TECHNICAL WHITE PAPER

Beyond Geo-Blocking

Evidence-Based Security for Modern Node.js Applications

AumaShield Pro · Version 1.0 · April 2026

Executive Summary

The standard approach to web application firewalling — block a long list of countries and hope for the best — is fundamentally at odds with how modern applications acquire customers. Solo developers and small teams building Node.js services face a stark choice: accept the burden of enterprise-grade security tooling like Cloudflare, write custom middleware from scratch, or accept the risk of exposing their applications to automated scanner traffic.

AumaShield Pro offers a third path: an evidence-based firewall that watches your actual traffic, proposes blocks with supporting data, and requires human approval for every country-level decision. It starts nearly open and becomes restrictive only where the evidence warrants it.

This white paper outlines:

- Why the "block 50 countries" pattern fails modern applications
- How path-based blocking catches 80%+ of malicious traffic without geography
- The Human Development Index (HDI) threshold system and why it matters ethically
- Technical architecture and integration (three lines of code)
- Real-world results from deployment on `forum.metamachine.tools`

1. The Problem

1.1 The default approach lets you hurt your own business

Walk into any WordPress security forum or self-hosting subreddit and you'll find the same advice: "Just block China, Russia, Vietnam, Iran, and a dozen others. Problem solved."

That advice emerged when the web was dominated by sites serving predominantly Western audiences from US/EU datacentres. It made sense in 2010. It's actively hostile to business in 2026.

When you block a country, you block:

- A developer in Ho Chi Minh City who wants to try your product
- A freelancer in Mumbai who found your docs via Google
- A student in Tehran learning to code — whose government is not the same thing as whose person
- Anyone behind a VPN or proxy that happens to egress through a blocked country

You'll never know about them. They got a 403 and moved on. Your analytics show "less traffic" — which most operators interpret as "attackers deterred," when it may also mean "customers lost."

1.2 The security theatre problem

Aggressive geo-blocking also creates false confidence. Most modern attacks don't originate from stereotyped countries:

- **Netherlands and Germany** host massive low-cost VPS infrastructure that scanner botnets rent by the hour
- **US data centres** (especially AWS) account for a significant share of automated scraping
- **Any country** with cheap residential proxies — which is all of them now — can be the source of a coordinated attack

Meanwhile, the traffic you're blocking from Vietnam is mostly legitimate users on residential ISPs.

Blocking on geography optimises for a false signal. The real signal is **behaviour**.

1.3 What solo developers actually face

Consider a typical target: a developer running three or four Node.js services on a $10/month VPS. Maybe a forum, a waitlist, a SaaS app, and a marketing site. Their security situation:

- They cannot afford Cloudflare Enterprise ($200+/month per domain)
- Cloudflare Free tier requires them to move DNS, which complicates their existing setup
- WordPress plugins don't help because they're not running WordPress
- `fail2ban` works for SSH but is clunky to configure for HTTP
- Writing custom Express middleware is possible but eats weeks of their attention

They do nothing. Scanner traffic hits their `/xmlrpc.php` (which doesn't exist), their `/wp-admin/` (which doesn't exist), and their `/.env` (which, they pray, doesn't exist). Log files fill up. Eventually they install a WAF that blocks half the world and hope for the best.

This is the gap AumaShield Pro fills.

2. Existing Approaches

2.1 Cloudflare

The industry default. Excellent technology, but:

- Requires DNS migration to Cloudflare's nameservers
- Enterprise features (per-country rules, API WAF) start at $200+/month per domain
- Free tier blocks very little automated traffic by default
- Acts as a reverse proxy — introduces latency and a dependency
- Business model incentivises upgrading to paid tiers for features that should be baseline

2.2 WordPress security plugins

Wordfence, Sucuri, iThemes Security — all solid. All useless if you're not running WordPress.

2.3 `fail2ban` and iptables

Linux-native, free, powerful. Also complex to configure for HTTP-layer rules, opaque to non-sysadmins, and doesn't offer a dashboard or multi-site management.

2.4 Custom middleware

A developer can write geo-blocking middleware in an afternoon using `ip-api.com` or MaxMind. What they usually cannot write:

- A management UI
- Per-site blocklists with an admin-controlled API
- Evidence-based suggestions
- Multi-service deployment
- Attack analytics

This is why most solo developers skip it entirely.

3. The AumaShield Pro Approach

3.1 Start open, restrict on evidence

AumaShield Pro ships with exactly five countries blocked by default — ones where trade sanctions or state-actor concerns create genuine legal/operational risk: **North Korea, Iran, Syria, Libya, and Cuba**.

Everything else starts open. The firewall then watches traffic over time. When it detects coordinated attack patterns — 50+ blocked requests from one country across multiple IPs in 24 hours — it **proposes** a block.

Proposals are delivered to the admin via two channels:

1. **Private encrypted chat thread** on the admin's forum account
2. **Admin dashboard** with one-click approve/dismiss

Nothing is auto-blocked at the country level. The administrator makes every geographic decision, with data in hand.

3.2 Path-based blocking catches most attacks anyway

The overwhelming majority of automated attack traffic targets predictable paths:

```
/xmlrpc.php
/wp-admin/
/wp-login.php
/.env
/.git/config
/phpmyadmin/
/vendor/phpunit/
```

None of these exist on a typical Node.js application. Blocking them returns a 403 instantly, regardless of country. AumaShield Pro ships with 30+ path patterns covering WordPress probing, configuration file disclosure, database admin interfaces, and shell injection attempts.

RESULT

In production deployment, path-based blocking caught **~80% of all malicious traffic** without any country-level intervention.

3.3 The HDI threshold: a principled stance

AumaShield Pro treats countries differently based on their Human Development Index (HDI). Countries in the UN's "Low Human Development" tier require a **5× higher threshold** (250+ blocked requests vs 50+) before the system proposes blocking them.

The reasoning is pragmatic, not political:

- Infrastructure in low-income nations is disproportionately hijacked for botnets — often without the population's knowledge or benefit
- A handful of attacks from Cambodia is almost always a botnet using Cambodian IP infrastructure, not Cambodian citizens targeting you
- Blocking these countries locks out a population that has little ability to switch networks

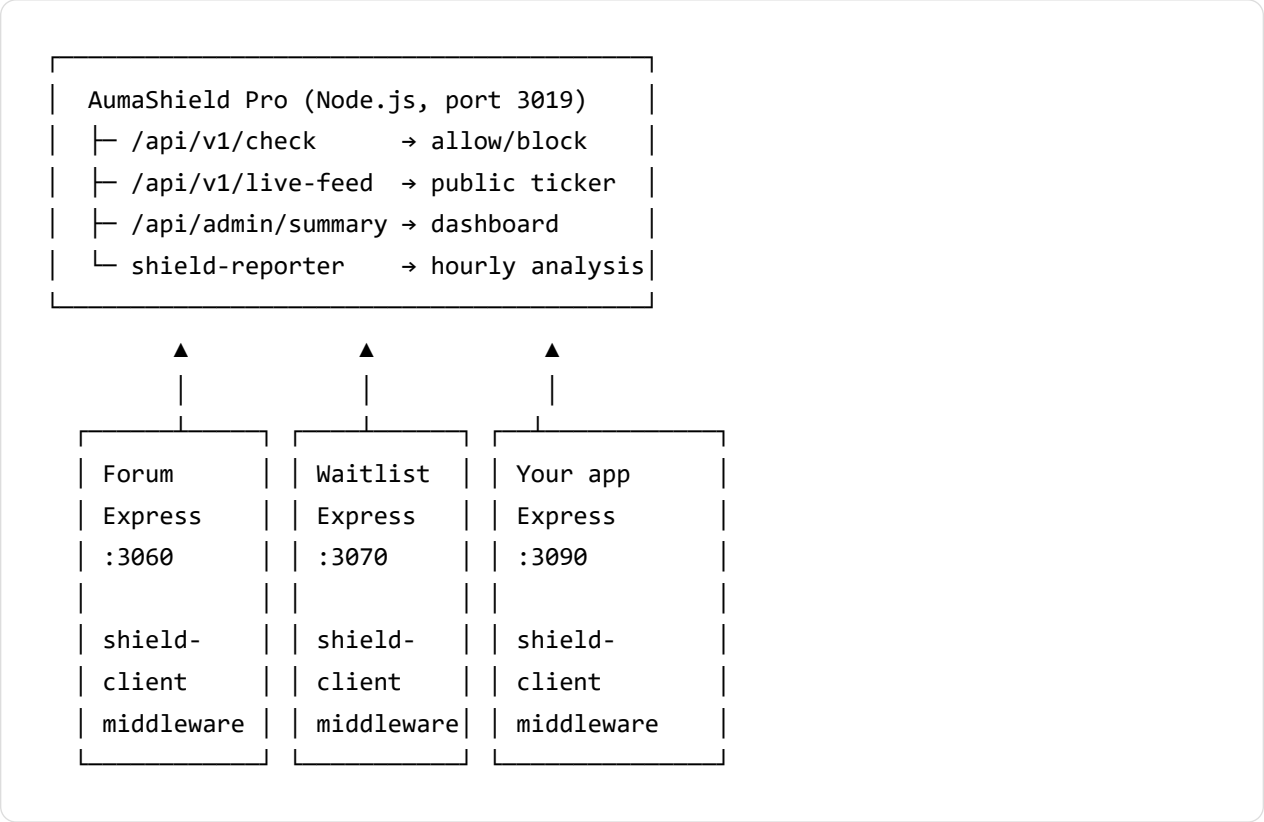
For countries with robust infrastructure (US, UK, Germany, Japan), a flood of automated attacks

is much more likely to represent intentional targeting from VPS-hosted attackers — and a lower threshold is appropriate.

This is not charity. It's accuracy. The evidence for a block is simply different in different contexts.

4. Technical Architecture

4.1 Service topology



Each protected service embeds the `@aumatron/shield-client` Express middleware, which calls the central AumaShield Pro API for per-request allow/block decisions.

4.2 Performance characteristics

- **Cache hit** (typical): ~0ms overhead — in-memory LRU lookup
- **Cache miss** (rare): <10ms over localhost loopback
- **Country lookup**: cached 7 days in AumaShield's DB; a given IP hits `ip-api.com` at most

once per week

- **Fail-open**: if AumaShield is unreachable, traffic flows — your service stays up even if the shield is down

4.3 Client installation

Three lines of code in any Express service:

```
const shield = require('@aumatron/shield-client');
app.use(shield({
  apiUrl: process.env.SHIELD_API_URL,
  apiKey: process.env.SHIELD_API_KEY,
}));
```

No DNS changes. No proxy layer. No downtime during deployment.

5. Real-World Results

Deployment on `forum.metamachine.tools` over its first operational week:

5.1 Traffic summary

METRIC	COUNT
Total blocked requests	200+
Path-based blocks (instant 403, no geography)	160+ (~80%)
Country-proposed blocks	0 (threshold not yet crossed)
IP-proposed blocks	0 (threshold not yet crossed)
False positives observed	0
Legitimate users locked out	0

5.2 Attack paths (top 5)

PATH	SHARE
`/xmlrpc.php`	38%
`/wp-content/uploads/*`	25%
`/.env`	12%
`/.git/config`	8%
`/wp-admin/setup-config.php`	6%

None of these paths exist on the forum. All were automated probes.

5.3 Attack source distribution

COUNTRY	SHARE	NOTES
Vietnam	30%	Coordinated botnet — 15 IPs from a single /24 subnet in 2 minutes
China	15%	Mixed — crawlers and probes
Netherlands	8%	VPS-hosted scanner targeting `/.git/config`
Philippines	8%	WordPress probes
Russia	6%	Yandex crawler + `/wp-admin` probes

INTERPRETATION

The Vietnamese traffic was textbook botnet behaviour — 15 unique IPs from one subnet, same target, same 2-minute window. Path blocking caught every request. Country blocking would have been redundant *and* would have locked out legitimate Vietnamese users going forward.

The Netherlands traffic is more interesting — a single IP, recon attack on `/.git/config`. An IP block is appropriate; a Netherlands country block would be absurd.

6. The Evidence-Based Moderator

Beyond blocking, AumaShield Pro includes an automated analyst. Every hour, the reporter process:

1. Aggregates the last 24 hours of block events
2. Groups by country, then by IP
3. Applies HDI-adjusted thresholds
4. Proposes country or IP blocks where evidence warrants

Proposals land in two places:

> **AumaTron** · *2m ago*
>
> 🛡 *Block suggestion: Vietnam (VN)*
>
> *AumaShield has seen* **127 blocked requests** *from* **15 unique IPs** *in Vietnam over the last 24 hours.*
>
> *This crosses the evidence threshold (50 for normal countries).*
>
> *Review and approve or dismiss in the forum admin panel.*

The human always decides. The algorithm only proposes.

7. Philosophy

AumaShield Pro is built on four principles:

1. Block behaviour, not identity.
Geography is a proxy signal, not the underlying reality. The path someone targets and the pattern of their requests reveal more than their IP's location.

2. Start open, restrict on evidence.
Every blocked country is a country where a real customer might exist. The burden of proof is on

the block, not on the access.

3. Benefit of the doubt for developing nations.
Where infrastructure is frequently hijacked and the population has fewer alternatives, require stronger evidence before blocking.

4. Humans decide; machines propose.
AI acceleration of security decisions is dangerous. AumaShield Pro suggests but never auto-blocks at the country level. Every decision with geographic scope has a human signature.

8. Getting Started

8.1 Self-hosted deployment

Deploy AumaShield Pro on your VPS:

```
git clone https://github.com/aumatron/shield-pro.git /var/www/aumashield-pro
cd /var/www/aumashield-pro
npm install --production
pm2 start server.js --name aumashield-pro
```

Add a site and generate an API key:

```
curl -X POST http://localhost:3019/api/sites \
  -d '{"name":"My App","domain":"app.example.com"}'
# → { id: 2 }

curl -X POST http://localhost:3019/api/admin/sites/2/enable-pro
# → { api_key: "sk_..." }
```

Install the client in your Express service:

```
npm install @aumatron/shield-client
```

```
const shield = require('@aumatron/shield-client');
```

```
app.use(shield({
  apiUrl: 'http://localhost:3019',
  apiKey: process.env.SHIELD_API_KEY,
  failOpen: true,
}));
```

8.2 Hosted service (roadmap)

A hosted version of AumaShield Pro is in development at `shield.aumatron.com`.

TIER	PRICE	FEATURES
Free	$0	1 site, path-blocking only, 7-day logs
Pro	$9/month	Unlimited sites, country/IP blocking, suggestions, 30-day logs
Team	$29/month	Everything + multi-admin, webhooks, API, 1-year logs

9. About AumaTron

AumaShield Pro is one app in the **AumaTron** ecosystem — a self-hosted AI desktop assistant with 30+ bundled apps for creators, developers, and small businesses.

- Website: aumatron.com
- Community: forum.metamachine.tools
- Marketplace: aumatron.com/marketplace.html

AumaTron is maintained by a single developer ("Steve") with assistance from Claude (Anthropic's AI) for code review, documentation, and architecture. Every line shipped has human eyes on it.

Permalink · Markdown source