CLOUDFLARE®

Guide de survie du fournisseur SaaS

Principes élémentaires en matière de performances, de sécurité et de chiffrement pour les applications en ligne

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

Résumé

Le marché SaaS devrait connaître une croissance de 196 % entre 2016 et 2020.[1] Tandis que ce marché continue d'augmenter et de s'imposer comme une composante à part entière de l'infrastructure commerciale, la sécurité et les performances restent les principales préoccupations des fournisseurs SaaS et de leurs clients. Face à cette croissance, les fournisseurs SaaS devront se livrer à une concurrence acharnée pour fournir à leurs clients les applications les plus sûres et les plus performantes. Les applications sous-performantes et vulnérables aux attaques affectent inévitablement les revenus, l'implication des utilisateurs finaux, la réputation et le taux d'attrition. Pour pouvoir proposer des domaines personnalisés de marque à leurs clients, une partie importante des fournisseurs SaaS doit gérer les cycles de vie SSL manuellement, ce qui entraîne de longs temps de déploiement et des coûts élevés. D'un autre côté, l'élaboration d'une solution complexe automatisée en interne empêche les ressources d'ingénierie de se concentrer sur le cœur de compétence.

La solution Cloudflare de performances et de sécurité pour les fournisseurs SaaS protège les fournisseurs autant que les clients et les visiteurs finaux, et dynamise leur expérience. Combiné au routage intelligent Argo, à l'équilibrage de charge et aux optimisations des performances, le réseau de diffusion de contenu (CDN) global de 10 Tbits/s de Cloudflare réduit jusqu'à deux fois la latence des visiteurs. Utilisée en parallèle avec la limitation du débit et un pare-feu applicatif Web (WAF), la protection DDoS avancée de Cloudflare atténue autant les attaques volumétriques d'envergure que les attaques complexes qui visent les couches réseau, transport et application. De plus, les fournisseurs SaaS ont la possibilité de sécuriser le transfert des données client à l'aide d'une solution SSL pour les domaines personnalisés facile à déployer et entièrement gérée.

Impacts commerciaux de la latence et d'une sécurité insuffisante

La latence et une sécurité insuffisante peuvent avoir de lourdes conséquences dans le cas des applications SaaS : expériences client négatives, faibles taux de conversion et mauvais classement dans les moteurs de recherche, ainsi que pertes de revenu et augmentation du taux d'attrition.

Impacts des performances et de la disponibilité sur l'implication vis-à-vis des applications SaaS

Les clients exigent une expérience rapide et hautement disponible lorsqu'ils se tournent vers un site Web, une application ou une API. Lorsque les ressources en ligne sont lentes ou indisponibles, l'implication vis-à-vis des applications SaaS et le taux de conversion en pâtissent de manière significative.

À titre d'exemple, Google indique que 100 à 400 millisecondes de latence supplémentaire suffisent pour modifier significativement le comportement des consommateurs [1]. Walmart a enregistré un taux de conversion inférieur après que le temps de chargement du site a augmenté de quelques secondes seulement[2]. De même, Amazon a observé qu'une diminution de 100 millisecondes de la latence de leur site avait entraîné une hausse de 1 % des revenus.[3]

Généralement, les problèmes de performances des applications SaaS sont liés à des facteurs internes nuisant à l'infrastructure d'hébergement partagée du fournisseur SaaS ou à la configuration de l'application. La distance physique entre les visiteurs et les emplacements des serveurs d'origine des applications fait partie de ces facteurs. On estime que 160 km ajoutent 0,82 milliseconde de latence supplémentaire.[4] Et la latence augmente encore lorsqu'à la distance s'ajoute un contenu statique, lourd et non optimisé.

Toutefois, les performances ne sont pas uniquement déterminées par les serveurs, les réseaux et les applications. Elles dépendent également des pics de trafic, saisonniers ou non, qui peuvent surcharger l'infrastructure partagée, rendant les applications plus lentes, voire complètement indisponibles.

Les applications SaaS qui chargent lentement ou ne sont pas disponibles peuvent avoir un impact dramatique sur les revenus, les taux de conversion et de rebond, le référencement dans les moteurs de recherche, la réputation, la satisfaction client et les contrats de niveau de service (SLA).

[1] http://www.sfgate.com/business/article/Google-s-speed-need-instantaneous-Internet-3251049.php
[2] https://www.slideshare.net/devonauerswald/walmart-pagespeedslide
[3] https://blog.gigaspaces.com/amazon-found-every-100ms-of-latency-cost-them-1-in-sales/
[4] http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

L'impact d'une attaque ciblée contre les applications SaaS

Qu'il s'agisse d'un nouveau fournisseur SaaS entrant sur le marché ou d'un éditeur de logiciel éprouvé qui transfère une application locale vers le cloud, l'influence d'une application en ligne sur la sécurité doit être prise en compte.

Les applications et services SaaS deviennent plus vulnérables une fois exposés à l'Internet public et, dans la plupart des cas, aux charges de travail étendues à travers les infrastructures partagées. Les vecteurs d'attaque pour un fournisseur SaaS comptent notamment les portails de connexion, l'hébergement et les DNS partagés, ainsi que les vulnérabilités d'application complexes. Par ailleurs, de nombreux fournisseurs SaaS hébergent plusieurs applications client au sein d'une infrastructure partagée ; chaque fuite de donnée, incident de fiabilité ou attaque subie par l'infrastructure partagée entraîne des retombées négatives pour les autres clients.

Les attaques spécifiques qui ciblent les vecteurs mentionnés ci-dessus comprennent les attaques DDoS volumétriques et complexes, les tentatives de connexion par force brute, l'exploitation des vulnérabilités d'application et l'interception des données client non chiffrées. Elles visent les sites Web, les applications et les API sur différents types d'appareils. Si une attaque réussit, les répercussions commerciales vont de l'interruption des services aux pertes de revenu majeures et aux coûts de limitation des dégâts, en passant par la dégradation de la marque et l'attrition des clients.

En 2013, des pirates ont infiltré Adobe, obtenant un accès aux informations de carte de crédit et aux autres données personnelles de 2,9 millions de clients.[5] Le responsable de la sécurité d'Adobe, Brad Arkin, s'était alors montré conscient des risques du commerce en ligne, affirmant : « les cyberattaques sont l'une des tristes réalités des activités commerciales à l'heure actuelle ».

Le 16 octobre 2016, Airbnb, Amazon.com, Netflix, The New York Times, PayPal, Pinterest, Reddit, Tumblr, Twitter, Verizon, Visa, The Wall Street Journal, Yelp, Zillow et d'autres sites ont subi une panne prolongée à cause d'une attaque de Mirai, un botnet tristement célèbre. L'attaque n'a pas directement visé les applications elles-mêmes, mais Dyn, le fournisseur de services DNS partagé par ces sites Web et applications. Il a fallu 11 heures pour que Dyn vienne à bout de l'incident et rétablisse le fonctionnement normal des services des sites Web touchés.[6]

Chiffrement ou domaine personnalisé ?

L'adoption du chiffrement SSL/TLS est devenue l'une des pratiques idéales en matière de sécurité pour les organisations en ligne. Et avec les efforts déployés par les géants de la technologie pour construire un Internet plus sûr, elle est de plus en plus souvent considérée comme une nécessité. À la fin de l'année 2016, par exemple, le navigateur Web Google Chrome a commencé à signaler les sites Web qui n'utilisent pas HTTPS comme « Non sécurisés » à ses utilisateurs.[7] Apple exige également que toutes les applications iOS soient dotées de connexions HTTPS pour qu'elles soient publiées sur l'App Store.[8]

À l'aube du SSL, les organisations en ligne étaient confrontées à un dilemme : chiffrer le trafic à l'aide du protocole HTTPS ou offrir à leurs visiteurs des performances à la hauteur de leurs attentes. Il y a quelques années encore, le protocole SSL provoquait une augmentation de la latence, tout en altérant les performances des sites Web et applications. Et même si une organisation décidait de sacrifier ses performances par souci de sécurité, les difficultés opérationnelles de la mise en œuvre du SSL limitaient à l'époque son adoption à grande échelle. Grâce aux améliorations modernes du SSL comme le développement de HTTP/2 (successeur de HTTP 1.1), l'utilisation du SSL pour sécuriser le trafic via HTTP permet d'atteindre des performances supérieures à celles du HTTP non chiffré.

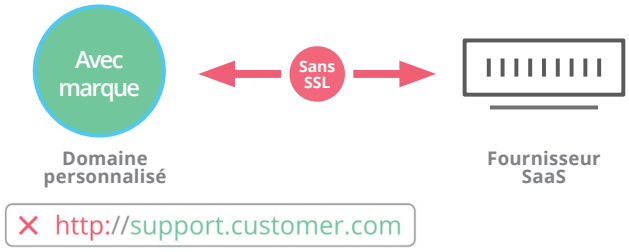
Le choix cornélien entre sécurité et performances auquel devaient faire face les organisations par le passé a changé de nature : une grande partie des fournisseurs SaaS doivent aujourd'hui choisir entre le chiffrement du trafic de leur client et la prise en charge des domaines personnalisés des clients. L'un comme l'autre sont nécessaires pour profiter à la fois d'une représentation adéquate, d'une sécurité suffisante, d'un bon classement dans les résultats des moteurs de recherche et des meilleures performances.

[5] http://www.nytimes.com/2013/10/04/technology/adobe-announces-security-breach.html
[6] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[7] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/
[8] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/

Ces fournisseurs SaaS offrent généralement à leurs clients la possibilité de créer des ressources en ligne destinées au public, comme des pages d'accueil, des sites Web, des portails de support, etc. Bien souvent, les fournisseurs SaaS hébergent les nouvelles ressources client dans un sous-domaine, et non dans leur domaine principal. Par exemple, l'URL d'une ressource créée par le client d'un fournisseur SaaS peut ressembler à **sociétéduclient.fournisseursaas.com**, au lieu d'une URL personnalisée avec marque comme **sociétéduclient.com** ou **support.sociétéduclient.com**. C'est problématique pour les clients, car l'absence de marque entraîne une diminution de la représentation, des résultats dans les moteurs de recherche et de la confiance des visiteurs.

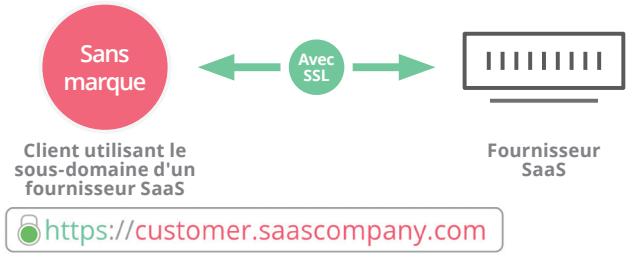
Les fournisseurs SaaS et leurs clients ont répondu aux défis des marques en ajoutant les URL sociétéduclient.com ou support.sociétéduclient.com par CNAME à sociétéduclient.fournisseursaas.com. Le client peut ainsi utiliser son propre domaine personnalisé. En revanche, le fournisseur SaaS ne peut plus activer facilement le SSL et éprouvera des difficultés à gérer tout le processus de cycle de vie SSL. Tant la gestion manuelle du cycle de vie SSL que l'élaboration d'une solution en interne pour les clients finaux sont coûteuses et nécessitent un investissement en temps et des efforts manuels importants.

Face aux défis cités ci-dessus, les fournisseurs SaaS peuvent se retrouver dans trois situations différentes :



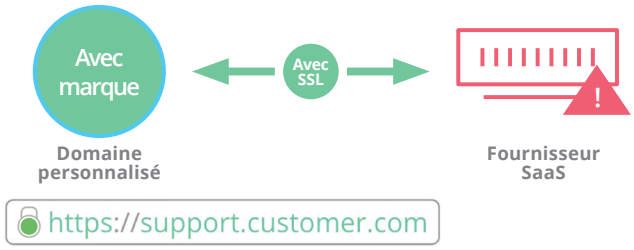
DOMAINE PERSONNALISÉ NON CHIFFRÉ, MAIS AVEC MARQUE

Les domaines personnalisés sans SSL ne bénéficient pas des avantages de performances liés au protocole ni du transfert sécurisé des données. Ils sont donc vulnérables au snooping, ainsi qu'à la modification et l'injection du contenu avant qu'il atteigne les visiteurs.



DOMAINE CHIFFRÉ, MAIS SANS MARQUE

Les domaines pour qui le SSL a été activé via un fournisseur SaaS n'ont pas de nom de domaine personnalisé, ce qui porte atteinte à leur image de marque et les fait descendre dans le classement des résultats des moteurs de recherche.

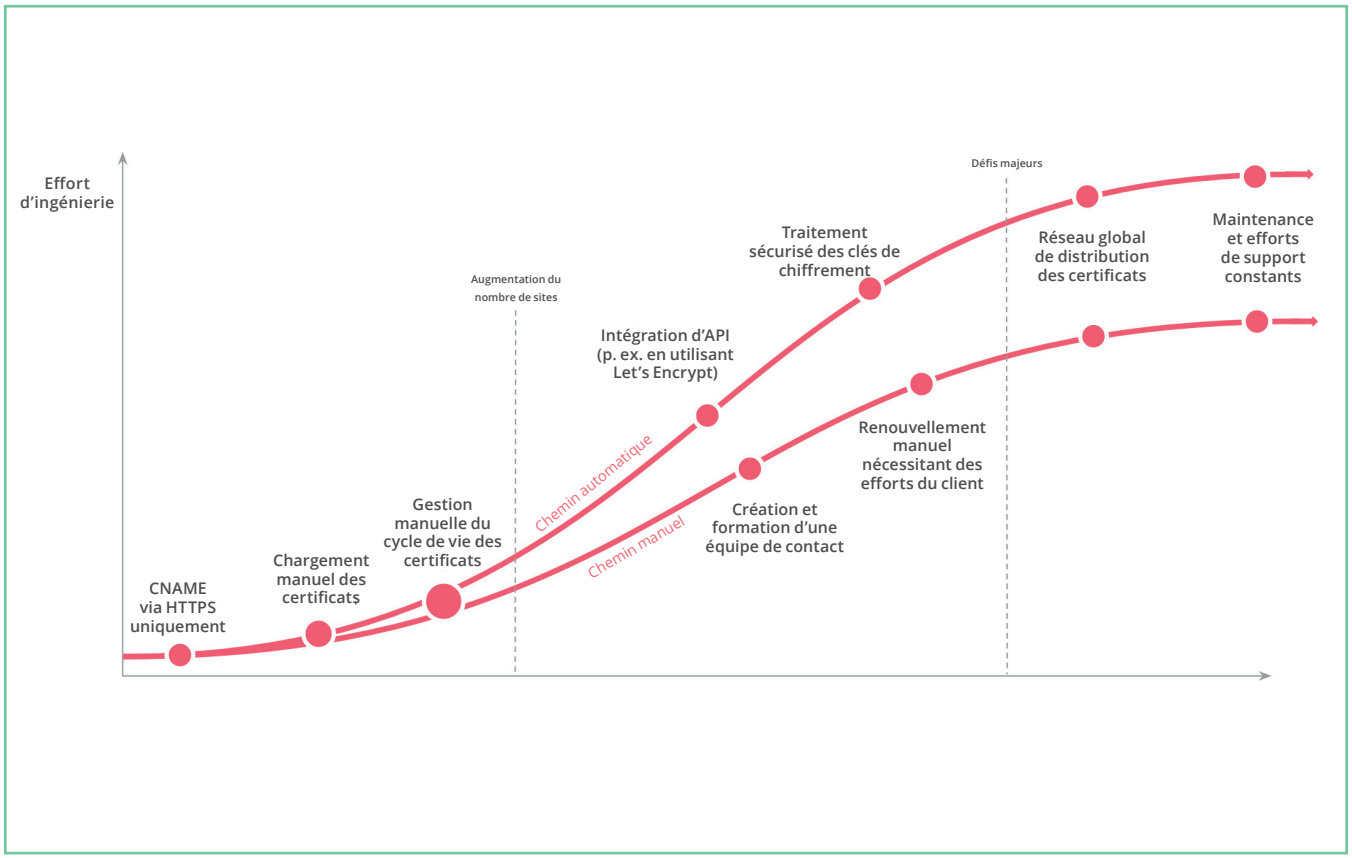


APPROCHE EN INTERNE COMPLIQUÉE

Les fournisseurs SaaS qui veulent des domaines personnalisés avec marque et chiffrement peuvent soit gérer manuellement les cycles de vie des certificats SSL, provoquant l'allongement des temps de déploiement et l'augmentation des coûts, soit construire une solution automatisée complexe en interne.

Il est important de prendre en compte les défis techniques qui attendent les fournisseurs SaaS lors de l'élaboration d'une solution en interne pour gérer le SSL pour les domaines de leurs clients. Le graphique ci-dessous illustre le plan d'action habituel des fournisseurs SaaS qui essaient d'élaborer une solution SSL automatisée en interne.

Pour ce faire, il y a deux chemins possibles, mais aucun d'eux n'est idéal. Le premier chemin (en haut) automatise le processus SSL, mais exige un travail d'ingénierie conséquent et présente des défis complexes. Le second demande à la fois des efforts manuels de la part du fournisseur SaaS et du client final.



Sécurité, performances et disponibilité pour les applications SaaS avec Cloudflare

Cloudflare améliore l'expérience des utilisateurs finaux des sites Web, des applications et des API des fournisseurs SaaS en réduisant la latence et en optimisant les performances de distribution de contenu ; Cloudflare offre les mêmes avantages aux clients finaux des ressources Internet.

Présence mondiale garantie

Le réseau de distribution de contenu (CDN) global Anycast de 117+5 datacenters répartis dans 57 pays, qui se trouve au cœur de la solution Cloudflare, rapproche le contenu des applications SaaS des visiteurs de chaque région. Cloudflare assure également le fonctionnement de 38 % des domaines DNS gérés et gère l'un des réseaux DNS autoritaires les plus étendus du monde. Avec une vitesse de requête de quelques millisecondes en moyenne, Cloudflare offre des performances globales supérieures à tous les autres fournisseurs de DNS géré.

Applications disponibles à grande échelle

Déployé sur l'infrastructure DNS hautement disponible de Cloudflare et le réseau global Anycast™, l'équilibrage de charge de Cloudflare réduit la latence en équilibrant la charge du trafic entre différents serveurs et en acheminant le trafic vers la région géographique la plus proche. L'équilibre de charge comprend des contrôles d'intégrité avec basculement rapide pour réagir rapidement aux défaillances et permettre aux visiteurs de les éviter. De plus, il peut être utilisé avec plusieurs fournisseurs de services cloud ou une infrastructure sur site pour réduire l'impact des interruptions provoquées par un seul fournisseur ou serveur, tout en laissant le choix de prestataire cloud.

Expérience plus rapide pour les visiteurs

Le CDN de Cloudflare est doté d'optimisations avancées, notamment l'auto-minimisation de HTML, CSS et JavaScript, ainsi que la compression Gzip qui permet de réduire de plus de 20 % la taille des fichiers et des ressources. Et avec les optimisations propriétaires pour les images et le mobile, les performances de vos applications SaaS passent au niveau supérieur.

Tandis qu'il fournit 10 % du trafic Internet mondial, Cloudflare analyse en temps réel l'état de santé et de fiabilité réel des chemins de réseau. L'algorithme du routage intelligent Argo de Cloudflare utilise ces informations pour orienter le trafic vers les chemins les plus rapides, tout en maintenant des connexions ouvertes et sûres afin d'éviter la latence imposée par certaines configurations. En moyenne, le routage intelligent Argo réduit la latence de 35 % supplémentaires et les erreurs de connexion de 27 %.

> « Cloudflare a optimisé la qualité de service et minimisé le temps de réponse de Crisp. C'est une uniformisation d'infrastructures réseau coûteuses au profit du grand public. On ne peut plus s'en passer. »

crisp™

Valérian Saliou
Directeur de la technologie de Crisp

Protéger les applications SaaS et les données client

La solution Cloudflare de sécurité orientée cloud protège les sites Web, les applications et les API des fournisseurs SaaS, mais aussi les ressources Internet des clients finaux.

Avec son débit de 10 Tbits/s, le réseau Anycast mondial de plus de 117 datacenters de Cloudflare est dix fois plus étendu que la plus grande attaque DDoS jamais enregistrée. Il offre donc une protection contre les attaques ciblant les couches 3, 4 et 7 du modèle OSI. Combinée à la limitation de débit et au pare-feu applicatif Web (WAF), la solution de sécurité de Cloudflare atténue également les attaques complexes contre la couche application. Et avec le SSL pour SaaS de Cloudflare, les fournisseurs SaaS et leurs clients finaux peuvent à la fois compter sur des communications chiffrées qui les protègent de l'interception des données et de l'injection de contenu malveillant, et continuer d'utiliser des domaines personnalisés.

Protéger et sécuriser les données client sensibles

Les applications SaaS contiennent de plus en plus de données personnelles et commerciales sensibles, il est donc impératif d'assurer leur protection contre les tentatives de connexion par force brute, les fuites de données et les attaques de l'homme du milieu.

Le pare-feu applicatif Web (WAF) de Cloudflare offre une première protection contre ces attaques : il atténue les attaques complexes visant la couche application. Par défaut, le WAF de Cloudflare comprend une protection contre les dix vulnérabilités les plus fréquentes identifiées par l'OWASP, mais aussi contre les failles spécifiques à certaines applications qui touchent des intégrations et langages usuels, comme : PHP, Magento, WordPress, Drupal, Atlassian parmi d'autres. Le WAF de Cloudflare permet aux fournisseurs SaaS de créer des ensembles de règles sur le moment pour réagir aux nouveaux vecteurs d'attaque et vulnérabilités, tout en propageant les règles à travers le réseau Cloudflare en moins de 30 secondes.

Parallèlement à la protection DDoS de Cloudflare, la limitation de débit garantit un contrôle affiné pour bloquer les visiteurs dont le débit de requêtes est suspect. La limitation de débit sert à empêcher les tentatives de connexion par force brute qui ont pour objectif d'atteindre les zones non autorisées d'une application ou d'un site Web. Cette fonctionnalité limite le nombre de requêtes envoyées par une même adresse IP, à un point terminal particulier, pour une période déterminée.

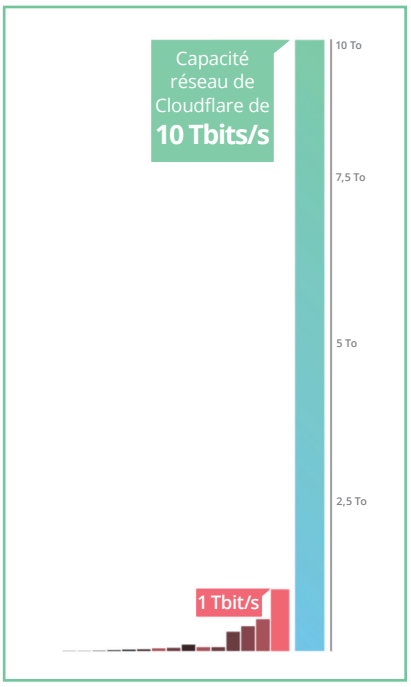
« Les solutions Cloudflare fonctionnent, c'est tout. Leur équipe a satisfait toutes nos demandes, et la mise en œuvre des personnalisations s'est faite quasi instantanément. »

zendesk | **Amanda Kleha, Directrice générale**
Unité des services en ligne de Zendesk

Le SSL pour SaaS de Cloudflare est le meilleur moyen d'automatiser la gestion des certificats SSL/TLS pour les domaines personnalisés avec CNAME, ce qui garantit une protection sans faille contre l'interception des données par attaque de l'homme du milieu, ou contre le snooping du trafic causé par des connexions non chiffrées.

Garantir la disponibilité en bloquant le trafic malveillant

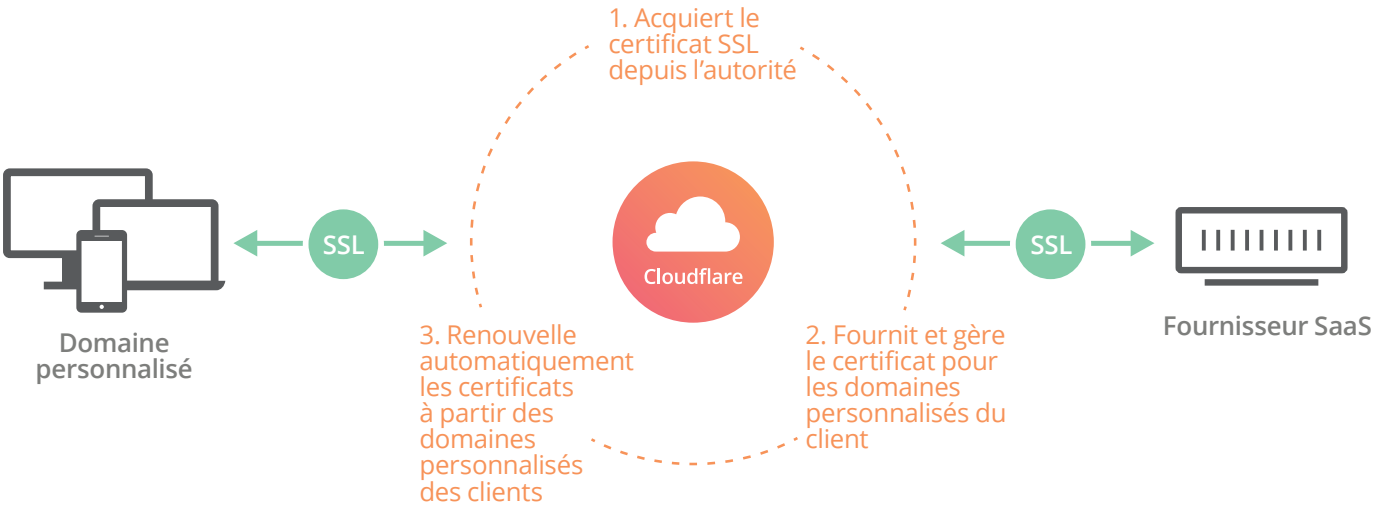
Le vol ou la perte de données client sensibles peut être désastreux, mais une attaque visant la disponibilité de vos services n'est pas moins catastrophique. La pierre angulaire de Cloudflare est son réseau de distribution de contenu (CDN) global de plus de 117 datacenters répartis dans 57 pays différents. Le débit total de ce réseau dépasse 10 Tbits/s, c'est-à-dire dix fois plus que l'attaque DDoS la plus étendue jamais enregistrée. Toute tentative d'attaque volumétrique contre les couches 3, 4 et 7 est absorbée et distribuée uniformément à travers le réseau Cloudflare, assurant aux clients SaaS une disponibilité ininterrompue. La solution de limitation de débit de Cloudflare fonctionne en parallèle avec la protection DDoS pour un contrôle affiné, ce qui permet de bloquer les visiteurs dont le débit de requêtes est suspect. Lorsqu'une adresse IP spécifique dépasse les seuils définis, il est possible de l'empêcher d'envoyer des requêtes supplémentaires vers un point terminal particulier, pour une période déterminée.



Une solution SSL automatisée pour les fournisseurs SaaS

Le SSL pour SaaS offre aux fournisseurs SaaS la possibilité d'élargir les avantages de Cloudflare en matière de performances et de sécurité aux clients finaux qui possèdent leurs propres domaines personnalisés. La solution SSL de Cloudflare pour les fournisseurs SaaS permet

aux clients de continuer à doter leurs domaines personnalisés d'un CNAME sur le sous-domaine du fournisseur SaaS et de profiter des avantages d'une URL avec marque, pendant que Cloudflare active et gère le cycle de vie complet des certificats SSL pour les fournisseurs SaaS et leurs clients. En activant le protocole SSL sur les domaines des clients, vous tranquillisez les visiteurs, vous optimisez le classement dans les moteurs de recherche et vous débloquez le protocole HTTP/2 moderne, ce qui améliore encore votre vitesse.



Expérience visiteur marquée

Les clients des fournisseurs SaaS peuvent continuer à utiliser leurs domaines personnalisés, tout en profitant des avantages d'un certificat SSL entièrement pris en charge. Les domaines personnalisés avec CNAME améliorent la visibilité des clients SaaS et leur classement dans les moteurs de recherche, tout en mettant les visiteurs du site Web ou de l'application en pleine confiance.

Ressources clients sécurisées et performantes

Le SSL pour SaaS permet d'ajouter des certificats SSL/TLS dédiés aux domaines personnalisés avec CNAME. Grâce à HTTPS, les données client sensibles sont transférées de manière sécurisée et protégées contre les attaques de l'homme du milieu et du snooping de réseau. Une fois le SSL activé, le protocole HTTP/2 devient disponible pour augmenter encore votre rapidité.

Gestion automatisée des cycles de vie et déploiements SSL rapides

Cloudflare s'occupe du cycle de vie complet des SSL pour le domaine personnalisé avec CNAME d'un client SaaS : de la création d'une clé privée à la protection par validation de domaine, l'émission, le renouvellement et la réémission. Le fournisseur SaaS et son client final n'ont plus à s'inquiéter de la gestion du cycle de vie SSL. Lors de l'émission du SSL, Cloudflare transmet les requêtes de nouveau certificat et active HTTPS en quelques minutes seulement.

« En tant qu'ingénieur, rien ne me ravit plus que de travailler avec Cloudflare. »

UDACITY

Paul Bauer
Ingénieur plateformes chez Udacity

Conclusions

Inscrivez-vous sur Cloudflare pour améliorer les performances et la sécurité de vos applications SaaS, tout en déployant facilement le SSL pour les URL personnalisées avec CNAME de vos clients finaux. La configuration est aisée et prend généralement moins de 5 minutes. Consultez nos offres, de gratuite à Entreprise, sur www.cloudflare.com/fr/plans/ et rendez-vous sur www.cloudflare.com/fr/saas/ pour en savoir plus sur Cloudflare pour les fournisseurs SaaS.

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