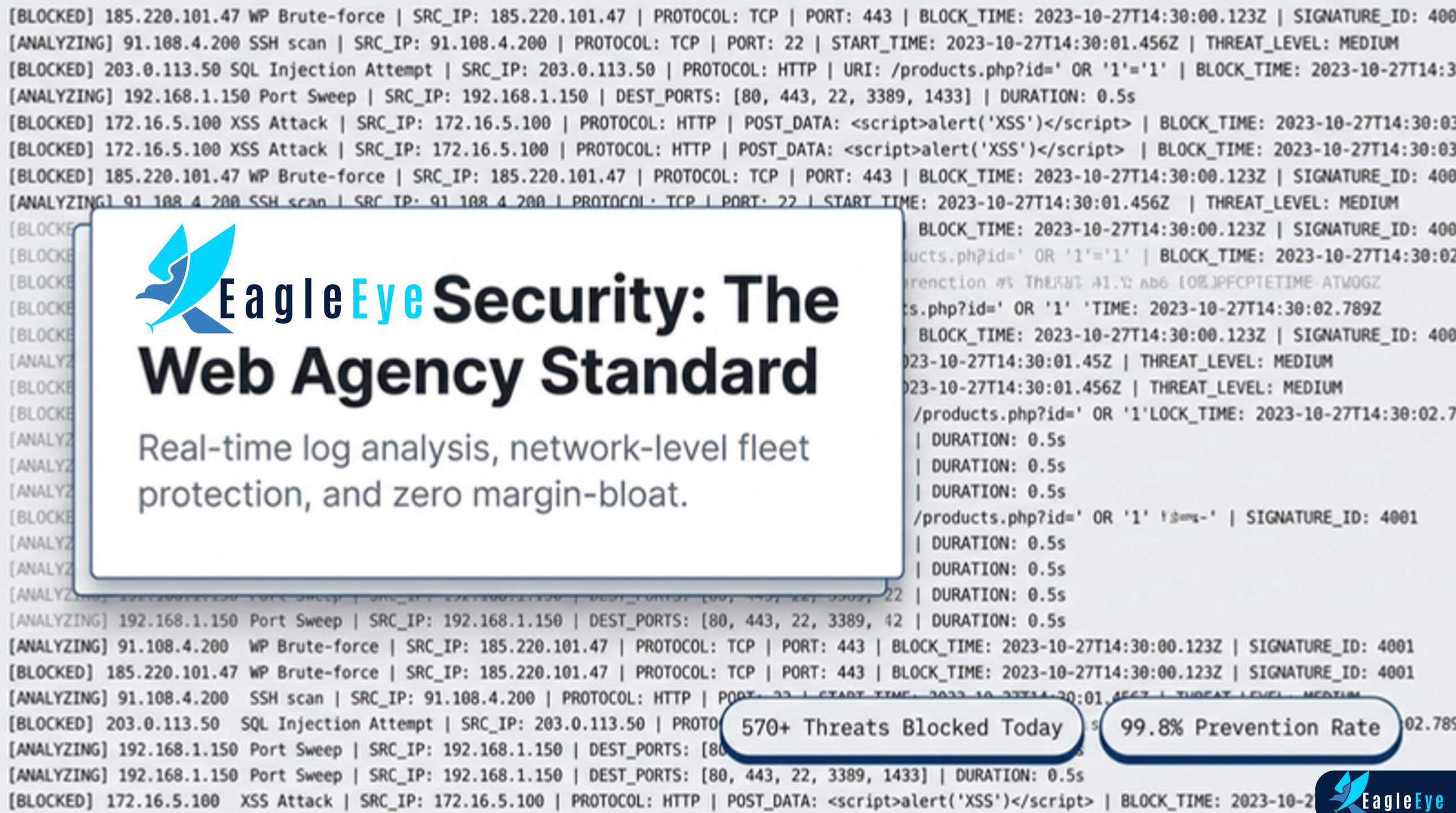
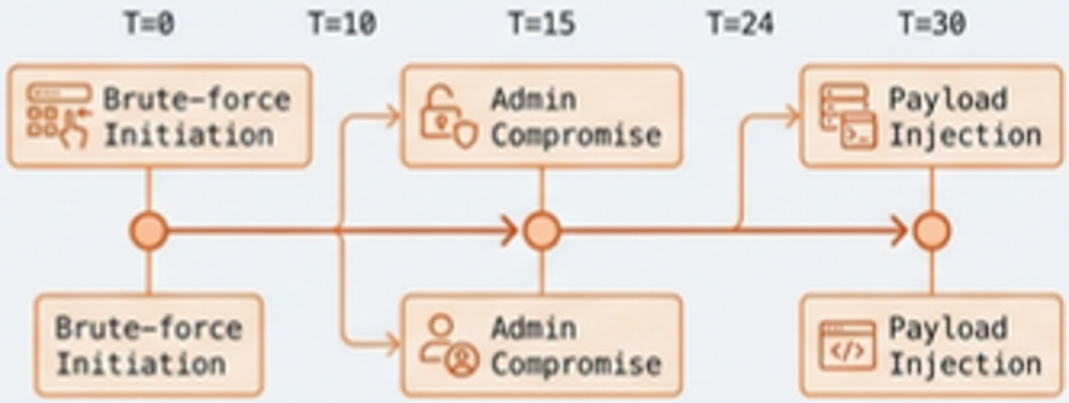
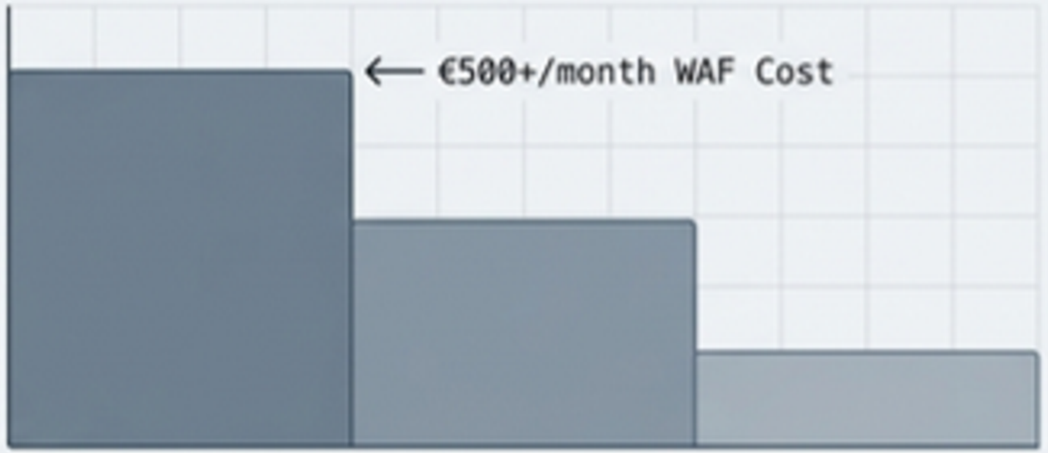

EagleEye Security: The Web Agency Standard
Real-time log analysis, network-level fleet protection, and zero margin-bloat.
570+ Threats Blocked Today
99.8% Prevention Rate
EagleEye

The 30-Minute Compromise



Free security plugins rely on manual intervention. In 30 minutes, automated bots can compromise an admin account, inject payload, or exfiltrate client data.

The Enterprise Tax



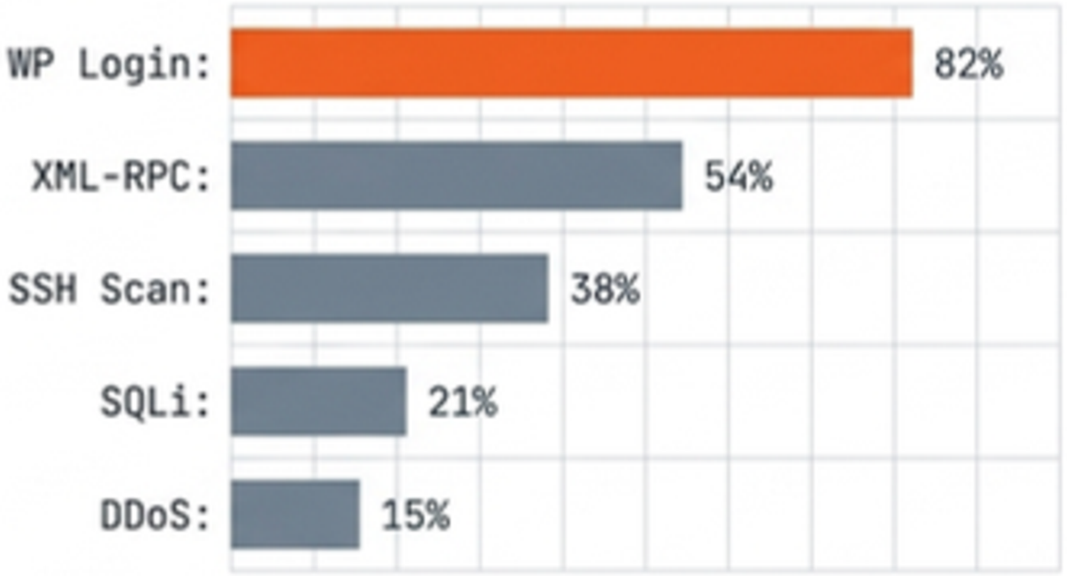
Traditional enterprise WAFs demand €500+/month and dedicated security teams. Agencies are forced to absorb the cost or pass it to clients, destroying hosting margins.

Agencies need enterprise-grade automated protection at a price point that protects profitability.

Automated bots target infrastructure, not just sensitive data.

Every server in your client fleet faces dozens of daily automated probes—brute-force attempts, XML-RPC floods, and SSH scans—searching for a single weak link.

Attack Vectors (Last 7 Days)



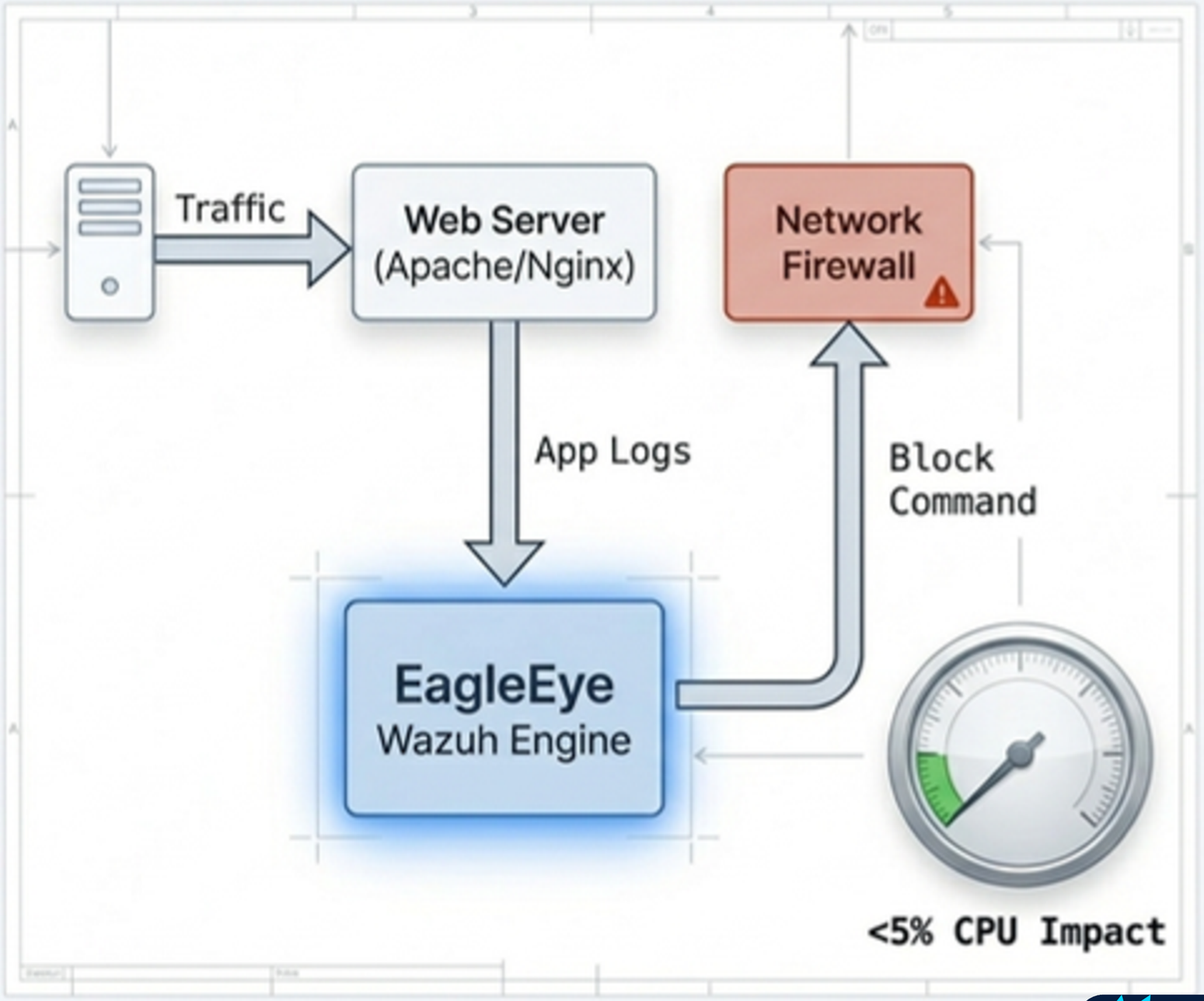
100+ Attacks Daily Per Server

```
[BLOCKED]   185.220.101.47 WP Brute-force    2s ago
[BLOCKED]    45.33.32.156  XML-RPC flood     7s ago
[ANALYZING] 91.108.4.200   SSH scan          12s ago
[BLOCKED]   198.244.190.82 Login attack      18s ago
```

The Log-Based Network Paradigm

Real-Time Detection:
Wazuh actively parses every server log line across Apache, Nginx, WP, and SSH.

Network-Level Blocking:
Malicious IPs are dropped at the network firewall, entirely preventing them from reaching the application layer.



The 10-Second Automated Kill Chain

T=0s

Continuous Monitoring

Wazuh ingests all HTTP/SSH system logs in real-time. Every request is parsed.

<1s

Pattern Alert

Engine detects a volumetric anomaly (e.g., SSH scan) and generates an internal alert with source IP and criticality.

<3s

Smart Analysis

IP is contextualized against global threat feeds and agency-specific parameters.

<10s

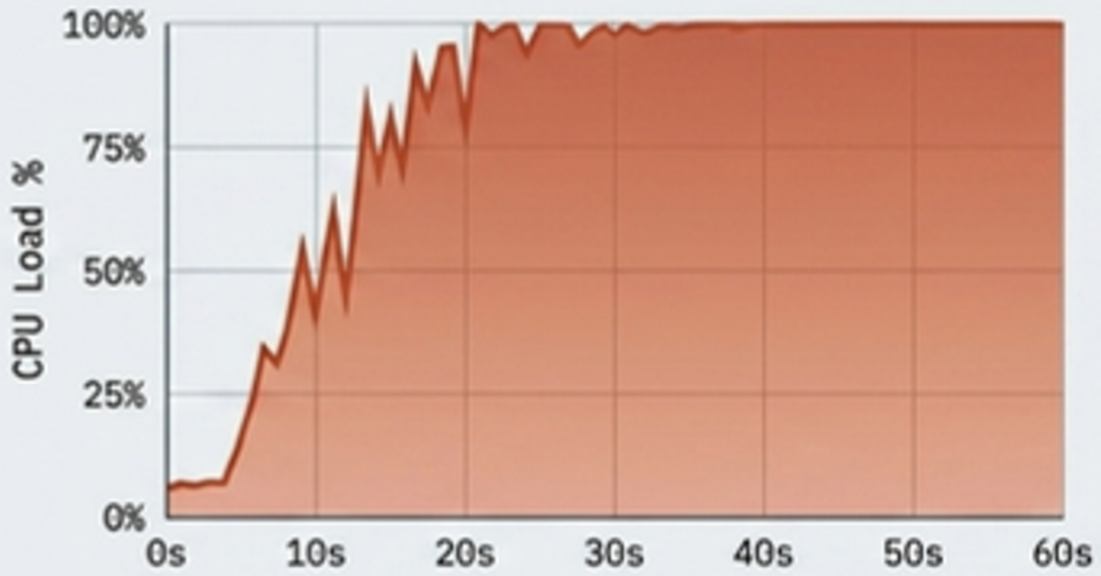
Block & Notify

IP is instantly added to the server's firewall drop rules. Telegram/Email alerts trigger simultaneously.

EagleEye

Performance Under Fire: Surviving Brute-Force

App-Layer Plugins



Classic plugins load PHP and query MySQL for *every* blocked request. A brute-force attack will still crash the server through resource exhaustion.

EagleEye Network Drop

EagleEye drops attackers at the network firewall level. The malicious traffic never hits PHP or the database. Client sites remain lightning-fast, even under heavy volumetric attack.

EagleEye

Zero False Positives.
Zero SEO Disruption.

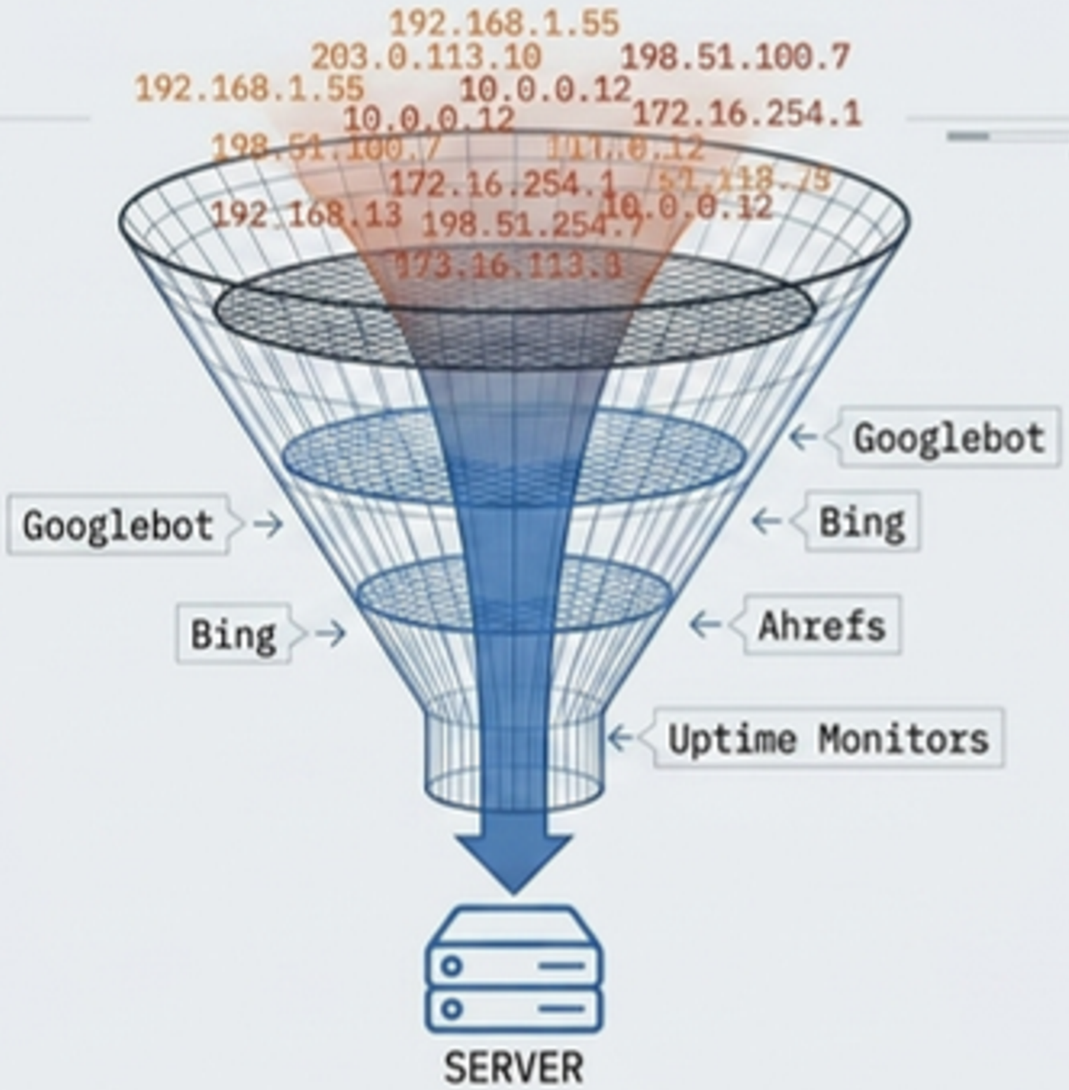
380+ Pre-Whitelisted IP Ranges

The intelligence engine actively contextualizes every IP against geographic, organizational, and threat-level databases.

Automatically Authorized Infrastructure

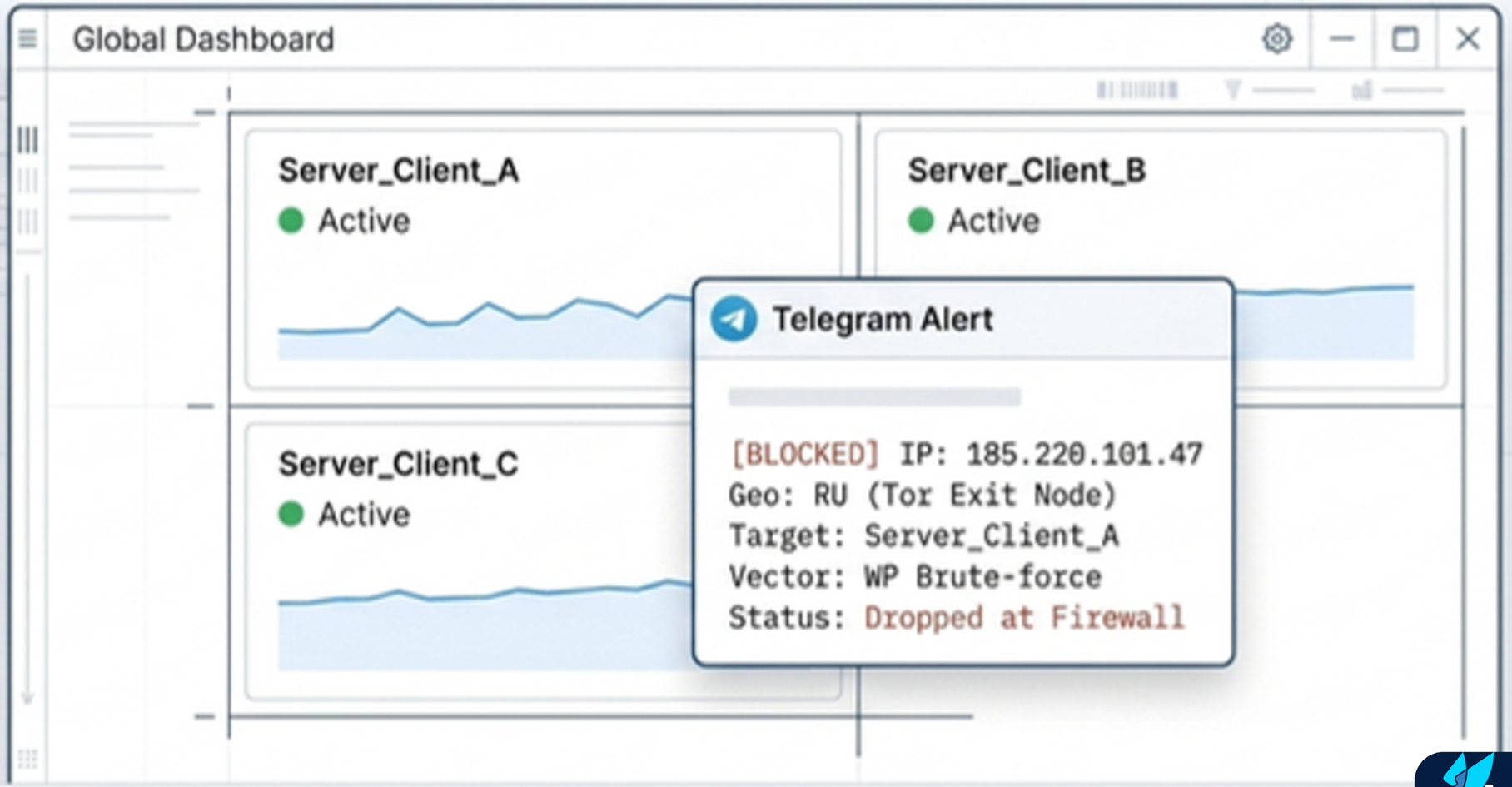
- Googlebot & Bing
- Ahrefs & SEMrush
- Uptime monitors & payment gateways

Smart Filtering Funnel



Centralized Fleet Management

Monitor all client servers from a single pane of glass. When an attack occurs, your technical team receives instant context via Telegram, removing the need to dig through raw access logs.



Architectural Diagnostics

	Traditional WAF	Security Plugin	EagleEye
Detection Speed	Minutes to Hours	Hours	**<10 Seconds**
False Positives	5-20%	High	**0%** (380+ Whitelists)
Network Blocking	Partial	No	**Yes**
Server Impact	Significant	Moderate	**<5% CPU**
Live Fleet Dashboard	No	No	**Yes**

The Agency Margin Matrix

Secure your entire client portfolio for a fraction of the cost of outfitting a single server with an enterprise WAF.

Legacy WAF Infrastructure

~€1,000+/mo

- Cost: €200–€500 per server.
- Destroys hosting margins.
- Requires passed-on costs to clients.

EagleEye Professional

€59/mo total

- Covers a 3-server fleet.
- Immediate margin expansion.
- Upgraded security posture.
- Centralized Telegram alerts included.

EagleEye

Predictable Scaling. No Surprises.

Starter

€29/mo

- 1 Server
- WP/Server attack detection
- Auto-blocking
- Email alerts

Agency Standard

Professional

€59/mo

- 3 Servers
- WP + SSH + Nginx
- Smart Blocking (380+ Whitelist)
- Live Fleet Dashboard
- Telegram + Email Alerts
- IP Geolocation

Enterprise

Custom

- Unlimited Servers
- Custom rules
- Full API access
- Dedicated 24/7 Support
- GDPR/PCI-DSS compliant SLA

Secure Your Infrastructure Today

- ✓ Setup complete in under 2 hours.
- ✓ 14-day free trial. No credit card required.
- ✓ Technical support and onboarding included.
- ✓ 100% GDPR compliant (Data hosted in Europe).

```
> eagleeye install --fleet

[OK] Fetching Wazuh packages...
[OK] Applying whitelist rules (380+)...
[OK] Binding to Network Firewall...

Deployment successful. Active protection
running.
```

14-Day Free Trial

Start your trial today. Our engineering team will contact you within 2 hours to configure your active protection.

EagleEye