# Silent Push Module Overview

**Understanding How Our Modules Work Together**

The majority of security organizations are forced into a reactive model because traditional tools only identify threats after they have been weaponized. Relying on known indicators means the adversary has already completed staging and launched their campaign. This delay is financially damaging; the global average cost of a data breach has reached $4.88 million (IBM), while the average cost for U.S. organizations has surged to $10.22 million (IBM).

Despite the proliferation of platforms claiming proactive defense, legacy security tools still struggle to identify the majority of breaches internally. External actors or ransomware groups currently disclose the incident in 82% of all cases (Verizon).

Silent Push provides real-time visibility into adversary infrastructure management. We move the defense line upstream to allow your team to identify and neutralize threats weeks before a campaign is weaponized.

## Core Modules and Business ROI

### 1. Insight: Understand Unknown Infrastructure

Insight gives security teams immediate clarity into unknown threat infrastructure. It consolidates enrichment, risk scoring, and correlation into a single view, eliminating the need to pivot across multiple point tools. Analysts can rapidly assess domains and IPs with 100+ contextual attributes, proprietary Risk Scores, and automated clustering capabilities.

- **Ideal for**: SOC analysts and incident responders who need to quickly understand what an observable is, how it's being used, and why it matters.

**Insight Key Outcomes**

- **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.

© 2026 Silent Push. All rights reserved. 010826

**Insight Business ROI**

- **Accelerated Triage Efficiency:** Drastically reduce Mean Time to Triage by replacing manual data reconstruction with deterministic technical context. Organizations that contain a breach in less than 200 days save an average of $1.14 million compared to those with longer lifecycles (IBM).
- **High-Value Resource Optimization:** Ensure high-cost senior analysts spend their time on strategic mitigation rather than manual research.
- **Tool Consolidation:** Lower operational complexity and licensing costs by eliminating tool sprawl, providing analysts with a unified source of truth in a single interface.

## Reconnaissance: Reveal Adversary Campaigns Early

Reconnaissance focuses on exposing adversary infrastructure during setup and staging phases before campaigns are weaponized. Using Indicators of Future Attack (IOFA™), it enables teams to discover and map attacker controlled domains, IPs, and services as they are being prepared, providing weeks or months of early warning.

- **Ideal for:** CTI and intelligence analysts focused on discovering and disrupting adversary activity before attacks are launched.

**Reconnaissance Key Outcomes**

- **Preemptive Identification of Staging Infrastructure:** Uses IOFA™ to discover and map attacker domains, IPs, and services during setup and staging phases.
- **Behavioral Fingerprinting:** Connects related infrastructure by tracking adversary tactics, techniques, and procedures (TTPs) across 200+ parameters.
- **Expose Unknown Infrastructure:** 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.

**Reconnaissance Business ROI**

- **Operational Stability:** Identify intent during the staging phase to move from emergency mode to planned mitigation.
- **Downtime Cost Avoidance:** Protect against unplanned outages, which now cost large enterprises an average of $23,750 per minute (Splunk).
- **Strategic Risk Reduction:** Rapidly cluster known and unknown attacker assets into defined campaigns to reduce exposure time. Mapping the full scope of a campaign

© 2026 Silent Push. All rights reserved. 010826

early prevents the recurring costs of reactive defense against fragmented infrastructure.

## Defend: Act Early with Confidence

Defend operationalizes IOFA™ data to prioritize alerts, reduce noise, and enable early action against pre-weaponized infrastructure. It integrates directly into existing SIEM, SOAR, firewall, and TIP workflows, allowing teams to take proactive measures at the earliest stages of threat detection.

- **Ideal for:** Security operations and automation teams seeking to reduce noise, prioritize threats, and automate defensive actions across their security stack.

### Defend 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.

### Defend Business ROI

- **Operational Overhead Reduction:** Focus only on verified attacker infrastructure to eliminate noise. Organizations that extensively deploy security automation save an average of $2.2 million in breach-related costs compared to those that do not (IBM).
- **Stack Optimization:** Maximize the ROI of your existing security stack by ensuring tools block the correct upstream targets automatically.
- **Retention and Staff Longevity:** Neutralize the primary driver of SOC burnout by automating false-positive removal. Reducing alert fatigue helps retain skilled analysts and prevents the high costs associated with recruitment and staff turnover.

| Feature | Insight | Reconnaissance | Defend |
|---|---|---|---|

© 2026 Silent Push. All rights reserved. 010826

| | | | |
|---|---|---|---|
| Primary focus | Rapid assessment and triage | Proactive threat discovery | Automated defense |
| Key capability | Total View enrichment and Risk Scoring | IOFA™ discovery and infrastructure mapping | SIEM, SOAR, and firewall integration |
| Primary users | SOC analysts and responders | Incident Response (IR) and CTI teams | SOC, Operations and automation teams |
| Use when | Investigating unknown domains or IPs | Hunting for emerging threats | Blocking threats before weaponization |
| Strategic ROI | Eliminate manual research and tool sprawl to drastically reduce Mean Time to Triage | Identify attacker intent during staging to prevent unplanned emergency work | Automate upstream blocking to neutralize threats before they reach the perimeter |

## How the Modules Work Together

While each module serves a distinct purpose, they are designed to complement each other throughout the threat lifecycle. Organizations can deploy modules individually or combine them for end-to-end coverage.

- **Investigation Workflow:** When an alert surfaces an unknown domain, analysts use Insight to rapidly understand its context and risk level. If the domain appears malicious, Reconnaissance helps map related infrastructure and campaign scope. Defend then operationalizes these findings by pushing verified indicators into security controls.
- **Proactive Defense:** Reconnaissance continuously discovers adversary staging infrastructure. Insight enriches these findings with detailed context. Defend automates the blocking or monitoring of pre-weaponized threats across the security stack.
- **Preemptive Threat Detection:** Incident Response and CTI teams leverage Reconnaissance to identify suspicious patterns and infrastructure clusters. Insight provides deep forensic context for investigation. Defend ensures verified threats are actioned early across all security tools.

**Additional Offerings**

© 2026 Silent Push. All rights reserved. 010826

Beyond our core modules, Silent Push offers specialized data products and services:

- **Bulk Data:** Large-scale access to Silent Push datasets for integration into custom analytics platforms, data lakes, or threat intelligence systems.
- **Anonymization Lists:** Curated lists of residential proxy exit nodes and VPN endpoints to help distinguish between legitimate anonymization services and malicious infrastructure.
- **Analyst on Demand Tokens:** Commission Silent Push's Preemptive Cyber Defense Team to conduct targeted research and analysis on specific threats relevant to your organization.

**Flexible Deployment**

Silent Push modules can be purchased individually or combined based on your security priorities. Organizations typically start with Insight for foundational visibility, add Reconnaissance for proactive hunting, and layer Defend for automated response. Our team works with you to design the right solution for your specific needs.

© 2026 Silent Push. All rights reserved. 010826