptive Cyber Defense Platform. Silent Push shifts security teams upstream by identifying Indicators of Future Attack (IOFA™), providing early visibility into adversary infrastructure so threats can be disrupted before attacks occur. "Neutralize Before Compromise". MSD Rule: NEVER refer to Silent Push as a 'preemptive threat intelligence platform".
Adversary Campaigns	What is it: Operational construct. Coordinated sets of adversary infrastructure and activity associated with a specific threat actor, objective, or attack pattern.
Infrastructure Relationships	What is it: How Silent Push creates context The technical and behavioral connections between domains, IPs, certificates, DNS records, and hosting that reveal attacker infrastructure before the infrastructure is used in an attack.
PADNS	What is it: Passive Aggressive DNS PADNS is a proprietary Silent Push data collection method that actively forces the resolution of DNS records (such as domains and IPs), rather than relying solely on historical or passive traffic data. This active approach provides a comprehensive, real-time view of internet infrastructure, allowing analysts to track daily changes in A records, name servers, and other DNS data points that traditional passive DNS might miss.
Traffic Origin	Silent Push Traffic Origin shifts your security posture from reactive to proactive by exposing the true upstream country-of-origin of the adversary, whether they are hiding via residential proxy, laptop farm, VPN or other obfuscation techniques. By providing origin certainty where other tools see only obfuscation, Traffic Origin allows investigators to identify high-risk remote sessions before they escalate into attacks or credential theft.
The Context Graph	The **Context Graph** serves as the foundational engine for preemptive cyber defense, mapping the "Internet's DNA" to expose the 95% of adversary infrastructure hidden from traditional security tools. By pre-correlating a massive global dataset, comprising of Passive-Aggressive DNS (PADNS), WHOIS, certificates, traffic sensors, and content hashes, the Context Graph continuously analyzes benign, gray, and malicious infrastructure to detect adversary "management patterns" rather than just active exploits.

	This approach targets the **preparation phase** of the attack lifecycle, identifying threats during staging and configuration to generate **Indicators of Future Attack (IOFAs)** ™ with deterministic certainty. By delivering this high-fidelity context, the Context Graph allows security teams to automate the neutralization of threats weeks or months before weaponization occurs.

Products / Market Categories

Insight	Reconnaissance	Defend
Understand unknown infrastructure quickly and at scale. Key Capabilities • Accelerated Triage via Total View Consolidates 10+ data types (passive DNS, WHOIS, web content, infrastructure variance) into a single view to eliminate manual pivots across point tools. • Granular Data Categorization Enriches domains and IPs with 70–100+ attributes (fuzzy hashes, certificates, JARM) to provide deep context beyond DNS alone. • Automated Risk Scoring Assigns proprietary Risk Scores to prioritize alerts, reduce false positives, and lower analyst workload. • Instant Threat Clustering Uses Context Similarity to quickly identify related malicious infrastructure and guide investigations. • Seamless Security Stack Integration Feeds enrichment directly into SIEM, SOAR, and TIP workflows to	Reveal adversary campaigns before they are weaponized. Key Capabilities • Preemptive Identification of Staging Infrastructure Uses IOFA™ to discover and map attacker domains, IPs, and services during setup and staging phases. • Granular Behavioral Fingerprinting Connects related infrastructure by tracking adversary TTPs across 200+ parameters. • Exposure of the “Hidden 98%” Surfaces attacker infrastructure missed by traditional tools through first-party IPv4/IPv6 scanning. • Advanced Content Correlation Applies fuzzy hashing (e.g., ssdeep) via Context Similarity and Web Scanner to uncover clusters of related malicious domains. • Seamless Security Stack Integration Enriches alerts with IOFA™ context and enables automated	Act early with confidence using deterministic signals. Key Outcomes • Alert Prioritization Reduce alert fatigue by surfacing only signals tied to verified attacker infrastructure. • Early Action Take proactive measures against pre-weaponized infrastructure at the earliest stages of detection. • Maximize Existing Investments Integrate IOFA™ data directly into SIEM, SOAR, firewalls, and TIP workflows to strengthen defenses and increase ROI, enabling security teams to preemptively detect and block threats by analyzing pre-weaponized patterns in domains and hosting environments.

accelerate response and maximize existing investments.	response via SIEM, SOAR, and TIP platforms.	

Insight — Copy Blocks

Insight — 1 Sentence

Insight gives security teams immediate clarity into unknown threat infrastructure, enabling fast, confident decisions without manual investigation overhead.

Insight — 25 Words

Insight helps security teams quickly understand unknown infrastructure by consolidating enrichment, risk scoring, and correlation into a single view—reducing noise and accelerating investigations.

Insight — 50 Words

Insight enables security teams to rapidly assess unknown domains and IPs by consolidating enrichment, correlation, and risk scoring into a single platform. By eliminating manual pivots across point tools, analysts gain immediate clarity into what an observable is, how it's being used, and why it matters.

Insight — 100 Words

Insight gives security teams immediate clarity into unknown and emerging threat infrastructure. By consolidating enrichment, analysis, and correlation into a single platform, Silent Push enables analysts to quickly understand what an observable is, how it's being used, and why it matters—without relying on multiple point tools or manual pivots.

Using Total View, domains and IPs are enriched with dozens of contextual attributes, correlated across infrastructure patterns, and assigned a proprietary Risk Score. This allows teams to prioritize relevant threats, reduce false positives, and accelerate investigations while seamlessly integrating findings into existing SIEM, SOAR, and TIP workflows.

Insight — 150 Words

Insight enables security teams to quickly make sense of unknown and emerging threat infrastructure. By unifying enrichment, correlation, and analysis into a single platform, Silent Push eliminates the need for analysts to pivot across multiple tools to understand what an observable is and why it matters.

Through Total View, domains and IPs are enriched with 70–100+ contextual attributes—including web content, certificates, DNS data, and infrastructure patterns—and evaluated using a proprietary Risk Score. Analysts can immediately assess risk, prioritize relevant threats, and reduce investigation time and alert fatigue.

Insight also provides directionality during investigations. Using capabilities such as Context Similarity, analysts can identify related malicious infrastructure, cluster threats by shared patterns, and efficiently expand investigations. All insights integrate directly into existing SIEM, SOAR, and TIP workflows, accelerating response while maximizing the value of existing security investments.

Reconnaissance — Copy Blocks

Reconnaissance — 1 Sentence

Reconnaissance reveals adversary infrastructure and campaigns early, allowing teams to disrupt threats before they are weaponized.

Reconnaissance — 50 Words

Reconnaissance enables security teams to uncover attacker-controlled infrastructure during setup and staging phases. By identifying domains, IPs, and services early, teams gain visibility into emerging campaigns before phishing, fraud, or intrusion activity begins.

Reconnaissance — 100 Words

Reconnaissance focuses on exposing adversary infrastructure before it is weaponized. Using Indicators of Future Attack (IOFA™), Silent Push enables analysts to discover and map attacker-controlled domains, IPs, and services as campaigns are being prepared.

Behavioral fingerprinting and content correlation allow teams to connect related infrastructure, identify shared deployment patterns, and understand the full scope of adversary activity—well before attacks are launched.

Defend — Copy Blocks

Defend — 1 Sentence

Defend enables security teams to act early with confidence using verified indicators tied to verified attacker infrastructure.

Defend — 50 Words

Defend operationalizes Indicators of Future Attack (IOFA™) to prioritize alerts, reduce noise, and enable early action against pre-weaponized infrastructure—helping teams disrupt campaigns before they become incidents.

Defend — 100 Words

Defend turns early warning indicators into action. By operationalizing Indicators of Future Attack (IOFA™), Silent Push helps security teams focus on verified attacker infrastructure, reduce alert fatigue, and take proactive measures at the earliest stages of detection.

IOFA™ data integrates directly into SIEM, SOAR, firewall, and TIP workflows, enabling faster response and maximizing the value of existing security investments.

Data Principles

Silent Push is built on data that is **preemptive**, providing visibility early enough for defenders to block, alert on, or harden against threats before an attack is launched. The platform is **proactive**, enabling security teams to act upstream on adversary-controlled infrastructure rather than reacting to downstream alerts or incidents. Silent Push data is **deterministic**, representing verified attacker-controlled infrastructure linked to known adversary behavior—not probability scores, generic feeds, or ambiguous signals. Together, these principles ensure teams can take confident, actionable steps **before attackers act**.

Value Proposition

For: (Target customer)	The Silent Push Preemptive Cyber Defense platform is designed for organizations with security teams for earlier visibility into adversary-controlled internet infrastructure to detect and disrupt threats before attacks occur**.** **Organizations with active security operations** • SOC teams, threat analysts, incident response, and threat hunting functions **Enterprises and regulated organizations** • Financial services, technology, healthcare, energy, critical infrastructure. This is applicable across all verticals. **Government and public sector** • Federal, defense, and law enforcement organizations monitoring external threat activity **Security teams overwhelmed by reactive alerts** • Teams looking to move upstream from detection to prevention
Who are: (Pain or need)	Security teams lack visibility into adversary-controlled internet infrastructure before it is used in attacks, forcing them to operate reactively instead of preventing threats early. • **They only see threats after damage is possible** Alerts arrive after phishing emails are sent, malware is delivered, or exploitation begins. • **Attackers operate infrastructure long before attacks** Domains, hosting, and IPs are created days or weeks in advance but remain invisible to defenders. • **Existing tools focus on internal telemetry, not external adversary activity** SIEM, EDR, and email security see what hits the organization—not what's being prepared elsewhere, before the attack occurs.

	• **Teams rely too heavily on known indicators** Traditional Blocklists and signatures fail against new, clean, or short-lived infrastructure. • **Investigations are slow and incomplete** Analysts must pivot across many tools, and data sources, to understand how infrastructure is related. This is an impossible task with current tools. • **They lack context to prioritize response** Without knowing how assets connect to campaigns, teams struggle to decide what matters most. • **They want to prevent, not just respond** Buyers want time and options—to disrupt threats before incidents occur.
Silent Push (solution)	The Silent Push Preemptive Cyber Defense platform provides real-time visibility into adversary-controlled internet infrastructure that was previously unknown. By continuously discovering and tracking attacker infrastructure, the platform enables security teams to detect emerging threats earlier, investigate activity faster, and respond before attacks escalate.
(key benefits)	The Silent Push Preemptive Cyber Defense platform identifies Indicators of Future Attack (IOFAs) by uncovering adversary-controlled internet infrastructure before it is used in campaigns. This early visibility allows security teams to investigate and disrupt threats before attacks occur, reducing risk and response cost
Unlike (Alternate solution)	Traditional security solutions are reactive by design, surfacing threats only after adversaries have launched activity. Silent Push provides earlier visibility into adversary infrastructure and IOFAs, enabling prevention rather than response.
(Unique differentiation)	The Silent Push Preemptive Cyber Defense platform enables a preemptive, proactive, and deterministic approach to security by uncovering previously unknown adversary-controlled internet infrastructure and identifying Indicators of Future Attack (IOFAs) before threats are operational. By revealing how attackers build and operate infrastructure upstream, Silent Push enables earlier, more confident action than reactive security tools—before attackers act.

Customer Pain Points

1. Security teams only see threats after they are already active

Most security tools surface threats once malware is delivered, phishing emails are sent, or alerts are triggered internally. By the time teams are alerted, the adversary has already built and operated infrastructure elsewhere, limiting response options and forcing reactive containment instead of early prevention.

---

2. Adversary infrastructure exists long before attacks, but remains invisible

Attackers register domains, provision hosting, and establish internet infrastructure days or weeks before using it. This infrastructure is often clean, transient, and deliberately designed to avoid detection, leaving security teams blind to activity that precedes attacks.

---

3. Too much reliance on known indicators and historical data

Many teams depend on blocklists, signatures, and previously observed indicators. These approaches fail against new infrastructure and emerging campaigns, forcing analysts to chase threats only after indicators become widely known.

---

4. Investigations are slow, manual, and fragmented

Analysts are forced to pivot between multiple tools, data sources, and spreadsheets to understand how domains, IPs, and hosting assets are related. This slows investigations, increases analyst fatigue, and makes it difficult to understand the full scope of an adversary's activity.

---

5. Limited context makes prioritization difficult

Without understanding how infrastructure fits into a broader campaign, teams struggle to determine which findings matter. This leads to wasted effort on low-impact artifacts while more significant threats go unnoticed.

---

6. Short-lived infrastructure evades traditional monitoring

Attackers increasingly use infrastructure that appears briefly and disappears quickly. Traditional tools often miss these assets entirely, leaving gaps in visibility and incomplete investigations.

---

7. Teams are forced into reactive defense

Without early visibility, organizations are left responding to incidents rather than preventing them. This increases operational cost, response time, and business risk, while limiting defenders' ability to disrupt threats upstream.

How Silent Push Directly Addresses These Pain Points

Silent Push provides a Preemptive Cyber Defense platform with real-time visibility into adversary-controlled internet infrastructure that was previously unknown, allowing teams to detect emerging threats earlier, investigate infrastructure in context, and act before attacks reach their environment.

Key Platform Features

Feature	What It Does	Why It Matters
Continuous Infrastructure Discovery	Continuously discovers attacker-controlled domains, IPs, hosting assets, and related infrastructure across the global internet.	Reveals adversary infrastructure that exists before attacks occur and before indicators are widely known.
Real-Time Infrastructure Monitoring	Tracks changes to infrastructure over time, including registrations, hosting shifts, and ownership changes.	Helps teams identify emerging campaigns and evolving adversary activity as it happens.
Infrastructure Relationship Mapping	Connects domains, IPs, certificates, hosting providers, and other assets to show how infrastructure is related.	Provides context needed to understand the full scope of adversary operations, not just isolated indicators.
Early Threat Detection	Surfaces infrastructure associated with malicious activity earlier in the attack lifecycle.	Enables proactive investigation and response before phishing, malware delivery, or exploitation begins.

Feature	What It Does	Why It Matters
Analyst-Driven Investigation	Allows analysts to pivot across infrastructure, explore relationships, and investigate activity in context.	Reduces manual effort and accelerates investigations without sacrificing control or accuracy.
Automated Discovery with Human Oversight	Combines automation with analyst workflows instead of fully opaque automation.	Speeds detection while keeping analysts in control of decisions and outcomes.
Historical Infrastructure Tracking	Maintains historical records of infrastructure and how it has changed over time.	Helps teams understand adversary patterns, reuse of infrastructure, and campaign evolution.
Monitoring & Alerting	Allows teams to monitor specific infrastructure, domains, or patterns and receive alerts on changes.	Ensures analysts are notified when new or suspicious infrastructure appears.
Operational Integration	Supports integration into security operations and investigative workflows.	Makes infrastructure visibility actionable within existing processes.
Scales Across Threat Types	Applicable to phishing, malware delivery, command-and-control, fraud, and other threat activity.	Enables broad coverage without separate tools for each threat category.

Buyer Persona

Title	Role	Goals
CISO	• Drives strategies to limit security risks and protect brand(s) • Balances security strategies with business' tolerance for risk • Defines the security policies. • Implements security architecture and engineering. • Ensures compliance within regulatory requirements, industry standards and best business practices. • Stay in front of threat vectors. • Incident response and recovery	• Minimize risk. • Protect customer's privacy. • Create an organizational culture of security. • Collaborate as a trusted business advisor. • Talking "business risk" vs. "IT security" • Quantify the business' risk appetite. • Identify risk issues to business assets. • Detect and correlate multi-level attacks
Security Architect	• Designs the overall approach and implementation. • Runs and monitors security technologies.	• Prevent breaches. • Prevent data loss events either by attacker or insiders. • Satisfy audits and compliance mandates

	• Heavily engaged in the process for running POCs for new security technologies	
Threat Analyst	• Collects information, stays on top of trends about malware-related cybercriminal activity. • Makes predictions about cybercrime and future activities. • Counters the activities of cyber criminals. • Creates threat intelligence reports on the results of analyses	• Identify early indicators of compromise before they do damage. • Ensure the threat analysis process is fast, easy, and thorough. • Obtain required tools and resources to gain timely, early insights that aren't complex or require too much time to operate
Security Analyst	• Identify and investigate serious incidents. • Compliance responsibilities • Incident response and recovery • Evaluate new solutions to support buying decisions. • Conduct security reviews and risk assessments. • Oversee change management with new solutions and policies. • Maintain product updates and vulnerability assessments	• Protect the organization from threats and attacks. • Minimize security risk. • Manage threat hunting and forensic analysis to keep organization protected. • Ensure solutions provide value. • Successfully complete compliance and regulatory audits • Develop security skill set.

Silent Push – Value by Persona

CISO

What CISOs Care About	How Silent Push Helps
Reducing business risk from cyber threats	Reveals adversary infrastructure earlier, enabling action before attacks impact the organization.
Avoiding surprise incidents	Provides visibility into previously unknown attacker activity happening outside the enterprise.
Improving security ROI	Shifts teams from reactive response to proactive detection, reducing costly incidents and response effort.
Confidence in security posture	Offers measurable visibility into threats that traditional tools cannot see.
Supporting strategic decision-making	Helps leaders understand how adversaries operate and where risk is emerging.

Security Architect

What Architects Care About	How Silent Push Helps
Closing visibility gaps in the security stack	Adds external infrastructure visibility that complements internal controls.
Designing layered defenses	Enables earlier detection upstream of email gateways, EDR, and SIEM tools.
Integrating tools and workflows	Fits into existing security operations without replacing core platforms.
Future-proofing defenses	Detects new and changing adversary infrastructure, not just known indicators.
Reducing tool sprawl	Consolidates external infrastructure visibility into a single platform.

Threat Analyst / Threat Hunter

What Threat Analysts Care About	How Silent Push Helps
Finding emerging threats early	Discovers attacker infrastructure before it's used in campaigns.
Understanding adversary behavior	Maps how attackers build, reuse, and evolve infrastructure over time.
Conducting deep investigations	Enables fast pivoting across domains, IPs, hosting, and relationships.
Avoiding blind spots	Exposes short-lived and hidden infrastructure that other tools miss.
Producing actionable insights	Provides context that can be operationalized by SOC and IR teams.

Security Analyst / SOC Analyst

What Security Analysts Care About	How Silent Push Helps
Faster investigations	Reduces time spent correlating data across tools.
Better alert context	Provides infrastructure relationships that explain why something matters.
Clear prioritization	Helps distinguish high-risk activity from noise.
Fewer false positives	Focuses attention on infrastructure with meaningful adversary signals.

What Security Analysts Care About	How Silent Push Helps
Confidence in response actions	Enables analysts to act with context instead of guesswork.

One-Line Persona Summary

- **CISO:** Reduces risk by exposing threats earlier and outside the perimeter
- **Security Architect:** Closes visibility gaps and strengthens upstream defenses
- **Threat Analyst:** Reveals how adversaries build and operate infrastructure
- **Security Analyst:** Speeds investigations and improves response confidence

The Silent Push Approach: Preemptive, Proactive, Deterministic

Modern adversaries build and operate internet infrastructure long before launching attacks. To stop threats earlier, security platforms must move upstream and take a different approach.

Silent Push enables a preemptive, proactive, and deterministic approach to security by uncovering previously unknown adversary-controlled internet infrastructure before it is operational.

Preemptive means visibility early enough to block, alert, or harden defenses before an attack is launched. Proactive means acting upstream instead of reacting to downstream alerts or incidents. Deterministic means findings are based on verified adversary-controlled infrastructure, not probability scores or inferred signals.

Silent Push provides Preemptive, Proactive, Deterministic Identification of future attacks.

Indicators of Future Attack (IOFAs)

Silent Push identifies Indicators of Future Attack (IOFAs) by discovering attacker-controlled internet infrastructure before it is used in phishing, malware delivery, or exploitation.

IOFAs represent real, verifiable adversary infrastructure that exists prior to weaponization. Unlike traditional indicators, IOFAs provide early, defensible signals that allow security teams to investigate, prioritize, and disrupt threats before attacks occur.

Reducing Reliance on Reactive Intelligence

Many security tools rely on alerts, historical indicators, or internal telemetry that only surface threats after adversary infrastructure is already active. This reactive model limits response options and increases business risk.

Silent Push shifts the focus from reactive intelligence to real-time visibility into attacker infrastructure, enabling teams to understand adversary behavior earlier and act with greater confidence.

How the Silent Push Platform Works Together

The Silent Push Preemptive Cyber Defense platform is designed to support the full lifecycle of identifying and responding to Indicators of Future Attack.

Insight provides continuous discovery and visibility into adversary-controlled infrastructure. **Reconnaissance** enables analysts to investigate relationships, track changes over time, and understand how infrastructure is used across campaigns. **Defend** allows teams to operationalize findings through monitoring, alerting, and integration into security workflows.

Together, these capabilities allow security teams to move from discovery to investigation to action without losing context or control.

How to Sell Silent Push

Start with the problem: attackers build infrastructure long before launching attacks, but most security tools only surface threats after activity begins.

Position Silent Push as a Preemptive Cyber Defense platform that makes previously unknown adversary-controlled infrastructure visible early through Indicators of Future Attack (IOFAs), enabling security teams to preemptively detect and block threats by analyzing pre-weaponized patterns in domains and hosting environments.

Anchor the conversation on the three pillars: **preemptive** (early enough to act), **proactive** (upstream action), and **deterministic** (verified infrastructure, not probability).

Contrast the Silent Push Preemptive Cyber Defense platform with reactive tools that depend on alerts, signatures, or historical indicators.

Close by reinforcing outcomes: earlier detection, faster investigations, fewer incidents, and greater confidence in response decisions.

CISO Value Lens

From a CISO perspective, Silent Push provides earlier visibility into adversary activity, reduces reliance on reactive detection, and strengthens confidence in security decision-making across SOC, IR, and threat teams. By exposing verified attacker infrastructure and origin signals before attacks occur, Silent Push helps CISOs reduce risk, improve response readiness, and provide clearer assurance to executive leadership.

Two Core Differentiators

Silent Push delivers two complementary, deterministic capabilities that address gaps left by traditional security tools.

First, Silent Push identifies Indicators of Future Attack (IOFAs) by uncovering adversary-controlled internet infrastructure before it is operational. This provides preemptive visibility into how attackers build and stage campaigns upstream, enabling security teams to preemptively detect and block threats by analyzing pre-weaponized patterns in domains and hosting environments.

Second, Silent Push extends this visibility through true-origin determination. This capability reveals the real geographic or national origin of traffic even when adversaries attempt to mask activity using VPNs, proxies, or residential infrastructure.

HYAS: Strategic Capability Expansion

The integration of HYAS expands Silent Push from infrastructure visibility into true-origin determination, enabling defenders to understand not just what infrastructure is being used, but who is actually behind it.

This capability is especially critical for identifying nation-state activity, remote worker infiltration, fraud, and other threats where adversaries deliberately obscure origin. Together, Silent Push and

HYAS strengthen the platform's deterministic approach by providing evidence-backed signals teams can trust.

From Reactive Intelligence to Deterministic Visibility

Traditional security approaches rely heavily on alerts, historical indicators, and probabilistic intelligence that surface threats only after activity begins. These models increase uncertainty and limit response options.

Silent Push shifts the focus to real-time visibility into adversary-controlled infrastructure and origin signals, providing deterministic data that enables confident investigation and action before attacks impact the organization.

Why Other Solutions Fall Short

Most security tools depend on IP reputation, geolocation, or inferred scoring models that attackers can easily evade. These approaches struggle with short-lived infrastructure, VPN masking, and residential IP abuse.

Silent Push uniquely combines infrastructure-first discovery with true-origin determination, allowing teams to see what attackers are building and who is actually behind it. This enables earlier, more reliable decisions than reactive or probabilistic solutions can provide.

Silent Push — CISO Executive Brief

Silent Push enables a preemptive, proactive, and deterministic approach to cybersecurity by uncovering previously unknown adversary-controlled internet infrastructure and identifying Indicators of Future Attack (IOFAs), enabling security teams to preemptively detect and block threats by analyzing pre-weaponized patterns in domains and hosting environments before threats are operational.

From a CISO perspective, Silent Push provides earlier visibility into attacker activity occurring outside the enterprise, reducing reliance on reactive detection and post-incident response. This upstream visibility allows organizations to act sooner, with more confidence, and with greater assurance for executive leadership and the board.

Unlike traditional security tools that depend on alerts, signatures, or probabilistic scoring, Silent Push focuses on verified attacker-controlled infrastructure and true-origin determination, even when adversaries attempt to hide behind VPNs, proxies, or residential IPs. This enables CISOs to understand not just what infrastructure is being used, but who is actually behind it.

Silent Push complements existing security investments by closing critical visibility gaps, helping security teams prevent incidents earlier, reduce operational risk, and make more defensible security decisions. Silent Push also replaces several existing tools and data sources teams use today.

Sales Objection Handling Appendix

Objection: “We already have threat intelligence feeds.”

Response: Most feeds focus on known indicators (IOCs) after activity has begun. Silent Push uncovers previously unknown adversary-controlled infrastructure and s before attacks occur, enabling security teams to preemptively detect and block threats by analyzing pre-weaponized patterns in domains and hosting environments.

Objection: “We already have EDR / SIEM / email security.”

Response: Those tools detect activity inside the environment. Silent Push provides upstream visibility into attacker infrastructure before threats reach your perimeter, giving those tools better inputs and more time to act.

Objection: “How is this different from reputation or blocklists?”

Response: Reputation and blocklists are historical and reactive. Silent Push identifies real attacker infrastructure early, including short-lived and newly created assets that never appear on blocklists.

Objection: “Isn’t this just probabilistic intelligence?”

Response: No. Silent Push focuses on deterministic signals—verified adversary-controlled infrastructure and true-origin determination—rather than probability scores or inferred behavior.

Objection: “Will this replace our existing tools?”

Response: Silent Push is designed to complement existing security investments by filling visibility gaps upstream, not to replace SOC, SIEM, or endpoint platforms. Many of your existing data sources can be replaced by Silent Push.

Objection: “Is this only for nation-state threats?”

Response: While Silent Push is effective against nation-state activity, it is equally valuable for phishing, malware, fraud, and other adversary operations that rely on attacker-controlled infrastructure.

Q1 Campaign Messaging:

The Traffic Origin Problem

Modern enterprises rely on remote workers, cloud access, and third-party users, but traditional IP reputation and GeoIP tools only see the last visible IP. When adversaries use residential proxies, VPNs, or laptop farms, sessions appear local and legitimate even when they are remotely controlled from high-risk or sanctioned regions. This creates a serious blind spot where hostile actors blend in as trusted insiders.

Traffic Origin addresses this problem by **identifying the most likely upstream country-of-origin controlling a connection**, even when the observed IP and geolocation appear clean. By shifting attribution from where traffic appears to where it is actually controlled, Traffic Origin provides origin certainty rather than ambiguity.

This allows organizations to identify high-risk remote sessions earlier, detect identity obfuscation that traditional tools miss, and intervene before activity escalates into credential theft, insider abuse, regulatory exposure, or significant financial loss. The outcome is a shift from reactive investigation to preemptive defense across identity, access, fraud, and SOC workflows.

About Traffic Origin

Silent Push Traffic Origin shifts your security posture from reactive to proactive by exposing the true upstream country-of-origin of the adversary, whether they are hiding via residential proxy, laptop farm, VPN or other obfuscation techniques.

By providing origin certainty where other tools see only obfuscation, Traffic Origin allows investigators to identify high-risk remote sessions before they escalate into attacks or credential theft.

ICPs for Traffic Origin

Industries:

- *Financial Services (Banking, FinTech, & Crypto)*
- *Critical Infrastructure (Energy, Utilities, & Telecom)*
- *Law Enforcement (INTERNAL ONLY, NOT TO BE MARKETED)*

1. SOC and Incident Response Teams

- **The Problem:** Traditional security tools cannot see if a domestic login is actually being controlled by an attacker in a different country using a residential proxy.
- **The Solution:** Traffic Origin identifies the true physical location of the person controlling the connection.
- **The Result:** Teams can automatically block high-risk logins from sanctioned or high-risk regions that appear to be local.

2. Financial Compliance and Fraud Teams - Anti-Money Laundering (AML), Know Your Customer (KYC) and Know Your Employee (KYE)

- **The Problem:** Criminals use residential proxies to hide their location, making transactions from sanctioned countries look like they are coming from a safe, domestic address.
- **The Solution:** Traffic Origin reveals the upstream origin of the traffic, bypassing the proxy "mask."
- **The Result:** Teams prevent sanctions violations and money laundering by identifying the true geographic source of the user and their funds.

3. Insider Risk and Personnel Security Teams

- **The Problem:** Fraudulent job applicants (such as North Korean IT workers) use stolen identities and "laptop farms" to bypass background checks and appear as local remote workers.
- **The Solution:** Traffic Origin detects the technical "hop" between a domestic laptop and an operative located in another country during the interview or onboarding process.
- **The Result:** Companies stop the hire before the fraudulent worker gains access to company data or payroll.

How does Traffic Origin fit into Silent Push's platform and overall mission?

Traffic Origin supports the Silent Push mission to neutralize before compromise by verifying the country of origin for a user connection. It looks past domestic proxies and laptop farms to reveal the actual country of origin. This capability relates back to preemptive cyber defense because security teams can block access the moment a user's reported location does not match their country of origin. By providing this geographic truth, the platform stops North Korean operatives and state-sponsored attackers from hiding behind local internet addresses to infiltrate companies before they can do damage.