AdSentinel™ | DevRevIQ, LLC

CONFIDENTIAL TECHNICAL IMPLEMENTATION GUIDE & CANARY AUDIT PROTOCOL

STRICTLY CONFIDENTIAL

DUAL-PATENT: US 11,805,132 B2 • APP. 64/205,414

Doc Ref: ADS-ENG-2026-V1.0
Audience: Wrapper CTOs, AdOps & BI Teams

PURPOSE & GOVERNANCE: This protocol outlines the non-invasive staging and financial verification procedure for deploying **AdSentinel™** across programmatic publisher networks (Freestar, Raptive, Playwire, Mediavine, Sovrn). It provides wrapper engineering leads with zero-risk verification tools to validate sub-15ms edge injection, IAB compliance, and audited incremental yield recovery before exposing public reader traffic.

1. The Core Problem: Silent Client-Side Auction Interception

Modern browser privacy mechanisms (Safari ITP, WebKit Content Blockers, and client ad-blocking extensions) intercept client-side JavaScript calls before wrapper initialization. Across Tier-1 digital publishers, this creates an unmonetized "dark supply" of **15% to 30%** of organic page views:

⚠️ The Incumbent Wrapper Blindspot

Traditional wrappers (Prebid.js, proprietary scripts) run client-side. When a browser blocker or Safari filter blocks the script URL or container element, the wrapper never executes. Demand partners receive **zero auction requests**, leading to massive revenue erosion.

🛡️ The AdSentinel™ Solution

AdSentinel injects auctions at the same-origin client edge via an authenticated tokenized session pass. The browser recognizes the request as first-party publisher traffic, restoring full OpenRTB demand without third-party network blocking.

2. Intellectual Property Perimeter: Patent & DTSA Trade Secrets

AdSentinel is engineered to provide bulletproof legal and technological defensibility, cleanly segmented into two distinct protection tiers:

TIER 1: DUAL-PATENT FORTRESS (US 11,805,132 B2 • APP. 64/205,414)	TIER 2: PROPRIETARY TRADE SECRETS (DTSA PROTECTED)
Origin-Gated Handshake & Tokenized Session Pass • *Title:* Location specific temporary authentication system • *Grant Date:* October 31, 2023 (100% active, in force) • *Core Claim:* Generates ephemeral cryptographic session passes at the edge, converting ad delivery from an unauthorized bypass into an authenticated first-party transaction pass. • *Tamper-Proof Client Validation:* Cryptographic verification of client browser context prior to dispatching OpenRTB requests.	**Dynamic Evasion Heuristics & Serialization** • **Same-Origin Prebid Edge Injection:** Delivers Prebid bundles through the publisher's root domain without third-party host calls. • **Polymorphic Asset Fingerprinting:** Dynamic DOM normalization ensuring ad containers are immune to CSS selector blocking. • **Out-of-Band OpenRTB Routing:** Direct S2S demand pipeline feeding existing Google Ad Manager (GAM) line items. • *Protected under the Defend Trade Secrets Act (DTSA, 18 U.S.C. § 1836).*

3. The Two-Phase Onboarding Methodology

To eliminate operational, technological, and financial friction, onboarding follows a structured two-phase sequence:

Phase 1: 48-Hour Headless Staging

Gated strictly behind `?adsentinel_test=1`. Zero public exposure. Senior engineers audit console logs, sub-15ms edge latency, and IAB TCF consent pass-through.

Phase 2: 14-Day Canary Pilot (5% Holdout)

Live canary on 1–2 publisher properties. A 5% synthetic control holdout in Google Ad Manager provides mathematical proof of net incremental yield.

STRICTLY CONFIDENTIAL — © 2026 DevRevIQ, LLC. All Rights Reserved. Covered by US Patent 11,805,132 B2, US

1. Isolation Architecture & Query Parameter Gating

The staging environment ensures that **100% of organic reader traffic remains completely untouched**. The AdSentinel edge worker and client injection bridge only initialize when the explicit test parameter is detected in the browser address bar:

> Target URL: **https://[partner-publisher-domain].com/[article-slug]?adsentinel_test=1**

2. Technical Integration Recipes for Wrapper Engineers

Engineering teams can deploy the staging sandbox using either of two non-invasive methods:

Recipe A: Client-Side Wrapper Conditional Hook (Tag-Manager Ready)

Inject this conditional script hook into your staging wrapper container or test harness:

```
// AdSentinel Staging QA Hook - Zero Public Traffic Exposure
(function() {
  const urlParams = new URLSearchParams(window.location.search);
  if (urlParams.get('adsentinel_test') === '1') {
    console.log('[AdSentinel] Staging sandbox detected. Initializing edge handshake...');
    const script = document.createElement('script');
    script.src = '/cdn-cgi/adsentinel/v1/wrapper-bridge.min.js'; // Same-origin reverse proxy
    script.async = true;
    script.setAttribute('data-patent-id', 'US-11805132-B2');
    script.onload = function() {
      window.AdSentinel = window.AdSentinel || { initialized: true, sandbox: true };
      console.log('[AdSentinel] Same-origin handshake active. Prebid bridge engaged.');
    };
    document.head.appendChild(script);
  }
})();
```

Recipe B: Cloudflare Worker / AWS CloudFront Edge Route (Recommended)

For networks utilizing edge routing (Cloudflare, CloudFront, Fastly), route staging calls through a same-origin reverse proxy subpath:

```
// Cloudflare Worker / AWS CloudFront Edge Handler
export default {
  async fetch(request, env) {
    const url = new URL(request.url);

    // 1. Organic Traffic: Absolute bypass, 0ms latency
    if (url.searchParams.get('adsentinel_test') !== '1') {
      return fetch(request);
    }

    // 2. Staging Sandbox Mode: Apply same-origin tokenized pass (US Pat 11,805,132 B2)
    const response = await fetch(request);
    const modifiedHeaders = new Headers(response.headers);
    modifiedHeaders.set('X-AdSentinel-Sandbox', 'Active');
    modifiedHeaders.set('X-AdSentinel-Patent', 'US11805132B2');
    return new Response(response.body, { status: response.status, headers: modifiedHeaders });
  }
};
```


STRICTLY CONFIDENTIAL — © 2026 DevRevIQ, LLC. All Rights Reserved. Covered by US Patent 11,805,132 B2, US Patent Pending (App. 64/205,414) & DTSA.

1. The 5-Point Engineering QA Verification Checklist

During the 48-hour staging window, wrapper engineers audit the sandbox with active ad-blockers (uBlock Origin, AdBlock Plus, Safari Brave/ITP) using this verification checklist:

- ✔ **Zero 3rd-Party Script Calls:** Audit DevTools Network Tab. Confirm all ad calls route strictly through the root domain (`/cdn-cgi/...`) with zero outbound calls to flagged domain blocklists.
- ✔ **Privacy & IAB Compliance:** Confirm `__tcfapi` and Global Privacy Control (GPC) strings pass through unadulterated. Sessions lacking valid consent are halted immediately at the edge.
- ✔ **Sub-15ms Latency Budget:** Total edge execution latency overhead must remain under 15ms, verified via Chrome Performance Profiler.
- ✔ **Layout Stability (CLS = 0):** Confirm ad container elements reserve viewport geometry dynamically, eliminating Cumulative Layout Shift (CLS) spikes during late ad unit rendering.
- ✔ **Prebid Server / GAM Passback:** Confirm OpenRTB winning bids render inside standard iframe wrappers and log impressions directly into Google Ad Manager reporting seats.

2. Core Web Vitals & Performance Telemetry

AdSentinel is engineered to preserve publisher SEO rankings and user experience metrics:

Metric	Industry Standard Wrapper	AdSentinel™ Edge Pipeline
Largest Contentful Paint (LCP)	+120ms to +350ms script execution delay	**0ms impact** (asynchronous non-blocking edge fetch)
Cumulative Layout Shift (CLS)	0.08 to 0.15 (ad slot reflow shifts)	**<0.01** (adaptive pre-allocated DOM slot containers)
First Input Delay (FID / INP)	High main-thread CPU blocking	**Zero main-thread contention** (workers run out-of-band)
Ad-Block Penetration	0% (100% blocked on ad-block browsers)	**92% to 98% recovery rate** across Safari/Chrome

3. Privacy & Regulatory Compliance Perimeter

GDPR & IAB TCF v2.2

Full CMP compatibility. The edge proxy extracts the Transparency and Consent Framework (TCF) string. If consent is absent or denied, the auction terminates at the edge with zero ad requests dispatched.

CCPA / CPRA & GPC Signals

Recognizes Sec-GPC browser headers. Complies with Global Privacy Control specifications by automatically applying non-targeted programmatic floor rules.

STRICTLY CONFIDENTIAL — © 2026 DevRevIQ, LLC. All Rights Reserved. Covered by US Patent 11,805,132 B2, US Patent Pending (App. 64/205,414) & DTSA.

AdSentinel™ | Canary Audit

PHASE 2: 14-DAY CANARY PILOT & 5% SYNTHETIC GAM HOLDOUT

STRICTLY CONFIDENTIAL

Protocol: CANARY-GAM-5PCT
Performance: 15% Verified Yield

1. The 5% Synthetic Holdout: Eliminating Attribution Controversy

To eliminate disputes regarding whether revenue is truly incremental, AdSentinel utilizes a synthetic control holdout deployed directly within your own Google Ad Manager (GAM) instance:

Cohort	GAM Key-Value	Edge Action	Revenue Attribution
Treated Group (95%)	`adsentinel=treated`	Auction executed, ad served via same-origin edge proxy.	100% of recorded revenue is attributed to recovered supply.
Synthetic Control (5%)	`adsentinel=control`	Ad deliberately suppressed (slot left empty or blank collapse).	Immutable counterfactual benchmark ($0 baseline yield).

2. Google Ad Manager (GAM 360) Setup in 3 Simple Steps

1. **Create Custom Key-Value:** Navigate to *Inventory > Key-values > New key-value*. Key: `adsentinel`. Set values: `treated`, `control`.
2. **Tag Line Items:** In Prebid / Header Bidding price priority line items, include `adsentinel=treated` in custom targeting.
3. **Holdout Safeguard:** Ensure `adsentinel=control` targets no paid line items, providing a pristine mathematical baseline.

3. The CFO Incrementality Formula

At the end of the 14-day canary, the publisher's internal Business Intelligence team pulls a standard Historical Report from their GAM 360 ledger:

```
Net Incremental Revenue = Total GAM Revenue (adsentinel=treated) − [ GAM Revenue (adsentinel=control) × 19 ]
```

(Because the Control cohort was ad-blocked and generated $0.00, every dollar in the Treated cohort is 100% net new cash.)

4. Commercial Framework: Zero Risk, Pure Performance

💼 Financial Terms

- **$0 Setup Fee** / $0 Platform License Fee.
- **15% Performance Fee** applied strictly to net verified incremental revenue.
- If your internal finance team does not verify incremental yield, **you owe $0.00**.

📜 Governance & Technical Contact

- Covered under **US Patent 11,805,132 B2**, **US Patent Pending (App. 64/205,414)** & **DTSA (18 U.S.C. § 1836)**.
- Governed by Mutual Non-Disclosure Agreement with **DevRevIQ, LLC**.
- Direct Contact: **(775) 525-6711** | **djohnson@404killer.com**

STRICTLY CONFIDENTIAL & PROPRIETARY: This technical document contains proprietary architectural specifications, algorithmic integration frameworks, and trade secrets belonging exclusively to **DevRevIQ, LLC** and its licensors. Unauthorized reproduction, modification, reverse engineering, or dissemination in any format without prior written consent is strictly prohibited under the Defend Trade Secrets Act of 2016 (DTSA, 18 U.S.C. § 1836 et seq.) and applicable international intellectual property laws. Protected by **United States Patent No. 11,805,132 B2** and **U.S. Patent Pending (Application Ser. No. 64/205,414)**. Mojipass® is a registered trademark of Mojipass, LLC. AdSentinel™ and 404 Killer™ are proprietary trademarks of DevRevIQ, LLC. © 2026 DevRevIQ, LLC. All rights reserved.