EBOOK

CLOUDFLARE

6 moyens pour les start-ups d'optimiser la sécurité, les performances et la fiabilité de leurs activités en ligne

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

INDEX

Introduction 3

1 Sécurisez votre DNS afin d'éviter les attaques coûteuses 4

2 Accélérez la diffusion de contenu en acheminant le trafic sur les itinéraires les moins encombrés 5

3 Minimisez le risque de défaillance de votre site grâce à l'équilibrage de charge du trafic à l'échelle mondiale 6

4 Protégez vos applications web contre les attaques malveillantes 7

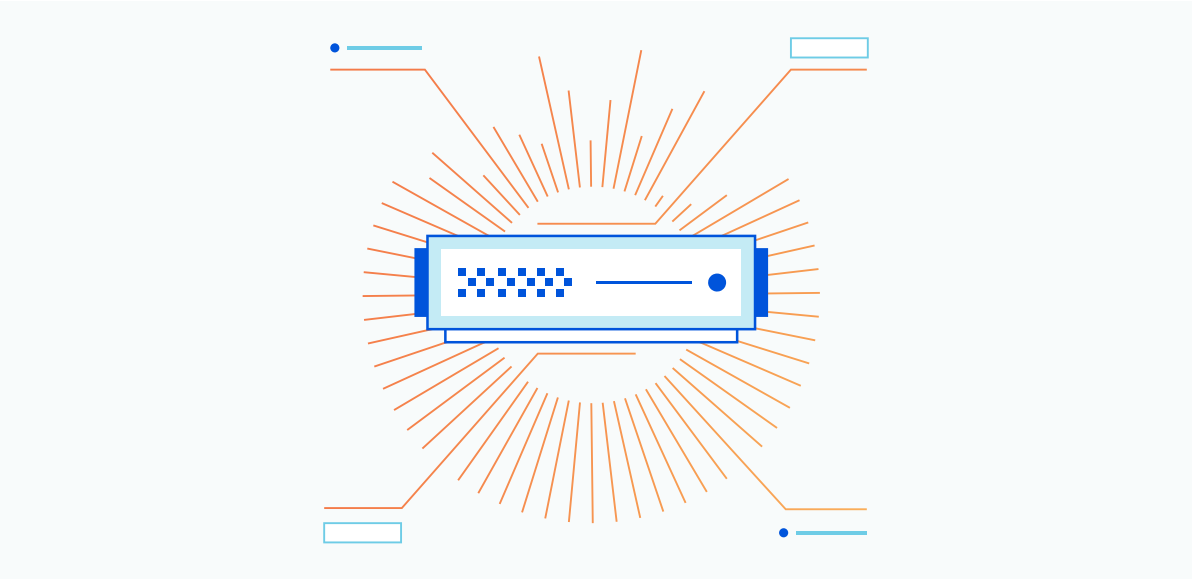
- A. Protection à l'aide d'un pare-feu d'applications web (WAF)
- B. Protection contre les attaques DDoS
- C. Atténuation des bots malveillants

5 Gardez un œil sur vos données d'analyse 9

6 Cherchez un fournisseur intégré 10

Conclusion 11

INTRODUCTION



L'un des points essentiels au développement d'une start-up consiste à proposer une expérience en ligne de première qualité aux clients. Afin de créer des expériences en ligne capables de satisfaire les clients et d'encourager la croissance de l'entreprise, les start-ups ont donc besoin d'applications et/ou de sites web sécurisés et performants.

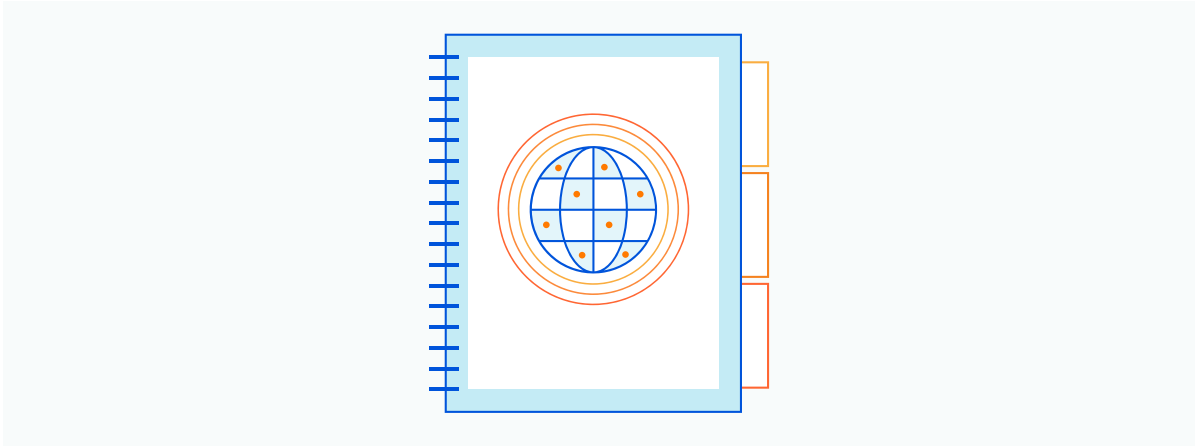
La création et la proposition d'une expérience en ligne positive reposent toutefois sur de nombreux éléments. Comme toutes les entreprises, les start-ups doivent devancer et satisfaire les besoins numériques des clients, établir une défense solide contre les attaques lancées depuis le web, surmonter les problèmes de latence et éviter les défaillances de site, tout en préservant la connectivité et les performances du réseau.

Les start-ups doivent également faire face à une pression particulière, puisqu'elles doivent répondre aux questions fondamentales et relever les divers défis liés au développement d'une entreprise. Ces derniers couvrent tous les aspects, de la recherche de capitaux à l'optimisation de leur positionnement sur le marché.

Fort heureusement, il existe de nombreux moyens de protéger et d'accélérer les propriétés Internet. Les start-ups ne disposant généralement que de peu de temps et de ressources, il est préférable pour elles d'adopter une approche intégrée. Les solutions complètes et faciles à utiliser permettent de réduire la complexité et le cloisonnement des données qu'entraîne la gestion de plusieurs fournisseurs. Par ailleurs, une solution efficace peut aider les start-ups à proposer d'excellentes expériences en ligne, afin de leur permettre de se concentrer sur le développement de leur activité, tout en leur épargnant du temps et des efforts.

Axés sur l'optimisation de la sécurité, des performances et de la fiabilité, les conseils suivants permettront aux start-ups d'offrir à leurs clients une expérience de premier ordre, qui contribuera ainsi à la croissance de leur entreprise.

CONSEIL Nº 1



Sécurisez votre DNS afin d'éviter les attaques coûteuses

Fréquemment surnommé « l'annuaire téléphonique d'Internet », le DNS (système de noms de domaine) traduit les noms de domaine en adresses IP numériques, afin de permettre aux navigateurs de charger les ressources Internet. La quasi-totalité du trafic web nécessite l'emploi de requêtes DNS, mais en l'absence de DNS sécurisé, ces requêtes rendent les entreprises vulnérables aux attaques. Voici quelques exemples courants d'attaques DNS :

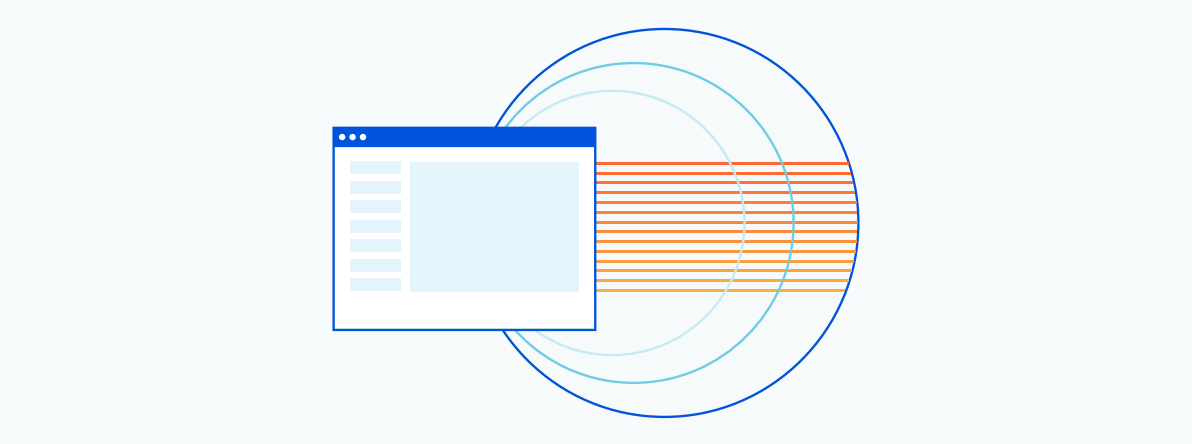
- **Attaques de l'homme du milieu (on-path) :** l'expression « de l'homme du milieu » (ou « on-path », sur le chemin d'accès) désigne une attaque qui intercepte les communications entre deux appareils afin de manipuler leurs échanges. Ses auteurs peuvent ainsi intercepter les requêtes DNS et les rediriger vers des sites différents. Dans certains cas, l'attaque redirige les utilisateurs vers une réplique du site de destination initial. Les pirates espèrent ainsi que cette réplique dupera les utilisateurs et les amènera à saisir leurs informations, qui pourront ainsi être volées par les cybercriminels. Cette forme d'attaque de l'homme du milieu se nomme « usurpation DNS ». Dans d'autres cas, les utilisateurs sont redirigés vers un site complètement différent, susceptible d'infecter les appareils de ces derniers en y introduisant des logiciels malveillants ou d'essayer de dérober leurs données.
- **Tunnellisation DNS :** lors d'une attaque par tunnellisation DNS, les pirates utilisent différents types de protocoles Internet (SSH ou HTTP, par exemple) pour transmettre des logiciels malveillants intégrés aux requêtes DNS.
- **Attaque NXDOMAIN :** une attaque NXDOMAIN permet aux pirates de saturer les serveurs DNS afin de provoquer un déni de service et d'empêcher les utilisateurs légitimes d'accéder à un site.

En l'absence de sécurité DNS, les entreprises se retrouvent vulnérables face à ces attaques (mais aussi à d'autres types de menaces), créant ainsi un maillon faible au sein d'une stratégie de sécurité globale. Comme ces entreprises s'efforcent bien souvent de s'attirer la confiance de leurs clients, la sécurisation des données contre les attaques s'avère essentielle pour les start-ups. Heureusement, les fournisseurs de services DNS gérés peuvent aider ces dernières à profiter d'un système DNS résilient.

Les fournisseurs de services DNS gérés comme Cloudflare hébergent tous les enregistrements DNS, résolvent les requêtes à la périphérie et prennent en charge le protocole de sécurité DNS Security Extensions (DNSSEC). Ce dernier permet de protéger les domaines contre les attaques DNS décrites ci-dessus en ajoutant une couche de sécurité par l'intermédiaire d'une signature cryptographique venant se greffer aux enregistrements DNS existants. Garante de la validité des données, cette signature doit intervenir à chaque étape du processus de recherche DNS.

La mise en place d'un DNS résilient s'avère cruciale, car la quasi-totalité du trafic Internet repose sur l'utilisation de requêtes DNS. Par ailleurs, un DNS non sécurisé expose les données des utilisateurs aux attaques. La protection des données des utilisateurs fait partie intégrante de la stratégie de sécurité globale de toute entreprise. Les start-ups ne pouvant s'appuyer sur une longue histoire pour soutenir la crédibilité de leur réputation, les efforts visant à combler les failles de sécurité, comme un DNS non sécurisé, se révèlent particulièrement importants pour elles.

CONSEIL Nº 2



Accélérez la diffusion de contenu en acheminant le trafic sur les itinéraires les moins encombrés

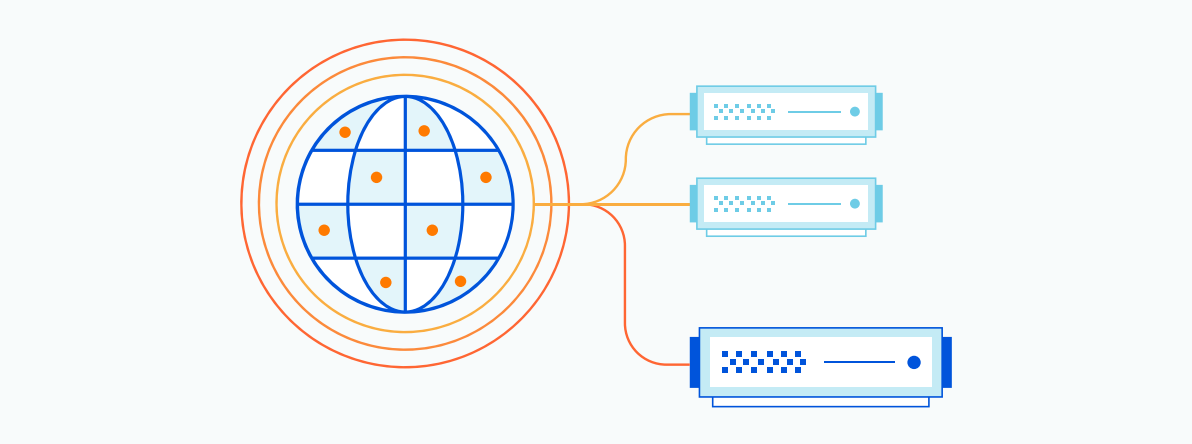
La majeure partie du trafic web d'aujourd'hui est acheminée par l'intermédiaire de réseaux de diffusion de contenu (Content Delivery Network, CDN), notamment le trafic issu de sites très fréquentés, comme Amazon et Facebook. Un réseau CDN se présente sous la forme d'un groupe de serveurs géographiquement distribués permettant de diffuser rapidement un contenu à des utilisateurs situés dans le monde entier.

Ce type de réseau s'appuie sur des serveurs répartis dans plusieurs endroits à travers le monde pour diffuser le contenu au plus près des visiteurs d'un site web, afin de réduire la latence du réseau et d'améliorer le temps de chargement des pages. Un réseau CDN permet également de mettre le contenu en cache, c'est-à-dire stocker et diffuser des ressources statiques, sur l'ensemble de son réseau. La mise en cache du contenu réduit le nombre de requêtes adressées aux serveurs web hébergés, entraînant ainsi une réduction en termes de bande passante et de coûts d'hébergement.

Les réseaux CDN contribuent à créer une expérience en ligne positive, car ils optimisent la rapidité avec laquelle les utilisateurs reçoivent le contenu. Si toutes les entreprises peuvent tirer parti d'un réseau CDN, les start-ups disposent quant à elles de moins de ressources en règle générale, un constat qui les contraint à maximiser autant que possible le rendement de leurs investissements. Les réseaux CDN représentent un investissement idéal en termes de performances en ligne, car ils permettent d'améliorer le temps de chargement des pages, tout en réduisant les coûts de bande passante.

Les réseaux CDN les plus efficaces se révèlent les plus étendus. Plus le réseau est vaste, plus la diffusion du contenu s'effectue à proximité des visiteurs. Les autres facteurs à prendre en compte lors du choix d'un fournisseur de réseau CDN sont la prévisibilité de sa tarification et le niveau de visibilité offert sur son cache. Un fournisseur de réseau CDN proposant une tarification prévisible s'assurera qu'une attaque ou un pic de trafic ne se traduise pas sous la forme d'une facture particulièrement élevée et imprévue pour votre organisation. En outre, un réseau CDN proposant une meilleure visibilité sur les données d'analyse permet d'offrir aux administrateurs les données dont ils ont besoin pour optimiser la mise en cache du contenu et réduire encore les coûts de bande passante.

CONSEIL Nº 3



Minimisez le risque de défaillance de votre site grâce à l'équilibrage de charge du trafic à l'échelle mondiale

L'optimisation des ressources et de l'efficacité des serveurs peut devenir un exercice d'équilibre délicat. Les serveurs surchargés ou géographiquement distants sont susceptibles d'augmenter la latence du trafic ou de provoquer une défaillance du serveur. Un serveur aux performances médiocres peut ainsi entraîner une perte de revenus, ainsi qu'une dégradation de la confiance des clients et de l'image de marque.

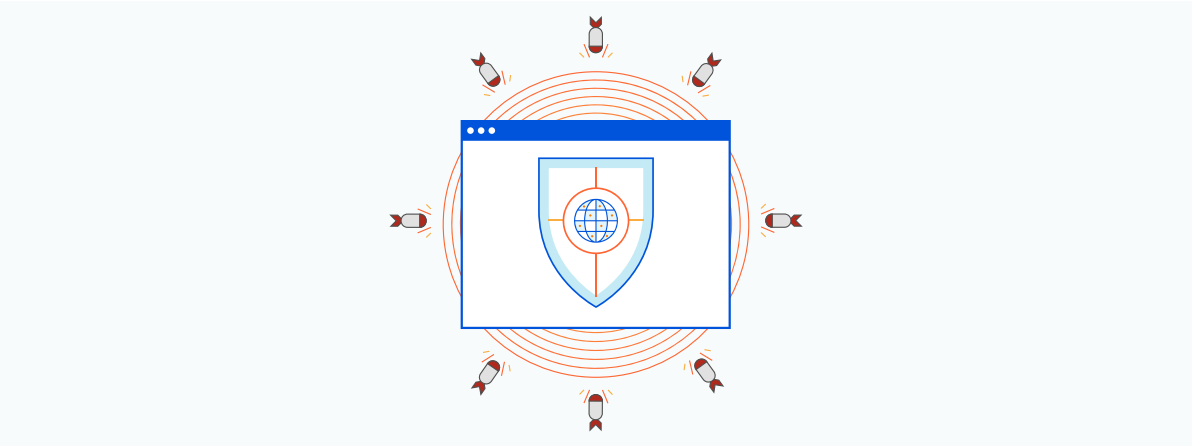
Les solutions d'équilibrage de charge dans le cloud contribuent à optimiser l'efficacité des serveurs en distribuant les requêtes sur plusieurs serveurs. La répartition du trafic sur plusieurs serveurs augmente ainsi la capacité globale, tout en réduisant les temps de chargement, en raison du traitement plus rapide des requêtes. Avec les solutions d'équilibrage de charge dans le cloud, les décisions d'équilibrage de charge sont prises à la périphérie du réseau, pour une rapidité optimale.

Les solutions d'équilibrage de charge dans le cloud permettent aux entreprises d'améliorer leurs temps de réponse et d'optimiser efficacement leur infrastructure, tout en minimisant le risque de défaillance de serveurs. Même en cas de défaillance d'un seul serveur, la solution d'équilibrage de charge peut rediriger et répartir le trafic parmi les serveurs restants, évitant ainsi aux clients de subir une latence importante ou une défaillance du site. Ce type de solution offre également la possibilité d'effectuer des contrôles d'intégrité actifs, afin de permettre aux entreprises d'identifier les serveurs moins performants et de prendre des mesures préventives avant qu'une défaillance ne se produise.

Lorsque vous choisissez une solution d'équilibrage de charge dans le cloud, cherchez un fournisseur proposant une fonctionnalité de basculement rapide. Le terme « basculement » désigne le processus consistant à rediriger le trafic d'un serveur défaillant vers un serveur pleinement opérationnel. Plus une solution d'équilibrage de charge fera preuve de rapidité en matière d'exécution du basculement, moins un site connaîtra d'interruptions de services et plus l'expérience de l'utilisateur se révélera satisfaisante.

En permettant d'éviter les pannes de serveur et d'accélérer les temps de chargement, l'équilibrage de la charge du trafic constitue un élément essentiel de la création d'une expérience en ligne positive. Une solution adaptée contribue également à la disponibilité d'un site ou d'une application pendant un pic de trafic. La préparation aux pics de trafic représente un aspect essentiel pour les start-ups, susceptibles de connaître des mouvements de trafic imprévisibles à mesure que leur activité se développe.

CONSEIL Nº 4



Protégez vos applications web contre les attaques malveillantes

Internet expose les entreprises fondées sur le web à un large éventail de menaces. Si n'importe quelle entreprise (indépendamment de sa taille) peut se retrouver paralysée des suites d'une attaque, une start-up doit généralement se battre davantage pour gagner la confiance des clients, ce qui place la réputation de sa marque dans une position plus précaire. La sécurité de son site web et des données de ses clients se révèle donc d'une importance vitale pour pérenniser durablement le succès d'une start-up. Dans un contexte de sécurisation des applications web et des autres propriétés essentielles à l'activité, une stratégie de sécurité à plusieurs niveaux peut vous aider à vous défendre contre de nombreux types de menaces.

A. Protection à l'aide d'un pare-feu d'applications web (WAF)

Un pare-feu d'applications web (WAF, Web Application Firewall) protège les applications web en filtrant et en surveillant le trafic HTTP. Avec ce type de pare-feu en place, les start-ups peuvent ainsi se défendre contre les attaques de type zero day et protéger leurs applications contre les menaces courantes, comme la falsification de requêtes intersites (CSRF), le cross-site scripting (XSS) et les attaques par injection SQL, susceptibles de compromettre les serveurs et de donner suite à un vol ou à une altération des données.

Un pare-feu WAF permet également aux entreprises de conserver un contrôle précis sur leurs politiques de sécurité, en définissant des règles visant à protéger les vulnérabilités de leurs applications et à défendre ces dernières contre les menaces émergentes. Les pare-feu WAF fondés sur le cloud constituent généralement la solution la plus flexible et la plus rentable à mettre en œuvre, car ils peuvent être mis à jour de manière constante afin de protéger l'utilisateur contre les nouvelles menaces sans accroître considérablement la charge en termes de travail ou de coût supplémentaire.

B. Protection contre les attaques DDoS

Une attaque par déni de service distribué (DDoS) constitue une tentative malveillante de surcharger les serveurs, les appareils, les réseaux ou l'infrastructure environnante sous un flot de trafic Internet illégitime. Ces attaques entraînent d'importantes interruptions de service et empêchent les clients d'effectuer des achats ou d'accéder aux ressources d'une entreprise.

De nombreux fournisseurs de solutions d'atténuation des attaques DDoS s'appuient sur l'une de ces deux méthodes pour arrêter une attaque : les centres de nettoyage (également appelés « scrubbing centers ») ou l'analyse et le filtrage sur site à l'aide d'équipements physiques. Le problème résultant de ces deux approches réside dans la génération d'une latence susceptible d'avoir une incidence négative sur l'entreprise.

Le « nettoyage » implique la redirection du trafic réseau vers des serveurs centralisés, afin d'en filtrer le trafic malveillant (le « nettoyer »). Le réacheminement de l'ensemble du trafic vers un centre de nettoyage géographiquement distant entraîne une latence supplémentaire considérable.

Une autre technique d'atténuation des attaques DDoS repose sur l'utilisation d'équipements physiques sur site pour analyser le trafic et filtrer les requêtes malveillantes. Comme pour le nettoyage, le matériel génère de la latence sur le réseau, car il redirige le trafic via les équipements dans le cadre du processus d'analyse.

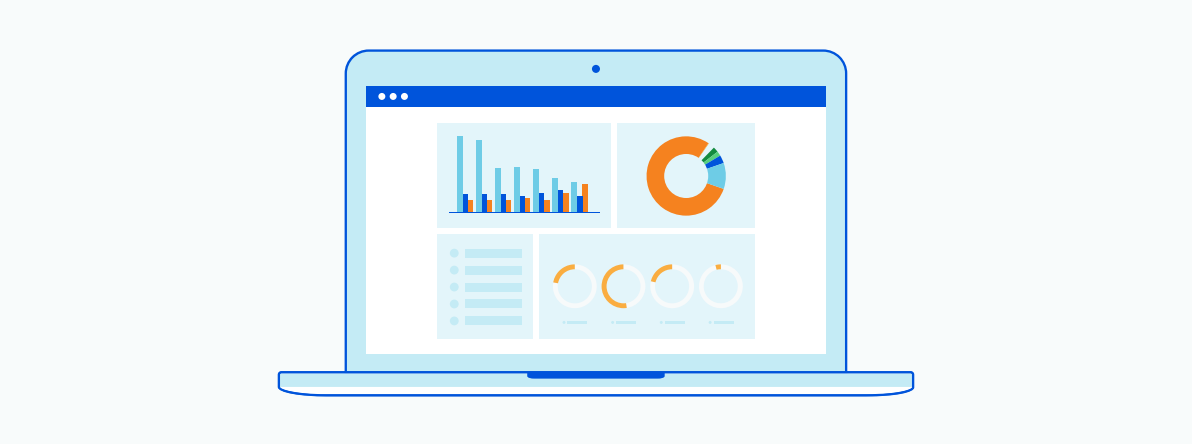
La meilleure façon de protéger votre réseau contre une attaque DDoS consiste à investir dans une solution d'atténuation des attaques DDoS qui n'a pas recours au « nettoyage » des données et ne repose pas sur des équipements physiques. Cherchez des fournisseurs disposant de réseaux étendus et de serveurs de capacité élevée, car ces facteurs leur permettent de protéger les propriétés Internet contre les attaques DDoS de grande ampleur. Les solutions d'atténuation des attaques DDoS les plus rapides se fondent sur des réseaux performants, qui leur permettent d'atténuer les attaques à la périphérie. En outre, comme les attaques DDoS s'appuient sur le volume de trafic pour surcharger un réseau, une solution d'atténuation puissante doit se montrer capable d'absorber une grande quantité de trafic pour protéger les propriétés Internet.

C. Atténuation des bots malveillants

De par leur activité, les bots malveillants peuvent compromettre les sites et les applications. Ces bots prennent souvent la forme de botnets, c'est-à-dire de réseaux d'équipements infectés travaillant de concert pour lancer différents types d'attaques. Voici quelques exemples d'actes de malveillance résultant couramment de l'activité des bots :

- **Infiltration de compte :** lors d'une attaque par infiltration de compte, un pirate tire parti d'identifiants volés (souvent à la suite d'une violation de données ou d'un achat illégal) afin de tenter d'accéder à un compte. Les auteurs de ce type d'attaque s'appuient sur le fait que de nombreuses personnes réutilisent leurs mots de passe et utilisent ainsi les identifiants associés à une plate-forme (un jeu, par exemple) pour accéder à des comptes plus lucratifs, comme les comptes bancaires. Les pirates passent par des bots pour automatiser ces tentatives de connexion dans l'espoir d'accéder à un plus grand nombre de comptes dans un court laps de temps.
- **Extraction de contenu :** certains bots peuvent « extraire » (c'est-à-dire, télécharger et dupliquer) le contenu d'un site. Les pirates se livrant à cette activité extraient du contenu afin d'augmenter le trafic organique vers leur site ou de tirer parti du référencement d'un autre site. Les attaques par extraction de contenu détournent une partie du trafic organique du site de la victime et dégradent la valeur du contenu original.
- **Fraude au clic :** les auteurs de ces attaques peuvent également programmer des bots afin de commettre une fraude au clic. Dans ce type d'activité, les bots interagissent avec un site web, une application ou une publicité en se comportant comme un visiteur légitime. En fonction du contexte de la fraude, les objectifs de cette dernière peuvent se révéler différents. Un pirate peut ainsi commettre une fraude au clic sur des annonces afin d'augmenter le budget publicitaire de la victime par l'intermédiaire d'un trafic illégitime.

Les bots malveillants peuvent saturer les serveurs web, fausser les données d'analyse, empêcher les utilisateurs d'accéder aux pages web, voler les données des utilisateurs et compromettre des fonctions opérationnelles essentielles. Le déploiement d'une solution de gestion des bots permet aux entreprises de distinguer l'activité des bots utiles de celle des bots nuisibles et d'empêcher les comportements malveillants de porter préjudice à l'expérience utilisateur.



Gardez un œil sur vos données d'analyse

Les start-ups changent souvent leur fusil d'épaule pendant la phase de détermination des solutions qui conviennent le mieux à leur activité, que ce soit en ajustant leur positionnement commercial ou en faisant évoluer leur infrastructure technique. Les données jouent un rôle essentiel dans le processus de prise de décision éclairée, indispensable au succès de ces changements de cap. Malheureusement, l'un des défis imposés par les déploiements multicloud ou hybrides réside dans l'absence de visibilité sur les données à l'échelle du réseau. En l'absence de données sur le réseau, les entreprises peuvent manquer des occasions d'accroître leurs performances ou de réagir aux tendances actuelles en matière de menaces.

Un fournisseur de solutions d'amélioration de la sécurité et des performances accompagnées d'une solide offre d'outils d'analyse permettra aux entreprises de disposer de données couvrant tous les aspects de leur infrastructure, de l'intégrité des serveurs au taux d'accès au cache. Le taux d'accès au cache décrit l'efficacité avec laquelle le cache répond aux requêtes de contenu. Ces informations offrent aux administrateurs la possibilité de mettre en œuvre des optimisations permettant d'éviter les interruptions et de réduire les coûts de bande passante.

CONSEIL Nº 6

Cherchez un fournisseur intégré

De nombreuses organisations doivent faire appel à plusieurs fournisseurs pour répondre à leurs besoins en matière de sécurité, de performances et de fiabilité. La gestion de plusieurs solutions ponctuelles peut cependant présenter certains défis pour la plupart des start-ups, en amplifiant la pression exercée par leurs moyens limités en termes de temps et de ressources. Pour commencer, l'accumulation de fournisseurs différents introduit une complexité inutile, car les équipes doivent se familiariser avec plusieurs solutions et apprendre à les utiliser. Par ailleurs, cette complexité entraîne bien souvent des dépenses inutiles, car les entreprises gèrent de nombreux contrats et ne sont probablement pas en mesure d'utiliser pleinement les outils.

La gestion de plusieurs fournisseurs engendre également un phénomène de cloisonnement des données, susceptible d'entraîner des failles de sécurité. Un pare-feu d'applications web (WAF) et une solution d'atténuation des attaques DDoS peuvent, par exemple, défendre les propriétés Internet contre des menaces bien distinctes. Un fournisseur intégré tirera toutefois parti de l'ensemble des données sur le réseau afin de protéger plus efficacement les propriétés Internet contre ces deux types d'attaques.

Il est tentant d'opter pour une combinaison des meilleures solutions ponctuelles disponibles sur le marché, mais l'association de ce type de solutions ne permet pas de bénéficier du niveau d'informations résultant d'une approche par couches, en plus d'imposer aux équipes la nécessité de gérer plusieurs outils individuels.

La réduction de la complexité chaque fois que l'opération est possible permet aux start-ups d'alléger la pression ressentie par les membres de l'équipe technique et de se recentrer sur la génération de revenus. Les solutions intégrées bénéficient en outre des informations offertes par la juxtaposition de différents produits. L'exhaustivité de ces dernières aide les entreprises à combler les failles susceptibles de les laisser vulnérables à de coûteuses violations de leur sécurité. La simplicité d'utilisation associée aux solutions intégrées permet également aux start-ups de gagner du temps et de se concentrer sur le développement de leur activité.

Conclusion

Pour offrir une expérience en ligne de qualité supérieure, les start-ups doivent accélérer la diffusion des contenus, assurer la fiabilité de leur réseau et protéger leurs propriétés web contre la défaillance des sites, le vol de données et d'autres attaques critiques. Il est particulièrement essentiel pour les start-ups de choisir des fournisseurs capables d'améliorer leur efficacité et de réduire la complexité. Les solutions intégrées reposant sur des réseaux solides permettent aux start-ups de protéger et d'accélérer leurs propriétés Internet sans compromettre leurs objectifs de croissance.

Soutenue par un réseau couvrant plus de 200 villes situées réparties dans plus de 100 pays à travers le monde, Cloudflare propose une plate-forme cloud mondiale, évolutive et intégrée, qui aide les start-ups à assurer la sécurité, les performances et la fiabilité de leurs applications sur site, dans le cloud et SaaS. Rendez-vous sur cloudflare.com/fr-fr/ pour découvrir comment protéger et sécuriser votre activité en ligne.