DataDome | SOURCE DEFENSE PARTNERSHIP OVERVIEW

Best-of-Breed Client-Side Security Through Strategic Partnership

Partnership Overview

Agentic AI is reshaping the web. According to Gartner's *"Top Strategic Technology Trends for 2025"* report, by 2028, AI agent machine customers will account for 20% of interactions currently handled at human-readable digital storefronts. As these AI agents transact at scale, organizations need protection across the entire commerce journey, from verifying agent identity and intent to securing payment completion.

DataDome + Source Defense delivers the only partnership purpose-built for this dual-threat environment, giving customers specialist-grade protection at every layer of the attack surface.

DataDome: Establishes AI agent trust and protects from malicious automated traffic. Prevents account takeovers, API abuse, and credential stuffing attacks.

Source Defense: Payment page security and PCI DSS compliance automation that protects customer payment data from client-side attacks

How do they work together?

DataDome protects your applications and APIs from malicious traffic before it reaches your payment flows, while Source Defense ensures both site-wide and payment page security against e-skimming, Mage Cart attacks, and inadvertent data leakage. Each company focuses on its expertise, giving you continuous innovation in both bot & agent trust management and client-side security.

About Source Defense

Source Defense is the pioneer in behavior-based, end-to-end client-side security. Serving ~200 enterprise customers, including Blackrock, Chipotle, and Victoria's Secret, Source Defense is purpose-built for PCI DSS 4.0 compliance and validated by leading QSAs, including CoalFire and VikingCloud. Source Defense maintains a 97% customer renewal rate and serves as a Board of Advisors member with the PCI Council.

Complementary Security Coverage

DataDome and Source Defense serve complementary security needs with zero capability overlap. Together, you get defense-in-depth with no coverage gaps.

Security Layer	DataDome	Source Defense
Agent Trust & Verification	Validates AI agent identity and intent to establish trust within guardrails	Behavioral monitoring ensures payment page scripts behave as intended
Threat Coverage	Bot attacks, ATO, API abuse, credential stuffing, agentic AI threats	eSkimming, Magecart/formjacking, supply chain attacks, unauthorized scripts, client-side data theft
Primary Use Case	Bot and AI agent verification/protection across websites, mobile apps, and APIs	PCI DSS compliance automation for payment pages and client-side security
Detection	ML-powered detection across behavioral, network & identity signals, validating bot and AI agent intent in real time	Runtime behavioral sandbox, AI-assisted anomaly detection, patented script behavior control
Compliance Focus	GDPR, CCPA compliance for bot management	PCI DSS 4.0 (requirements 6.4.3 and 11.6.1) specialization
Operational Impact	Real-time automated blocking of malicious bots and agents with no manual intervention	Automated protection against unauthorized scripts, eliminates manual code reviews
Innovation Focus	Agent Trust framework for the agentic AI era. Continuous investment in AI agent verification, governance, and threat intelligence	Dedicated focus on payment page security and compliance automation

Deployment

DataDome

- Cloud-based deployment with minimal implementation time
- Integrates with existing infrastructure (CDN, WAF, load balancers)
- Real-time protection without code changes

Source Defense

- Simple 2-line snippet insertion on payment pages
- Works seamlessly with CSP/SRI and tag managers (GTM, Adobe Launch)
- No performance impact on page execution

Learn More:

DataDome: https://datadome.co/partners/source-defense

| Contact: cynthia.dunphy@datadome.com

Source Defense: https://sourcedefense.com

| Contact: timothy.d@sourcedefense.com

Get Started:

Whether you're currently using DataDome, Source Defense, or neither. Contact our teams to discuss how this partnership delivers complete protection with no coverage gaps.

Partnership Benefits

Both solutions deploy independently with no conflicts or dependencies. Implementation can be phased or simultaneous based on your priorities.

✔ **Unified Security Strategy**

Deploy complementary solutions designed to work together, eliminating coverage gaps and vendor conflicts.

✔ **Specialist-Grade Innovation**

Each vendor focuses dedicated R&D on their specialty—you benefit from continuous innovation in both bot management and client-side security.

"As AI agents become the dominant consumers of digital interactions, this partnership ensures complete protection, from agent verification through secure payment completion, with no coverage gaps"

— Pradheep Sampath, Chief Product Officer, DataDome