**Summary of Findings**

After reviewing the website’s server logs, I found that most visits are focused on a handful of pages, each receiving more than 15,000 requests. The most visited include **/episodes/ep-42-synthesizer-history**, **/contact**, and **/about**. While some of this traffic may be from genuine users, the volume and pattern suggest that automated tools (bots) could be involved.

Another key observation is that only a few IP addresses are responsible for thousands of requests each—up to 5,400 per address. This is far higher than what is expected from normal website visitors. Even though all user agents in the logs appear to be standard browsers, it’s common for bots to disguise themselves in this way. This behaviour can slow down the website or cause outages, especially for a small company.

**Recommendations**

To keep the website running smoothly and avoid service interruptions, I recommend the following practical and budget-friendly steps:

1. **IP-Based Rate Limiting:** Limit how many requests each IP can make per minute or hour to prevent any single user (or bot) from overloading the server.
2. **Block High-Activity IPs:** Watch for IP addresses making excessive requests and block or challenge them when necessary.
3. **Add CAPTCHA:** Place simple CAPTCHA tests on forms or popular pages to filter out automated submissions.
4. **Use a Free Web Application Firewall:** Solutions like Cloudflare’s free plan are easy to set up and offer strong protection against bots and attacks.

**Notes**

These recommendations assume the company uses a standard web server setup and can make basic configuration changes. All steps are affordable and suitable for small businesses.

*Prepared by Vlad Stratan*  
[LinkedIn: Vlad Stratan](https://www.linkedin.com/in/vlad-stratan-1a607a218/)