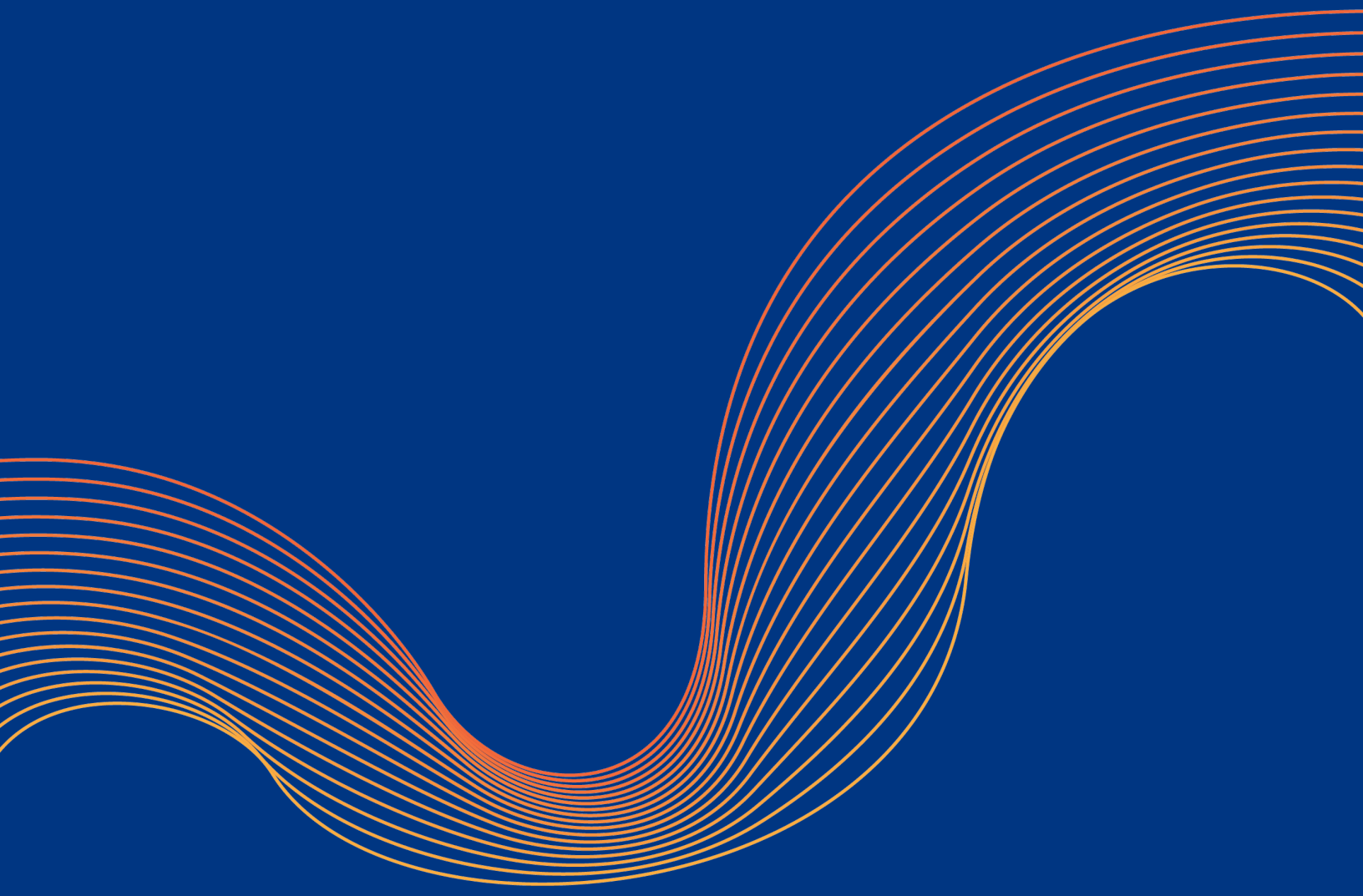
CLOUDFLARE

Une sécurité des applications efficace nécessite une protection globale, rapide et continue



+33 75 7 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

Qu’est-ce que Cloudflare ?

Grâce à Cloudflare, votre entreprise bénéficie d’un Internet plus performant. La société Cloudflare propose ainsi un réseau mondial, au plus près de vos clients et employés, quel que soit l’endroit où ils se trouvent dans le monde.

Les produits Cloudflare se consacrent à la protection et à l’accélération de vos sites web, applications et API. Ils vous permettent également d’acheminer en toute sécurité du trafic au sein de vos environnements sur site, SaaS et cloud, tout en protégeant les réseaux, vos collaborateurs et les appareils de votre entreprise contre les acteurs malveillants évoluant sur Internet.

Pilotable à partir d’un unique tableau de bord convivial, chaque service Cloudflare s’exécute n’importe où dans le monde sur notre réseau. Vous n’avez aucun compromis à faire entre sécurité et performances. Il n’est plus nécessaire d’assembler une multitude d’équipements réseau et de sécurité qui ne contribuent qu’à ralentir votre expérience. Enfin, cerise sur le gâteau, le réseau mondial de Cloudflare se révèle programmable, afin de permettre à vos développeurs peuvent déployer du code personnalisé, directement à la périphérie d’Internet.

Des millions de clients font confiance à Cloudflare pour rendre l’Internet plus sûr, confidentiel et fiable.

Votre entreprise dépend d’Internet ? Essayez Cloudflare. Nos solutions contribuent à bâtir un Internet meilleur.

INDEX

INTRODUCTION

Les menaces envers la sécurité des applications sont toujours présentes. En 2020, la National Vulnerability Database (NVD) a signalé plus de 18 000 vulnérabilités, établissant ainsi un nouveau record dans le domaine. De manière alarmante, plus de 10 000 de ces menaces se sont vues qualifiées de vulnérabilités de gravité critique ou élevée.

Parallèlement, les auteurs d'attaques continuent d'exploiter des vulnérabilités bien connues. Des recherches conjointes menées par la Cybersecurity and Infrastructure Security Agency (CISA) des États-Unis, le Federal Bureau of Investigation (FBI), le National Cyber Security Center (NCSC) du Royaume-Uni et l'Australian Cyber Security Center (ACSC) ont révélé que bon nombre des 30 principales vulnérabilités utilisées par les pirates informatiques en 2020 (et en 2021) étaient déjà familières, chacune d'elles disposant d'ailleurs d'un correctif sur le marché.

Le risque de sécurité lié à ces vulnérabilités notoires se perpétue, car les entreprises peuvent éprouver des difficultés concernant le déploiement de correctifs pour leurs logiciels. Pire encore, même lorsque les entreprises tentent de corriger une vulnérabilité avant son exploitation, le processus de mise à jour demande en moyenne 16 jours, laps de temps pendant lequel les applications restent à la merci des attaques.

Les vulnérabilités natives ne constituent malheureusement pas l'unique préoccupation en matière de sécurité pour les propriétaires d'applications. Les API introduisent ainsi leurs propres risques et les données du réseau Cloudflare montrent que plus de 50 % des requêtes sont liées aux API. De plus, comme les bots représentent 40 % du trafic Internet, la protection contre les attaques menées par ces derniers s'avère d'importance stratégique. Enfin, l'utilisation de code tiers (sur lequel de nombreux sites s'appuient pour fonctionner) expose les applications aux attaques sur la chaîne d'approvisionnement.

Face à la diversité des produits et des solutions disponibles pour protéger une application contre toutes les attaques possibles, la sécurité des applications peut rapidement se retrouver confrontée à un problème de fragmentation et de complexité excessive. La mise en œuvre d'une stratégie de sécurité complète peut vous aider à y faire face. Une stratégie de sécurité des applications efficace doit être capable de vous protéger contre un certain nombre de risques de manière globale, rapide et continue.

Panorama des risques envers la sécurité des applications

Les pages suivantes décrivent les problèmes de sécurité les plus pressants pour les propriétaires d'applications.

Vulnérabilités des applications

Les vulnérabilités au sein des applications s'avèrent incroyablement courantes. Un récent rapport signé Veracode sur la sécurité des logiciels a révélé que 83 % des applications présentaient au moins un défaut de sécurité, de nombreuses applications en abritant plus d'une. En outre, plus de 20 % des applications concernées par l'étude faisaient preuve d'au moins une faille grave.

Attaques sur les API

Les applications s'appuient de plus en plus sur des interfaces de programmation d'applications (API) pour fonctionner. Gartner a prédit que, « d'ici 2022, l'utilisation abusive des API passera d'un vecteur d'attaque peu fréquent au vecteur le plus répandu, avec pour résultat des violations de données au niveau des applications web des entreprises.[1] »

[1] Gartner a prédit que, « d'ici 2022, l'utilisation abusive des API passera d'un vecteur d'attaque peu fréquent au vecteur le plus répandu, avec pour résultat des violations de données au niveau des applications web des entreprises. » Source : Gartner « API Security: What You Need to Do to Protect Your APIs », Mark O'Neill, Dioniso Zumerle, Jeremy D'Hoinne, 1er mars 2021 (abonnement à Gartner requis).

Attaques de bots

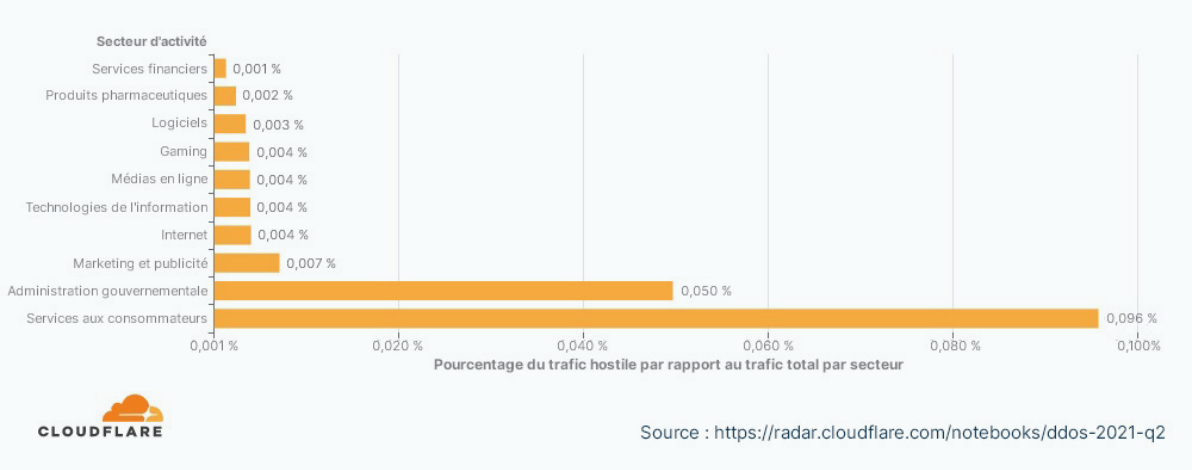
Les attaques de bots s'avèrent très courantes et leurs auteurs tirent souvent parti de réseaux d'appareils infectés (appelés botnets) pour effectuer diverses actions malveillantes. Un bon exemple de ces pratiques se nomme le bourrage d'identifiants (credential stuffing), une activité voyant les bots tenter d'accéder illégalement aux comptes via les pages de connexion à ces derniers en procédant au « bourrage » de centaines ou de milliers d'identifiants volés. Les bots servent également lors des opérations d'extraction de contenu (content scraping), un type d'attaque visant à télécharger et à dupliquer le contenu d'un site afin de s'emparer de certains avantages en matière d'optimisation pour les moteurs de recherche (SEO).

Attaques sur la chaîne d'approvisionnement

Dans les attaques sur la chaîne d'approvisionnement, les pirates tentent de trouver un point d'entrée par l'intermédiaire d'une source externe, comme un logiciel issu de fournisseurs de confiance, des dépendances de sites web tiers ou des fournisseurs. En 2015, un groupe appelé Magecart a mené plusieurs de ces attaques, en volant des informations de paiement sur des sites d'e-commerce et en infectant les dépendances tierces du site au moyen de code malveillant. Les navigateurs des utilisateurs finaux chargent la page contenant les dépendances infectées, permettant ainsi aux pirates de dérober des informations sur cette page web et de les vendre. Le constat implicite montre ici que le fait de travailler avec des tierces parties, qu'il s'agisse de fournisseurs ou de dépendances de sites web, peut considérablement augmenter la surface d'attaque.

Attaques DDoS

Les auteurs d'attaques DDoS s'appuient sur un afflux de trafic indésirable pour tenter de mettre une application hors ligne. Ces attaques changent constamment de taille ou de vecteur utilisé (entre autres paramètres) et ne cessent de se développer. Les données du réseau Cloudflare ont révélé qu'une requête HTTP sur 200 adressée à des entreprises situées aux États-Unis au cours du deuxième trimestre 2021 faisait partie d'une attaque DDoS.



Attaques de l'homme du milieu (on-path)

Les applications peuvent également se montrer la proie d'attaques de l'homme du milieu (on-path), qui voient les auteurs de ces dernières tenter d'intercepter la communication entre deux parties (par exemple, un navigateur et un serveur) à des fins malveillantes. Le pirate peut ainsi usurper l'identité de l'une des parties et en modifier la communication ou recueillir des informations sensibles. Les attaques de l'homme du milieu peuvent prendre de nombreuses formes et viser divers éléments, comme les serveurs de système de nom de domaine (DNS) et les serveurs de messagerie, par exemple. Lors d'attaques de l'homme du milieu sur le DNS, un acteur malintentionné intercepte le processus de recherche DNS et renvoie les utilisateurs vers un autre site web, généralement malveillant. De même, lors d'opérations de détournement de messagerie électronique, un pirate intercepte la connexion entre un serveur de messagerie et l'Internet, gagnant par là la possibilité de lire et d'interférer avec les communications par e-mail.

Meilleures pratiques en matière de défense contre les menaces visant les applications web

La défense contre ces types d'attaques doit faire partie de la stratégie de sécurité des applications de chaque entreprise. Toutefois, la manière dont les organisations se protègent contre ces attaques se révèle tout aussi importante. Une stratégie sophistiquée de sécurité des applications doit donc s'inscrire dans les catégories suivantes.

- **Pratiques basées sur un réseau en périphérie du cloud :** la protection sur site contre les menaces visant les applications web constituait la norme jusqu'ici, mais cette approche s'avère difficile à faire évoluer. Le seul moyen d'étendre la protection d'une application protégée par un pare-feu WAF matériel, par exemple, consiste à acheter de nouveaux équipements physiques. Le processus d'approvisionnement d'une application en équipements de protection supplémentaires peut prendre beaucoup de temps, pendant lequel l'application demeure vulnérable. Les solutions reposant sur le cloud ne présentent pas ce problème. Fort d'une capacité plus importante et toujours disponible, ce type de protection révèle en outre des possibilités d'évolution illimitées.

  Au-delà des limitations en termes de capacité, les mesures de protection sur site se montrent coûteuses à acheter et à entretenir. Les équipements physiques peuvent devenir obsolètes de manière relativement rapide et les coûts de réparation ou de remplacement ainsi s'accumuler. De même, l'embauche de personnel qualifié pour manipuler ces équipements contribue également à un coût total de possession élevé. À l'inverse, l'utilisation d'une solution fondée sur le cloud réduit considérablement ce dernier.

  Un autre avantage des solutions cloud réside dans la possibilité de les mettre à jour automatiquement, souvent et en toute simplicité. Cette fonctionnalité s'avère particulièrement utile pour les pare-feu d'applications web (WAF), par exemple, dont les règles, les mécaniques d'atténuation et la couche logicielle sous-jacente peuvent être rapidement mises à jour grâce à la diffusion dans le cloud. Les fournisseurs de solutions sur site peuvent également mettre à jour leurs produits à distance, mais le processus se révèle plus complexe et intervient généralement de manière moins fréquente.

  Les réseaux en périphérie du cloud vont encore plus loin. Ce type de réseau se compose d'un groupe de serveurs géographiquement dispersés et exécutant les mêmes services. La protection de la périphérie permet aux entreprises de tirer parti des avantages offerts par le cloud en termes d'évolutivité, tout en introduisant des avantages supplémentaires en matière de performances par rapport aux modèles centralisés.

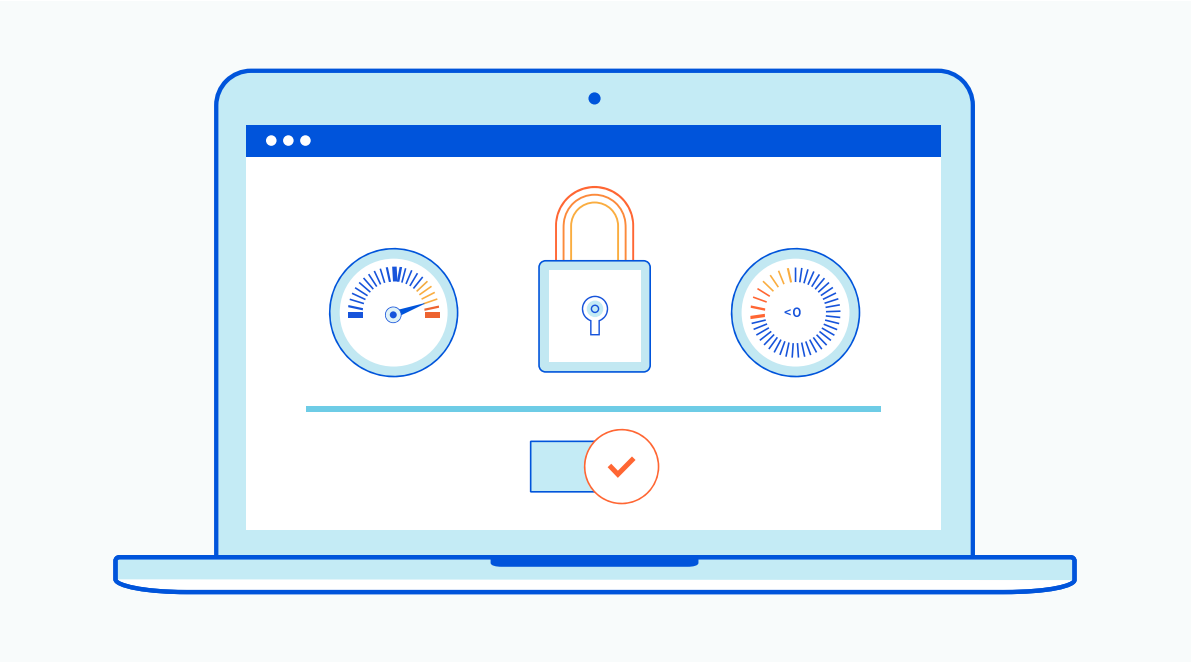
  Dans un réseau en périphérie du cloud, la protection a lieu aussi près que possible de l'utilisateur final. À l'inverse, dans un modèle centralisé, la protection a lieu dans un datacenter consolidé, beaucoup plus éloigné des utilisateurs finaux dispersés à travers le monde. Afin d'en assurer la sécurité, l'ensemble du trafic utilisateur doit être redirigé vers le datacenter centralisé dans lequel les équipements de sécurité sont déployés, quel que soit l'endroit où se trouve l'utilisateur final. Si les datacenters se situent dans l'État de Californie, le trafic devra d'abord y être redirigé avant d'être acheminé vers un utilisateur final situé à New York, par exemple.

- **Pratiques unifiées :** les tentatives de déploiement d'une protection cohérente sur plusieurs outils engendrent un risque d'erreur. Il est donc préférable d'utiliser un système unique et unifié pour se défendre contre les attaques plutôt que de juxtaposer plusieurs outils.

  Les équipes qui utilisent des outils déconnectés disposent souvent de personnes différentes gérant divers produits de sécurité. Certaines informations importantes peuvent alors ne pas être partagées plus largement et la situation se révéler susceptible d'engendrer un phénomène de cloisonnement en matière de sécurité, voire des lacunes en termes d'information. Tous les outils doivent également être configurés et gérés individuellement, un processus entraînant ainsi une charge supplémentaire pour les équipes et l'introduction d'une complexité inutile.

  De même, l'utilisation d'un trop grand nombre d'outils peut rendre difficile l'analyse de toutes les alertes. Chaque outil dispose de son propre ensemble de règles et de sa propre logique en matière d'émission d'alertes. L'accumulation d'outils vient donc encore compliquer la tâche visant à déterminer quelles alertes s'avèrent réellement importantes.

  Parallèlement, l'utilisation d'un système unifié permet aux équipes d'interagir avec moins d'outils et d'alertes centralisées, améliorant ainsi grandement la compréhension des éléments qui nécessitent une attention particulière. En outre, les outils intégrés s'appuient souvent sur des politiques cohérentes, facilitant d'autant l'application des politiques à l'échelle mondiale. Les propriétaires d'applications peuvent ainsi définir des règles de prévention des pertes de données une seule et unique fois, par exemple, et leur pare-feu WAF, leurs API et les autres outils concernés les appliqueront automatiquement.

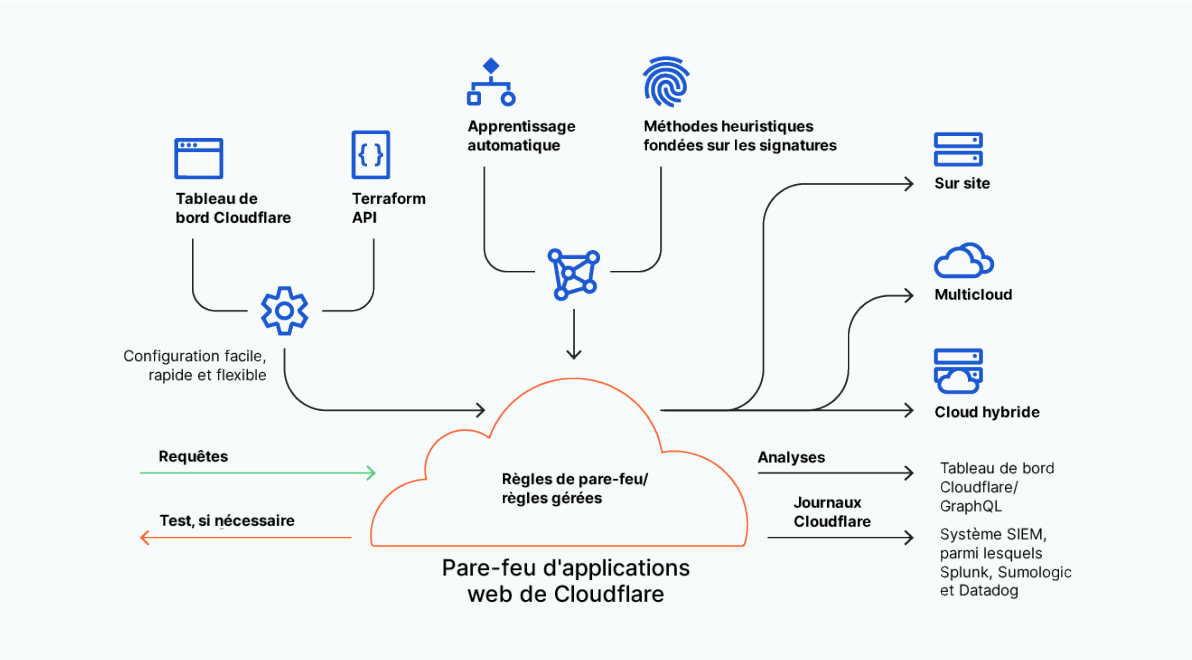


Stratégies spécifiques aux attaques

Avec autant de catégories différentes de risques envers la sécurité des applications, plusieurs types de protection s'avèrent nécessaires. Les lignes ci-dessous décrivent quelques-unes des stratégies spécifiques aux attaques que les propriétaires d'applications peuvent mettre en œuvre :

Vulnérabilités des applications

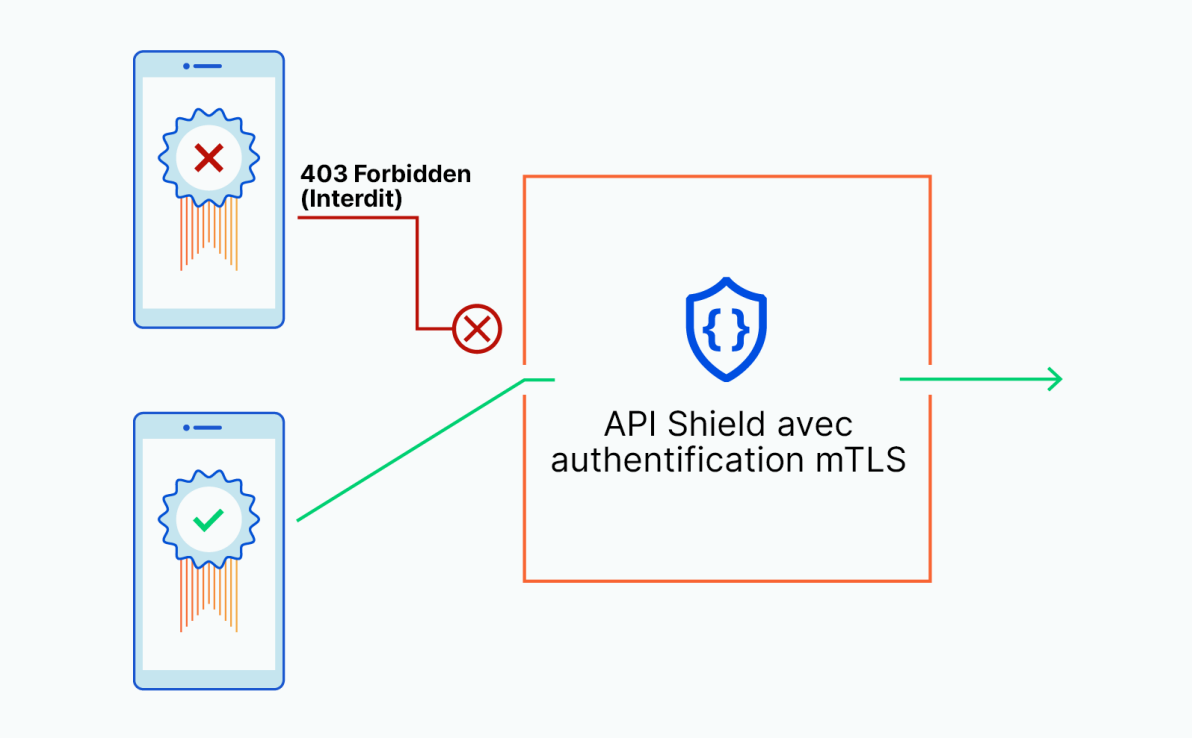
Pare-feu WAF : un pare-feu WAF constitue l'un des meilleurs moyens d'empêcher les pirates d'exploiter les vulnérabilités des applications. Ce type d'équipement s'appuie sur un ensemble de règles de sécurité destinées à filtrer le trafic malveillant et à empêcher les attaques. Les pare-feu WAF disposant de règles prédéfinies et d'options de personnalisation capables de déployer rapidement les modifications de règles se révèlent les plus efficaces. Ces fonctionnalités permettent d'atténuer deux des plus gros problèmes rencontrés par de nombreux pare-feu WAF : les faux positifs et la lenteur du déploiement des modifications de règles. Les faux positifs surviennent lorsque des règles WAF bloquent involontairement le trafic web légitime. Certains pare-feu WAF nécessitent des procédures de définition de règles complexes, qui compliquent la tenue de listes précises et le déblocage du trafic légitime. Les pare-feu proposant les ensembles de règles de l'OWASP en soutien d'ensembles gérés et personnalisés permettent de réduire la fréquence des faux positifs. Toutefois, si le déploiement de ces nouvelles règles prend trop de temps, les applications resteront vulnérables aux attaques.



Prévention des pertes de données : la stratégie de prévention des pertes de données (DLP, Data Loss Prevention) permet d'empêcher l'exfiltration de données (ou la migration non autorisée de données vers l'extérieur d'une entreprise). Les outils et solutions de DLP surveillent l'activité des applications et des API afin d'identifier les fuites potentielles et de les arrêter avant qu'elles ne surviennent. Pour ce faire, ces outils inspectent le trafic sortant et le comparent à des types de données connus, de manière à déterminer s'il s'agit d'une fuite de données qui doit être bloquée. Un outil de DLP peut, par exemple, identifier une chaîne de caractères en tant que nom d'utilisateur. Sur la base des règles définies par l'entreprise, l'outil peut également signaler une activité, la bloquer ou autoriser sa poursuite. Certains outils de DLP s'intègrent aux contrôles de l'accès en fonction des rôles (qui définissent le niveau d'accès des types d'utilisateurs) afin de sécuriser davantage les mouvements de données au sein d'une entreprise ou d'une application.

Risques envers la sécurité des API

Validation de schémas et modèles de sécurité positive : les schémas d'API désignent des contrats décrivant le comportement attendu des personnes qui interagissent avec une API. Ces schémas définissent les règles de base de ce que les utilisateurs sont autorisés à faire lorsqu'ils travaillent avec des API. Le format de schéma OpenAPI (ou Swagger) est le plus courant. Les schémas constituent de bons modèles en matière d'application de mesures de sécurité positive pour les API. Un modèle de sécurité positive compare les requêtes au schéma et les valide le cas échéant, afin de n'autoriser que les requêtes conformes à ce dernier et ainsi d'empêcher l'utilisation abusive et les attaques potentielles. Un modèle de sécurité positive se révèle plus strict qu'un modèle de sécurité négative, qui autorise toutes les requêtes par défaut, à l'exception de celles qu'il a été chargé de bloquer.



Authentification et autorisation : les procédures d'authentification (c'est-à-dire, le processus visant à s'assurer de la légitimité des requêtes liées aux API) et d'autorisation (la confirmation du niveau d'accès d'un point de terminaison ou d'un client) constituent également des aspects importants de la sécurité des API. Il existe de nombreuses façons d'authentifier et d'autoriser les requêtes liées aux API. Le protocole mTLS (Mutual Transport Layer Security, sécurité de la couche de transport à authentification réciproque) constitue, par exemple, un processus au sein duquel un client et un serveur disposent tous deux de certificats d'authentification qu'ils utilisent pour vérifier l'identité de l'autre.

Découverte des API : les API « fantômes » (Shadow API) désignent les API dont une équipe de sécurité peut ne pas avoir conscience. Comme aucune équipe de sécurité ne les surveille, les API fantômes peuvent introduire une possibilité de fuites de données, voire ne pas répondre aux normes de conformité. Pour une meilleure gestion des API, les outils de découverte des API surveillent les points de terminaison afin de découvrir ces API fantômes.

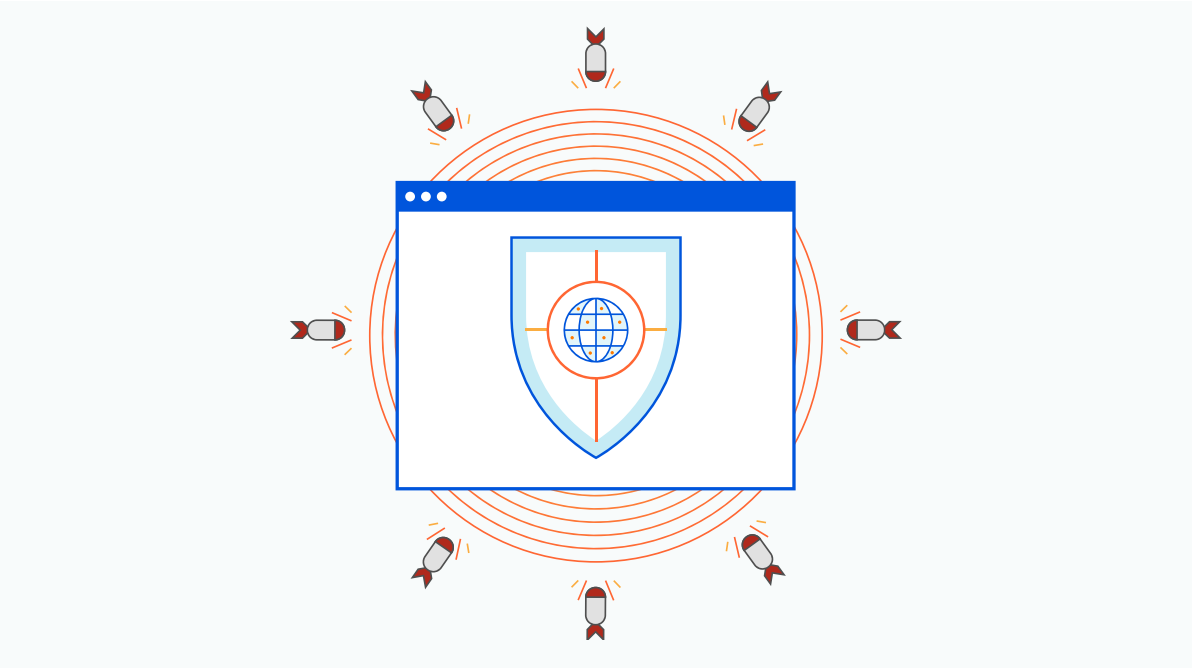
Prévention des pertes de données : les applications traditionnelles ne sont pas les seules à connaître le risque d'exfiltration de données, les API peuvent également en faire les frais. Les outils de DLP peuvent servir à surveiller le trafic API sortant afin de détecter et de bloquer les éventuelles données sensibles dans les réponses des API.

Bots malveillants

La gestion du trafic des bots implique de détecter et de bloquer les bots malveillants sans entraver les bots utiles. Les bots utiles, comme les robots d'indexation chargés du SEO des sites, se révèlent nécessaires pour comprendre les indicateurs clés d'une entreprise. Les bots malveillants, en revanche, peuvent causer des ravages au sein d'une application en procédant à des opérations de bourrage d'identifiants, de spam de contenu et à d'autres types d'attaques. Une solution de gestion des bots analyse le trafic afin de détecter l'activité des bots et détermine si cette dernière s'avère bénigne ou malveillante, avant de bloquer ou d'autoriser le trafic en conséquence. L'efficacité en matière de gestion des bots nécessite des méthodes de détection sophistiquées, la capacité de comprendre les tendances du trafic des bots au fil du temps par le biais d'analyses et la flexibilité nécessaire afin d'utiliser ces données pour personnaliser les règles de blocage des bots.

Attaques DDoS

Une défense efficace contre les attaques DDoS implique d'optimiser le délai d'atténuation et de ne pas sacrifier les performances sur l'autel de la sécurité. L'un des moyens permettant de réduire ce dernier consiste à mettre en œuvre une protection DDoS permanente, par opposition à l'autre approche que constitue la protection à la demande. À l'inverse de ce dernier type de protection, les mesures d'atténuation permanentes n'attendent pas que le trafic atteigne un seuil particulier pour que la protection se déclenche : l'ensemble du trafic se trouve ainsi filtré et l'atténuation intervient plus rapidement. L'atténuation DDoS depuis la périphérie permet aux propriétaires d'applications de profiter de performances et d'une sécurité supérieures. Contrairement à la protection centralisée (qui s'effectue dans un emplacement prédéfini, indépendamment de l'origine de l'attaque), l'atténuation des attaques DDoS se produit aussi près que possible de la source de l'attaque, améliorant d'autant les performances.



Vulnérabilités tierces

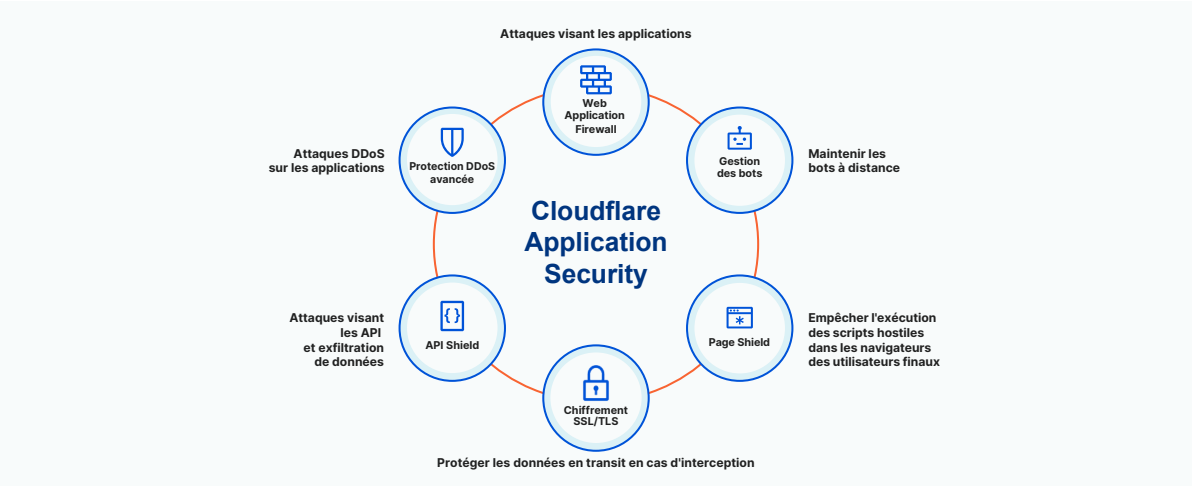
Solutions de sécurité côté client : les sites qui s'appuient sur des tierces parties, sans surveiller fréquemment ces dépendances, peuvent se retrouver vulnérables aux attaques sur la chaîne d'approvisionnement. L'approche de sécurité côté client permet de sécuriser l'activité du côté de l'utilisateur, généralement au sein de son navigateur. Ce type de sécurité protège les sites contre les attaques visant la chaîne d'approvisionnement en surveillant les modifications apportées aux dépendances tierces et en étudiant la nature des modifications du code. La technologie Content Security Policy (CSP) se repose, par exemple, sur une liste de ressources approuvées et bloque l'exécution de toute ressource ne figurant pas sur la liste. L'un des inconvénients de cette technologie réside toutefois dans le fait que cette dernière n'est pas dynamique. Si une ressource figurant sur la liste d'autorisation s'avère compromise et devient malveillante, la technologie CSP ne saura pas la bloquer. Fort heureusement, certaines offres de sécurité côté client capitalisent sur les avantages de la technologie CSP. Certains outils se révèlent capables de surveiller les nouvelles dépendances JavaScript et d'alerter les propriétaires de sites afin qu'ils procèdent à une enquête, le cas échéant. De même, certaines offres peuvent détecter les URL malveillantes connues transmettant du code JavaScript sur un site ou alerter les propriétaires de sites afin qu'ils enquêtent sur la nature des modifications de script détectées.

Attaques de l'homme du milieu (on-path)

Le chiffrement s'avère essentiel pour se défendre contre les attaques de l'homme du milieu. L'adoption du chiffrement Secure Sockets Layer (SSL)/Transport Layer Security (TLS) constitue l'une des meilleures méthodes de protection du trafic HTTP. Le protocole TLS chiffre les données, authentifie les parties qui les échangent et vérifie qu'elles n'ont pas été falsifiées. Ce processus protège les échanges entre les services web et les utilisateurs finaux, empêchant ainsi les attaques de l'homme du milieu. Certains pirates peuvent toutefois contourner le protocole SSL/TLS et c'est là que le HTTP Strict Transport Security (HSTS) entre en jeu. Ce mécanisme bloque ainsi l'ensemble des connexions non sécurisées des pirates, afin de protéger encore les utilisateurs finaux contre les attaques de l'homme du milieu.

Sécuriser votre application contre les menaces externes avec Cloudflare

Cloudflare rend possible la protection contre les menaces externes visant les applications. Le réseau périphérique de Cloudflare s'étend sur plus de 200 villes réparties dans plus de 100 pays et protège des millions de propriétés Internet contre les attaques DDoS, les vulnérabilités des applications, les bots malveillants et l'utilisation abusive des API, parmi bien d'autres menaces. Chaque service de sécurité Cloudflare s'exécute sur chaque serveur composant notre réseau et s'appuie sur la même base mondiale d'informations sur les menaces.



Les offres Cloudflare en matière de sécurité des applications intègrent les fonctionnalités suivantes :

- **Vulnérabilités des applications**
  - **Pare-feu WAF :** le pare-feu WAF Cloudflare propose un système de règles en couches composé d'un ensemble de règles gérées régulièrement mis à jour en réponse aux dernières attaques, d'un ensemble de règles fondé sur le Top 10 de l'OWASP et de règles personnalisées que les clients peuvent configurer et déployer en quelques secondes. Afin de garantir une protection cohérente, le pare-feu WAF de Cloudflare fonctionne sur le même moteur de règles (basé sur Rust) que les solutions de gestion des bots de Cloudflare et API Shield.
- **Risques liés aux API**
  - **API Shield : la solution** API Shield de Cloudflare protège les API à l'aide d'un certificat client et d'une procédure de validation fondée sur un schéma. La solution s'appuie sur le protocole mTLS pour contrôler les appareils/clients qui tentent d'accéder à une API et analyse le trafic sortant à des fins de prévention des pertes de données, parmi bien d'autres fonctionnalités.
    - **Prévention des pertes de données :** Cloudflare offre également une fonctionnalité de prévention des pertes de données aux API afin de bloquer les réponses contenant des données sensibles, comme les clés API ou les informations de carte de paiement. La fonctionnalité de prévention des pertes de données de Cloudflare s'étend bien au-delà des API, en sécurisant également les applications et les appareils, par exemple.
- **Vulnérabilités tierces et attaques sur la chaîne d'approvisionnement du navigateur**
  - **Page Shield :** la fonctionnalité Script Monitor, qui fait partie de la solution Page Shield de Cloudflare, enregistre les dépendances JavaScript d'un site au fil du temps et alerte les entreprises afin qu'elles enquêtent sur les modifications ou les nouvelles dépendances au fur et à mesure de leur apparition.
- **Attaques de bots**
  - **Gestion des bots :** la solution Cloudflare de gestion des bots s'appuie sur l'apprentissage automatique, l'analyse comportementale et des données issues du monde entier pour bloquer les bots malveillants. L'outil d'analyse des données des bots permet de comprendre les modèles de trafic et de définir les accès avec précision à l'aide de règles personnalisées et de listes d'autorisation.
- **Attaques DDoS**
  - **DDoS :** avec un réseau de 90 Tb/s bloquant en moyenne 87 milliards de menaces par jour, la solution Cloudflare d'atténuation des attaques DDoS protège contre les plus grandes attaques issues de la périphérie.
- **Chiffrement**
  - **Cloudflare Free SSL/TLS :** la solution Cloudflare Free SSL/TLS vous permet de chiffrer le trafic web afin de protéger votre application. Le protocole Cloudflare SSL prend également en charge le HSTS pour un degré de protection supplémentaire.

Pour en savoir plus, rendez-vous sur https://www.cloudflare.com/fr-fr/security/.