



Retargeting Evolved: Effective, Safe, and Non-intrusive

General brief for affiliate, marketing and product stakeholders

Retargeting Has Changed - for the Better

The classic model of retargeting - with 3rd party cookies and tracking pixels running in visitors' browsers - is being retired across the industry. Browsers block it. Users resent it. Compliance teams flag it. Security rejects it.

That's why the approach we bring to you through our retargeting partner replaces all of that through server-side technology: clean, transparent, and built for the privacy and security standards that matter today. Same marketing outcome, but fundamentally superior.

How We Compare

Partner tech: Server-side Intelligence	Legacy tech: Cookies & pixels
✓ Nothing runs inside your visitors' browsers	✗ Third-party code runs in your visitors' browsers
✓ Only anonymous, approved signals transmitted	✗ Visitor data sent to external networks, often without audit trail
✓ You control what leaves your environment	✗ When data leaves, your control is lost
✓ Works even where browsers block legacy pixels	✗ Increasingly blocked, effectiveness declining
✓ No third-party cookies; privacy-safe by design	✗ Third-party cookies; real compliance exposure
Result: Full control, full transparency, better business performance.	Result: Shrinking reach, compliance risk, limited control.

What You Gain

- **Better campaign reach:** The partner's ad tech is immune to ad blockers and browser restrictions.
- **Your data stays yours:** Nothing leaves your environment. No third party gets access to your visitor data.
- **No page speed impact:** The script loads asynchronously in the background, independently of your page content.



- **Compliant by design:** No third-party cookies. No personal data. Built for GDPR and CCPA from the ground up.
- **Re-engage through trust:** No hidden trackers following your visitors; tracking points only back to your audience.

Bringing Your IT & Tech Along

A fair question from your IT and security teams will be whether a third-party script can be trusted on a company website. Through the technology provided by our retargeting partner, this question has a genuinely reassuring answer.

In our standard setup, the script tag placed on your website contains no executable code.

Everything runs on the retargeting partner's servers, not yours. There is nothing in the delivered script that can read, access, or transmit any data from your site. Your environment stays exactly as it was.

This isn't a matter of trust - it's a matter of architecture. The script cannot do what the old retargeting technology did, because it is by design built differently from the ground.

Questions your IT & Tech will likely ask - and the answers

Q: "How do we know what the script actually does?"

Three levels of transparency are available, see the deployment options below. At minimum, your team can review the full source code and its behavior. At maximum, a cryptographic lock guarantees the code can never change without their approval.

Q: "Does this imply a GDPR risk?"

No. There are no third-party cookies, and no personal data transmitted in clear text. Data is retained for less than 24 hours. Our retargeting partner's legal basis under GDPR is legitimate interest; the same basis Google uses for its own measurement tools. The partner is also fully aligned with IAB TCF 2.2.

Q: "Can we audit and verify this on an ongoing basis?"

Absolutely. Our retargeting partner's infrastructure is certified to ISO 27001 and SOC 2 standards. Depending on the deployment option chosen, your team can verify the exact code running at any time, including cryptographically.

Three Deployment Options

The script is available in three formats, which gives your IT & Tech a flexibility to choose the level of verification they need. The retargeting performance is identical across all three.

Closed (default)	Open	SRI
------------------	------	-----



Standard deployment. No script logic visible in your environment.	Full script code visible for review and audit.	Cryptographic lock on the script; any change will break the implementation.
Best for: Most partners. Proof of non-interference and fastest deployment.	Best for: Partners requiring code-level transparency before approval.	Best for: High-security environments that require tamper-proof verification.

Most partners start with Closed and request the Open or SRI versions only if their security policy or platform requirements require it. We are more than happy to walk your IT & Tech through any of the options.

The Bottom Line

The retargeting service we bring you through Raccoon Rockets is built for how the industry should work: your audience, your data, your control. The partner's technology is transparent enough for your IT & Tech to approve, private enough for your compliance team to sign off, and effective enough to deliver strong business performance.

*This is not about “tracking people around the internet.” It’s about **helping you reconnect with your own audience** - without giving anyone else access to your data or harming your visitors’ right to privacy.*

Key Facts at a Glance

- No third-party cookies, regardless of deployment option.
- No executable code delivered to your site in the standard setup.
- No visitor personal data transmitted in clear text.
- Full source code available for review on request.
- Cryptographic verification available for highest-security environments.
- Data retained under 24 hours, or per your policy.
- The retargeting partner's infrastructure is certified to ISO 27001 / SOC 2.
- The partner's service is fully aligned with GDPR, CCPA, and IAB TCF 2.2.
- Script loads asynchronously; zero impact on page speed.

Disclaimer

The technology, platforms, assets and media described in this document are provided by third-party partners and remain the property of their respective owners. Raccoon Rockets acts as the commercial partner for the service.