CLOUDFLARE®

Sécuriser les applications dans le cloud

Protection multicouche rapide, facile à déployer et évolutive contre les attaques DDoS, les violations de données et les bots malveillants

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com/fr

Sécuriser les applications dans le cloud

Protection multicouche rapide et facile à déployer pour contrer les attaques DDoS, les violations de données et les bots malveillants

Les entreprises subissent de plus en plus de pression pour renforcer leur sécurité. Les trois facteurs qui contribuent à cette pression sont les suivants :

- Les pirates sont plus efficaces, hautement motivés et utilisent des techniques plus sophistiquées.
- La surface d'attaque augmente à cause des applications qui exposent plus d'API publiques, de l'adoption SaaS en hausse et de l'intégration avec davantage d'applications tierces.
- La vigilance du public et du gouvernement pour les questions de données, de confidentialité et de sécurité s'intensifie.

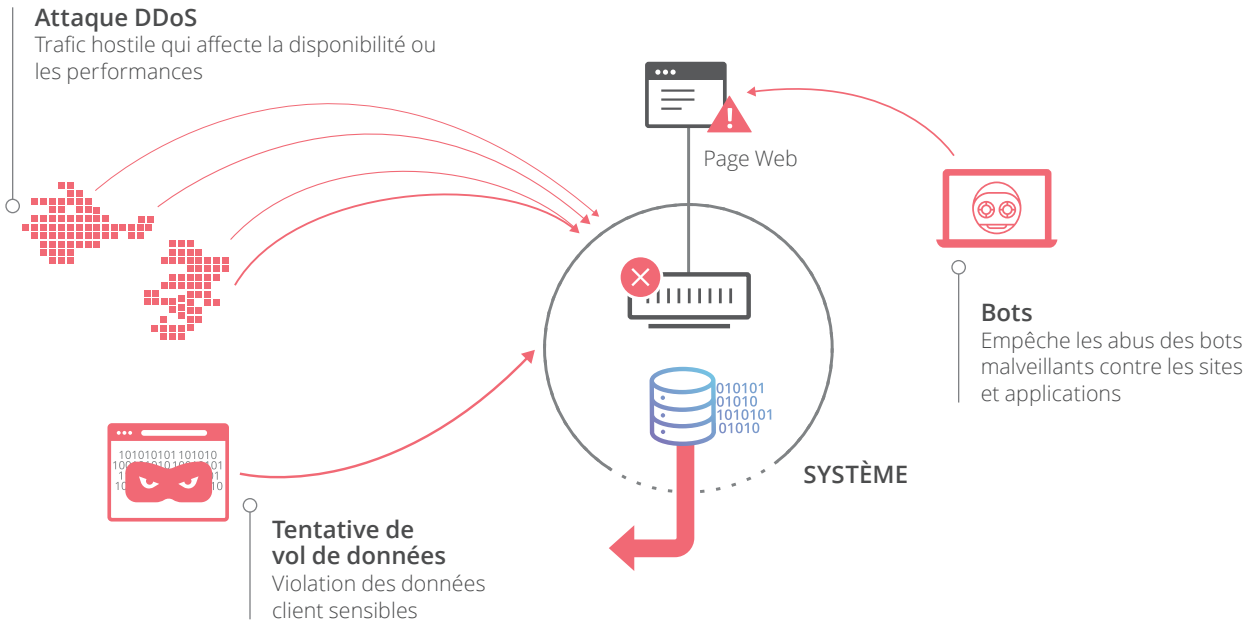
Les pirates augmentent la fréquence et le volume des attaques par déni de service distribué (DDoS). En se servant de botnets et des millions d'appareils connectés de l'Internet des objets (IdO), ils sont en mesure de lancer des attaques volumétriques largement distribuées avec plus de facilités et un impact plus important.

En plus d'envoyer des volumes plus élevés, les pirates s'intéressent désormais davantage à la couche d'application qu'à la couche réseau. Les attaques visant la couche d'application, ou couche 7, sont plus difficiles à détecter, elles requièrent généralement moins de ressources pour rendre un site indisponible et perturbent les opérations.

Les pirates sont désormais capables de monétiser leurs tentatives d'attaque contre les sites ou de vol de données sensibles, en exigeant des rançons par exemple. Par conséquent, après avoir extorqué avec succès de l'argent aux entreprises ciblées, les pirates gagnent en présence, en motivation et en organisation.

De plus en plus exposées, les entreprises doivent renforcer leurs défenses contre trois problèmes et risques principaux :

- Une attaque DDoS contre des applications, des sites Web ou des API affecte leur disponibilité et leurs performances, provoquant la chute des revenus, des coûts opératoires plus élevés et une dégradation de la réputation
- La violation des données sensibles des clients et des entreprises, comme les renseignements personnels ou la propriété intellectuelle, peut entraîner la perte de clients et entacher leur confiance
- Les bots malveillants emploient l'extraction de contenu, l'usurpation de compte et les fraudes au paiement pour s'attaquer aux applications client



Si le coût monétaire des attaques DDoS, violations de données ou bots malveillants peut varier en fonction de la taille ou du secteur des entreprises touchées, l'impact commercial se fait partout ressentir plus vivement.

Selon un rapport de l'IDC de 2015, le coût moyen de l'indisponibilité des infrastructures s'élève à 100 000 $ par heure.[1]

Une violation de données peut prendre différentes formes : de la fuite d'informations utilisateur à la subtilisation de données client sensibles, comme les données de cartes de paiement ou les mots de passe stockés dans une application. En 2017, le coût moyen d'une violation de données s'élevait à 141 $ par enregistrement perdu ou volé, pour un montant total moyen de 3,62 millions $ par violation.[2] Avec la vigilance croissante des gouvernements et des médias, les entreprises subissent de lourdes répercutions pour la moindre violation de données, en raison de sanctions financières, mais aussi de la perte de confiance du public.

Si les bots malveillants peuvent usurper le compte d'un utilisateur, ils seraient également capables d'effectuer des fraudes au paiement et d'extraire des contenus. En achetant automatiquement et à répétition des articles disponibles en quantité limité, les bots frauduleux peuvent entacher l'image de marque d'une enseigne, dissuader les clients futurs et donc diminuer les ventes, voire endommager la relation avec les fournisseurs. L'extraction de contenu peut directement affecter les revenus, notamment pour les entreprises qui dépendent de la publicité, en chutant dans le classement des résultats des moteurs de recherche, en réduisant le coût par mille impressions (CPM) ou en éloignant les publicitaires.

L'avantage

Pour lutter contre cette vulnérabilité croissante et les impacts commerciaux liés, les entreprises doivent non seulement s'attaquer aux questions tactiques spécifiques, mais aussi prendre l'avantage dans un environnement où les menaces évoluent constamment.

Les trois points critiques pour faire la différence sont **la taille, les performances et la facilité d'utilisation**.

La taille a son importance

Pour l'analyse des données, la taille du réseau de Cloudflare et la variabilité de son trafic sont des atouts importants. En protégeant plus de 6 millions de sites Web, Cloudflare jouit d'une connaissance approfondie des menaces émergentes au niveau mondial. Par conséquent, les clients de Cloudflare bénéficient de protections DDoS et d'un pare-feu applicatif Web qui les protègent proactivement des attaques, ainsi que de l'indisponibilité et des pertes de revenu qui en résultent.

Conçu pour fonctionner à grande échelle, le réseau de Cloudflare offre rapidité et résilience. Afin de pouvoir traiter plus de 300 milliards de requêtes par jour, les services fournis depuis chaque serveur dans tous les datacenters, comme le DNS, le chiffrement et le WAF, sont en mesure d'assumer d'importantes charges de trafic avec une latence réduite et une grande fiabilité.

Au fur et à mesure que les attaques DDoS gagnent en ampleur, la taille et la résilience du réseau profitent à nos clients. L'échelle de Cloudflare, avec plus de 116 datacenters combinés au réseau Anycast, lui permet de résister à la plus vaste des attaques distribuées.

Augmenter les performances tout en sécurisant les applications

En général, les clients doivent faire un choix entre performances et sécurité. Les solutions TLS et WAF affectent souvent les performances d'un site. Par exemple, le TLS, un protocole de chiffrement, peut introduire jusqu'à quatre allers-retours pour ouvrir une seule connexion sécurisée. Ces va-et-vient supplémentaires peuvent augmenter la latence. De même, étant donné qu'un WAF inspecte chaque requête une à une, il engendre des retards.

[1] IDC, « DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified » [DevOps et le coût de l'indisponibilité : Étude quantitative des bonnes pratiques des entreprises Fortune 1000], Stephen Elliot, mars 2015

[2] Institut Ponemon, « Étude 2017 sur le coût des violations de données », juin 2017

Avec Cloudflare, plus besoin de sacrifier les performances pour la sécurité. Au contraire, les fonctionnalités de sécurité offertes par Cloudflare peuvent augmenter les performances des applications grâce aux services de sécurité à faible latence intégrés à l'accélération du trafic. La prise en charge de TLS 1.3 et la reprise globale des sessions réduisent le nombre d'allers-retours, et HTTP/2 accélère les temps de chargement des pages en permettant les téléchargements multiplexés. Grâce à l'intégration des services de sécurité aux des services d'accélération du trafic, comme la mise en cache ou le routage intelligent, les applications deviennent plus performantes une fois protégées par Cloudflare.

La mise en cache rapproche le contenu statique des visiteurs du site Web. Les serveurs d'origines étant moins encombrés, la réponse de l'application est plus rapide. Le routage intelligent détermine le chemin le plus rapide entre Cloudflare et l'origine, accélérant au passage les contenus dynamiques et statiques.

Taille

Conçu de A à Z
pour la résilience

Facilité d'utilisation

Interface et API intuitives pour une
configuration et une gestion agiles

Rapidité

Sécurité hautes performances avec
accélération du trafic intégrée

La facilité d'utilisation améliore la gestion de la sécurité

La facilité d'utilisation pour les utilisateurs et les administrateurs ne se limite pas à une jolie interface. Elle contribue à améliorer la gestion de la sécurité d'une entreprise. Une étude de Gartner indique que d'ici 2020, 99 % des failles de pare-feu seront dues à des erreurs de configuration et non à des failles.[3]

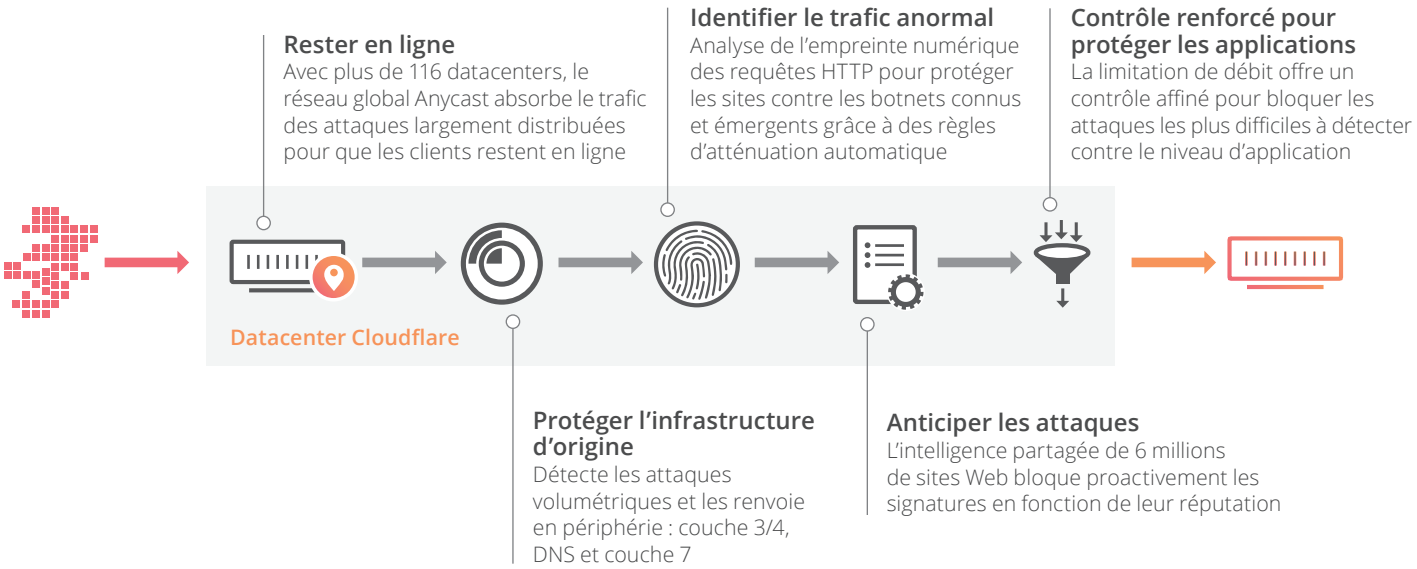
Une bonne expérience utilisateur (UX) diminue les risques de sécurité dus aux erreurs de configuration et renforce l'agilité dans un environnement où les menaces évoluent constamment. Il faut moins de 5 minutes pour configurer Cloudflare. Cette facilité d'utilisation permet aux entreprises d'étendre leur politique de gestion de la sécurité à davantage d'employés (même s'ils ne sont pas spécialistes), de fluidifier le changement et le déploiement de nouvelles politiques, et d'améliorer les ajustements en temps opportun de la gestion de la sécurité pour les applications complexes.

Cloudflare applique ces avantages pour protéger ses clients contre trois défis de taille : Les attaques DDoS qui nuisent aux performances et à la disponibilité de leurs applications, la violation des données client par attaques multivectorielles et les abus des bots malveillants contre leurs sites Web.

Protéger vos applications contre les attaques DDoS

Une attaques DDoS envoie de gros volumes de trafic à un site ou un service pour le rendre indisponible.
En surchargeant les serveurs d'origine, le trafic malveillant ralentit l'application ciblée, voir la rend complètement indisponible pour les utilisateurs. Cloudflare offre une défense multicouche.

[3] Gartner, Inc., « One Brand of Firewall Is a Best Practice for Most Enterprises » [Une seule marque de pare-feu, la meilleure solution pour la plupart des entreprises], Adam Hils et Rajpreet Kaur, 5 juin 2017



Réseau Anycast global

Le réseau Anycast comprenant plus de 116 datacenters augmente la surface sur laquelle Cloudflare peut disperser les attaques DDoS. Grâce à Anycast, plusieurs machines peuvent utiliser la même adresse IP. Lorsqu'une requête est envoyée à une adresse IP Anycast, les routeurs l'envoient à la machine la plus proche sur le réseau. Les attaques largement distribuées de botnets sont ainsi atténuées, puisque le trafic DDoS est absorbé en partie par chaque datacenter, au lieu d'être concentré en un seul point.

Atténuation intelligente et automatique en périphérie

La perspective dont Cloudflare jouit grâce aux 6 millions de sites sous sa protection permet à son service de protection DDoS de développer des heuristiques basées sur les attaques contre un site pour protéger les autres.

L'atténuation automatique se fonde sur l'empreinte numérique des flux réseau et du trafic HTTP hostile pour identifier et bloquer les attaques avant qu'elles n'atteignent le site des clients.

En envoyant ces attaques volumineuses à la périphérie du réseau, les serveurs d'origine du client restent protégés et en ligne.

Pile intégrée de protections du DNS, du réseau et de la couche 7

En périphérie, chaque serveur est doté d'une pile de services de sécurité (DNS, pare-feu, limitation de débit et WAF), c'est pourquoi Cloudflare est en mesure de proposer non seulement une protection distribuée, mais aussi une défense multicouche contre différents types d'attaques DDoS, notamment les attaques visant le DNS, le réseau et la couche d'application.

Le service de DNS distribué de Cloudflare peut résister aux attaques contre les serveurs de nom de domaine. Les attaques réseau, contre les couches 3 et 4 par exemple, ne sont pas bloquées automatiquement, mais l'utilisateur peut configurer le service afin de bloquer certaines sources par IP, pays d'origine ou ASN à l'aide d'un pare-feu IP. Les paramètres de sécurité peuvent mettre à profit la perspective de Cloudflare sur la réputation de n'importe quelle adresse IP à travers ses 6 millions de sites Web pour proactivement bloquer le trafic malveillant identifié.

> « Nous apprécions cette tranquillité d'esprit qu'offre Cloudflare : on le configure, on l'oublie et on est confiant qu'on ne subira aucun type d'attaque DDoS malveillante.

BUYCRAFT

LEE MCNEIL
Directeur de la technologie

Atténuations adaptables basées sur le débit

Bien que la solution DDoS de Cloudflare protège automatiquement ses clients des attaques volumétriques contre le réseau et les applications, certains clients ont besoin de commandes adaptables pour se défendre contre le trafic d'ampleur moindre, mais tout aussi malveillant.

La possibilité de personnaliser les seuils pour les taux de requêtes, l'URI cible et les attributs des requêtes, comme la méthode ou le code de réponse, offre aux clients la liberté d'ajuster leurs défenses en fonction de leur profil d'application et de trafic.

Réduire les risques de violation de données avec une défense multicouche

Les pirates emploient souvent plusieurs vecteurs d'attaque quand ils tentent de mettre la main sur des données client. Pour se défendre, les entreprises ont besoin d'une protection multicouche.

LES ATTAQUES	SOLUTIONS CLOUDFLARE
1. Injectent des données malicieuses dans les formulaires et API	**Bloquent les attaques OWASP principales et les attaques émergentes au niveau applicatif grâce au WAF**
2. Subtilisent les données sensibles non chiffrées entrées par les clients	**Le chiffrement via SSL/TLS bloque le snooping**
3. Franchissent les pages d'authentification par force brute	**La limitation du débit protège l'authentification**
4. Les pirates tentent de créer des réponses DNS pour intercepter les identifiants des clients	**La sécurisation DNS et DNSSEC empêche les réponses falsifiées**

Diminuer les risques d'usurpation d'identité à l'aide d'un DNS sécurisé

L'empoisonnement de cache, ou « spoofing », amène les visiteurs à entrer des données sensibles, comme le numéro d'une carte de paiement, sur un site compromis. Ce type d'attaque a lieu lorsqu'un pirate empoisonne le cache d'un serveur de noms DNS avec des enregistrements incorrects. Tant que l'entrée de cache est active, le serveur de noms renvoie des enregistrements de DNS falsifiés. Les visiteurs ne sont pas dirigés vers le bon site, mais vers celui du pirate, qui peut alors voler les données sensibles.

DNSSEC contrôle les enregistrements de DNS à l'aide de signatures cryptographiques. En contrôlant les signatures associées à un enregistrement, les serveurs DNS de résolution vérifient si l'information requise vient du bon serveur de nom, et pas d'un pirate intermédiaire non autorisé.

Diminuer les risques d'usurpation d'identité à l'aide du chiffrement

On parle de « snoop » quand un pirate intercepte la session d'un client pour voler ses données, notamment ses identifiants, mots de passe ou numéros de carte de paiement. En cas d'attaque de « l'homme du milieu », le navigateur pense qu'il s'adresse au serveur sur un canal chiffré et inversement, mais ils s'adressent en réalité tous deux à un intermédiaire malveillant. L'ensemble du trafic passe donc par cet homme du milieu, qui lit et modifie les données à son gré.

Le chiffrement/la désactivation rapide, la gestion facile des certificats et la prise en charge des normes de sécurité les plus récentes permettent aux clients de sécuriser le transfert des données utilisateur.

Bloquer les charges malveillantes via un WAF adaptable avec mises à jour automatiques

Les pirates exploitent les vulnérabilités des applications en envoyant des charges malveillantes capables d'extraire les données sensibles à partir d'une base de données ou du navigateur du client, ou en injectant un malware qui s'attaque aux systèmes visés.

Le WAF analyse le trafic Web à la recherche de trafic suspect. Il peut automatiquement filtrer les requêtes illégitimes sur la base des ensembles de règles que vous avez configurés. Il examine les requêtes HTTP GET et POST, et applique un ensemble de règles, comme le « ModSecurity core rule set », qui couvre les 10 vulnérabilités principales identifiées par OWASP, afin de déterminer quel trafic il doit bloquer, vérifier ou autoriser. Il peut bloquer le spam de commentaires, les attaques de type XSS (Cross-Site Scripting) et les injections SQL.

Le WAF de Cloudflare met à jour les règles en fonction des menaces identifiées parmi 6 millions de clients, protégeant les applications client sans affecter leurs performances grâce à ses mécanismes de vérification à faible latence et à l'intégration à l'accélération du trafic.

Diminuer l'usurpation de compte en protégeant l'authentification

Les pirates peuvent lancer des « attaques de dictionnaire » en automatisant l'authentification avec des identifiants sauvegardés pour la franchir par « force brute ». Cloudflare permet à ses utilisateurs de personnaliser des règles de limitation de débit afin d'identifier et de bloquer en périphérique ces attaques difficiles à détecter.

Surveiller et évaluer pour mieux protéger

En surveillant les vulnérabilités d'un site, en évaluant le niveau de sécurité d'une entreprise et en s'intégrant à votre processus de développement, les applications tierces de Cloudflare offrent une couche de protection proactive supplémentaire.

> « Grâce aux fonctionnalités de sécurité de Cloudflare, nos développeurs passent moins de temps à s'inquiéter de la disponibilité du site et peuvent se concentrer sur d'autres améliorations.

Gazeta Esportiva | DAVID VERZOLLA
Directeur de la technologie

Empêcher les abus de bots

Trois types de bots abusifs augmentent en fréquence, en complexité et en impact sur le client. Les solutions anti-bots doivent donc mobiliser différents éléments pour répondre à la multitude de profils d'attaque potentiels.

Les attaques les plus fréquentes sont l'usurpation de compte, l'extraction de contenus et la fraude au paiement. Ces trois attaques emploient trois « styles » de bots différents qui nécessitent chacun une approche particulière.

Détection et atténuation basées sur le débit

Certains bots sont automatisés et ne parviennent à leur objectif qu'en lançant un débit élevé d'attaques. La limitation de débit permet de détecter et d'atténuer ces attaques. Par exemple, les connexions par force brute ont un taux d'échec de connexion par adresse IP supérieur à celui d'un utilisateur normal. Les seuils de débit peuvent détecter ce type de tentatives d'usurpation de compte. C'est le même principe pour les extracteurs de contenus : ils tombent sur des pages introuvables (erreur 404) plus souvent que les utilisateurs normaux.

Blocage des signatures en fonction de la réputation

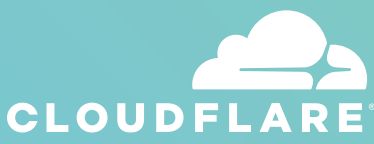
Avec 6 millions de sites Web protégés par Cloudflare, si la signature d'un bot abusif connu est détectée sur un site, elle est bloquée sur tous les autres.

Conclusion

Pour maintenir la sécurité et la disponibilité dans un environnement où les menaces évoluent constamment, les entreprises ont besoin de performances, d'une sécurité intelligente à grande échelle et de défenses multicouches pour se protéger contre les attaques par déni de service, le vol de données et les bots malveillants.

Comme les humains resteront toujours un élément central, la facilité de déploiement, de configuration et d'ajustement des politiques de sécurité influence la gestion générale de la sécurité en réduisant les maladresses et en permettant à davantage d'employés de réagir aux changements sans risques ou frictions inutiles.

La sécurité du cloud de Cloudflare est un rempart contre les attaques DDoS de plus en plus complexes, les tentatives de violations de données et les bots malveillants.



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com/fr