**Traffic Analysis & Bot Mitigation Recommendations**

An investigation into recent server logs reveals significant indicators of bot-like activity across several endpoints. A handful of IP addresses generated thousands of requests in one day, with some bursts exceeding 20 requests in less than five seconds. These patterns suggest automated scraping, not genuine human interaction.

Our assessment is based on the assumption that the company runs a lightweight Apache-style web infrastructure with minimal bot protection, a small technical team, and a limited budget for third-party services.

To mitigate this, we propose a layered, cost-effective solution:

1. **Integrate Google reCAPTCHA v2** on high-impact pages like login, signup, and submission forms. It is free at scale and requires only a few lines of HTML and a server-side verification step. This will immediately block most automated scripts without affecting user experience.
2. **Leverage Cloudflare’s Free Tier** for CDN caching, rate-limiting, and basic bot filtering. It protects against aggressive traffic and reduces the load on your origin server by handling static content delivery efficiently.
3. **Schedule daily audits** using the existing Python log analysis tool. These automated reports will help monitor trends, identify suspicious IPs, and inform threshold tuning.
4. **Implement lightweight rate-limiting** via NGINX or a similar web proxy. Simple configuration rules (e.g., max requests per IP per second) offer adequate protection without new infrastructure.

This strategy offers immediate impact with minimal complexity. It blends automation, free-tier cloud services, and intelligent client-side ddefencesto keep infrastructure resilient. By deploying reCAPTCHA, using Cloudflare, and analysing logs daily, the company can maintain performance, preserve analytics integrity, and stay ahead of evolving bot behaviour without incurring significant costs or administrative overhead.