Cloudflare Sécurité — Tour Complet des Modules Activables 2026

Cloudflare propose en 2026 une suite complète de modules de sécurité activables par domaine : WAF, protection DDoS L3/L7, Bot Management, Page Shield (CSP), Turnstile, API Shield et Email Security. Ce guide technique couvre chaque module, sa configuration recommandée et le plan Cloudflare requis.

La plupart des équipes qui passent un domaine derrière Cloudflare activent le proxy et s'arrêtent là. C'est dommage — parce que **Cloudflare sécurité modules** représente une suite de protection en profondeur dont chaque composant résout un problème précis. Le **WAF** bloque les attaques applicatives (SQLi, XSS, LFI). La **protection DDoS** absorbe les floods volumétriques avant qu'ils n'atteignent votre infrastructure. Le **Bot Management** distingue le bon trafic automatisé (Googlebot, monitoring) du mauvais (scrapers, credential stuffing). **Page Shield** détecte les scripts malveillants injectés sur vos pages. **Turnstile** remplace reCAPTCHA sans dégrader l'expérience utilisateur. **API Shield** protège vos endpoints REST. En 2026, Cloudflare protège plus de 20 % du trafic web mondial selon ses propres déclarations, ce qui lui donne une visibilité sur les menaces émergentes impossible à obtenir individuellement. Ce tour complet des modules de sécurité Cloudflare activables couvre la configuration recommandée pour chaque module, les règles d'exemple prêtes à l'emploi, le comparatif Free/Pro/Business/Enterprise et les configurations à activer en priorité sur n'importe quel domaine.

À RETENIR

À retenir

WAF géré : les règles gérées Cloudflare couvrent les exploits connus (WordPress, Drupal, Log4j) sans configuration — disponibles à partir du plan Pro.

DDoS automatique : la protection DDoS L3/L7 est activée par défaut sur tous les plans, même Free, sans configuration.

Bot Management : disponible uniquement à partir de Business/Enterprise ; le Bot Fight Mode (version simplifiée) est gratuit mais moins précis.

Mode "I'm Under Attack" : active un challenge JavaScript sur 100 % des visiteurs — arme de dernier recours lors d'une attaque active.

Turnstile remplace reCAPTCHA : gratuit, sans friction utilisateur, sans cookie tiers, compatible RGPD.

Vue d'ensemble de l'architecture de sécurité Cloudflare

Cloudflare fonctionne comme un **proxy inverse en ligne** — tout le trafic HTTP(S) de votre domaine (si le nuage orange est actif) passe par les edge servers Cloudflare avant d'atteindre votre serveur d'origine. Cette position intermédiaire est ce qui permet d'appliquer tous les contrôles de sécurité : le trafic est visible, analysable et filtragle avant d'impacter votre infrastructure.

La pile de traitement d'une requête entrante dans Cloudflare suit cet ordre :

IP Reputation / Access Rules — blocage par IP, ASN ou pays

DDoS Protection — détection et absorption des floods

Bot Management — scoring et classification du trafic automatisé

WAF — analyse de la requête HTTP contre les règles de sécurité

Rate Limiting — limitation de débit par IP/path

Page Shield — surveillance côté client (CSP, scripts)

Cache / Origin — forward vers l'origine ou service depuis le cache

Comprendre cet ordre est important pour le dépannage : si une requête légitime est bloquée, elle l'est à un niveau précis de cette pile. Les logs Cloudflare Security indiquent exactement quelle règle a déclenché l'action.

Web Application Firewall : configuration et règles personnalisées

Le *WAF Cloudflare* opère à la couche applicative (L7) et analyse le contenu des requêtes HTTP — URL, en-têtes, corps de requête, cookies — pour détecter les patterns d'attaque connus. Il existe trois types de règles WAF :

Règles gérées Cloudflare (Managed Rules) : ensemble de règles maintenues par les équipes sécurité de Cloudflare, mises à jour en temps réel lors de l'émergence de nouvelles vulnérabilités. Couvrent les OWASP Top 10, les CVE critiques (Log4j, Spring4Shell, ProxyShell) et les attaques spécifiques aux CMS populaires (WordPress, Drupal, Joomla). Disponibles à partir du plan **Pro**.

Règles OWASP Core : implémentation du ruleset OWASP ModSecurity Core Rule Set, adaptée par Cloudflare. Paranoia level réglable de 1 (peu de faux positifs) à 4 (très strict). Recommandation : commencer en mode "Log" avant de passer en "Block" pour identifier les faux positifs sur votre application.

Règles personnalisées (Custom Rules) : règles que vous créez sur mesure avec le langage de filtrage Cloudflare Firewall Rules :

```
 # Exemple : bloquer les requêtes vers wp-login.php depuis des pays hors Union Européenne
# (via le dashboard Cloudflare → Security → WAF → Custom Rules)

# Condition
(http.request.uri.path eq "/wp-login.php" and not ip.geoip.country in {"FR" "DE" "BE" "NL" "ES" "

# Action : Block

# Exemple 2 : rate limiting sur /api/login — max 5 requêtes/minute par IP
# (via Rate Limiting, distinct des Custom Rules)
# Path: /api/login
# Threshold: 5 requests per 60 seconds
# Action: Block for 1 hour
```

Configuration recommandée par ordre de priorité :

Activer les Managed Rules en mode **Log** pendant 48h — analyser les faux positifs

Passer les règles sans faux positifs en mode **Block**

Créer des règles personnalisées pour les chemins critiques (admin, API, login)

Activer le OWASP Core Ruleset en Paranoia Level 1, puis ajuster

Astuce expert : Utilisez le mode "Challenge" plutôt que "Block" pour les règles ambiguës — les humains passent le challenge JavaScript, les bots automatisés échouent. Moins de faux positifs visibles côté utilisateur, même filtrage côté sécurité.

Protection DDoS L3/L7 : comment ça marche réellement ?

La protection DDoS de Cloudflare est **automatique et activée par défaut** sur tous les plans, même Free. Contrairement à ce qu'on pourrait croire, vous n'avez pas à "configurer" la protection DDoS — Cloudflare absorbe les attaques volumétriques automatiquement en détectant les patterns anormaux dans le trafic.

Comment fonctionne la détection ? Cloudflare analyse en temps réel le trafic sur l'ensemble de son réseau mondial (>5 Tbps de capacité). Quand une IP ou un groupe d'IPs génère un volume

anormal de requêtes vers votre domaine, le système de détection automatique classe le trafic comme potentiellement malveillant et applique des challenges ou des drops selon la sévérité.

Ce que couvre chaque niveau :

DDoS L3/L4 (réseau/transport) : floods UDP, SYN floods, amplification DNS/NTP. Absorbé avant même que le trafic n'atteigne les edge servers applicatifs.

DDoS L7 (application) : HTTP floods, Slowloris, requêtes malformées en masse. Détecté par analyse comportementale des sessions HTTP.

Pour personnaliser les seuils (plans Business et Enterprise) :

```
 # Cloudflare API — créer une règle DDoS Override
curl -X PUT "https://api.cloudflare.com/client/v4/zones/ZONE_ID/ddos_protection/overrides"   -H "
    "name": "Override agressif pour /api/",
    "description": "Seuils plus stricts pour endpoint API",
    "rules": [{
      "id": "fdfdac75430c4dfb9b3a08b5bec0d1c0",
      "override_values": {"sensitivity_level": "high", "action": "block"}
    }]
  }'
```

Pour voir les attaques DDoS en cours et leur volume : Security → Overview dans le dashboard affiche les requêtes bloquées en temps réel avec répartition géographique et classification.

Bot Management : détecter et filtrer le trafic automatisé

Tout le trafic automatisé n'est pas malveillant — Googlebot, les outils de monitoring (Uptime Robot, Pingdom) et les APIs de partenaires sont légitimes. Le *Bot Management* de Cloudflare attribue un **Bot Score** de 1 à 99 à chaque requête :

Score 1–29 : bot automatisé avec forte certitude (crawler malveillant, scraper, credential stuffer)

Score 30–49 : trafic probablement automatisé

Score 50–99 : humain ou bot légitime (Googlebot a généralement un score de 95+)

Le Bot Management complet est disponible uniquement à partir du plan Business/Enterprise. Pour les plans Free et Pro, le **Bot Fight Mode** (version simplifiée) est disponible gratuitement — il bloque les bots les plus évidents sans le scoring granulaire.

Configuration recommandée avec Bot Management :

```
 # Règle Custom — bloquer les bots à score faible sur les endpoints sensibles
# (http.request.uri.path eq "/checkout" and cf.bot_management.score lt 30)
# Action : Block

# Permettre les bots légitimes vérifiés (Googlebot, Bingbot)
# cf.bot_management.verified_bot eq true
# Action : Allow (bypass les autres règles)

# Activer le mode "Super Bot Fight" pour les plans Pro
# Security → Bots → Super Bot Fight Mode → Definitely Automated → Block
```

Page Shield : Content Security Policy et détection de scripts malveillants

Page Shield surveille les scripts JavaScript chargés sur vos pages côté client. Les attaques Magecart — injections de JavaScript malveillants dans les pages e-commerce pour voler les données de carte bancaire — sont invisibles pour les WAF côté serveur : le HTML est légitime, c'est le script tiers chargé dans le navigateur qui est malveillant.

Page Shield résout ce problème en surveillant activement tous les scripts chargés par vos pages, en détectant les changements (nouveau script apparu, script modifié) et en alertant en cas de comportement suspect. Il génère aussi automatiquement une **Content Security Policy (CSP)** basée sur les scripts légitimes détectés.

Disponible sur les plans **Pro** et supérieurs. Configuration minimale :

Security → Page Shield → Enable Page Shield

Laisser tourner 24h en mode observation — Page Shield apprend les scripts légitimes

Générer la CSP suggérée et la déployer en mode report-only d'abord

Activer les alertes email pour les nouveaux scripts détectés

Turnstile : remplacer reCAPTCHA sans friction utilisateur

Cloudflare Turnstile est l'alternative à reCAPTCHA v3 de Google, disponible gratuitement sur tous les plans. Contrairement à reCAPTCHA qui affiche une case à cocher ou des images à identifier, Turnstile fonctionne de façon invisible : il analyse le comportement du navigateur (mouvements de souris, temps de chargement, caractéristiques TLS) pour distinguer humains et bots sans interaction de l'utilisateur.

Intégration HTML en 3 lignes :

```
 # 1. Ajouter le script dans le head
# <script src="https://challenges.cloudflare.com/turnstile/v0/api.js" defer></script>

# 2. Widget dans le formulaire
# <div class="cf-turnstile" data-sitekey="VOTRE_SITEKEY"></div>

# 3. Vérification côté serveur (Python exemple)
import requests
response = requests.post('https://challenges.cloudflare.com/turnstile/v0/siteverify',
    data={'secret': 'SECRET_KEY', 'response': token_from_form})
result = response.json()
if not result['success']:
    return "Bot détecté", 403
```

Avantages vs reCAPTCHA : pas de cookie Google tiers (meilleure conformité RGPD), pas d'images à identifier, pas de dépendance à l'historique de navigation Google, fonctionnement identique sur navigateurs privés. Pour les sites soumis à des exigences de conformité strictes, Turnstile est supérieur à reCAPTCHA sur tous les critères.

API Shield : protéger vos endpoints REST en production

API Shield est conçu pour les applications qui exposent des APIs REST ou GraphQL. Il apprend automatiquement les patterns de vos APIs (endpoints valides, méthodes HTTP autorisées, structure des paramètres) et bloque les requêtes qui dévient de ces patterns — une technique appelée **positive security model**.

Fonctionnalités clés d'API Shield :

API Discovery : détection automatique de tous vos endpoints exposés (y compris ceux non documentés — les "shadow APIs")

Schema Validation : validation des paramètres contre votre schéma OpenAPI 3.0

Sequence Analytics : détection des flux d'appels anormaux (un bot qui tente chaque ID d'utilisateur séquentiellement)

mTLS Authentication : certificats clients pour les APIs machine-to-machine

Disponible à partir du plan **Enterprise** pour les fonctionnalités avancées. Schema Validation basique est disponible en Business.

Quel plan Cloudflare choisir selon votre besoin de sécurité ?

Module	Free	Pro (25$/m)	Business (200$/m)	Enterprise
DDoS L3/L7 auto	Oui	Oui	Oui	Oui + SLA
WAF Managed Rules	Non	Oui (CF + OWASP)	Oui (avancé)	Oui (personnalisé)
Custom Rules (Firewall)	5 règles	20 règles	100 règles	Illimité
Bot Fight Mode	Basique	Super Bot Fight	Non	Non
Bot Management complet	Non	Non	Oui	Oui + ML
Page Shield	Non	Oui (basique)	Oui (avancé)	Oui (complet)
Turnstile	Oui	Oui	Oui	Oui
API Shield	Non	Non	Partiel	Oui complet
Rate Limiting	Non	Oui (basique)	Oui (avancé)	Oui (custom)

Pour la majorité des sites et applications, le **plan Pro à 25 $/mois** est le point d'entrée raisonnable : WAF géré, Super Bot Fight Mode, Page Shield basique et 20 règles personnalisées couvrent 90 % des scénarios d'attaque courants. Pour des APIs ou des sites e-commerce critiques, le plan Business ajoute Bot Management complet et le Rate Limiting avancé. Pour une architecture Zero Trust complète intégrant Cloudflare, consultez notre guide sur l'architecture Zero Trust et sur la micro-segmentation Zero Trust par IA.

Mode "I'm Under Attack" : quand et comment l'activer

Le **mode "I'm Under Attack"** est l'arme de dernier recours lors d'une attaque DDoS ou d'une tentative de compromise en cours. Quand ce mode est activé, Cloudflare présente un challenge JavaScript à **100 % des visiteurs** avant de les laisser accéder au site — humains et bots confondus. Les visiteurs légitimes passent ce challenge automatiquement (2–5 secondes), les bots non.

```
# Activer via l'API Cloudflare (plus rapide qu'un clic en situation de stress)
curl -X PATCH "https://api.cloudflare.com/client/v4/zones/ZONE_ID/settings/security_level"   -H "

# Revenir en mode normal après l'incident
curl -X PATCH "https://api.cloudflare.com/client/v4/zones/ZONE_ID/settings/security_level"   -H "
```

Quand l'activer ? Uniquement lors d'attaques actives confirmées — flood de requêtes visibles dans les Analytics, erreurs 5xx en cascade sur votre serveur d'origine, alerte monitoring de saturation. Ce mode dégrade l'expérience des vrais utilisateurs (délai de 2–5 secondes à chaque première visite) et bloque les crawlers SEO légitimes. Ne jamais l'utiliser en prévention permanente.

Les 5 niveaux de Security Level par ordre croissant : Essentially Off → Low → Medium (défaut) → High → I'm Under Attack.

Configuration de sécurité recommandée : checklist par priorité

Voici l'ordre dans lequel configurer les modules Cloudflare pour maximiser la protection rapidement, sans risquer de bloquer du trafic légitime.

Étape 1 — Immédiat (5 minutes, sans risque) :

Activer le **Bot Fight Mode** (Security → Bots) — bloque les bots évidents gratuitement

Passer le Security Level à **Medium** (valeur par défaut, à vérifier)

Activer **HTTPS Everywhere** et la redirection HTTP → HTTPS

Activer **TLS 1.3** et désactiver TLS 1.0/1.1

Étape 2 — Dans les 24h (observation préalable conseillée) :

Activer les **Managed Rules WAF** en mode Log — vérifier les faux positifs

Créer une Custom Rule de blocage pour `/wp-login.php` et `/wp-admin/xmlrpc.php` si WordPress

Configurer le **Rate Limiting** sur les endpoints d'authentification

Étape 3 — Dans la semaine (après analyse des logs) :

Passer les Managed Rules en mode Block après validation

Activer **Page Shield** en mode observation

Déployer **Turnstile** sur les formulaires de contact et d'inscription

Configurer les **IP Access Rules** pour restreindre les pays non servis si pertinent

Pour les organisations qui souhaitent un accompagnement dans la configuration de leur stack Cloudflare, notre service RSSI externalisé inclut un audit et une configuration de la sécurité Cloudflare. Pour les architectures Zero Trust plus complexes, notre guide sur Cloudflare Zero Trust complet et l'implémentation réseau Zero Trust 2026 détaillent les configurations avancées.

Email Security : protection contre le phishing entrant

Cloudflare Area 1 (rebaptisé *Cloudflare Email Security*) est une solution anti-phishing qui s'intègre en MX record ou en journal de messages. Elle utilise une analyse des patterns de phishing collectés sur l'ensemble du trafic Cloudflare pour détecter les campagnes de phishing **avant qu'elles n'atteignent les boîtes mail** de vos utilisateurs.

Contrairement aux solutions anti-spam classiques (basées sur réputation IP et blacklists), Cloudflare Email Security analyse le contenu des messages, les pièces jointes et les URLs pour détecter les indicateurs de phishing sophistiqués — y compris les attaques BEC (Business Email Compromise) qui ne contiennent aucun lien malveillant mais usurpent un contexte légitime.

Disponible à partir du plan Business. Pour les organisations qui se posent la question de l'outillage de sécurité email dans un contexte Microsoft 365, notre article sur la sécurisation des accès Microsoft 365 avec MFA est complémentaire. Pour aller encore plus loin dans la protection des identités et des accès, notre service de pentest Active Directory permet d'identifier les failles avant qu'elles ne soient exploitées.

Questions fréquentes

Les modules de sécurité Cloudflare ralentissent-ils le site ?

Non, l'impact sur les performances est négligeable et généralement compensé par les gains liés au CDN Cloudflare. Le WAF, Bot Management et les autres contrôles de sécurité s'exécutent sur les edge servers Cloudflare en parallèle du traitement de la requête, avec une latence ajoutée typiquement inférieure à 5 ms. L'activation du mode "I'm Under Attack" est la seule configuration qui ajoute un délai visible (2–5 secondes de challenge JavaScript) — et c'est intentionnel.

Comment éviter les faux positifs du WAF Cloudflare ?

Deux approches complémentaires : (1) démarrer toujours en mode **Log** (pas de blocage) et analyser les logs Security pour identifier les règles qui déclenchent sur du trafic légitime. (2) Créer des règles d'exception (Skip Rules) pour les IPs de vos outils internes (CI/CD, monitoring, équipe dev). Dans Security → WAF → Custom Rules, une règle "Skip : Managed Rules" pour votre IP de bureau évite de bloquer vos propres outils. Après 48–72h d'observation en mode Log, vous pouvez passer en Block avec un niveau de confiance élevé.

Cloudflare peut-il bloquer les attaques par injection SQL et XSS ?

Oui — c'est précisément ce que couvrent les **OWASP Managed Rules** et les règles Cloudflare gérées. Le WAF détecte les patterns SQLi classiques (`UNION SELECT` , `OR 1=1` , encodages) et les payloads XSS (`<script>` , attributs `onerror` , encodages JavaScript obfusqués) dans les paramètres GET, POST et les en-têtes HTTP. Selon l'OWASP Top 10 2021, les injections et les XSS restent parmi les vecteurs d'attaque les plus fréquents — les managed rules Cloudflare couvrent ces catégories en priorité.

Turnstile est-il conforme au RGPD ?

Oui, Cloudflare Turnstile est conçu avec la conformité RGPD comme priorité. Contrairement à reCAPTCHA v2/v3 de Google, Turnstile ne dépose pas de cookies tiers, ne collecte pas d'historique de navigation pour scorer les utilisateurs, et ne partage pas de données avec des tiers publicitaires. Cloudflare publie une DPA (Data Processing Agreement) conforme RGPD, et le traitement des données Turnstile peut être limité à l'Europe dans les plans Enterprise. Pour les sites soumis à des audits de conformité RGPD, Turnstile est significativement plus simple à justifier que reCAPTCHA.

Quelle est la différence entre Security Level et WAF ?

Le **Security Level** (Essentially Off / Low / Medium / High / I'm Under Attack) est un contrôle global basé sur la réputation des IPs — il challenge ou bloque les IPs Cloudflare a priori identifiées comme malveillantes. Le **WAF** analyse le contenu de chaque requête individuellement, quelle que soit la réputation de l'IP. Ces deux mécanismes sont complémentaires : une IP avec bonne réputation mais envoyant une payload SQLi sera bloquée par le WAF, pas par le Security Level. Combinez les deux pour une défense en profondeur efficace selon les principes du NIST SP 800-207 Zero Trust Architecture.

> Besoin d'un audit de votre configuration Cloudflare ou d'une mise en place complète des modules de sécurité ? Notre équipe intervient sur la configuration WAF, Bot Management, Page Shield et la définition de la stratégie Zero Trust. Contactez notre RSSI externalisé.

