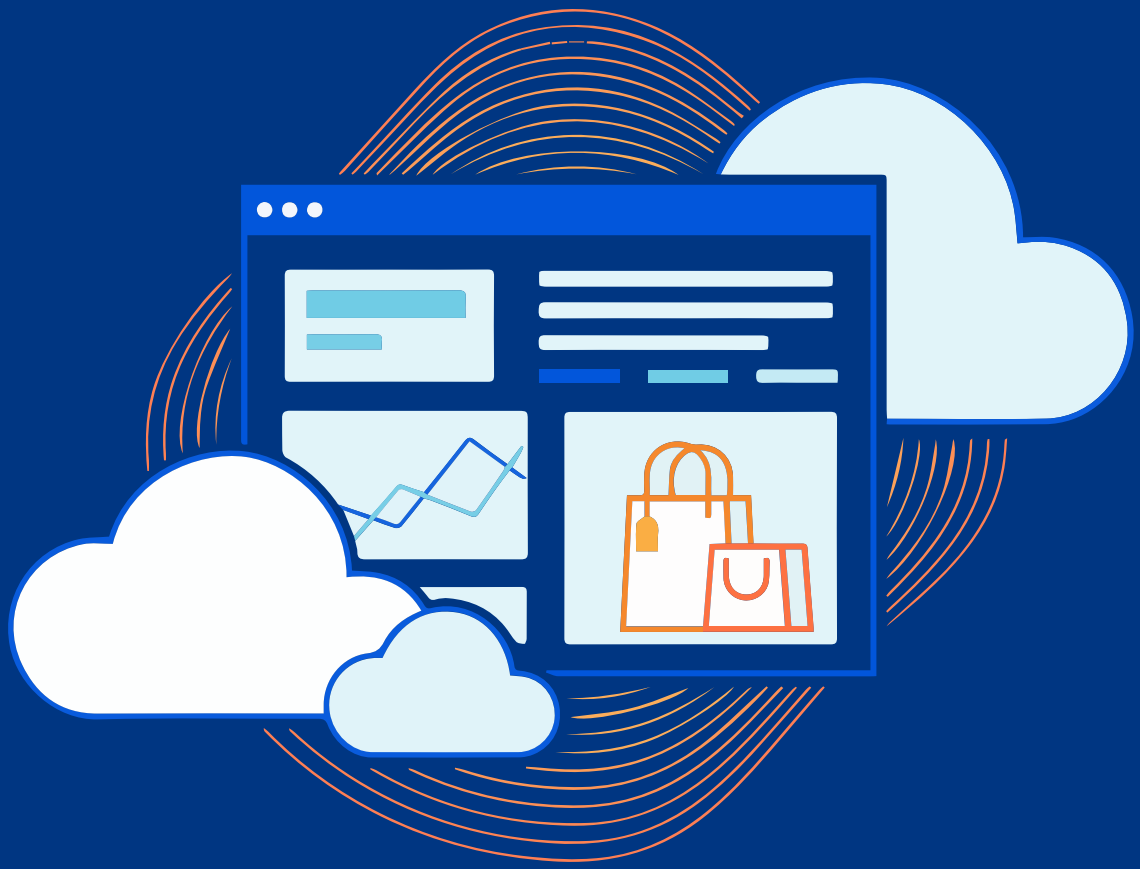
CLOUDFLARE®

CAHIER DE TENDANCES 2022 - N° 1

Cloud et Cyberattaques

En 2022, une sécurité intelligente et préventive s'impose face aux nouvelles attaques et menaces inconnues.



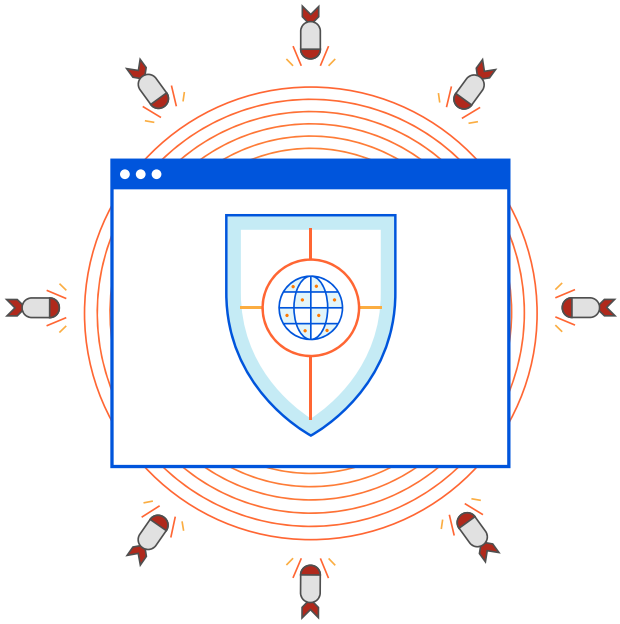
Le point de vue de Boris Lecoeur,
Directeur Général de Cloudflare France

20% du trafic Internet mondial est assuré par la plateforme de Cloudflare.

Une activité qui enrichit sans cesse notre connaissance de ce qui se passe en temps réel. À l'affût des moindres failles et faiblesses du trafic sur le réseau, nous ne cessons de détecter et prévenir des attaques, en constante augmentation. Et au vu de la crise actuelle en Ukraine, l**a prévention des risques prend tout son sens**.

TOUJOURS PLUS D'ATTAQUES, TOUJOURS PLUS VARIÉES

En pleine période Covid, le nombre de cyberattaques a été multiplié par un facteur de 3 à 5. Les plus sophistiquées sont automatisées et utilisent des traitements parallèles distribués.



Au second trimestre de l'an dernier par exemple, nous avons traité **plus de 25 millions de requêtes HTTP par seconde**. Et pendant l'éte, notre infrastructure a pu détecter et atténuer automatiquement l'une des plus grandes attaques DDoS jamais rencontrées évaluée à 17,2 millions de requêtes par seconde. Attaque menée par des bots dont le trafic représente aujourd'hui entre 30% à 50% du trafic internet mondial.

Les attaques se diversifient en matière de cibles : terminaux, serveurs, objets connectés et applications. Elles visent aussi les APIs ou les services applicatifs comme la voix sur IP ou la visioconférence, qui servent de passerelles pour attaquer les serveurs et applications critiques. D'ailleurs, l'indisponibilité de Zoom, Google Meet ou Microsoft Teams porte une atteinte essentielle à la continuité d'activité d'une entreprise.

MÊME LE RANSOMWARE A ÉVOLUÉ... OU SERAIENT-CE LES HACKERS ?

Traditionnellement, les demandes de rançon sont le fait de groupes de hackers plutôt identifiés, comme Lazarus ou d'autres utilisant REvil. En 2021, les menaces ont été plus diffuses et les groupes moins identifiés.

En outre, lorsque l'entreprise a payé sa rançon pour obtenir la clé de chiffrement, les hackers ont souvent exigé une deuxième rançon pour ne pas divulguer les données saisies (sans garantie). Autre nouveauté : des groupes d'hacktivistes exigent désormais des rançons contre une menace d'attaques DDos à venir...

Aux États-Unis, les activités des assureurs ont d'ailleurs évolué, en intégrant des **audits beaucoup plus poussés**. Signalons que les sociétés qui utilisent Cloudflare pour véhiculer leur trafic sont moins attaquées, et paient donc moins de primes d'assurance. Les sociétés qui proposent de couvrir le cyber-risque ne sont pas forcément les assureurs traditionnels. Cloudflare travaille aussi avec de nouveaux entrants comme intermédiaires afin de faciliter les évaluations visant à établir le juste équilibre entre primes et risques.

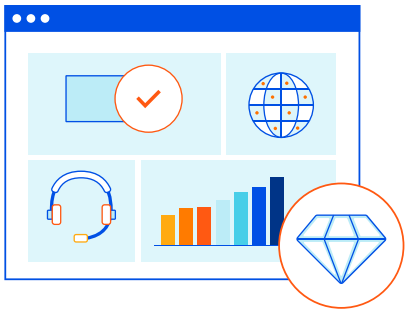
DE LA COTTE DE MAILLES À LA PROACTIVITÉ

L'une des tendances importantes consiste à moins se concentrer sur la hauteur des murailles et de la forteresse mais plutôt à porter plus son attention sur plus de réactivité et de contrôle.
De nombreuses PME/PMI tentent de gérer elles-mêmes la sécurité de leur infrastructure (ou via un prestataire).

Puis, constatant la complexité, le temps et l'expertise nécessaire de l'exercice, elles se tournent alors vers des **solutions nées sur le Cloud comme Cloudflare** pour confier la gestion de leur trafic et automatiser les contrôles via des politiques réseau et de sécurité globales.

Le groupe de courtage en assurance et de crédit Assu2000 a fait évoluer sa sécurité qui reposait sur ses propres boîtiers. Situés dans ses datacenters, les matériels de sécurité accusaient régulièrement des retards de mises à jour et nécessitaient une maintenance complexe.

Assu 2000 a délégué la protection de son SI à Cloudflare, qui a repris toutes les politiques de sécurité réseau en quelques jours sur une plateforme évolutive, opérée par des professionnels.



Lors des dernières vagues d'attaques sur les failles Log4j [bibliothèque de fonctions Java pour générer des logs, très utilisée par les développeurs], l'infrastructure de Cloudflare a été mise à jour en quelques heures pour éviter toute exploitation de la faille chez nos clients, alors que des centaines d'entreprises sont encore en train d'effectuer ces mises à niveau plusieurs semaines après la révélation de ce type d'incident.

- Parce que nous gérons une grande partie du trafic Internet, nous sommes les **premiers informés sur les nouveaux « patterns » d'attaque**.
  Un avantage qui nous procure une grande réactivité et une grande facilité, pour une tâche qu'une entreprise réalise difficilement et dans des délais plus importants.

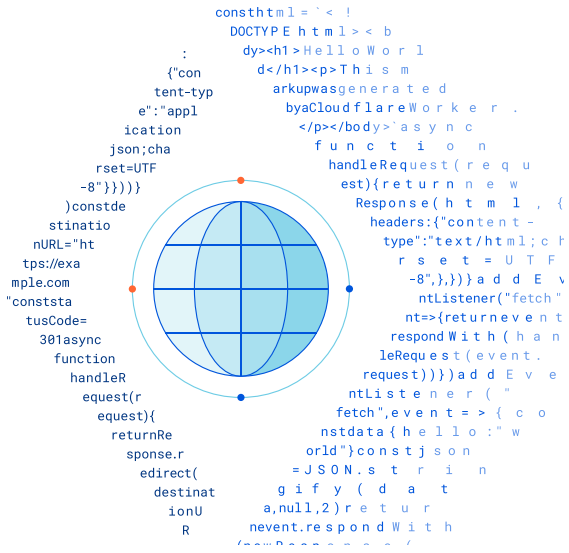
- Nos services n'interviennent pas directement sur l'infrastructure du client (datacenters et services cloud – SaaS, PaaS…). Le service est positionné entre l'utilisateur et la ressource pour véhiculer le trafic.
  Notre plateforme protège les DNS en analysant et traitant toutes les requêtes adressées, et véhicule le trafic sur le réseau le plus connecté au monde avec plus de 10 000 points d'interconnexion.

- Cette dernière caractéristique permet également d'accélérer le trafic de nos clients, puisqu'il passe essentiellement sur notre réseau au plus près des utilisateurs et au plus près du service/application (dans le datacenter ou dans le Cloud). **Les données empruntent ainsi la route la plus courte** d'un point A à un point B, et la moins encombrée.

L'UTILISATEUR FINAL AVANT TOUT, AVEC PLUS DE SIMPLICITÉ

Originellement positionnée sur la protection et l'accélération du Web, Cloudflare s'est spécialisée depuis 4 ans sur l'utilisateur, ses accès et sa protection. Aujourd'hui nous protégeons les réseaux internes et externes par redirection du trafic depuis le terminal de l'utilisateur et jusqu'au datacenter ou au cloud. Ce qui autorise un contrôle spécifique selon le à terminal, serveur, équipement…

Avec l'ouverture des systèmes d'information, les hackers sont toujours dehors, mais la surface d'attaque s'avère plus importante. C'est pourquoi les projets de déploiement de type **Zero Trust** (passerelles de sécurité -Security Gateway) ont été accélérés pendant la période de pandémie.
Afin d'améliorer l'authentification et la protection des utilisateurs, où qu'ils se trouvent.



Alors que notre plateforme offre le contrôle et la supervision des accès à la fois vers les datacenters et les SaaS, **les VPN restent limités et nécessitent des déploiements invasifs** (y compris sur les terminaux ou postes de travail) et s'avèrent complexes à maintenir. D'ailleurs, le VPN a été inventé en même temps que les VD…
Et, il en va de même pour les liaisons MPLS : désormais, **Internet est LE réseau !**

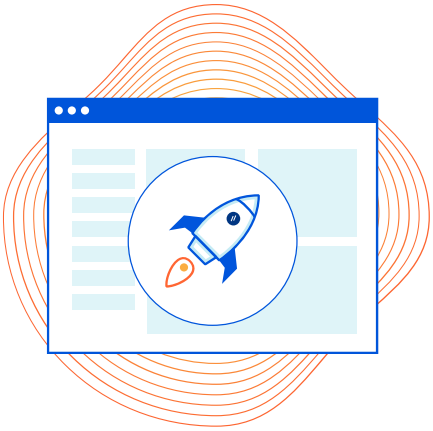
Cependant, la migration vers ces nouveaux paradigmes peut s'effectuer progressivement et de façon totalement transparente pour l'utilisateur. Un projet offrant à l'entreprise l'opportunité de renforcer et simplifier ses règles d'accès : **SSO** (authentification unique pour plusieurs applications et SaaS), authentification multi facteurs (biométrique ou autres) ...

Et la plateforme peut compléter les vérifications : géolocalisation, patterns d'utilisation et analyse comportementale, accès autorisé selon l'heure et pour une durée prédéfinie, etc. Et toutes ces informations permettent une supervision de l'activité en temps réel, ou pour de l'analyse a posteriori.

UNE PLATEFORME AUTOMATISÉE QUI RÉPOND AUX ATTENTES

Nous comptons environ **1,6 million de phishings tous les mois**. Et même si Cloudflare empêche les e-mails d'entrer grâce à un filtrage efficace, un seul suffit pour causer des dommages. C'est pourquoi les bases de signatures virales et les équipements de l'infrastructure de Cloudflare sont mis à jour instantanément à travers le monde afin de procurer un filtrage optimal.

Autre atout qui répond à une attente importante : l'**automatisation**. L'entreprise délègue à nos spécialistes le suivi et l'application de règles de sécurité et de politiques réseau, autant de tâches différenciantes qui exigent cependant des compétences spécifiques.



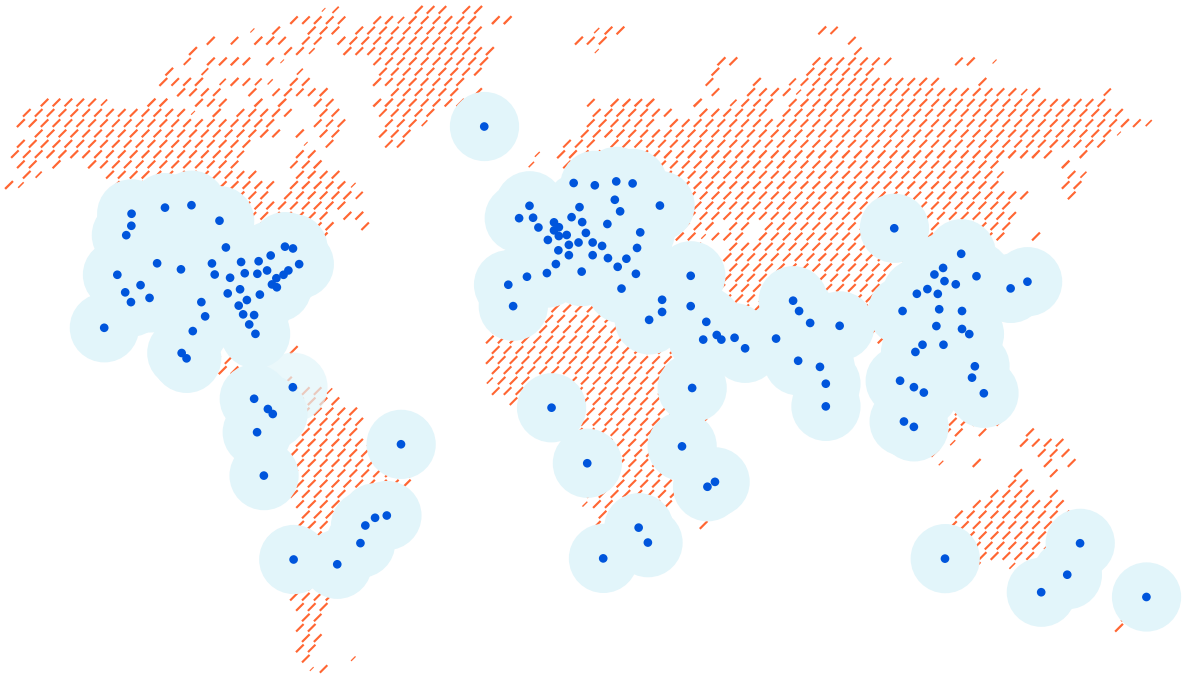
D'après l'enquête Cloudflare réalisée en fin 2021 par **Adelanto** auprès de 172 décideurs informatiques de sociétés françaises, **62,6 %** d'entre eux mettent en avant le **manque de compétences en sécurité** comme premier frein à l'efficacité contre les cyberattaques.

Après le **manque de budget (50,3 %)** et ils mentionnent « des **systèmes obsolètes et difficiles à mettre à jour** » **(43,3 %)** ou encore « **la complexité de l'infrastructure IT** » **(42,1 %)**. Autant de points faibles sur lesquels peut agir l'automatisation des mises à jour et d'une partie de la remédiation, pour apporter enfin la réactivité indispensable.

Cloudflare propose aussi le "**SOC as a Service**" qui rassemble et corrèle toutes les informations nécessaires à la supervision, aux alertes et à la remédiation. Malgré une forte automatisation, la remédiation est toujours supervisée par un humain en fonction du contexte de chaque client.

RAPPEL

Cloudflare bloque aujourd'hui 76 milliards de cybermenaces par jour, 28 millions de requêtes HTTP et 13,6 millions de requêtes DNS. *Et sans porter atteinte aux performances !*



Pendant cette période de transition vers le numérique, les décideurs mettent souvent en avant les coûts et effort de migration alors que **la migration vers une infrastructure Cloud de type Cloudflare peut être réalisée en quelques heures**.

Pour les convaincre, **nous proposons le rachat des contrats sur les solutions en place**, afin que l'entreprise puisse bénéficier d'une **plateforme unique assurant la cohérence du réseau et de la sécurité**, avec la possibilité d'intégrer d'autres solutions via nos partenaires (EDR comme Crowdstrike, ou IDP comme Okta).

Pour toute information additionnelle, vous pouvez contacter les services de Cloudflare au +33(0)7 57 90 52 73