Raccoon Rockets

Modernised Retargeting Stack: From Client-Side to Server-Side

Technical brief for IT, security, and compliance stakeholders

Architecture Overview

Legacy retargeting relies on client-side JavaScript that sets cookies and pushes data directly from the visitor's browser to third-party servers.

Our server-side approach replaces that with controlled, **auditable server-to-server event transmission** - putting precision, control, and compliance at the centre.

How We Compare

Our tech: Server-side	Legacy tech: Client-side
✓ Backend API call → controlled endpoint	✗ Browser JS executes → external request
✓ Hashed / pseudonymous session IDs	✗ Cookies and local storage IDs
✓ Data flows through your infrastructure	✗ Data bypasses your backend
✓ Immune to blockers; fully auditable	✗ Blocker vulnerability; data leakage risk
✓ Can operate under legitimate interest	✗ Typically requires explicit consent banner
✓ No third-party cookies	✗ Third-party cookies; compliance exposure

Script Delivery & Isolation

The script tag placed on your website references an external file hosted exclusively on our ad servers. Execution is fully isolated from the host page - the script cannot access or interact with site content, user accounts, local storage, or any other domain data.

The hosted script executes only on HTTPS pages. In the default (closed) configuration, the script body delivered to your environment contains no executable logic; all processing occurs server-side when the src URL is fetched.

How a Script Invocation Works

Every script load triggers a one-time signal processed server-side.

A hashed session identifier is derived from a predefined set of anonymous technical parameters; browser type, device class, timestamp.

This identifier enables anonymous retargeting using first-party technical signals, without exposing site data or personal information.

Script Variants

We offer three delivery formats. The underlying technology, privacy guarantees, and infrastructure are identical across all three. The difference is the level of code visibility and verification available to your team.

	Closed (Default)	Open	SRI
Script body delivered	Empty function	Full readable source	Obfuscated; locked by SHA-384 integrity hash
First-party cookie	None	A session cookie scoped to your domain	A session cookie scoped to your domain
Third-party cookies	None	None	None
Auditability	Server-side; proof by absence of client code	Full client-side code review	Cryptographic hash verification
Code change protection	N/A; no client code delivered	Requires periodic review	Full; execution blocked if script is altered
Typical use	Standard; deployed by most partners	Security review requirement before sign-off	Highest-security; tamper-proof requirement

Closed (default)

The standard deployment. The script body delivered to your site is an empty IIFE; there is no client-side logic whatsoever:

```
(function () {

})();
```

All processing occurs server-side on fetch of the script source file. This is the clearest proof of non-interference: nothing in the delivered script can access, read, or transmit any data from your environment. Most partners deploy this version.

Implementation tag:

```
<script id="rr_[client_id]" src="https://[servername]/scripts/rr_[client_id].js" async>
</script>
```

Open

When a thorough review of script behaviour is required, including validation that code does not change over time, we make the full code source available.

The open script is human-readable JavaScript. It operates on first-party signals only, sets a first-party session cookie (_p_uid) scoped to your domain, and makes no third-party calls.

The implementation tag is structurally identical to the closed version, with the only difference being in the content of the hosted .js file.

```
<script id="rr_[client_id]" src="https://[servername]/scripts/rr_[client_id].js" async>
</script>
```

SRI (Subresource Integrity)

For the highest level of tamper-proof control, the SRI implementation adds a cryptographic integrity check via the browser's native Subresource Integrity mechanism. The script tag includes a SHA-384 hash of the approved script content. If the hosted file changes, even by a single byte, the browser will refuse to load or execute it.

Your team can independently verify the hash against the delivered script at any time. The SRI script operates on first-party signals only, with no third-party calls.

```
<script>
    (function () {
        var script = document.createElement("script");
        script.setAttribute("src", "https://[servername]/scripts/rr_[client_id].js");
        script.setAttribute("async", "true");
        script.setAttribute("referrerPolicy", "origin-when-cross-origin");
        script.setAttribute("id", "rr_[client_id]");
        script.setAttribute("crossorigin", "anonymous");
        script.setAttribute("integrity", "sha384-[hash_provided_by_account_manager]");
        document.body.appendChild(script);
    })();
</script>
```

Infrastructure

- Script loads ASYNC; no impact on page rendering or business-critical elements.
- Delivered through Cloudflare CDN.
- Phusion Passenger on Apache, returns a blank script during any server downtime, preventing errors on your site.
- Entire infrastructure 2FA-secured, protected against DNS hijacking and similar attacks.
- ISO 27001 / SOC 2-certified cloud infrastructure with full encryption.
- SRI validation supported across all deployment models.

Compliance & Standards Alignment

- Aligned with IAB TCF 2.2 and Google Ads Data Policies.
- Architecture mirrors GA4 Server-Side, CAPI, and Enhanced Conversions.
- Operates under first-party lawful basis; no personal IDs or data exposed.
- Compatible with GDPR, CCPA, and ePrivacy; consent signalling via TCF-registered CMPs.

Privacy Commitments - All Variants

By relying only on modern, future proof technology, we offer a fully transparent retargeting stack that any security and compliance teams can audit, approve, and trust.

- No third-party cookies.
- No third-party calls.
- IP anonymised and not stored.
- Data retained under 24 hours, or per your policy.
- Hash salt rotated regularly.
- GDPR lawful basis: legitimate interest (no profiling).