

Sécurité temps réel pour votre PME.

EagleEye détecte, analyse et bloque automatiquement les cyberattaques avant qu'elles n'atteignent vos serveurs. Zéro faux positif, protection 24/7.



[BLOQUÉ] 185.220.101.47 | WP Brute-force | 2s ago

[ANALYSE] 91.108.4.200 | SSH scan | 12s ago

[BLOQUÉ] 45.33.32.156 | XML-RPC flood | 15s ago

[BLOQUÉ] 103.209.65.112 | SQL Injection | 21s ago

570+ menaces bloquées aujourd'hui

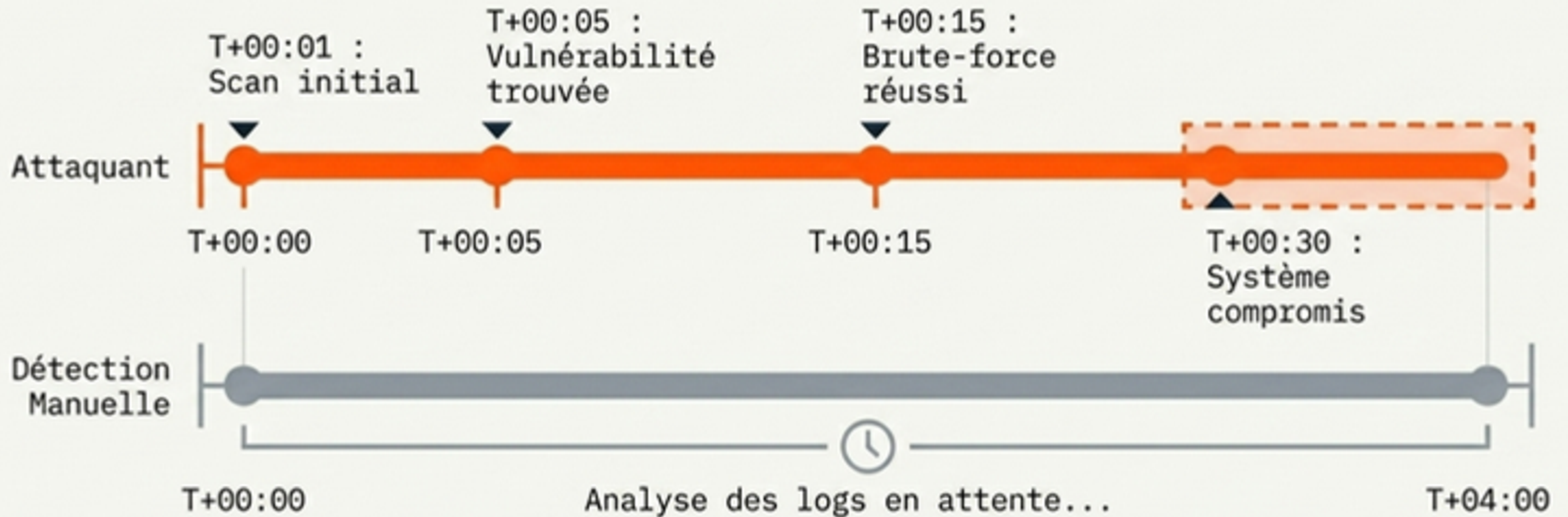
L'illusion de l'invisibilité : 100+ attaques quotidiennes.

Chaque site WordPress reçoit des dizaines d'attaques quotidiennes – bots, brute-force, scans – même si aucune donnée sensible n'est stockée.

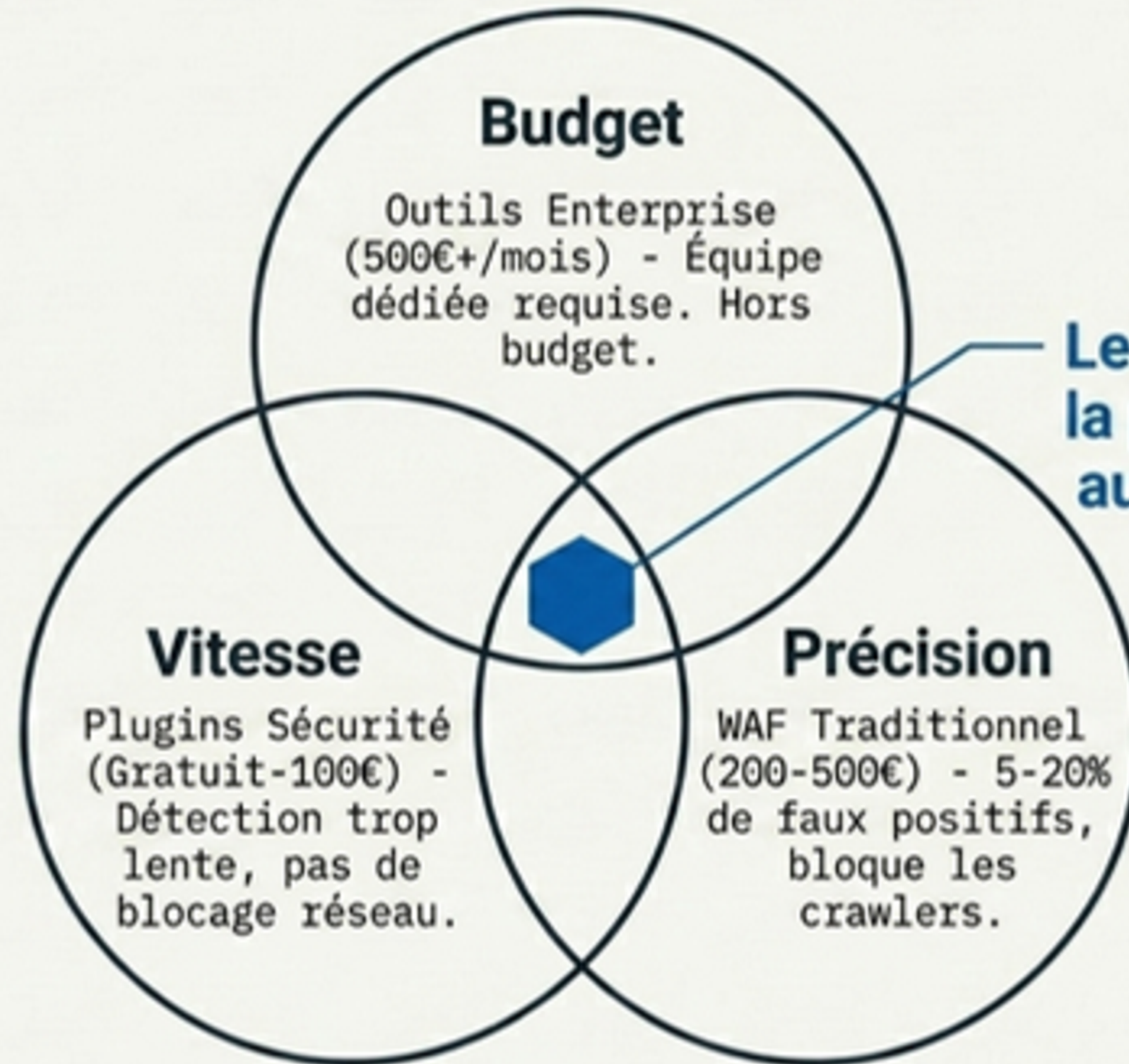


La détection manuelle est une course perdue d'avance.

En 30 minutes, un attaquant peut compromettre un compte admin, injecter du code malveillant ou voler des données.



Le paradoxe de la sécurité pour les PME.



Les PME ont besoin de la puissance Enterprise au prix d'un plugin.

Protection complète, sans la complexité.

Zéro configuration complexe :
Protection active immédiate.

Zéro faux positif :
Le trafic légitime passe, les menaces s'arrêtent.

< 10

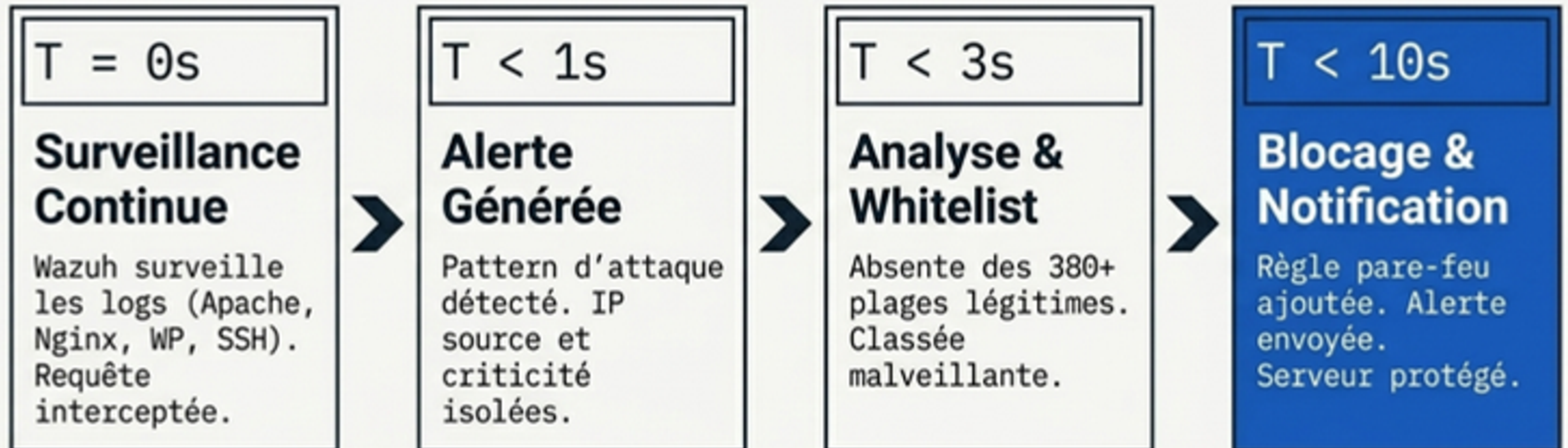
**< 10
secondes**

99.8% Taux de prévention.

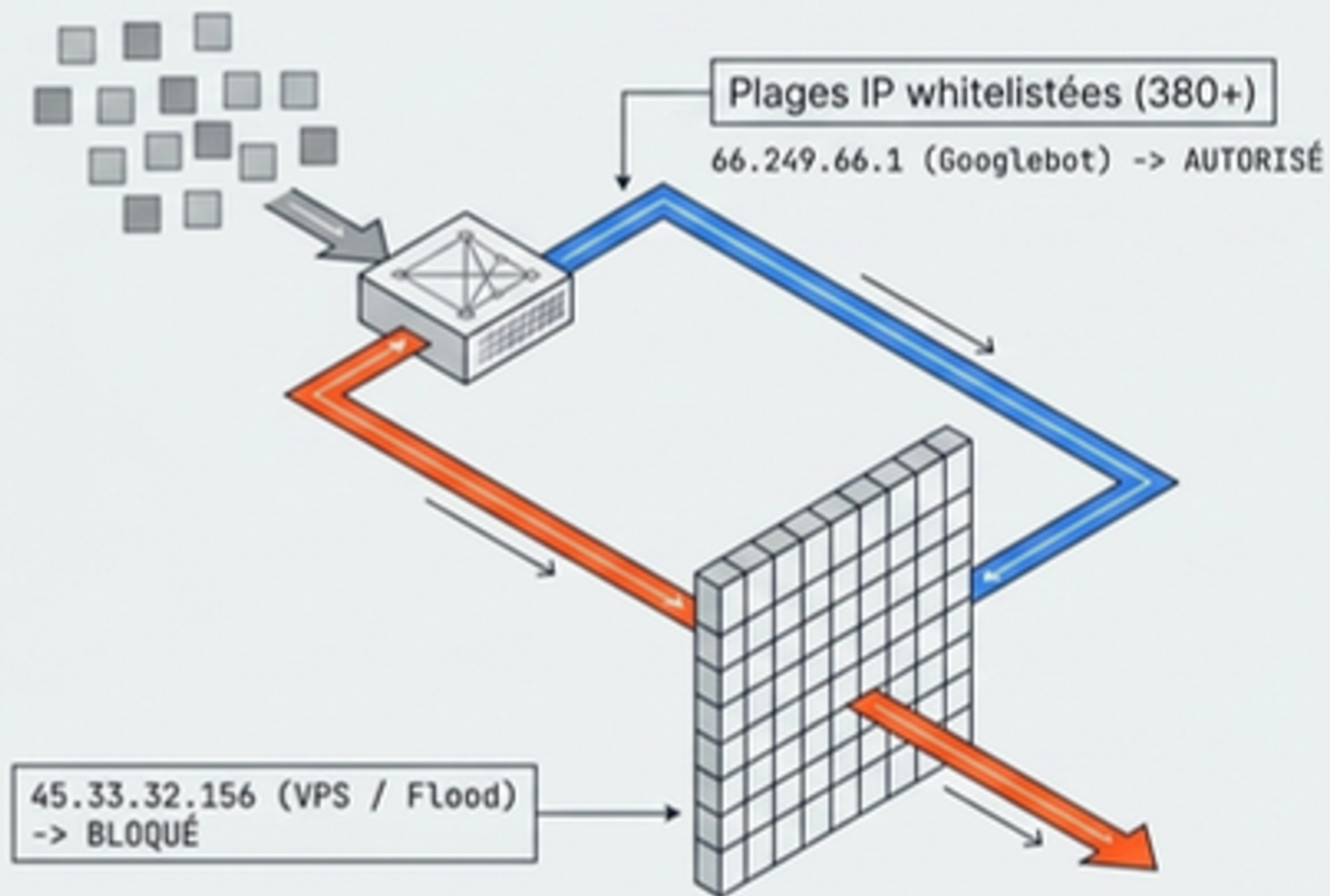
Zéro interruption de service : Impact serveur minime (<5% CPU).

Anatomie d'une neutralisation : De la requête au blocage en moins de 10s.

CIBLE: IP 185.220.101.47



Analyse intelligente : Zéro faux positif, trafic SEO préservé.



Les crawlers légitimes (Google, Bing, Ahrefs, SEMrush) ne sont jamais bloqués.

Analyse géographique, niveau de menace et type d'organisation. Blocage strict des acteurs malveillants.

Une architecture conçue pour la réactivité.

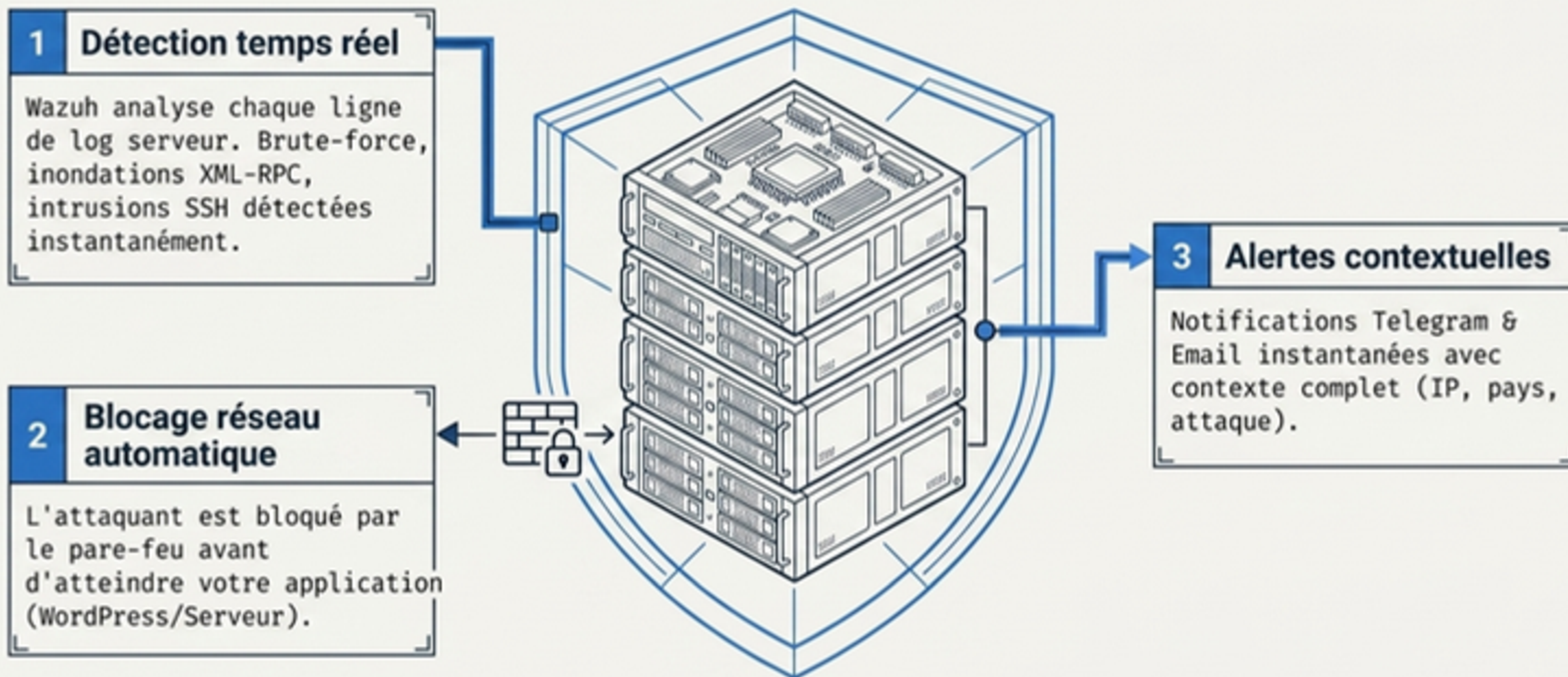


Tableau de bord tactique : Votre infrastructure en un coup d'œil.

Statut : EN DIRECT ●

Détection -> Blocage : <10s

Vecteurs d'attaque (7 jours)



■ WP Login : 82% ■ SQLi : 21%
■ XML-RPC : 54% ■ DDoS : 15%
■ SSH Scan : 38%
■ SQLi : 21%

Flux en direct

185.220.101.47	RU • Tor exit	WP Brute-force	BLOQUÉ
45.33.32.156	US • VPS	XML-RPC flood	BLOQUÉ
66.249.66.1	US • Googlebot	Scan légitime	AUTORISÉ

Le standard de la sécurité moderne.

	WAF Traditionnel	Plugin sécurité	EagleEye
Temps de détection	Minutes -> heures	Heures	✓ <10 secondes
Coût mensuel	200-500€	Gratuit -> 100€	✓ 29-99€
Faux positifs	5-20%	Élevés	✓ 0%
Blocage crawlers	Fréquent	Très fréquent	✓ Jamais (380+ pages)
Blocage réseau	Partiel	✗	✓ Total
Impact serveur	Significatif	Modéré	✓ <5% CPU

Une tarification simple, prévisible et sans surprise.

Tous les plans incluent un essai gratuit de 14 jours. Aucune carte de crédit requise.

PLAN STARTER — 29€/mois

- ✓ Protection essentielle.
- ✓ Inclus: 1 serveur/site, attaques WordPress, blocage auto, alertes email.

★ Le plus populaire

PLAN PROFESSIONAL — 59€/mois

- ✓ Inclus: 3 serveurs/sites, WordPress+SSH+Nginx, blocage intelligent (whitelist 380+), alertes Telegram+Email, tableau de bord live.

PLAN ENTERPRISE — Sur mesure

- ✓ Pour infrastructures complexes. Inclus: Serveurs illimités, règles sur mesure, support 24/7, API, SLA/RGPD.

Protégez votre infrastructure dès aujourd'hui.

- ✓ Configuration experte en moins de 2 heures
- ✓ Essai gratuit de 14 jours (Aucune carte requise)
- ✓ Accompagnement technique inclus
- ✓ Données hébergées en Europe (Conformité RGPD)

[Démarrer mon essai gratuit ->]

Plateformes supportées : WORDPRESS • WOOCOMMERCE • SHOPIFY • MAGENTO • WAZUH

Notre équipe configure votre protection sous 2 heures.