



Total Security Guide d'utilisation

Module PrestaShop · Compatible avec PrestaShop 1.7 → 9

Pare-feu, captcha, 2FA et scanner de malwares, en un seul module

Total Security réunit dans un seul module un pare-feu applicatif, un captcha pour les formulaires de la boutique, l'authentification à deux facteurs (2FA) pour le back-office et les clients, un scanner local de malwares/webshells et un score de sécurité en temps réel qui vous indique quoi améliorer. Tout s'exécute sur votre propre serveur : rien ne quitte votre boutique. Aucun code, aucune modification de thème.

1. Installation

1. Dans le back-office, allez dans **Modules → Gestionnaire de modules → Ajouter un module** et sélectionnez le fichier ZIP du module.
2. Une fois le module installé, cliquez sur **Configurer**. Un court panneau s'ouvre avec un bouton **Aller à la configuration** qui mène à la page complète.

🛡 Total Security: Firewall, Captcha, 2FA & Malware Scanner

Your security score, the web application firewall, captcha, two-factor authentication and the local malware scanner are all managed on the configuration page.

⚙ Go to configuration

Le panneau Configurer ouvre la page de configuration complète

Les mises à jour sont automatiques. Les mises à jour sont incluses. Les domaines de développement (`.local` , `.test` , `localhost`) sont toujours autorisés. Quand une nouvelle version est disponible, elle s'affiche directement dans le module.

2. Configuration — les onglets

La page du module est organisée en onglets en haut de l'écran : **Dashboard**, **Règles du pare-feu**, **Journal des blocages**, **Protection des connexions**, **Captcha**, **Authentification à deux facteurs**, **Scanner de malwares** et **Paramètres**.

Dashboard score de sécurité

Un **score de sécurité** en temps réel avec une note en lettre (A/B/C/D), calculé à partir des réglages de votre boutique, des couches pare-feu/captcha/2FA et du dernier scan de malwares (rien ne quitte votre serveur). En dessous, une **Checklist** des contrôles de sécurité (exemples visibles : mode debug désactivé en production, HTTPS forcé partout, pare-feu applicatif actif, captcha sur la connexion/l'inscription, authentification à deux facteurs sur le back-office, aucun malware/webshell détecté, nom du dossier back-office non devinable, jeton de sécurité du back-office activé). Les éléments à corriger affichent un raccourci **Corriger maintenant** qui mène directement au réglage concerné.

The screenshot displays the PrestaShop 9.1.4 interface, specifically the 'Total Security' section. The left sidebar contains navigation menus for 'WELCOME', 'SELL', 'IMPROVE', 'CONFIGURE', and 'COMMUNITY'. The main content area features a 'Total Security' header with a 'Help' button. Below this, a 'Covallini.net' logo is visible. A row of tabs includes 'Dashboard', 'Firewall rules', 'Blocked log', 'Login protection', 'Captcha', 'Two-factor auth', 'Malware scanner', and 'Settings'. The 'Dashboard' tab is active, showing a 'Security score' of 67 (GRADE C) with a note that 6 of 10 checks pass and 4 items need attention. A 'Checklist' section follows, listing 10 items with status indicators (red, orange, or green dots) and 'Fix now' buttons for items that need attention.

Item	Status	Action
Debug mode off in production	Red	
HTTPS enforced everywhere	Orange	Fix now
Web application firewall active	Green	
Captcha on login / registration	Orange	Fix now
Two-factor authentication on the back office	Green	
No malware / webshell detected	Green	
Back-office folder name is not guessable	Orange	
Back-office security token enabled	Green	
Cookies use SameSite protection	Green	
Core overrides under control	Green	

Dashboard — score de sécurité et checklist

Règles du pare-feu

Ajoutez et gérez les listes de règles avec un seul formulaire **Ajouter une règle : Liste blanche IP/CIDR** (adresses de confiance, qui contournent tous les contrôles), **Liste noire IP/CIDR** (adresses bloquées), **Règles par pays** (codes ISO-2), **User-agents indésirables** (correspondance par sous-chaîne), **Motifs d'attaque personnalisés** (correspondance par sous-chaîne), et une **Liste blanche de motifs** (sous-chaînes d'URI exemptées du blocage par motif). Une bannière affiche votre IP actuelle et vous avertit de la mettre en liste blanche avant d'activer le mode verrouillage ou le back-office réservé aux IP en liste blanche, afin de ne jamais vous retrouver bloqué à l'extérieur.

PRESTASHOP 9.1.4

Quick Access

Search

View my store

Configure > Total Security

Help

WELCOME

Dashboard

Care Center

SELL

Orders

Catalog

Customers

Customer Service

Stats

IMPROVE

Modules

Design

Shipping

Payment

International

Marketing

CONFIGURE

Shop Parameters

Advanced Parameters

Total Security

COMMUNITY

Wall of Fame

Cavallini.net

Dashboard

Firewall rules

Blocked log

Login protection

Captcha

Two-factor auth

Malware scanner

Settings

Your current IP is 172.18.0.1. It is NOT whitelisted. Add it to the whitelist before enabling lockdown / BO-whitelist-only.

Add a rule

Whitelist IP / CIDR

e.g. 203.0.113.10 or 203.0.113.0/24 or RU or badbot

note (optional)

+ Add

Whitelist (trusted IP / CIDR, bypass everything) 2

Value	Note	Added
::1	Auto-added at install (anti-lockout)	2026-07-08 19:20:48
127.0.0.1	Auto-added at install (anti-lockout)	2026-07-08 19:20:48

Blacklist (blocked IP / CIDR) 0

Value	Note	Added
No rules.		

Country rules (ISO-2) 0

Value	Note	Added
No rules.		

Bad user-agents (substring match) 0

Value	Note	Added
No rules.		

Custom attack patterns (substring match) 0

Value	Note	Added
No rules.		

Pattern whitelist (URI substrings exempt from pattern blocking) 0

Value	Note	Added
No rules.		

Règles du pare-feu — liste blanche, liste noire, pays, user-agents et motifs

Journal des blocages

Chaque requête bloquée est enregistrée avec la date, l'IP, le pays, le motif (par ex.

user_agent , attack_pattern , ip , rate , login), le détail, l'URI demandée et le user-agent.

Filtrez par motif ou par IP, **Exporter en CSV**, **Vider le journal**, ou débloquez une IP directement depuis cette page.

PRESTASHOP9.1.4

Quick Access

Search

View my store

WELCOME

Dashboard

Care Center

SELL

Orders

Catalog

Customers

Customer Service

Stats

IMPROVE

Modules

Design

Shipping

Payment

International

Marketing

CONFIGURE

Shop Parameters

Advanced Parameters

Total Security

COMMUNITY

Wall of Fame

Configure

Total Security

Help

Cavallini.net

Dashboard

Firewall rules

Blocked log

Login protection

Captcha

Two-factor auth

Malware scanner

Settings

All reasons

IP contains...

Filter

Export CSV

Clear log

27

Date	IP	Country	Reason	Detail	URI	User-Agent
2026-07-21 21:44:19	172.18.0.1		user_agent	sqlmap	/favicon.ico	sqlmap/1.5.2wstable (http://sqlmap.org)
2026-07-21 21:44:19	172.18.0.1		user_agent	sqlmap	/	sqlmap/1.5.2wstable (http://sqlmap.org)
2026-07-21 21:41:08	172.18.0.1		attack_pattern	ifn_passwd	/?x=/etc/passwd	Mozilla/5.0 (Windows NT 10.0; Win64; x64)
2026-07-21 21:41:07	172.18.0.1		user_agent	sqlmap	/	sqlmap/1.5.2
2026-07-21 21:22:29	172.18.0.1		user_agent	sqlmap	/	sqlmap/1.0
2026-07-18 23:42:15	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=7257d964683..Nht1Qxo543LAipa3jNk2QdZUnudD4D7j4k08yCCpvo	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC
2026-07-18 23:41:15	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=ccf7.gzXn9F..lrgtWuq9vdAKzJj2e_y9ktT54Q	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC
2026-07-18 23:40:34	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=7ba68255093..	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC
2026-07-18 23:38:09	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=500b134a561..	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC
2026-07-18 23:36:28	172.18.0.1		attack_pattern	xss_script	/address?id_address=0	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC
2026-07-18 23:26:39	172.18.0.1		attack_pattern	xss_handler	/admin-dev/?controller=AdminController&token=b1260b7..7_dvpMRQfjNh_HiDu4FF4.Z7lVHwo2EtMUP	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36
2026-07-18 23:26:37	172.18.0.1		attack_pattern	xss_handler	/admin-dev/?controller=AdminController&token=b1260b7..7_dvpMRQfjNh_HiDu4FF4.Z7lVHwo2EtMUP	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36
2026-07-18 23:25:47	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=724e95e..Zr5o.wVZ7Q16fGh	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36
2026-07-18 23:25:46	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=724e95e..Zr5o.wVZ7Q16fGh	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36
2026-07-18 23:24:21	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=5822b68..x0L7QvvpdM.3aLDL	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36
2026-07-18 23:24:21	172.18.0.1		attack_pattern	xss_script	/admin-dev/?controller=AdminController&token=5822b68..x0L7QvvpdM.3aLDL	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36
2026-07-18 23:23:29	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=566e2be783b..	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC
2026-07-18 23:22:28	172.18.0.1		attack_pattern	xss_script	/?x=%3Cscript%3Ealert(1)%3C/script%3E	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 Chrome/126.0 Safari/537.36
2026-07-18 23:21:12	172.18.0.1		attack_pattern	xss_script	/admin-dev/index.php?controller=AdminController&token=15a5721..Y4owHwr7gHJN9G8qihFQhzyOR95yfmk.CkLOUF435..	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessC
2026-07-18 19:16:02	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1
2026-07-18 19:15:59	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1
2026-07-18 19:15:45	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1
2026-07-18 19:15:45	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1
2026-07-18 19:15:36	172.18.0.1		user_agent	curl/	/index.php?fc=module&module=cli_withdrawal&controlle..	curl/8.14.1
2026-07-18 19:15:36	172.18.0.1		user_agent	curl/	/	curl/8.14.1
2026-07-18 19:15:30	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1
2026-07-18 19:15:30	172.18.0.1		user_agent	curl/	/withdrawal	curl/8.14.1

Journal des blocages — filtrer, exporter ou débloquer une IP

Protection des connexions

Surveille les tentatives de connexion au back-office et bloque un compte/une IP après trop de tentatives échouées dans une fenêtre de temps donnée ; vous pouvez débloquent une entrée manuellement. Configurez les seuils dans Paramètres (Protection des connexions au back-office).

PRESTASHOP 9.1.4

Quick Access

Search

View my store

WELCOME

Dashboard

Care Center

SELL

Orders

Catalog

Customers

Customer Service

Stats

IMPROVE

Modules

Design

Shipping

Payment

International

Marketing

CONFIGURE

Shop Parameters

Advanced Parameters

Total Security

COMMUNITY

Wall of Fame

Configure > Total Security

Help

Cavallini.net

Dashboard

Firewall rules

Blocked log

Login protection

Captcha

Two-factor auth

Malware scanner

Settings

Back-office login attempts

Failed back-office logins are tracked per IP and username. After the configured threshold the source is locked out temporarily.

IP	Username	Attempts	Locked until	State
No failed back-office login attempts recorded.				

Protection des connexions — tentatives échouées et blocages actifs

Captcha

- **Fournisseur de captcha** — choisissez Google reCAPTCHA v2 (case à cocher), reCAPTCHA v3, hCaptcha, Cloudflare Turnstile, ou le fournisseur **Lightweight** qui ne nécessite aucune clé et reste entièrement sur votre serveur.
- **Clé de site / Clé secrète** — depuis le tableau de bord du fournisseur choisi, **seuil de score reCAPTCHA v3, thème du widget, position du badge, durée de vie du jeton** pour le fournisseur Lightweight.
- **Formulaires protégés** — Connexion, Inscription, Mot de passe oublié, Formulaire de contact, Newsletter, Avis produit, Commande invité (chacun activable/désactivable).
- **Avancé** — **Fail closed** (bloquer quand le fournisseur est injoignable), **Ignorer le captcha pour les clients connectés, Délai de vérification, Liste blanche d'IP de confiance, vérification du hostname, vérification de l'action.**
- **Rate limiting** — limite les tentatives de captcha échouées avec un maximum et une fenêtre de temps.

PRESTASHOP 9.1.4

Quick Access

Search

View my store

Configure > Total Security

Help

WELCOME

Dashboard

Care Center

SELL

Orders

Catalog

Customers

Customer Service

Stats

IMPROVE

Modules

Design

Shipping

Payment

International

Marketing

CONFIGURE

Shop Parameters

Advanced Parameters

Total Security

COMMUNITY

Wall of Fame

Cavallini.net

Dashboard

Firewall rules

Blocked log

Login protection

Captcha

Two-factor auth

Malware scanner

Settings

Captcha provider

Enable captcha protection

Yes

No

Provider

Google reCAPTCHA v2 (checkbox)

Choose your anti-spam provider. Create the keys in the provider dashboard. The Lightweight provider needs no keys and keeps everything on your server.

Site key (public)

reCAPTCHA / hCaptcha / Tur

Secret key (server-side only)

reCAPTCHA / hCaptcha / Tur

reCAPTCHA v3 score threshold (0.0 bot, 1.0 human)

0.5

Widget theme

Light

Badge position (v3 / invisible / Turnstile)

Bottom right

Lightweight token lifetime (seconds)

180

Protected forms

Login

Yes

No

Registration

Yes

No

Forgot password

Yes

No

Contact form

Yes

No

Newsletter

Yes

No

Product review

Yes

No

Guest checkout

Yes

No

Advanced

Fail closed (block when the provider is unreachable)

Yes

No

Skip captcha for logged-in customers

Yes

No

Verification timeout (seconds, 1 to 30)

5

Trusted IP whitelist (one per line, skip captcha)

Verify hostname (reject tokens solved on another domain)

Yes

No

Expected hostname (optional, empty = auto)

www.example.com

Verify action (reCAPTCHA v3 and Turnstile)

Yes

No

Rate limiting

Rate-limit failed captcha attempts

Yes

No

Max failed attempts (1 to 1000)

5

Window in minutes (1 to 1440)

15

Save captcha settings

Captcha — fournisseur, formulaires protégés et rate limiting

Authentification à deux facteurs (2FA)

Codes à usage unique basés sur le temps (Google Authenticator, Authy, 1Password et toute application compatible). Rien ne quitte votre serveur : les secrets sont chiffrés au repos et vérifiés localement.

- **Votre compte** — activez la 2FA pour le compte avec lequel vous êtes connecté (scannez un QR code, saisissez un code à 6 chiffres).
- **Activer la 2FA pour le back-office** (personnel) et/ou **pour les clients** (front-office).
- **Forcer la 2FA pour des profils employé spécifiques**, par ID (1 = SuperAdmin, 2 = Logisticien, 3 = Traducteur, 4 = Vendeur) ; les profils listés ne peuvent pas utiliser le back-office tant qu'ils ne se sont pas inscrits.
- **Fenêtre de tolérance, nombre de codes de secours, nom de l'émetteur** affiché dans l'application.
- **Employés inscrits** et **clients inscrits** sont listés et peuvent être réinitialisés.

PRESTASHOP 9.1.4 Quick Access Search

View my store

WELCOME

Dashboard

Care Center

SELL

Orders

Catalog

Customers

Customer Service

Stats

IMPROVE

Modules

Design

Shipping

Payment

International

Marketing

CONFIGURE

Shop Parameters

Advanced Parameters

Total Security

COMMUNITY

Wall of Fame

Configure > Total Security

Total Security

Cavallini.net

Dashboard Firewall rules Blocked log Login protection Captcha Two-factor auth Malware scanner Settings

Your account

Two-factor authentication for the account you are signed in with. Not set up

Set up 2FA on my account

You will scan a QR code with an authenticator app (Google Authenticator, Authy, 1Password) and enter a 6-digit code to confirm.

Two-factor authentication

Time-based one-time codes (Google Authenticator, Authy, 1Password and any compatible app). Nothing leaves your server: secrets are encrypted at rest and verified locally.

Enable 2FA for the back office (staff) Yes No

This makes 2FA available: an employee can turn it on for their own account, and is then asked for a code at every login. To make it mandatory instead, list the profiles below.

Enable 2FA for customers (front office) Yes No

Force 2FA for these employee profiles (comma-separated IDs) 1, 2

Employees in these profiles cannot use the back office until they enrol. Leave empty to keep 2FA optional. Profiles: 1 = SuperAdmin 2 = Logistician 3 = Translator 4 = Salesman

Tolerance window (steps of 30s, 0 to 5) 1

Number of backup codes (4 to 20) 8

Issuer name shown in the app (empty = shop name) PrestaShop

Save 2FA settings

Enrolled employees 0

ID	Name	Email	Status	Updated
No one has enrolled yet.				

Enrolled customers 0

ID	Name	Email	Status	Updated
No one has enrolled yet.				

Scanner de malwares

Analyse locale de malwares/webshells : recherche les signatures connues de webshells et de code obfusqué, le code exécutable caché dans les dossiers médias, et les fichiers ajoutés ou modifiés depuis votre base de référence de confiance. Tout s'exécute sur le serveur : aucun fichier, hash ou chemin ne quitte jamais la boutique.

- **Métriques** — fichiers suspects, fichiers en référence, dernière analyse.
- **Lancer l'analyse maintenant** et **Définir les fichiers actuels comme base de référence de confiance**.
- Les résultats sont listés avec la **gravité**, le **quoi**, le **fichier** et le **quand**.

The screenshot displays the PrestaShop Total Security dashboard. The interface includes a top navigation bar with the PrestaShop logo, version 9.1.4, and a search bar. A left sidebar contains various menu items categorized under 'WELCOME', 'SELL', 'IMPROVE', 'CONFIGURE', and 'COMMUNITY'. The main content area is titled 'Total Security' and features a 'Cavallini.net' logo. Below the logo are several tabs: 'Dashboard', 'Firewall rules', 'Blocked log', 'Login protection', 'Captcha', 'Two-factor auth', 'Malware scanner' (which is highlighted), and 'Settings'. Three key metrics are displayed in a row: '0 SUSPICIOUS FILES', '18105 FILES IN BASELINE', and '2026-07-18 23:19:01 LAST SCAN'. A section titled 'Local malware / webshell scan' provides a description of the scan process and includes two buttons: 'Run scan now' and 'Set current files as trusted baseline'. Below this, a 'Findings' table is shown with columns for 'Severity', 'What', 'File', and 'Seen'. The table currently contains one entry: 'Clean: no suspicious or changed files found.'

Scanner de malwares — métriques, analyse et résultats

Paramètres **configuration du pare-feu**

La configuration propre du pare-feu, regroupée par section.

- **Général** — Activer le pare-feu ; **Derrière un proxy/CDN** avec un en-tête de proxy de confiance et des IP/CIDR de proxy de confiance — n'activez cette option que derrière un proxy réellement fiable, sinon les en-têtes IP/pays peuvent être falsifiés.
- **Blocage IP/CIDR.**
- **Blocage par pays** — mode liste noire ou liste blanche, codes ISO-2, chemin optionnel vers une base MaxMind GeoLite2 ou un en-tête CDN indiquant le pays — la base n'est jamais fournie avec le module, pour des raisons de licence.
- **Bots / user-agents indésirables** — activer le blocage par user-agent, bloquer les user-agents vides, sous-chaînes supplémentaires à bloquer fusionnées avec une liste intégrée.
- **Rate limiting** — nombre maximum de requêtes par fenêtre, durée de la fenêtre en secondes, durée du blocage temporaire.
- **Blocage par motifs d'attaque** — SQLi/XSS/LFI/probing.
- **Protection des connexions au back-office** — nombre maximum de tentatives échouées, fenêtre de tentative, durée du blocage, autoriser le back-office uniquement depuis les IP en liste blanche.
- **Maintenance et journalisation** — **Mode verrouillage** (autoriser uniquement les IP en liste blanche), journaliser les requêtes bloquées, durée de conservation du journal en jours, supprimer toutes les données à la désinstallation.
- **Rapport de sécurité hebdomadaire** — envoie un court rapport par e-mail ; s'exécute en arrière-plan par petites étapes pour ne jamais ralentir la boutique.

Max failed attempts

Attempt window (seconds)

Lockout duration (seconds)

Allow back office only from whitelisted IPs ☐ Yes ☒ No

Make sure your current IP is whitelisted before enabling this.

Maintenance & logging

Lockdown mode (allow only whitelisted IPs) ☐ Yes ☒ No

Log blocked requests ☒ Yes ☐ No

Log retention (days)

Drop all data on uninstall ☐ Yes ☒ No

Weekly security report

Once a week we run a scan, compute your security score and email you a short report. It runs in the background in small steps, so it never slows the shop down.

Send the weekly security report ☒ Yes ☐ No

Send to (leave empty for the shop email)

The test report uses your most recent scan.

Dans le front-office

Quand le pare-feu bloque une requête, le visiteur voit une simple page 403 « Forbidden — votre requête a été bloquée par le pare-feu du site » : les bots et les scanners n'atteignent jamais votre boutique.

403 Forbidden

Your request has been blocked by the site firewall.

Dans le front-office — la page 403 affichée quand le pare-feu bloque une requête

3. Vérifier que tout fonctionne

- Ouvrez le *Dashboard* et consultez votre score de sécurité et la checklist.
- Envoyez une requête avec un user-agent semblable à celui d'un scanner (ou une URL de probing) et vérifiez que vous obtenez la page de blocage 403 et une nouvelle ligne dans le *Journal des blocages*.
- Après plusieurs échecs de connexion au back-office, le compte/l'IP est bloqué dans *Protection des connexions*.
- Activez le captcha et vérifiez qu'il apparaît sur le formulaire de connexion/d'inscription.
- Configurez la 2FA sur votre compte et reconnectez-vous avec un code à 6 chiffres.
- Lancez le *Scanner de malwares* et consultez les résultats.

4. FAQ

Est-ce que cela ralentit la boutique ?

Non : le pare-feu s'exécute en premier avec des vérifications légères et indexées ; le scanner et le rapport hebdomadaire s'exécutent en arrière-plan.

Est-ce que je risque de me retrouver bloqué à l'extérieur ?

Mettez d'abord votre IP actuelle en liste blanche (la page vous avertit, et `127.0.0.1 / ::1` sont en liste blanche dès l'installation) ; n'activez le mode verrouillage ou le back-office réservé aux IP en liste blanche qu'après.

Des données quittent-elles mon serveur ?

Non : le pare-feu, l'option de captcha Lightweight, les secrets 2FA et le scanner de malwares s'exécutent tous localement sur votre serveur.

Remplace-t-il des modules séparés de pare-feu / captcha / 2FA ?

Oui : c'est la suite de sécurité unique et unifiée.

Dois-je modifier mon thème ?

Non : il fonctionne via les hooks standards et est compatible avec tous les thèmes.