Lighthouse



MANAGED INCIDENT BOT RESPONSE SERVICE

Over 50% of internet traffic is generated by bots

Up to 57% of eCommerce traffic can be automated during peak periods

The exact moments that matter most commercially, such as Black Friday, seasonal campaigns, and product launches, can also be the moments of highest exposure.

AI-driven bot traffic has grown by around 300% year over year

Bot activity is becoming more advanced, harder to filter with static rules, and more capable of bypassing traditional protections.

Why this matters

It can inflate paid acquisition metrics, waste ad budget, distort conversion and attribution data, increase infrastructure load, and reduce site responsiveness. This means teams may be making strategic decisions based on misleading analytics while losing efficiency across channels.

How it works

Effective bot protection requires more than tooling alone. Our approach combines two layers: Managed Incident Response as the primary operational layer, with continuous monitoring, real-time detection, dynamic rule tuning, and targeted mitigation actions. A complementary protection layer, which can optionally include Cloudflare Business for automated capabilities such as traffic filtering, WAF, baseline bot mitigation, DDoS protection, and performance optimization.

This is not passive protection. It is active management of bot incidents as they happen.

How it helps your business

- Reduces revenue leakage caused by invalid and non-converting traffic
- Protects data quality across funnels, attribution, and reporting
- Improves resilience during campaigns, launches, and peak revenue periods
- Helps reduce strain on infrastructure and site performance
- Aligns protection with business-critical flows such as checkout, campaigns, and APIs
- Minimizes the impact on legitimate users through continuous optimization

How much of your traffic is actually valuable?

Contact us for more info:

+30 211 109 4500

sales@lighthouse.gr