

5 bonnes pratiques à adopter pour préparer votre site d'e-commerce à la période des fêtes

INDEX

Introduction	3
Préparer votre site à un pic de trafic	3
Trouver l'équilibre entre un contenu riche et une expérience mobile optimale	3
Défendre votre site contre les attaques DDoS	4
Protéger votre site contre les bots malveillants	4
Sécuriser votre boutique à l'aide d'un pare-feu WAF	5
Conclusion	6

INTRODUCTION

Selon l'association américaine des commerçants, la [National Retail Federation \(NRF\)](#), les ventes en ligne réalisées pendant les fêtes de fin d'année augmentent plus rapidement que l'ensemble des ventes au détail. Ces dernières se sont ainsi élevées à un total de 787,1 milliards de dollars pour les mois de novembre et décembre 2020, soit une hausse de 8 % par rapport à la même période de l'exercice 2019. Les ventes en ligne, quant à elles, ont connu une croissance nettement plus rapide, avec une hausse de 22,6 % par rapport à 2019 pour un total de 206,9 milliards de dollars.

Si la croissance des ventes en ligne représente une opportunité pour les revendeurs de tirer profit des fêtes de fin d'année, elle engendre également un certain nombre de défis techniques. Les entreprises d'e-commerce doivent ainsi se tenir prêtes à :

- Préserver la disponibilité et la rapidité de leurs sites, notamment lors des pics de trafic.
- Développer des expériences d'achat intégrant le contenu riche (vidéos et images) attendu par les clients, sans sacrifier les performances.
- Protéger leurs sites et leurs clients contre les pirates opportunistes qui cherchent à dérober leurs données.

Les bonnes pratiques suivantes permettront aux entreprises de commerce électronique de s'assurer une période des fêtes lucrative et sans incident.

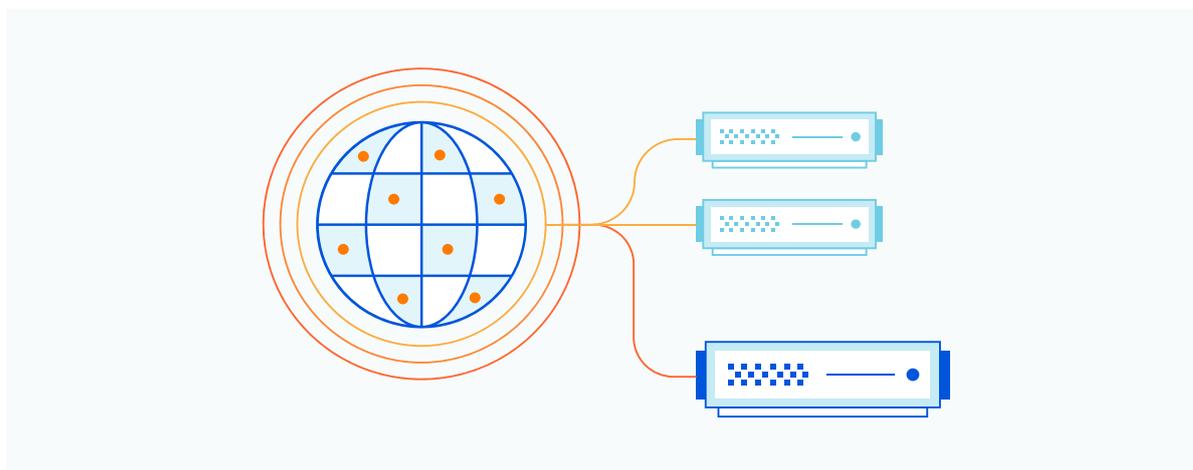
1. Préparer votre site à un pic de trafic

En raison de l'augmentation de l'activité durant cette période, les sites d'e-commerce doivent s'attendre à un pic de trafic. Ces événements liés aux fêtes de fin d'année peuvent mettre à rude épreuve la capacité des serveurs et dégrader leurs performances.

Si ces pics n'entraînent pas toujours l'arrêt complet d'un site d'e-commerce, la latence constitue néanmoins toujours un frein à l'achat. Certaines études estiment qu' [une seconde de latence suffit à induire une baisse du taux de conversion capable de s'élever jusqu'à 7 %](#). C'est pourquoi s'assurer que les sites d'e-commerce restent à la fois accessibles et réactifs constitue un aspect important de la préparation des fêtes.

Les services de répartition de charge peuvent améliorer la fiabilité et les performances de votre site, même pendant les pics d'affluence de fin d'année. En répartissant le trafic sur plusieurs serveurs, l'équilibrage de charge permet ainsi de diminuer les délais de traitement des requêtes.

Afin d'éviter les pannes et de réduire la latence, [Cloudflare Load Balancing](#) contrôle périodiquement l'intégrité des serveurs et protège ces derniers en procédant à un basculement rapide. Le produit vous permet également de définir des règles de redirection du trafic en fonction de différents facteurs, tels que la localisation géographique ou la disponibilité des serveurs, parmi bien d'autres.



En complément des solutions d'équilibrage de charge, les réseaux de diffusion de contenu ([CDN](#)) peuvent également contribuer à améliorer les performances de votre site en cas de pic de trafic. Un réseau CDN se présente sous la forme d'un groupe de serveurs distribués qui stockent et diffusent différents types de contenu statique aux utilisateurs finaux. Le stockage (ou la mise en cache) du contenu sur des serveurs distribués permet de réduire les temps de chargement, car le contenu est alors transmis par le serveur le plus proche de l'utilisateur.

La mise en cache de votre contenu à l'aide d'une solution comme le [réseau CDN de Cloudflare](#) libère de la bande passante, afin de vous faciliter la gestion des augmentations soudaines du trafic sur votre site d'e-commerce.

2. Trouver l'équilibre entre un contenu riche et une expérience mobile optimale

L'intégration d'images captivantes constitue un élément essentiel de l'expérience d'achat. Toutefois, [l'utilisation d'images de grande taille sur mobile](#) implique le téléchargement d'une grande quantité de données par les appareils des clients.

Il s'agit là d'un véritable défi pour les entreprises d'e-commerce, car un pourcentage important du trafic observé pendant les fêtes de fin d'année provient d'appareils mobiles. Selon BigCommerce, [43 % des achats effectués pendant la Cyber Week 2020](#) l'ont été depuis des smartphones. Afin de proposer une expérience d'achat satisfaisante, les revendeurs doivent donc atteindre un point d'équilibre entre la proposition de contenus riches et l'optimisation de l'expérience mobile.

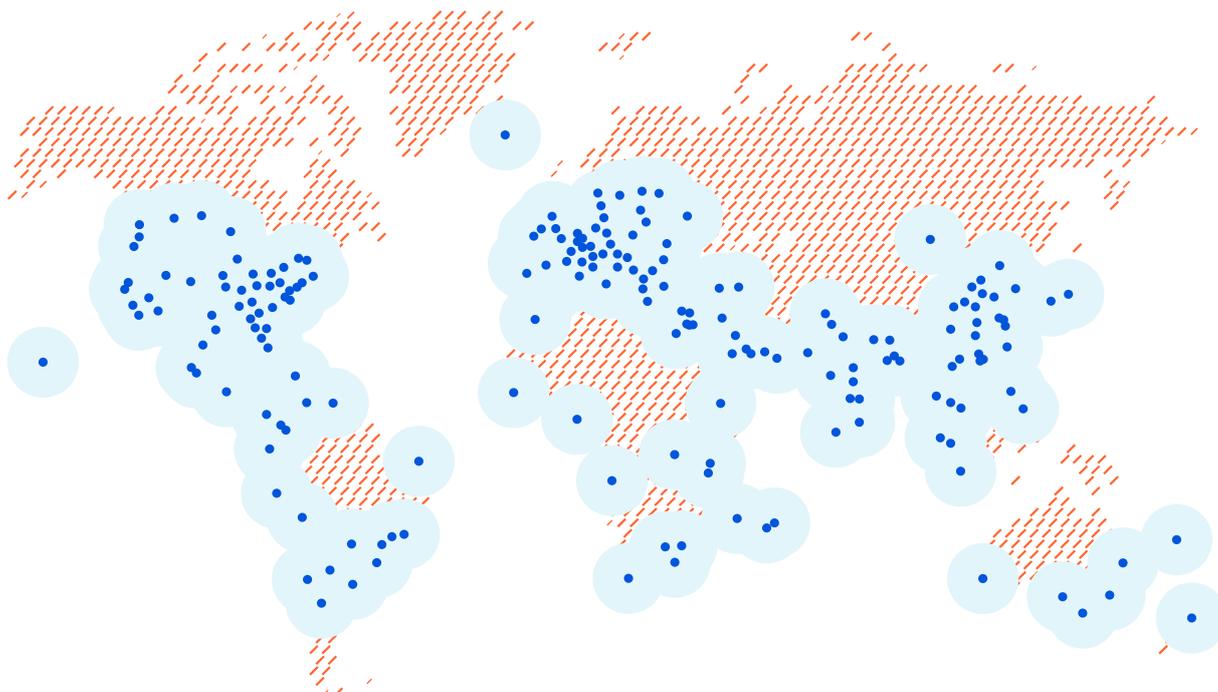
L'un des moyens d'optimiser cette dernière, sans en compromettre la richesse, consiste à utiliser un réseau CDN. Le [réseau CDN de Cloudflare](#) met les images en cache sur chaque serveur de notre réseau mondial, afin d'accélérer le chargement de votre site pour les acheteurs du monde entier, quel que soit l'appareil utilisé.

3. Défendre votre site contre les attaques DDoS

Les attaques par déni de service distribué (DDoS) bombardent les sites ou les applications de trafic indésirable afin de dégrader leurs performances ou d'entraîner leur mise hors ligne. Une attaque DDoS peut se révéler particulièrement préjudiciable lors d'une période particulièrement rentable, comme la fin d'année. Malheureusement, [les attaques DDoS ne sont que trop fréquentes pendant les fêtes](#).

Une solution d'atténuation des attaques DDoS participe à la protection de votre site, application ou réseau. Avec la tendance des attaques DDoS à [utiliser de nouveaux vecteurs et, dans certains cas, gagner en persistance](#), se protéger contre les attaques de grande ampleur et les différents vecteurs d'attaque devient une nécessité toujours plus croissante.

Grâce à son réseau d'une capacité de 67 Tb/s, la [protection anti-DDoS de Cloudflare](#) peut préserver les sites de vente en ligne contre les attaques les plus vastes. Nos services bénéficient en outre d'un système d'information sur les menaces résultant de la protection de près de 25 millions de propriétés Internet. Malgré l'augmentation de la taille et de la sophistication des attaques, Cloudflare peut protéger votre activité d'e-commerce en vous aidant à prévenir les pannes et en veillant à ce que vos clients légitimes puissent accéder à votre contenu.



4. Protéger votre site contre les bots malveillants

Les « [Grinch bots](#) », c'est-à-dire les bots d'accaparement d'inventaire qui sévissent pendant la période des fêtes, constituent un autre risque de sécurité auquel les entreprises de vente en ligne doivent se préparer. [Walmart a ainsi déclaré avoir bloqué des millions de tentatives d'attaques par bots](#) dans la première demi-heure suivant la mise en vente de la console de jeu PlayStation 5 à la fin de l'année 2020.

Les pirates s'appuient sur des bots malveillants pour lancer, entre autres, des attaques par infiltration ou usurpation de compte. Les bots d'infiltration de compte tentent, par exemple, d'accéder à des comptes à l'aide d'identifiants volés en masse. Dans le cas des attaques par usurpation de compte, les bots s'emparent directement des comptes afin d'accéder aux données personnelles, comme les informations de paiement. Ces attaques peuvent compromettre les données des clients et empêcher les utilisateurs légitimes d'accéder à votre site. Si l'utilisation de [CAPTCHA](#) peut contribuer à bloquer les bots, un service de gestion des bots permet aux propriétaires de sites de mieux contrôler l'activité des bons et des mauvais bots.

La solution de [gestion des bots de Cloudflare](#) met à profit les données issues de près de 25 millions de propriétés Internet pour identifier et bloquer les bots malveillants. Aisément configurable afin de répondre aux besoins de votre activité de commerce électronique, ce produit ne nécessite pas de code JavaScript et peut donc être déployé rapidement.

5. Sécuriser votre boutique à l'aide d'un pare-feu WAF

Les entreprises de vente en ligne doivent protéger leurs sites contre plusieurs [attaques courantes sur la couche applicative](#), comme le Cross-Site Scripting (XSS) et l'injection SQL. Lors d'une attaque XSS, les pirates recourent à l'injection de code pour dérober les cookies de leurs victimes et se faire passer pour elles en ligne. Les attaques par injection SQL emploient également une technique d'injection de code, mais visent à voler ou modifier les données contenues dans les bases de données SQL.

Outre les considérations relatives aux vulnérabilités, les entreprises d'e-commerce doivent également protéger les données des clients et respecter les [exigences de la norme PCI-DSS](#) (Payment Card Industry Data Security Standard). L'une de ces contraintes impose, par exemple, l'utilisation d'un pare-feu d'applications web (WAF), c'est-à-dire une protection permettant de surveiller et de filtrer le trafic HTTP circulant d'Internet vers une application web afin de bloquer les attaques par Cross-Site Scripting et injection SQL, entre autres menaces.

Grâce à sa présence au sein du réseau soutenant déjà les solutions d'atténuation des attaques DDoS et de gestion des bots de Cloudflare, le [pare-feu WAF](#) bénéficie des informations issues de ce même réseau. Son intégration aux autres services d'amélioration de la sécurité et des performances de Cloudflare lui permet également d'offrir une expérience utilisateur parfaitement fluide. Le pare-feu WAF de Cloudflare peut non seulement aider les entreprises de vente en ligne à respecter les obligations liées à la norme PCI-DSS, mais aussi à se protéger contre les attaques les plus courantes pendant les fêtes et tout au long de l'année.

Cloudflare at a Glance



Conclusion

Les fêtes de fin d'année peuvent avoir un impact positif sur le chiffre d'affaires annuel des entreprises d'e-commerce. Toutefois, les pirates ne connaissent pas le repos et la préparation de la période nécessite donc une protection renforcée. De même, l'augmentation du trafic requiert certains efforts de consolidation sur le plan technique.

Qu'il s'agisse de vous protéger contre les attaques DDoS ou d'éviter la surcharge de vos serveurs, une préparation réussie des fêtes de fin d'année nécessite une stratégie globale. Fort heureusement, les solutions intégrées de Cloudflare peuvent vous aider à préserver la disponibilité, les performances et la sécurité de votre site de commerce électronique.

Cliquez sur le lien suivant pour en apprendre davantage sur les solutions Cloudflare pour l'e-commerce :

<https://www.cloudflare.com/fr-fr/ecommerce/>



© 2021 Cloudflare Inc. Tous droits réservés. Le logo Cloudflare est une marque commerciale de Cloudflare. Tous les autres noms de produits et d'entreprises peuvent être des marques des sociétés respectives auxquelles ils sont associés.