SILENT PUSH

ENTERPRISE VALUE ASSESSMENT

Most security stacks are reactive by design. They trigger alerts only after an attacker has already staged infrastructure, targeted users, and launched a campaign. By that point, your organization is already paying for the incident through investigation, remediation, and potential damage.

Silent Push identifies and blocks threats during the setup phase. We shift the defensive timeline from mitigation to prevention.

DEFENSIVE MATURITY STARTS BEFORE THE INFRASTRUCTURE EXISTS

Traditional tools operate on a post-compromise timeline. Silent Push stops the process before the first strike.

STAGE	TRADITIONAL STACK	SILENT PUSH
Core Question	Invisible	Detected and Blocked
Primary Focus	Invisible	Prevented
Primary Users	Alert Generated	N/A (Stopped at source)
Timing	Costly Recovery	Avoided

Stopping an attacker earlier in the kill chain delivers a level of ROI that reactive tools cannot match. Once a compromise happens, you are already spending money to find and remove the threat. Silent Push ensures the compromise never occurs.

QUANTIFYING THE ENTERPRISE-WIDE IMPACT

While the SOC sees immediate operational benefits, the true value of Silent Push scales across the entire organization. When you stop threats before they reach your perimeter, you protect revenue and reduce global risk.

BUSINESS AND REVENUE RESILIENCE

Strategic impact for CMO, CRO, and Digital Leadership.

AREA	STRATEGIC OUTCOME	ANNUAL IMPACT ($10B REVENUE
Marketing and Brand	Eliminates brand spoofing and protects media spend.	$4.5M to $24M
Digital Commerce	Prevents site clones and secures acquisition funnels.	$5M to $30M
Fraud and Trust	Stops account takeover and payment risk at the source.	$10M to $40M
Enterprise Risk	Reduces global exposure and ensures resilience.	$3M to $20M

CYBER OPERATIONS EFFICIENCY

Operational impact for CISO and Security Engineering.

AREA	STRATEGIC OUTCOME	ANNUAL IMPACT ($10B REVENUE
Threat Intelligence	Deterministic data for proactive hunting.	$2M to $4M
SOC Operations	Massive reduction in alert fatigue and noise.	$2M to $8M
Incident Response	Elimination of fire drills from active breaches.	$1M to $4M
Attack Surface	Total visibility into threats before they pivot.	$1.5M to $6M

THE BOTTOM LINE

Silent Push is a cost-avoidance engine. We provide the preemptive data required to stop reacting to the past and start securing the future. Our approach is deterministic, not probabilistic. We show you what is happening, not what might happen.

METHODOLOGY AND ASSUMPTIONS

*The financial impacts in this assessment are modeled for a representative enterprise with **$10B in annual revenue**. These figures are derived from a Risk-Reduction ROI calculation that measures the delta between reactive mitigation and preemptive prevention.*

ROI=Cost of Solution(Current Risk−Mitigated Risk)−Cost of Solution

DATA SOURCES AND VARIABLES

To ensure these projections remain grounded in operational reality, the model incorporates the following industry benchmarks:

- ***Cost of Breach:** Based on the IBM Cost of a Data Breach Report (Global Average: $4.88M per incident).*
- ***Operational Drag:** Calculated using average Tier 1 through Tier 3 analyst hourly rates and industry-standard Mean Time to Resolve (MTTR).*
- ***Revenue Loss:** Modeled on average downtime costs for Tier 1 digital commerce platforms, estimated at $500,000 per hour.*
- ***Brand Protection:** Based on typical recovery costs for high-visibility consumer brands following a wide-scale spoofing or phishing campaign.*

These ranges are projections based on a $10B revenue baseline. Because every environment has a unique risk profile, the deterministic value for a specific organization will vary. Silent Push provides tailored Business Impact Analysis (BIA) sessions to calculate these figures based on individual telemetry and incident history.

SILENT PUSH

NEUTRALIZE BEFORE COMPROMISE