CLOUDFLARE

PRÉSENTATION DE SOLUTION

Cloudflare Bot Management

Bloquez les bots malveillants et gérez les bots IA sans nécessairement passer par la proposition d'un CAPTCHA.

Des bots se dissimulent au sein de votre trafic. Les bots malveillants nuisent à vos revenus et à l'expérience utilisateur.

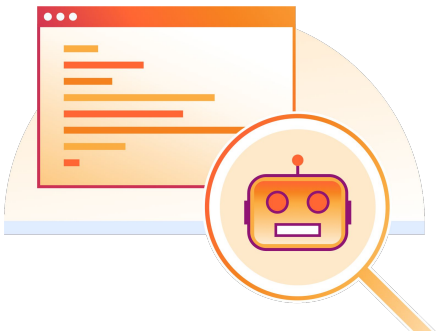
30 % du trafic applicatif circulant sur Internet se compose de trafic automatisé[1]. Les bots modernes parviennent facilement à contourner les défenses traditionnelles (comme les mesures heuristiques basées sur la position géographique et l'adresse IP, par exemple) ou les CAPTCHA. Or, ces outils de protection engendrent une frustration énorme chez les utilisateurs légitimes.

Grâce à sa visibilité sur **près de 20 %** d'Internet, Cloudflare peut analyser un plus grand nombre d'empreintes numériques que beaucoup d'autres fournisseurs afin de détecter la présence de davantage de robots d'exploration IA et de recherche[2].

Le service de gestion des bots **Cloudflare Bot Management** aide les entreprises à gérer les robots d'exploration IA, ainsi que le trafic automatisé à destination des applications web et mobiles, sans CAPTCHA. Autorisez les bots vérifiés et les robots d'exploration IA en conformité avec vos politiques à accéder à vos applications, tout en imposant des mesures de contrôle et en bloquant les bots IA non conformes ou les bots malveillants. Le service remplit ainsi une capacité essentielle au sein de notre catalogue de produits de sécurité des applications.

Avantages proposés par le produit

- Protégez-vous contre la fraude et les pertes, tant en termes financiers que de réputation de la marque.
- Assurez une meilleure expérience applicative web et mobile.
- Émancipez-vous des robots d'exploration IA et des bots de recherche indésirables.



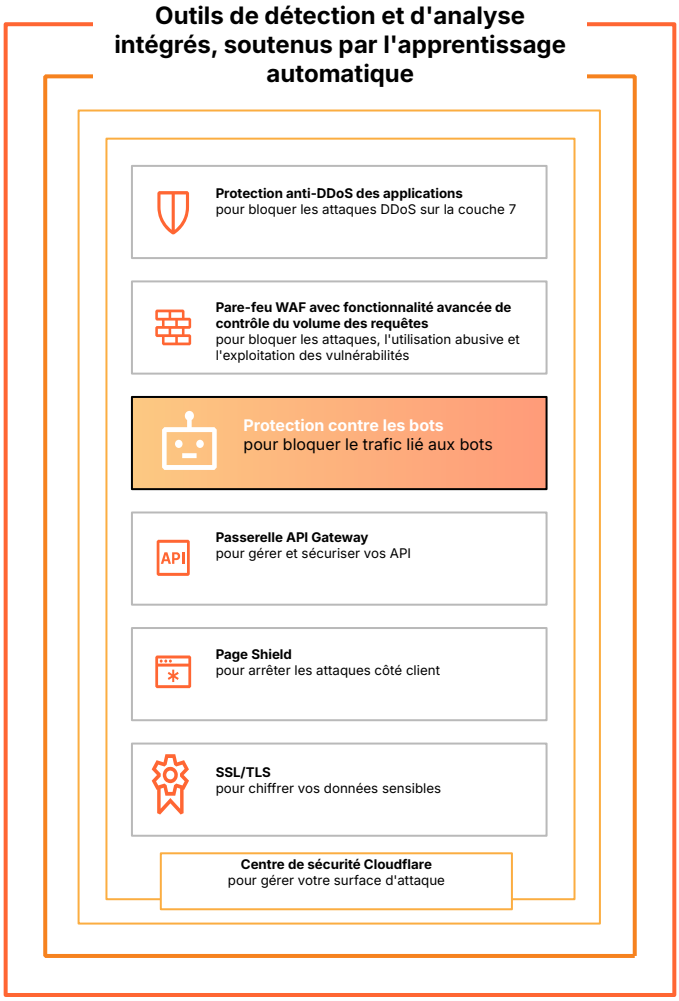


Figure 1 : l'intégration du service Cloudflare Bot Management à notre catalogue de produits de sécurité des applications

Sources

1. Données Cloudflare Radar, 2024
2. W3techs, Usage statistics and market shares of reverse proxy services (statistiques concernant l'utilisation et parts au sein du marché des services de proxy inverse), 2025

Fonctionnement du service Cloudflare Bot Management

Cloudflare combine les données issues d'une fonctionnalité de détection multicouches reposant sur l'apprentissage automatique (ML, Machine Learning) au niveau mondial et par application, le JavaScript côté client, les appareils mobiles et l'heuristique sous un score de bot unique attribué à chaque requête HTTP. Ce score évalue la probabilité qu'une requête donnée provienne d'un bot. Il entre dans l'élaboration des réponses standard (bloquer ou autoriser, par exemple), ainsi que des politiques de réponse personnalisées utilisées par d'autres produits Cloudflare. Les outils d'analyse des bots (comme le score de bot et les métadonnées des requêtes HTTP, parmi d'autres instruments de mesure) sont disponibles dans l'interface utilisateur du tableau de bord Cloudflare ou par l'intermédiaire de l'API Cloudflare au sein des outils tiers.

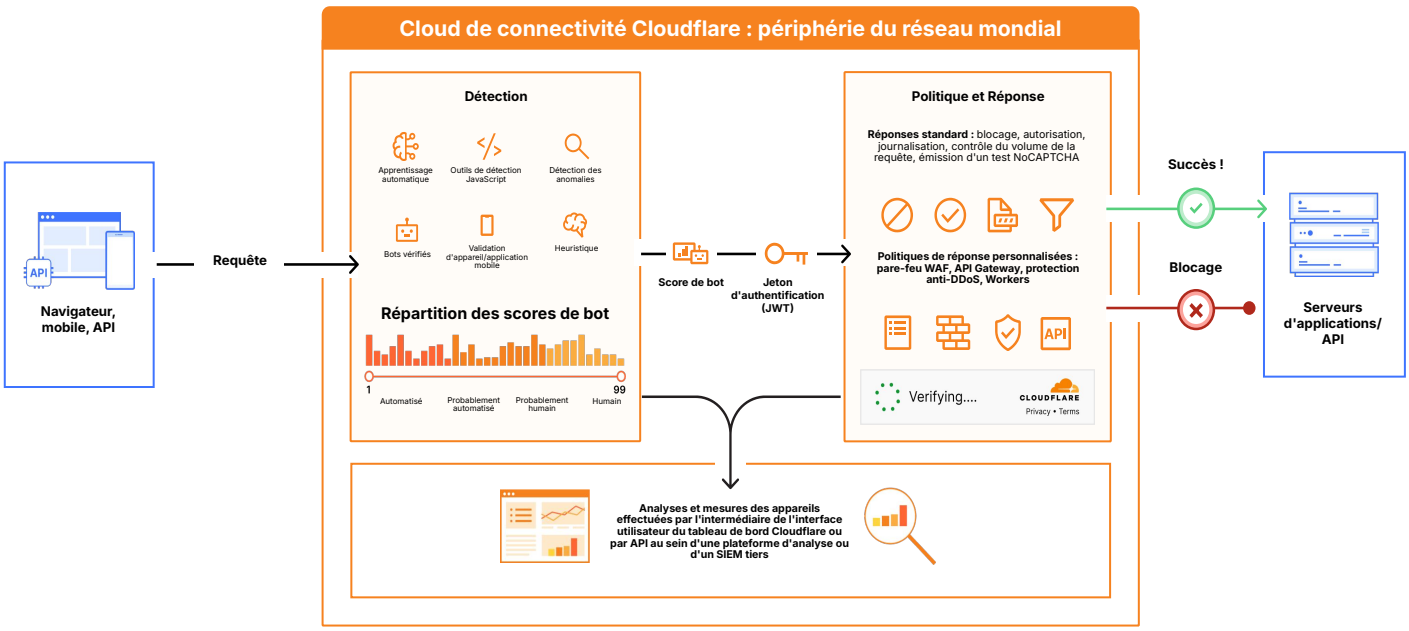


Figure 2 : exemple de parcours d'une requête passant à travers le prisme du service Cloudflare Bot Management

Fonctionnalités essentielles du service Cloudflare Bot Management

Usurpations de comptes et utilisation abusive

Protégez-vous contre les attaques zero-day grâce à des modèles soutenus par apprentissage automatique, capables de détecter les vulnérabilités plus rapidement que les procédures de divulgation publique en vigueur. Mettez en place une défense contre les attaques DDoS record, protégez vos données sensibles, réduisez les risques côté client et surveillez la chaîne d'approvisionnement logicielle de vos applications web.

Mettez en place une défense contre les bots et la fraude

Protégez vos utilisateurs contre l'usurpation de compte et arrêtez les bots malveillants qui affectent l'expérience de l'utilisateur final. Bloquez les botnets malveillants, le bourrage d'identifiants et d'informations de carte bancaire, ainsi que l'extraction de contenu et l'accaparement de stock, en combinant les modèles d'apprentissage automatique à nos informations sur les menaces, le client et le réseau.

Gérez les robots d'exploration et les bots IA

Exercez un degré de contrôle supérieur sur votre contenu et vos coûts en bloquant les robots d'exploration IA, en facturant leurs activités ou en les piégeant au sein de boucles sans fin. Gagnez en visibilité sur les tendances liées aux requêtes et sur la conformité grâce aux directives contenues dans votre fichier robots.txt. Cette fonctionnalité est accessible à l'ensemble des clients Cloudflare.

Principales fonctionnalités	
Moteurs de détection	
Apprentissage automatique	Notre modèle d'apprentissage automatique est entraîné sur l'ensemble du trafic traité par le réseau mondial Cloudflare, qui met chaque jour des milliards de requêtes en proxy afin d'identifier le trafic automatisé et le trafic généré par des humains. Ces facteurs sont inclus dans le score de bot général. Les clients bénéficient d'une mise à jour automatique vers le dernier modèle.
Détection des anomalies	Nos modèles d'apprentissage des anomalies comportementales non supervisés établissent une base de référence pour les schémas de trafic spécifiques à chaque application et calibrent les seuils de règles afin d'identifier les comportements anormaux des bots au fur et à mesure de l'évolution des schémas de trafic client dans le temps. Ces facteurs sont inclus dans le score de bot général.
Heuristique	Pour identifier les bots, nous nous servons de schémas connus en matière de comportement des bots malveillants. Ces schémas sont issus du trafic de bots, déjà analysé par le passé. Nous mettons régulièrement à jour nos outils heuristiques, pour l'ensemble de nos clients. Ces facteurs sont inclus dans le score de bot général.
Bots vérifiés et bots IA	Comme le prescrit la politique Cloudflare relative aux bots vérifiés, notre répertoire des bots contient les identifiants de détection de bots connus exécutant des fonctions légitimes et fonctionnant de manière transparente en tant que bots vérifiés. Nous disposons d'une catégorie distincte pour les bots IA connus, qui respectent ou non le fichier robots.txt et dissimulent leur comportement à vos applications.
Détection JavaScript	Le module de détection JavaScript identifie les navigateurs headless (sans interface graphique) et les autres empreintes numériques malveillantes par l'intermédiaire d'une injection JavaScript légère et invisible côté client dans chaque requête. Nous respectons des normes de confidentialité très strictes et ne collectons aucune information d'identification personnelle (PII, Personally Identifiable Information) au cours de ce processus.
Score de bot	Le score de bot vous permet de détecter la majorité des bots en rédigeant un moins grand nombre de règles, plutôt que d'élaborer une règle pour chaque ID ou type de bot. Il agrège les informations issues de nos moteurs de détection afin de générer un score de 1 à 99 qui indique la probabilité qu'une requête donnée provienne d'un bot. Un score de 1 révèle la présence d'une requête assurément automatisée, tandis qu'un score de 99 indique celle d'une requête sans conteste humaine.
Validation d'appareil à l'aide des SDK pour appareils mobiles	Rédigés pour l'ensemble des principales plateformes d'applications mobiles (comme Android, iOS, React Native, Unity, etc.), ces SDK valident l'intégrité des applications, détectent les environnements non sécurisés et authentifient le trafic API (à l'aide de jetons cryptographiques auto-fournis ou approuvés par Cloudflare).
Politiques et réponses	
Réponses standard	Configurez le blocage, l'autorisation, la journalisation, le contrôle du volume des requêtes ou toute une gamme de tests conviviaux à adresser en réponse au trafic de bots identifié par nos moteurs de détection.
Politiques de réponse personnalisées	Intégrez les signaux issus du service Cloudflare Bot Management aux politiques d'autres produits Cloudflare (comme le pare-feu Cloudflare WAF ou le service de protection contre les attaques DDoS) et définissez des actions personnalisées via Workers.
Analyses	
Tableau de bord Cloudflare	Examinez l'activité des bots sur une période remontant jusqu'à 30 jours et filtrez les résultats en fonction du score de bot, ainsi que d'autres filtres liés aux bots, au trafic et aux requêtes. La boucle de rétroaction des bots permet aux clients Cloudflare de signaler les éventuels faux positifs ou faux négatifs afin de donner lieu à une enquête plus approfondie.
Outils tiers (SIEM, lacs de données, outils d'analyse, etc.)	Analysez les signaux de gestion des bots issus de l'examen de l'ensemble de vos applications au sein d'un tableau de bord unique grâce à la solution Cloudflare Security Analytics, explorez davantage de données de journalisation dans Log Explorer et associez les données tierces aux données Cloudflare au sein d'une plateforme d'analyse ou d'un SIEM tiers via Log Push.

Vous êtes prêts à en voir davantage ? Inscrivez-vous à notre série de démos consacrées à la sécurité des applications.