

How Redmob Strengthens Pre-Bid Traffic Quality With IP Intelligence

Redmob is a mobile Supply-Side Platform connecting in-app publishers in emerging markets with global demand partners. Redmob screens every incoming bid request against a layered quality stack — including IPinfo's Residential Proxy, Privacy Detection, and IP Geolocation data — so that flagged traffic is removed before the auction opens, not after the ad is served.



6.76B

bid requests in one full day of US traffic



160M

unique IPs enriched with IPinfo data in Snowflake



>99.85%

agreement with IPinfo's country-level location for legitimate traffic



100%

of incoming bid requests screened across all operating regions



ABOUT REDMOB

Founded in 2024, Redmob helps mobile-first companies scale through smart monetization technology. Redmob operates a mobile Supply-Side Platform handling billions of bid requests per day across the US, APAC, Africa, and LATAM.

Customer since: **2026**

Data used: **Residential Proxy, Privacy Detection, IP Geolocation**

The problem: adding more context to traffic quality decisions

As an SSP, Redmob evaluates traffic before it reaches the auction. Making accurate decisions at this stage requires more than a single risk flag, particularly as residential proxies can appear similar to legitimate household traffic.

Redmob wanted additional IP-level context to better distinguish between legitimate users and potentially high-risk traffic, while avoiding unnecessary filtering of valid publisher inventory.

The solution: building a layered quality stack

Redmob's approach is deliberately multi-layered, on the principle that no single signal catches everything and no single vendor should be a point of failure:

- Creative-level scanning to detect malicious and non-compliant ad creatives
- Internal supply-quality signals derived from Redmob's own traffic warehouse, monitored continuously by the engineering team
- Third-party IP intelligence from IPinfo, covering residential proxy, VPN, hosting and privacy-service detection at the request level
- Ongoing supplier-level review, so quality findings feed back into commercial relationships with supply partners

IPinfo's data addressed a specific gap in this stack. Residential proxy traffic uses genuine household ISP addresses rented out as exit nodes; it presents valid geolocation and plausible ISP attribution, and is therefore invisible to conventional privacy and datacenter detection. Redmob wanted coverage of that category specifically.

The process: validating the signal at production scale

Before deploying anything into the live bidding path, Redmob ran a controlled evaluation: a full day of US bid traffic — 6.76 billion requests across 160 million unique IPs — enriched with IPinfo data in Snowflake and tested through a series of hypothesis-driven experiments, with additional regional validation.

The evaluation confirmed that residential proxy activity is materially under-detected by conventional signals, and that flagged traffic behaves in ways that are measurably distinct from legitimate traffic. Redmob validated the signal along several independent dimensions before agreeing to act on it.

“

“A residential proxy doesn't look like fraud. It's a real home address, in the right country, on the right network, so the usual checks pass it. A flag on its own doesn't help much there. We wanted to understand what's actually happening behind an address, and that's what IPinfo gave us. Not a verdict, but enough detail to reach our own.”



Gabriele Vileikyte
Managing Director, Redmob

“

“As an SSP, we have an opportunity to assess traffic quality before it enters the auction. IP intelligence gives us additional context to make those decisions more accurately.”



Gabriele Vileikyte — Managing Director, Redmob

The result: filtering the high-risk requests, not the publishers

IPinfo expanded Redmob's visibility into residential proxy traffic that conventional IP-level signals may not identify, adding another layer to its existing pre-bid traffic verification stack. Across billions of requests, Redmob measured better than 99.85% agreement with IPinfo's country-level location for legitimate traffic, while identifying the infrastructure ranges where location data proved materially less reliable.

Redmob's pre-bid screening now covers 100% of incoming bid requests across all operating regions. Because flagging happens at the IP and user level rather than the app or publisher level, Redmob removes the flagged request while legitimate inventory from the same application continues to trade normally.

This matters commercially as well as technically. Blunt publisher-level blocking punishes developers for traffic they often did not source and cannot see. Redmob's approach treats publishers as partners in cleaning up the supply chain rather than as suspects.

“

“We filter the user, not the publisher. A developer with a good app should not lose their revenue because someone routed proxy traffic through it. Our job is to take that request out of the auction and let the legitimate inventory keep trading.”



Gabriele Vileikyte — Managing Director, Redmob

What comes next

Redmob is extending the same pre-bid screening philosophy across the rest of its quality programme, with the objective that supply quality becomes a stated product characteristic of the business rather than an operational back-office function.

“

“We didn't take the data on trust. We ran it against a full day of production traffic and tested it behaviorally: does this traffic move, appear and persist the way real people do? The patterns IPinfo identified lined up with our own quality indicators, so we brought them into our pre-bid controls.”



Gabriele Vileikyte — Managing Director, Redmob

How is your traffic quality?

Learn more about IPinfo's Residential Proxy and Privacy Detection data, and test it on your own traffic.

[Talk to Sales](#)