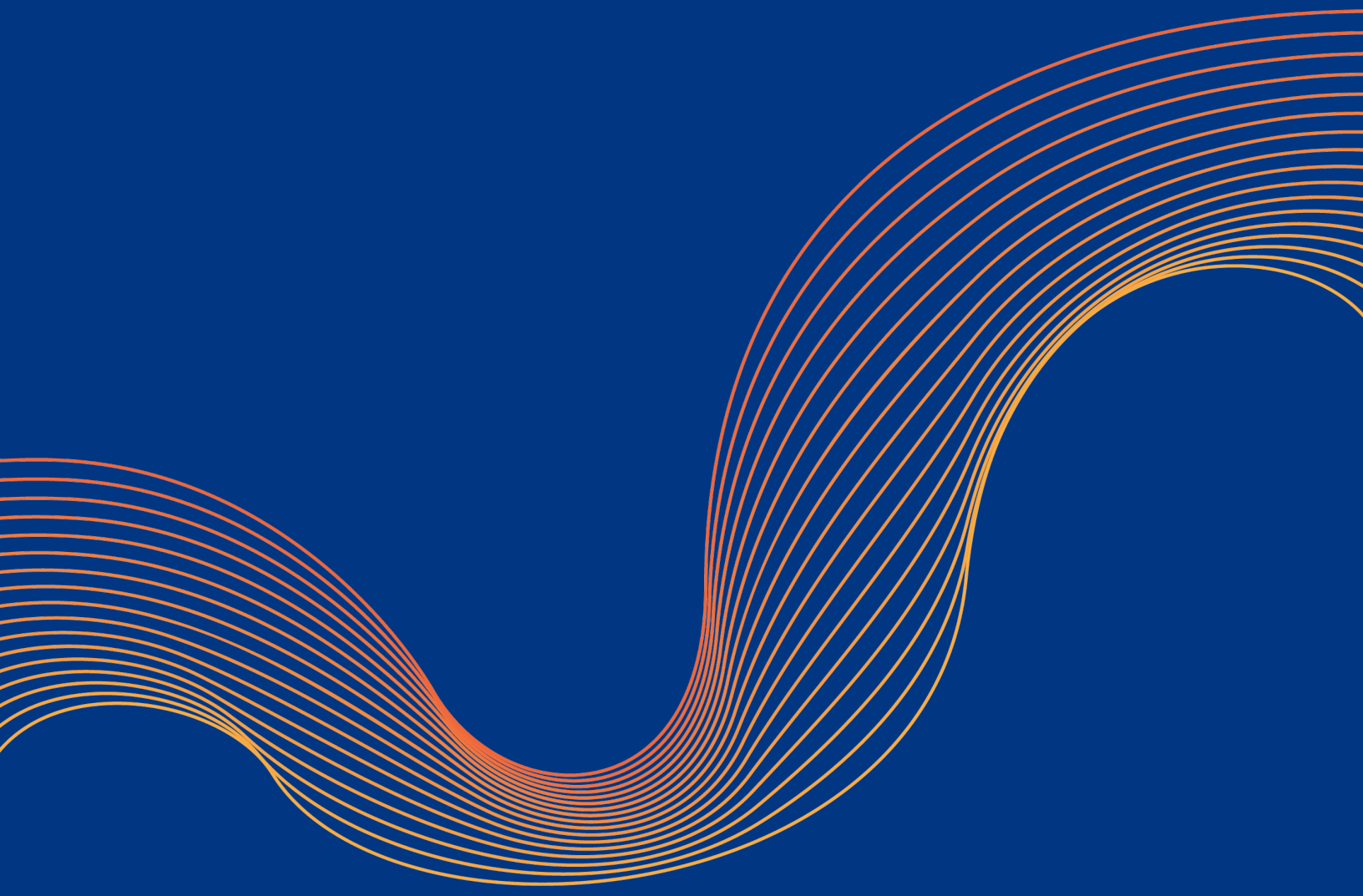
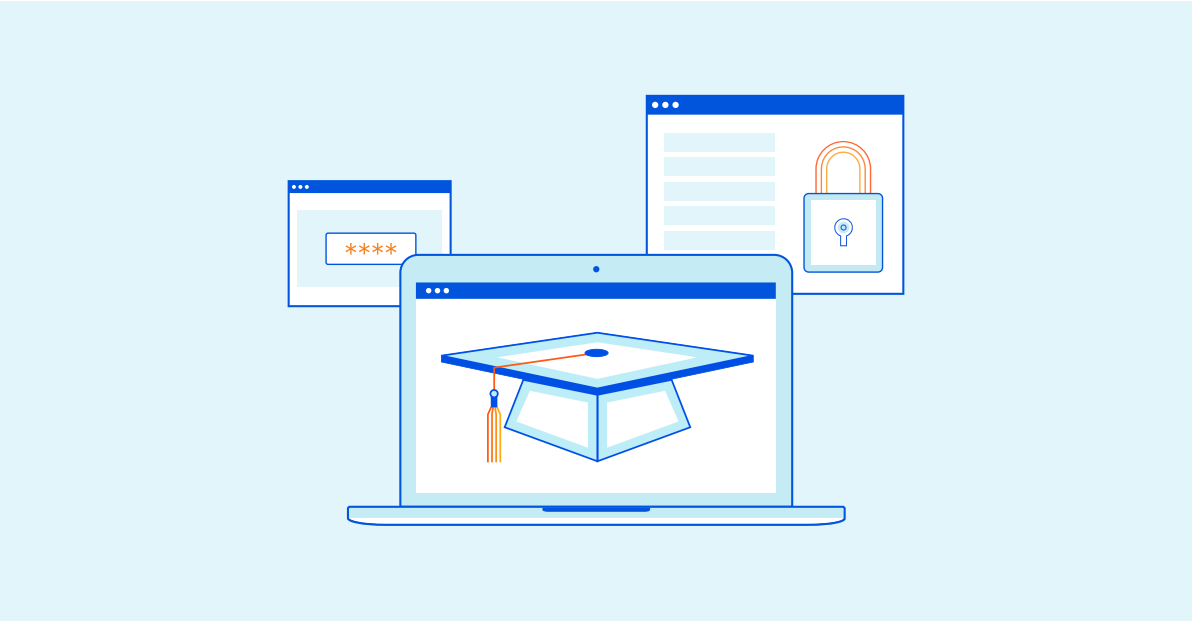
LIVRE BLANC

CLOUDFLARE

Concevoir une infrastructure d'enseignement à distance sécurisée et évolutive



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



Introduction

Ces dernières années, l'enseignement à distance s'est imposé comme un modèle éducatif de plus en plus populaire. En contraignant de nombreux établissements à passer à l'enseignement à distance afin de protéger les étudiants et les enseignants du virus, la pandémie de COVID-19 a accéléré la transition vers des modèles d'enseignement hybrides et administrés intégralement à distance.

L'enseignement à distance implique une démarche très différente de celle de l'apprentissage traditionnel en personne. Les enseignants doivent pouvoir prendre en charge toute une série de styles de formation et de types de contenus : cours magistraux, vidéos, contenus interactifs, etc. Dans un contexte d'enseignement à distance, tous les étudiants de la salle de classe doivent également doivent être en mesure d'accéder rapidement et simultanément au contenu partagé.

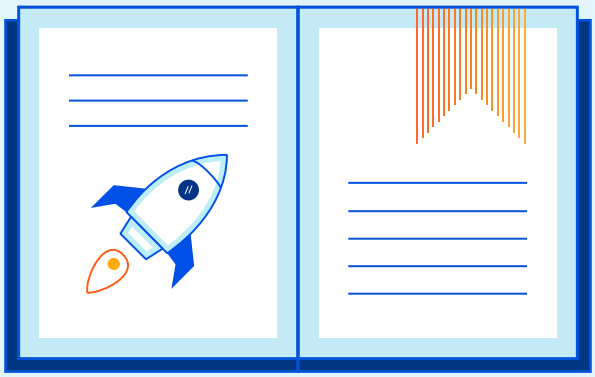
Sur le plan technique, les établissements éducatifs doivent disposer de la capacité de prendre en charge cette variété de types de contenus et de garantir la fonctionnalité des systèmes lorsque les étudiants en ont besoin.
Ces enjeux impliquent donc de résoudre certaines difficultés concernant :

- La diffusion de contenu à grande échelle.
- L'atténuation des attaques par déni de service distribué (DDoS).
- La prévention des usurpations de comptes.
- Le blocage des contenus et logiciels malveillants.

Diffusion de contenu à grande échelle

Dans un contexte d'enseignement à distance, l'infrastructure informatique des établissements constitue un élément essentiel de leur capacité opérationnelle. Les enseignants doivent pouvoir diffuser du contenu à de nombreux étudiants de manière simultanée et s'assurer de ce que cette diffusion s'effectue avec un temps de latence minimal.

Ils doivent en outre être en mesure de proposer à leurs étudiants une vaste gamme de contenus de formes diverses, des pages web statiques au contenu dynamique, comme les outils d'enseignement en ligne interactifs et les vidéos diffusées en continu. L'infrastructure informatique d'un établissement éducatif doit pouvoir diffuser ce contenu aux étudiants de manière efficace et évolutive.



Contenu statique

Une partie du contenu que les enseignants doivent fournir à leurs étudiants se compose de contenu statique, comme des pages web dont les informations ne changent pas et ne nécessitent pas de mises à jour fréquentes, par exemple.

L'évolutivité et la latence sont les principales difficultés informatiques à résoudre pour ce type de contenu. Le serveur web sera-t-il capable de soutenir la charge si de nombreux étudiants tentent d'accéder au même contenu en même temps ? La situation géographique du serveur web peut également avoir une influence considérable sur l'enseignement à distance. Plus l'étudiant est éloigné du serveur, plus la latence relative à la diffusion du contenu augmente.

La possibilité de créer des espaces locaux pour la mise en cache du contenu statique peut aider à résoudre ces difficultés. Ainsi, si un étudiant se rend fréquemment sur une page particulière, il est possible d'en effectuer une copie locale afin de lui permettre d'y accéder rapidement si nécessaire.

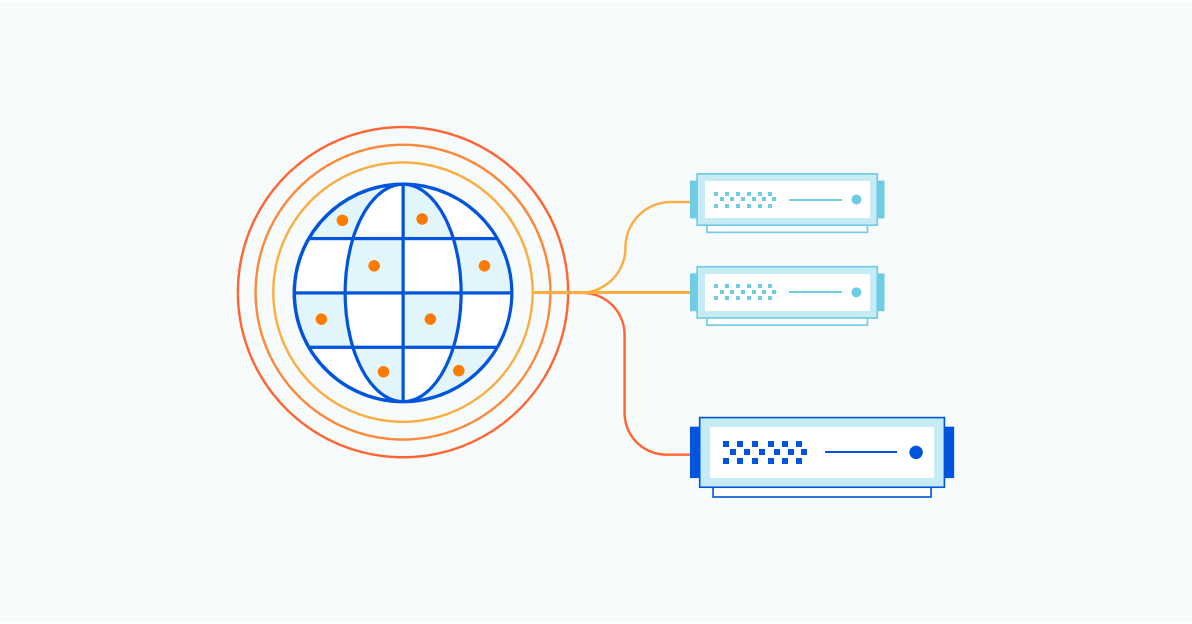
La mise en cache peut également faire l'objet d'un déploiement à grande échelle grâce à un réseau de distribution de contenu (Content Distribution Network, CDN).
Ce type de réseau se compose d'un entrelacement de nœuds qui stockent des copies locales du contenu statique et vérifient régulièrement l'existence de mises à jour de ce dernier. Un réseau CDN de portée mondiale offre l'évolutivité et la faible latence nécessaires à l'efficacité d'une structure d'enseignement à distance.

Contenu dynamique et interactif

Comme pour le contenu statique, l'enseignement interactif en ligne et les autres contenus du genre présentent certains problèmes potentiels en matière d'évolutivité. Toutefois, l'utilisation d'un réseau de nœuds CDN ne fonctionne pas aussi bien pour ce type de contenu. Si le contenu nécessite des mises à jour fréquentes ou quasi constantes, les nœuds du CDN interrogeront en permanence le serveur web principal afin d'obtenir une version mise à jour. Ce volume de requêtes entraîne une augmentation de la latence pour les utilisateurs et peut submerger le serveur web principal.

Les problèmes d'évolutivité du contenu dynamique peuvent cependant être résolus grâce à l'équilibrage de charge. Plutôt que de reposer sur un serveur unique pour traiter les demandes des étudiants, le trafic se voit ainsi réparti entre plusieurs serveurs. Cette solution permet de garantir qu'aucun serveur ne sera submergé et garantit une latence minimale.

Pour être efficace, un serveur à équilibrage de charge doit pouvoir agir de manière totalement indépendante ou ne dépendre que d'autres appareils à charge équilibrée. Si tous les serveurs sont configurés pour utiliser le même serveur de base de données, ce dernier peut agir en goulot d'étranglement et les serveurs supplémentaires à charge équilibrée n'apporter que peu, voire aucun avantage. Les solutions d'enseignement à distance doivent être soigneusement conçues de manière à garantir que l'échelle requise est bien disponible en cas de besoin et que l'architecture du système est pensée de manière à offrir tous les avantages de l'équilibrage de charge.

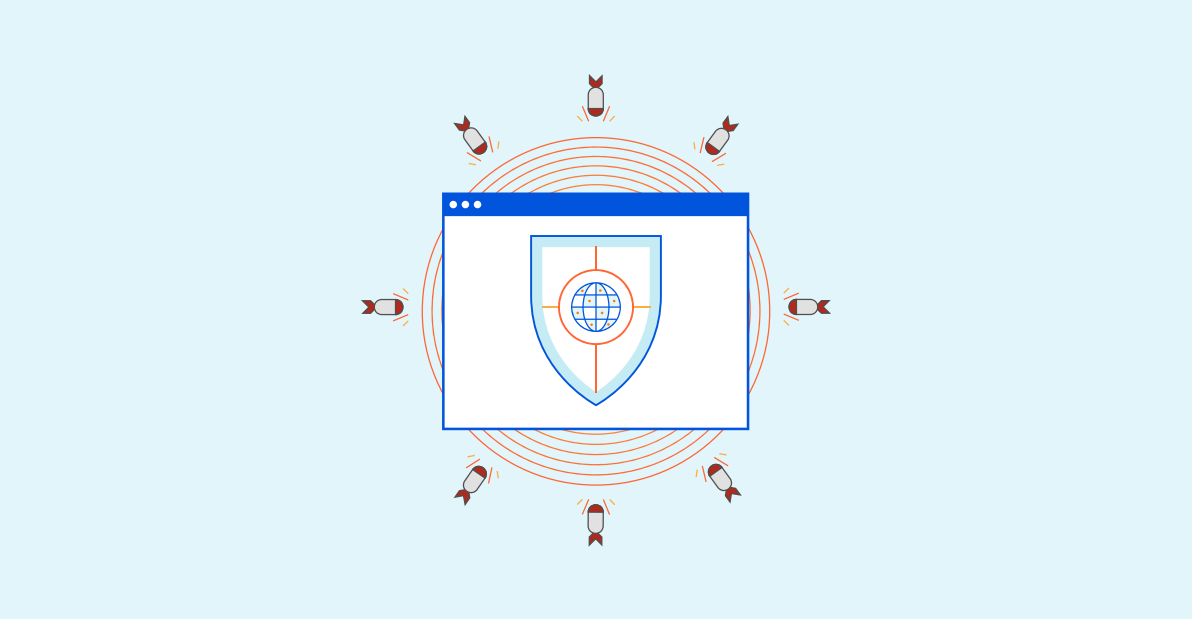


Attaques par déni de service distribué

Les attaques par déni de service distribué (DDoS) deviennent de plus en plus courantes. L'expansion de l'Internet des objets (IdO) et du cloud computing permet aux pirates d'avoir accès, plus facilement et pour moins cher, à une certaine puissance de calcul composée d'équipements connectés à Internet. Ces appareils compromis peuvent ensuite servir à envoyer du trafic malveillant vers un service afin d'empêcher ce dernier de répondre aux demandes légitimes.

Les attaques DDoS représentent un risque important pour les structures d'enseignement à distance, notamment au niveau de leur capacité à fournir des services. Au cours du premier semestre 2020, suite à la migration de nombreuses organisations vers la formation à distance, les attaques DDoS contre les ressources éducatives en ligne ont augmenté de 350 %[1].

Certaines attaques DDoS ont par ailleurs évolué de manière à intégrer un élément de rançongiciel. Un pirate peut ainsi menacer une organisation d'une attaque DDoS et exiger une rançon pour prévenir cette attaque. Bon nombre de ces menaces ne reposent sur rien de concret, mais sans protection anti-DDoS, une structure d'enseignement peut considérer que le risque pour son infrastructure se révèle trop important pour être ignoré.

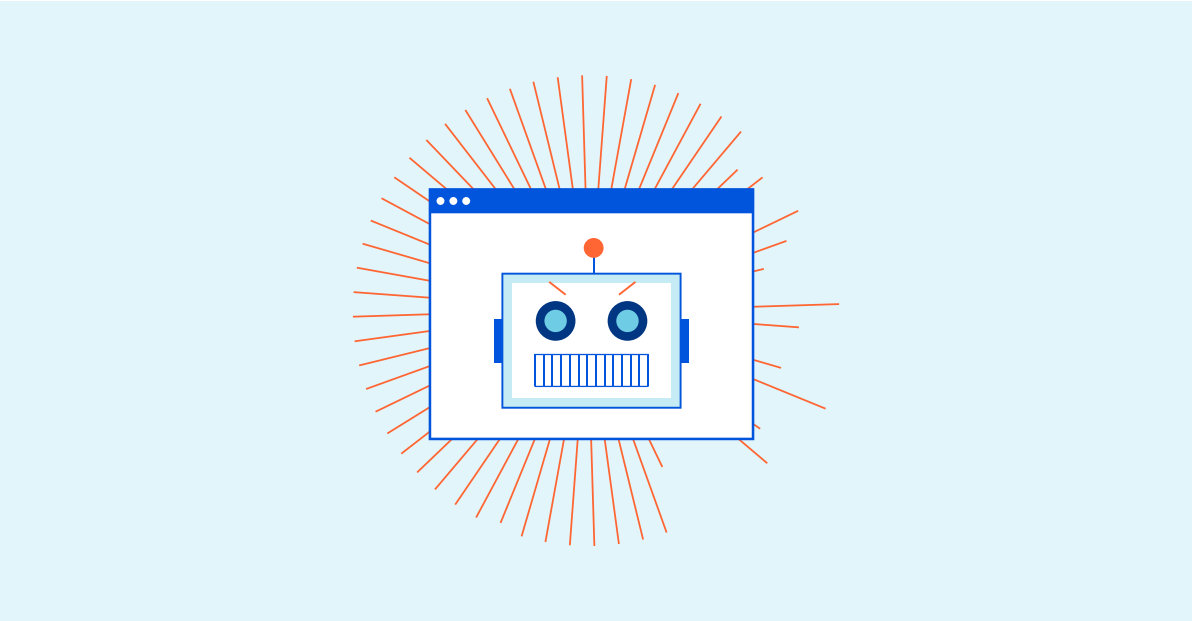


Fort heureusement, ces organisations peuvent toujours accéder à un vaste éventail de tactiques efficaces d'atténuation des attaques DDoS, même celles qui, comme souvent dans l'éducation, disposent de budgets peu extensibles. Elles doivent prendre en compte les points suivants :

- Une capacité d'atténuation élevée : il peut être tentant de ne payer que la protection dont votre organisation s'attend à avoir besoin, mais en cas d'attaque d'ampleur imprévue, le temps nécessaire à la mise à niveau de votre service peut entraîner une interruption plus longue de celui-ci.
- Atténuation distribuée : le nettoyage du trafic DDoS doit s'effectuer de manière distribuée, car la redirection de l'ensemble du trafic d'une organisation vers un point central unique à des fins de filtrage peut s'avérer impossible à faire évoluer et ainsi augmenter la latence du réseau.
- Protection à la demande ou protection permanente : dans un service d'atténuation des attaques DDoS à la demande, le trafic circule normalement de l'Internet public vers les serveurs ou l'infrastructure réseau d'une organisation jusqu'à ce qu'une attaque potentielle soit détectée, auquel cas il est inspecté et filtré de manière plus approfondie. Une protection permanente, quant à elle, filtre l'ensemble du trafic en permanence. Si ce type de protection s'avère plus coûteux qu'un service à la demande, il assure une protection ininterrompue et des temps de réponse plus rapides, car la protection n'a jamais besoin d'être activée manuellement.

Pour en savoir plus sur les stratégies d'atténuation des attaques DDoS, consultez le document « Cinq bonnes pratiques pour mitiger les attaques DDoS » disponible dans le centre de ressources Cloudflare.

[1] *https://www.infosecurity-magazine.com/news/ddos-attacks-on-virtual-education/*



Usurpation de compte

De nombreuses cyberattaques commencent par la prise de contrôle du compte d'un utilisateur légitime sur le système. Les attaques par usurpation de compte impliquent la compromission des identifiants d'un utilisateur légitime d'un réseau, d'une application ou de tout autre système. Un pirate peut obtenir l'accès aux informations d'identification d'un compte de différentes manières, notamment par le hameçonnage (phishing) et l'infiltration de compte.

Une fois en possession de ces identifiants, le pirate peut se faire passer pour un utilisateur légitime et installer des logiciels malveillants, voler des données ou atteindre d'autres objectifs sur le système cible. Il peut, par exemple, accéder à des données protégées par des réglementations telles que la loi sur la protection de la vie privée des enfants en ligne (Children's Online Privacy Protection Act, COPPA) et la loi relative à la confidentialité et aux droits des familles en matière d'éducation (Family Educational Rights and Privacy Act, FERPA). Ce type d'accès peut par ailleurs permettre aux pirates de supprimer des dossiers scolaires essentiels ou de prendre ces derniers en otage contre rançon à l'aide d'un rançongiciel.

Les établissements éducatifs doivent donc déployer une solution d'atténuation des attaques par hameçonnage capable de les détecter en s'appuyant à la fois sur les contenus malveillants connus et sur l'utilisation de l'apprentissage automatique (machine learning) dans le but de détecter des langages suspects et d'autres menaces inconnues. Pour ce faire, une des méthodes possibles est l'analyse des e-mails, une autre repose sur l'emploi d'une passerelle web sécurisée afin de bloquer les sites malveillants connus et d'empêcher les utilisateurs de télécharger certains types de fichiers.

Credential Stuffing

Un pirate peut également profiter des systèmes de connexion publics d'une organisation, comme les réseaux privés virtuels (VPN), le protocole RDP (Remote Desktop Protocol, le protocole de bureau à distance) ou les portails d'accès au web, pour compromettre les informations d'identification des utilisateurs. En moyenne, un individu donné se sert des mêmes identifiants de connexion pour 13 comptes en ligne [2]. De même, l'utilisation de mots de passe faibles et faciles à deviner constitue une pratique courante. Les attaques par infiltration de compte (credential stuffing) s'appuient sur des bots automatisés pour tenter de deviner le mot de passe d'un utilisateur sur ces portails d'authentification. S'il y parvient, le pirate obtient un accès illimité au compte de l'utilisateur légitime, car il connaît désormais ses identifiants de connexion.

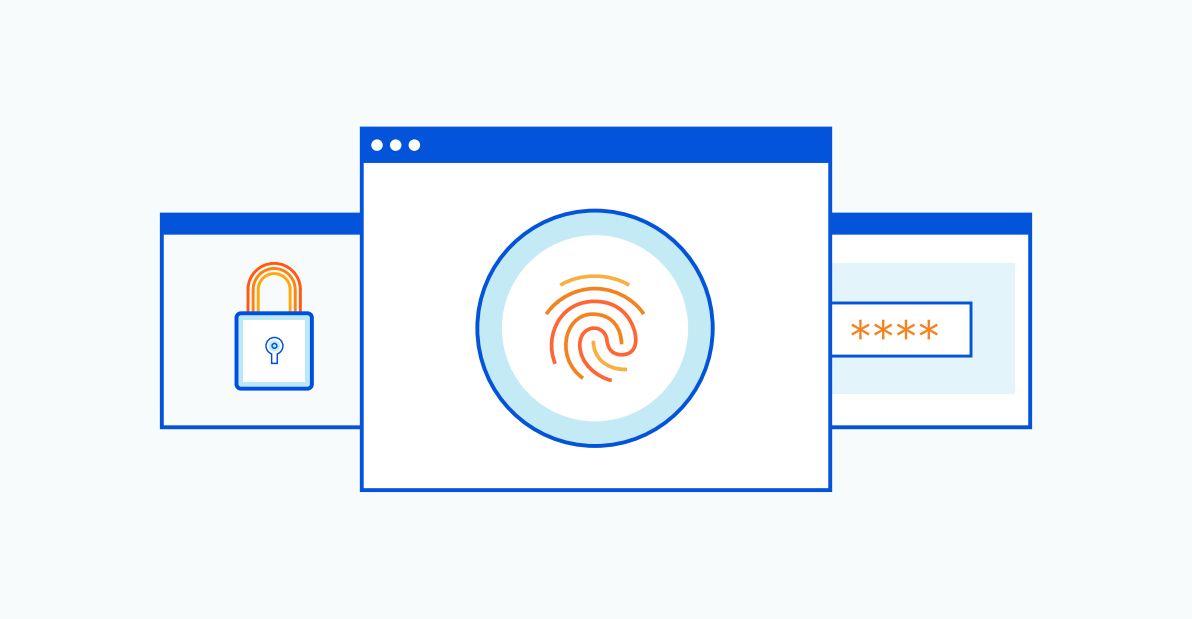
[2] *https://www.lastpass.com/state-of-the-password/global-password-security-report-2019*

Comme les attaques par infiltration de compte tirent pleinement parti de l'automatisation, la protection contre ces types d'attaques nécessite des solutions de détection des bots. Toutefois, il est essentiel de pouvoir faire la différence entre les bons et les mauvais bots.

Les bots peuvent être détectés et bloqués de diverses manières. Les éléments de base d'une stratégie d'atténuation des bots malveillants s'articulent autour des points suivants :

- **Limitation du débit :** elle permet de limiter le nombre de tentatives d'envoi de requête vers votre site ou votre réseau depuis une adresse IP donnée. Il s'agit de la solution la plus efficace contre les attaques des bots les plus simples, ceux par force brute.
- **CAPTCHA et authentification à deux facteurs :** ces deux techniques peuvent empêcher de nombreux bots d'accéder aux pages de connexion. Elles peuvent cependant affecter l'expérience utilisateur de manière négative.
- **Établissement d'une liste de blocage et d'une liste d'autorisation pour les bots :** ces outils permettent de suivre les bots malveillants connus et de s'assurer que les robots d'indexation des moteurs de recherche (de même que les autres bots utiles) restent en mesure d'effectuer leurs tâches.

Ces techniques peuvent toutefois ne pas se révéler aussi efficaces contre les bots plus avancés et spécialisés. Pour en savoir plus sur l'atténuation des effets des bots, consultez le « Guide des bots malveillants » disponible dans le centre de ressources Cloudflare.

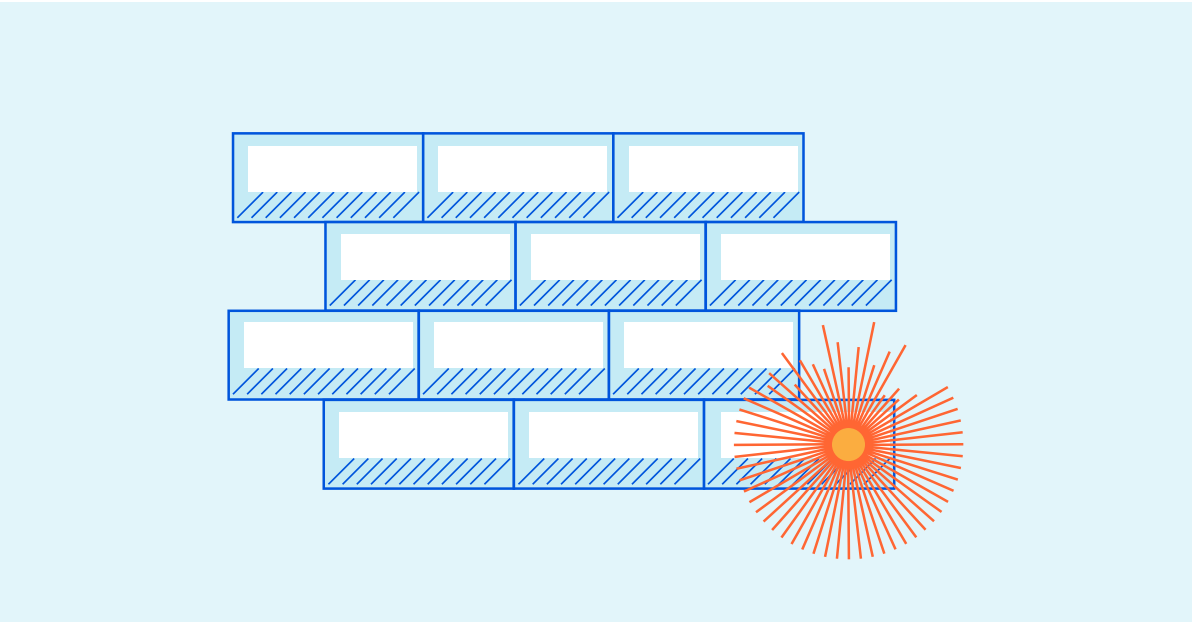


Contenus et logiciels malveillants

À mesure que les enseignants adopteront l'apprentissage à distance, un nombre croissant de systèmes se verront exposés à l'Internet public. Les étudiants peuvent profiter de l'enseignement en ligne par le biais d'applications web. Les utilisateurs de systèmes de formation en ligne (étudiants et enseignants) peuvent également disposer d'un accès à distance (au réseau et à leur ordinateur) reposant sur des VPN, des RDP et des solutions similaires. Ces systèmes doivent également être protégés contre les cybermenaces.

Sécurité des applications web

Les applications web pédagogiques peuvent avoir accès à un large éventail de données sensibles. Comme certaines informations couvertes par la COPPA, la FERPA et les autres lois similaires de protection des données des étudiants peuvent ainsi être enregistrées sur ces plates-formes, la sécurisation de ces données par les établissements éducatifs apparaît par conséquent indispensable.



Ces applications étant de nature logicielle, elles contiennent potentiellement des vulnérabilités exploitables. La protection de ces applications contre les cyberattaques nécessite donc une inspection du trafic réseau afin de détecter et de bloquer les tentatives d'exploitation de ces bogues logiciels.

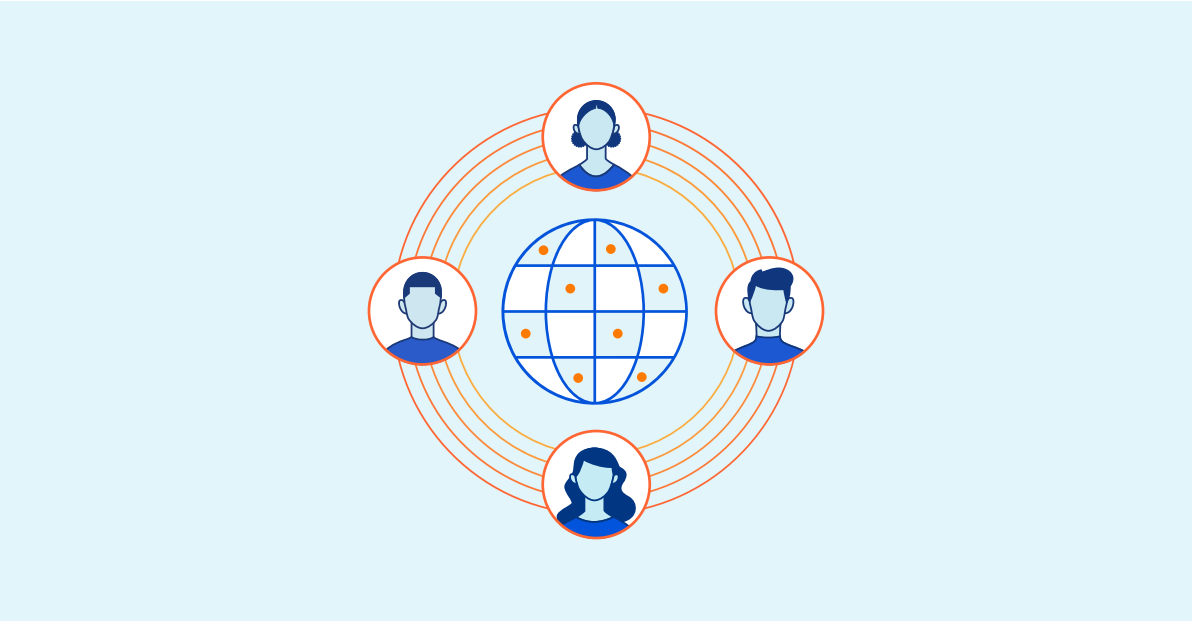
Un pare-feu d'applications web (WAF) assure une protection contre des vulnérabilités d'applications nombreuses et variées. Afin d'identifier à la fois les attaques connues et les nouvelles, le pare-feu peut combiner un service de détection fondé sur les signatures et une solution d'apprentissage automatique. Cette association lui permet de se protéger contre les attaques visant l'infrastructure web d'une organisation, même celles de type « zero-day ».

Protection contre les rançongiciels

Les rançongiciels sont actuellement l'un des types de logiciels malveillants qui se répandent le plus rapidement. Lorsqu'un rançongiciel parvient à accéder à un ordinateur, il chiffre les fichiers qui y sont enregistrés et exige un paiement pour rétablir l'accès à ces derniers. Même si l'école peut payer immédiatement la rançon, la restauration des systèmes touchés peut se traduire par une perte de temps et d'argent.

Les rançongiciels sont de plus en plus souvent transmis par l'intermédiaire des technologies d'accès à distance, comme le VPN et le RDP. Un pirate ayant accès à des identifiants de connexion légitimes peut s'en servir pour se connecter à un ordinateur et y installer des logiciels malveillants. Une fois à l'intérieur du réseau de l'organisation, les logiciels malveillants se propagent généralement de manière à infecter d'autres ordinateurs sur le réseau.

Les établissements éducatifs ont besoin d'une solution de pare-feu leur permettant d'inspecter l'ensemble de leur trafic réseau, aussi bien pour détecter les contenus malveillants entrants (comme les rançongiciels) avant qu'ils n'infectent les ordinateurs de l'organisation que pour bloquer les tentatives d'exfiltration des données (y compris les données personnelles protégées des étudiants).



Sécurisation de l'enseignement à distance avec Cloudflare

La pandémie de COVID-19 finira par prendre fin, mais la capacité d'assurer une transition en douceur vers l'enseignement à distance demeure un atout précieux pour un établissement éducatif. Les ressources de formation en ligne se révèlent d'ailleurs tout aussi précieuses pour l'apprentissage en classe, tandis que la mise en place de l'infrastructure nécessaire à l'enseignement à distance permet de rendre une organisation plus résistante aux perturbations résultant de mauvaises conditions météorologiques et d'autres événements inattendus.

Cloudflare met à disposition une plate-forme consolidée et conviviale proposant des solutions à toutes les difficultés les plus courantes en matière d'informatique et de sécurité auxquelles sont confrontés les établissements éducatifs. En profitant d'une solution unique et intégrée comme celle de Cloudflare, ces structures s'épargnent toute complexité inutile. Elles profitent ainsi d'une plus grande adaptabilité et d'une meilleure résistance aux scénarios imprévus. Les avantages offerts par Cloudflare sont les suivants :

- **Un réseau mondial de diffusion de contenu** doté de datacenters répartis dans plus de 200 villes à travers le monde.
- **Une capacité d'atténuation des attaques DDoS de 47 Tbit/s** dotée d'une solution d'atténuation permanente en périphérie du réseau.
- **Un pare-feu d'applications web** exploitant en continu les informations sur les menaces provenant des 25 millions de propriétés Internet protégées par le réseau de Cloudflare.
- **Un service avancé d'atténuation de l'activité des bots** qui s'appuie sur l'apprentissage automatique et les empreintes numériques pour analyser les schémas de trafic sur l'ensemble de notre réseau et détecter les bots les plus avancés.
- **Une passerelle web sécurisée** qui s'exécute à la périphérie du réseau et permet de réduire la latence résultant de la redirection du trafic vers un datacenter géographiquement isolé.

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