SILENT PUSH

AI-POWERED INFRASTRUCTURE CLUSTERING

WHAT IT IS

Silent Push has turned its analyst tradecraft into something a machine can run, so one indicator becomes a full campaign map with every step recorded automatically.

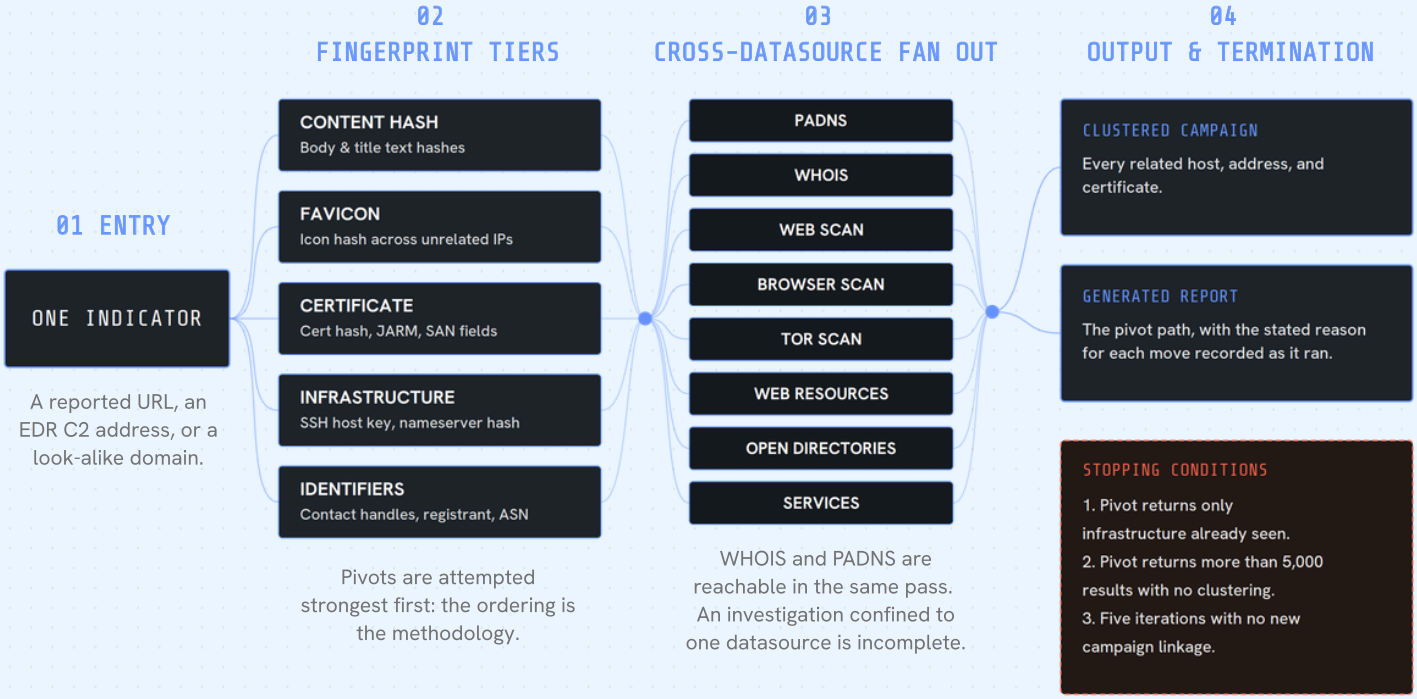
The product is a hosted MCP endpoint that runs on your existing Silent Push API key, so there's nothing to deploy, patch, or pay extra for. It provides fifty read-only tools across nine categories, and the server draws on seven built-in investigation playbooks as it works.

THE SHIFT

The real value of this system is automated pivoting: moving from content fingerprints down to identifiers in ranked order, crossing datasources at each step, applying rules that separate high-confidence links from coincidental infrastructure, and knowing when to stop.

Running all four of those steps without a person driving each one is what turns this into genuine automation.

THE CLUSTERING ENGINE - FROM ONE INDICATOR TO A MAPPED CAMPAIGN



Stopping conditions: the pivot returns infrastructure already seen, returns over 5000 results with no clustering, or five iterations pass with no new linkage.

THE OUTCOME

Infrastructure investigation stops being rationed to a handful of specialists and the cases that survive triage, and every conclusion arrives with its pivot path and rationale already attached.

The scanning is read-only and hosted at the vendor, so nothing runs from internal infrastructure and nothing new gets deployed, and the entire capability is included with the active subscription at no added cost.

CONTROLS ALREADY IN PLACE

None of the fifty tools write to an internal system, and there's no connection into internal infrastructure at all. Each API key operates as its own tenant, and Silent Push states the raw key is never logged or stored by the server. Requests are capped at a sliding window of 120 per minute per key, which bounds both a runaway loop and a leaked key.

The pivot graph records each step and its stated reason as it happens, and the report is generated directly from that history. The stopping conditions are enforced automatically, and an organization Owner must enable the connector before anyone can add it, with tools scoped per role from there.

IMPACT BY FUNCTION

01 SECURITY OPERATIONS & DETECTION

Tier 1 stops escalating infrastructure questions, because a signature built on TLS and certificate structure still catches the operator after the next rotation.

02 CYBER THREAT INTELLIGENCE

Campaign mapping becomes something an analyst reviews in minutes, since SSH host key fingerprints keep a cluster tied together even after the operator rotates domains.

03 INCIDENT RESPONSE

One C2 address leads to the SSH host key, and that key leads to every other address the operator runs, all without the team touching attacker hosts from its own IP space.

04 FRAUD

Investigation moves from one URL to the entire kit deployment, catching the subdomain abuse that new domain monitoring tends to miss.

05 IMPERSONATIONS & TAKEDOWN

Takedown submissions can cover a whole cluster at once, with screenshot evidence attached for every related site.

06 THIRD-PARTY RISK & ATTACK SURFACE

The capability surfaces vendor hosting and assets inherited through acquisition, along with scripts loading on payment and login pages that nobody recognizes.

LEARN MORE ABOUT SILENT PUSH FOR AI SECURITY

Ask us what your AI agents can already see in your threat environment. **silentpush.com**

HOW IT FITS INTO YOUR EXISTING AI STRATEGY

- Clears the governance bar since the data is public internet infrastructure, not internal or customer data
- A rehearsal for the pattern the organization will want everywhere else
- Redistributes a skill that's currently stuck with a dozen specialists

SILENT PUSH

NEUTRALIZE BEFORE COMPROMISE

silentpush.com