CLOUDFLARE

E-BOOK

Prévenir l'interruption de service : le guide des modèles de défense contre les attaques DDoS

Contenu

Cliquez pour passer directement à la section désirée

Introduction : la défense contre les attaques DDoS au sein d'un environnement professionnel hybride

L'entreprise moyenne utilise désormais plus de 1 400 services cloud distincts[1], poussée en cela par une demande accrue d'applications et d'expériences client mieux pensées et plus rapides. L'extension de la surface d'attaque constitue un corollaire de la transformation cloud : l'augmentation du nombre de services numériques entraîne l'augmentation du nombre de « points d'entrée » à exploiter par les acteurs malveillants. La surface d'attaque s'est également étendue sous l'impulsion du travail hybride (la combinaison mêlant travail au bureau et télétravail), rendu nécessaire par des années de pandémie mondiale.

Tous ces facteurs intensifient la pression exercée sur les entreprises aux ressources limitées. Les équipes chargées de l'informatique et de la sécurité doivent non seulement proposer des applications et des réseaux plus résilients, mais également protéger les utilisateurs et les appareils contre un paysage des menaces en pleine évolution, et ce indépendamment de leur position géographique.

Certaines de ces menaces se présentent sous la forme d'attaques par déni de service distribué (Distributed Denial-of-Service, DDoS) plus fréquentes, plus longues et plus imposantes. En février 2023, Cloudflare a détecté et atténué la plus puissante attaque DDoS HTTPS jamais enregistrée (71 Mr/s). Nos données montrent l'augmentation des attaques DDoS hypervolumétriques d'un trimestre sur l'autre (les attaques d'un débit supérieur à 100 Gb/s) en 2022.

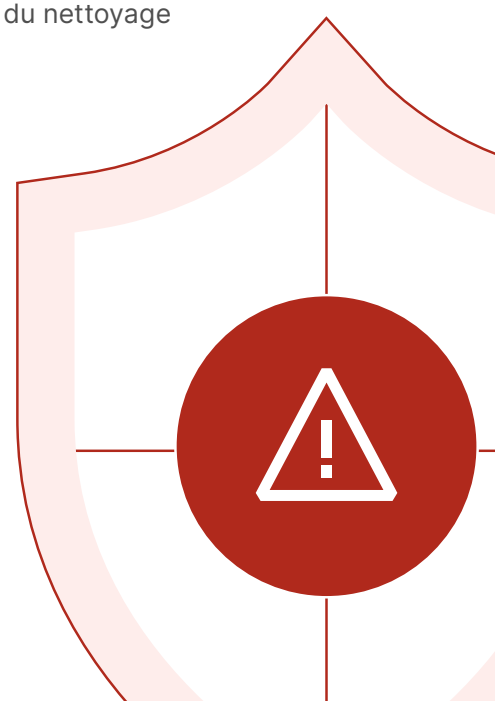
Les réalités d'aujourd'hui en matière d'économie et de travail hybride imposent aux entreprises de réévaluer leurs défenses anti-DDoS : le risque d'interruption de service, de vol de données, d'infiltration du réseau et de pertes financières est bien trop élevé.

Les recherches révèlent que, dans le panorama des pannes, plus de 60 % coûtent plus de 100 000 USD et 15 % plus d'un million[2]. Pour prendre un exemple, l'interruption de service résultant d'attaques DDoS a coûté plus de 12 millions de dollars à une entreprise[3].

Ces réalités rendent la défense contre les attaques DDoS essentielle pour les entreprises de toutes les tailles. Les approches manuelles du passé ne suffisent plus. Si les attaques sont lancées par des humains, elles sont mises en œuvre par des bots et pour avoir le dessus sur ces derniers, il convient de combattre le feu par le feu. Le processus de détection et d'atténuation doit être aussi automatisé que possible.

Cet e-book explore les thèmes suivants :

- Les différents modèles de protection contre les attaques DDoS basée sur le cloud.
- Les moyens de surmonter les limitations du nettoyage cloud actif en permanence.
- La manière dont une entreprise du Fortune Global 500 a déjoué une attaque DDoS avec demande de rançon grâce à Cloudflare.



Comprendre les approches en matière d'atténuation des attaques DDoS basée sur le cloud

Une attaque DDoS est une tentative malveillante de perturber le trafic normal du serveur, du service ou du réseau visé en submergeant la cible ou son infrastructure environnante sous un flot de trafic Internet. Une solution anti-DDoS vous indiquera exactement quand, à quel endroit et de quelle manière cet « embouteillage » se produit, tout en absorbant et en redirigeant le trafic malveillant afin qu'il n'interfère plus avec le trafic légitime. Les destinations à fort trafic sont des cibles courantes, de même que les propriétés Internet et les réseaux non protégés.

Si les attaques DDoS ne sont pas un phénomène nouveau, de nouvelles approches sont nécessaires pour les arrêter. Suite à la migration des applications vers le cloud, le marché des solutions anti-DDoS sur site s'est également réduit[4]. De plus en plus d'entreprises se tournent désormais vers le cloud pour leurs besoins en matière de protection contre les attaques DDoS.

Dans de nombreuses variantes de protection cloud, le fournisseur de cloud se place en amont des applications et de l'infrastructure de l'entreprise et redirige l'ensemble du trafic vers un centre spécialisé afin qu'il y soit « nettoyé ». Seul le trafic légitime est renvoyé au client. Ce processus de « nettoyage cloud » peut être déployé selon deux modes : ***à la demande*** ou ***en permanence***.

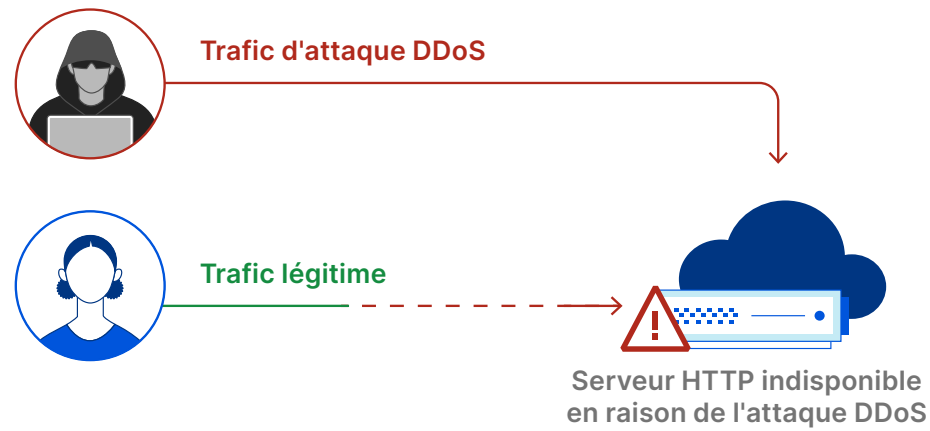
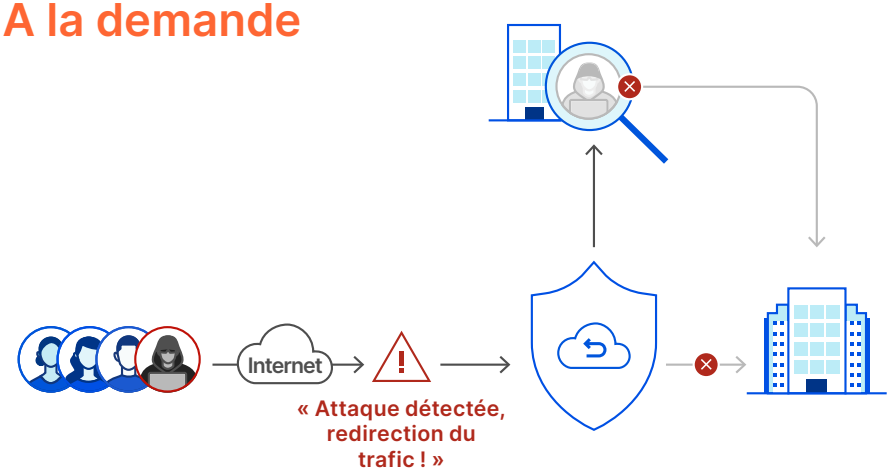


Schéma d'une attaque DDoS sur la couche applicative aboutissant à un événement de déni de service pour les utilisateurs légitimes

À la demande

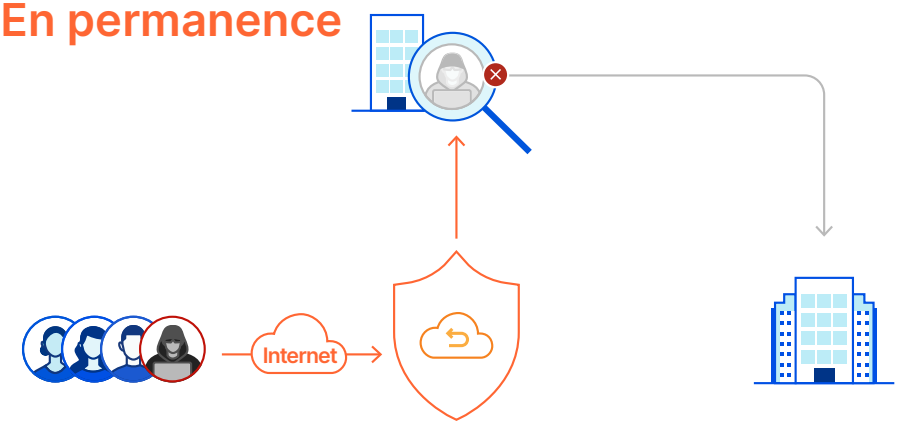


En temps normal, c'est-à-dire « en temps de paix », le nettoyage cloud à la demande permet de s'assurer que les applications et l'infrastructure reçoivent l'intégralité du trafic, sans redirection. Le trafic n'est redirigé vers le fournisseur de services de nettoyage dans le cloud qu'en cas d'attaque DDoS active.

Si le trafic entrant dépasse un seuil d'utilisation de la liaison préalablement configuré (par exemple, 70 % de la capacité de la liaison) ou si une attaque de grande ampleur est détectée, le mode d'atténuation cloud à la demande est activé et le trafic est redirigé vers le site de nettoyage cloud le plus proche afin d'y être traité.

ou

En permanence



Cette approche pratique du nettoyage cloud redirige toujours le trafic de l'entreprise vers les datacenters de votre fournisseur de services cloud à des fins d'identification des menaces, et ce même en temps normal.

Le modèle actif en permanence permet de minimiser le délai entre la détection et l'atténuation, tout en prévenant les interruptions de service.

Si les deux méthodes (protection à la demande et protection active en permanence) proposent des avantages différents, elles peuvent chacune présenter des limitations différentes dans des circonstances différentes, comme nous le verrons la prochaine section.

Les limitations courantes des méthodes de nettoyage dans le cloud

Les défis du nettoyage dans le cloud : déploiement à la demande

Retards dans la réponse aux attaques :

- Le modèle à la demande nécessite que le trafic soit redirigé vers le fournisseur de cloud lors d'une attaque DDoS. Le changement peut prendre plusieurs minutes à s'opérer, en plus du temps nécessaire au déclenchement d'une réponse manuelle à l'attaque (c.-à-d. demander au fournisseur d'activer le service). L'attaque peut avoir des conséquences dévastatrices si la protection à la demande n'est pas activée à temps.

Coût accru à long terme :

- Les fournisseurs de cloud à la demande facturent souvent chaque octet de trafic hostile. Si vous ne payez finalement que ce que vous utilisez, ce mode de facturation pourrait finir par vous coûter plus cher si votre entreprise fait face à de fréquentes attaques DDoS.

Attaques potentiellement manquées :

- Les attaques DDoS qui ne dépassent pas le seuil d'utilisation peuvent rester inaperçues et l'encombrement des liaisons réseau qui en résulte peut ainsi affecter le trafic légitime.
- Les liaisons réseau ne surveillent pas non plus les attaques basées sur un protocole de plus haute couche, comme les attaques au niveau du SSL et de l'application.

Modèle de nettoyage dans le cloud : déploiement permanent

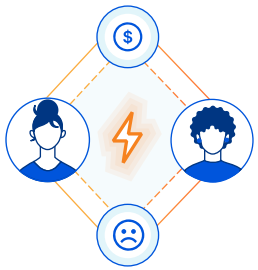
Problèmes de latence entraînant une dégradation de l'expérience utilisateur :

- De nombreux fournisseurs de solutions d'atténuation des attaques DDoS dans le cloud disposent d'un ensemble de datacenters distants, dédiés au nettoyage du trafic réseau et situés à bonne distance de l'endroit d'où le trafic hostile provient. En général, moins le fournisseur entretient de centres de nettoyage, plus la latence est importante. La redirection du trafic peut également introduire de la latence et entraîner des retards perceptibles.
- Les datacenters dédiés au nettoyage des attaques DDoS n'inspectent bien souvent que la couche réseau. Le trafic des fonctions résidant sur d'autres couches, comme le pare-feu d'applications web (WAF) ou la mise en cache du contenu, est généralement traité dans un autre datacenter, entraînant ainsi une nouvelle augmentation de la latence.

Coût total de possession plus élevé :

- Les solutions de nettoyage cloud actives en permanence et disposant d'une capacité réseau limitée peuvent répercuter leurs limitations de bande passante à leurs clients, sous forme de prix plus élevé. Les frais de services professionnels peuvent également être gonflés.

Le temps, c'est de l'argent : comment les interruptions de service et la latence peuvent affecter l'activité

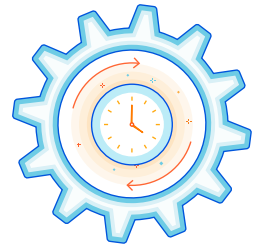


91 % des entreprises déclarent que **les interruptions de service peuvent leur coûter jusqu'à 300 000 USD/heure** du fait de la perte d'opportunités commerciales, des perturbations de la productivité et des efforts déployés pour résoudre les problèmes.[5]

Pour certaines entreprises d'e-commerce bien connues, une interruption de service peut coûter jusqu'à **220 000 USD** la minute.[6]

90 % des clients quitteront un site s'il ne se charge pas « dans un délai raisonnable », tandis que **57 % le quitteront et iront procéder à leurs achats sur un site similaire.**[7]

44 % des joueurs confrontés à la latence réagissent en **quittant le jeu auquel ils sont en train de jouer** pour le réessayer plus tard, tandis que **24 % d'entre eux quitteront leur jeu pour aller jouer à autre chose.**[8]



64 % des décisionnaires en informatique indiquent que le besoin de proposer une expérience client plus rapide et plus simple **« fait peser une charge considérable sur leur infrastructure technologique ».**[9]

Réaliser le plein potentiel d'une défense basée sur le cloud et se protéger contre la perte de revenus résultant d'une défaillance

Découvrez de quelle manière notre plateforme cloud unifiée et soutenue par un réseau mondial intelligent vous protège contre toutes les menaces DDoS

Le nettoyage cloud à la demande repose sur l'intervention humaine et ajoute ainsi du temps avant le déclenchement de l'atténuation. À l'inverse, une protection contre les attaques DDoS toujours active adopte une approche plus complète. Toutefois, de nombreux prestataires de solutions anti-DDoS cloud permanentes s'appuient sur des centres de nettoyage distants, qui ajoutent de la latence à l'expérience utilisateur.

Cloudflare répond à ces limitations à l'aide d'une plateforme de sécurité unifiée, comprenant trois couches de protection contre les attaques DDoS (couches 3, 4 et 7), ainsi que des fonctionnalités d'accélération du trafic pour les réseaux sur site, hébergés dans le cloud et hybrides. Comme le trafic hostile est atténué à proximité de la source, l'expérience de vos utilisateurs finaux s'avère fluide et performante.

Sécurité soutenue par un réseau

Cloudflare dispose de **datacenters dans plus de 285 villes** et d'une **capacité réseau de 197 Tb/s** (par contraste, un célèbre service d'atténuation des attaques DDoS s'appuie sur moins de 40 centres de nettoyage et une capacité réseau de 20 Tb/s).

Les attaques sont automatiquement absorbées par notre réseau avant d'atteindre le vôtre et la plupart du trafic hostile est bloqué en **moins de 3 secondes**. Aucune redirection n'est nécessaire.

Ergonomie, visibilité et libre-service

Comme la protection anti-DDoS de Cloudflare est proposée « en tant que service », aucune dépense d'investissement ni gestion du cycle de vie des équipements physiques n'est nécessaire.

En outre, notre solution est **en libre-service** et dispose de capacités de configuration personnalisées pilotables à l'aide d'un **tableau de bord unique**.

Système d'information sur les menaces à grande échelle

Surveillez plus pour protéger plus. Près de 20 % d'Internet tourne sur Cloudflare. Nos clients bénéficient de l'échelle et des informations de notre réseau mondial, qui **bloque plus de 112 milliards de menaces chaque jour**.

Nos modèles d'apprentissage automatique avancés améliorent nos défenses en permanence, afin de nous permettre de garder une longueur d'avance sur les menaces émergentes en votre nom.

Protection anti-DDoS reconnue sur le marché

Cloudflare a été reconnue comme **Leader dans le rapport GigaOm Radar 2022 consacré à la protection contre les attaques DDoS**. Le rapport évaluait neuf prestataires différents et Cloudflare est arrivée en première place. Cloudflare a également été désignée comme **« Leader » dans le rapport The Forrester Wave™: DDoS Mitigation Solutions (solutions d'atténuation des attaques DDoS) du premier trimestre 2021**.

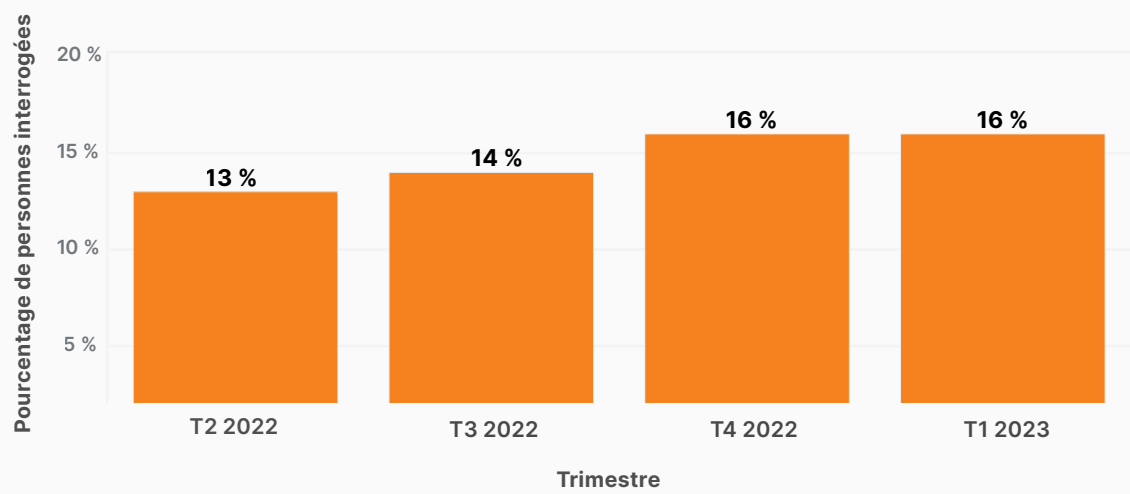
Cloudflare a reçu le meilleur score possible dans 15 critères, parmi lesquels ses centres d'opérations de sécurité, l'automatisation de ses interventions et ses performances.

Étude de cas : une entreprise du Fortune Global 500 visée par une attaque DDoS avec demande de rançon

Également connue sous le nom d'extorsion de rançon, une attaque DDoS avec demande de rançon (RDDoS) désigne une tentative effectuée par des acteurs malveillants d'extorquer une somme d'argent en menaçant un particulier ou une entreprise d'une attaque DDoS. Le nombre de tentatives d'attaques DDoS avec demande de rançon a augmenté de manière régulière tout au long de l'année 2022. Plus de 16 % des clients de Cloudflare ont ainsi reçu une menace ou une demande de rançon dans le cadre d'une attaque DDoS au premier trimestre 2023.

Souvent confondues avec les attaques de rançongiciels, les attaques DDoS avec demande de rançon fonctionnement différemment et sont plus simples à mettre en œuvre : elles ne nécessitent pas de tromper une victime afin de l'amener à ouvrir un e-mail ou à cliquer sur un lien. De même, elles n'ont aucunement besoin d'une intrusion réseau préalable ou de l'établissement d'une présence au sein des ressources de l'entreprise. La disponibilité croissante des rançongiciels en tant que service a également permis aux attaques DDoS avec demande de rançon de devenir une option à faible risque et faible investissement pour les acteurs malveillants.

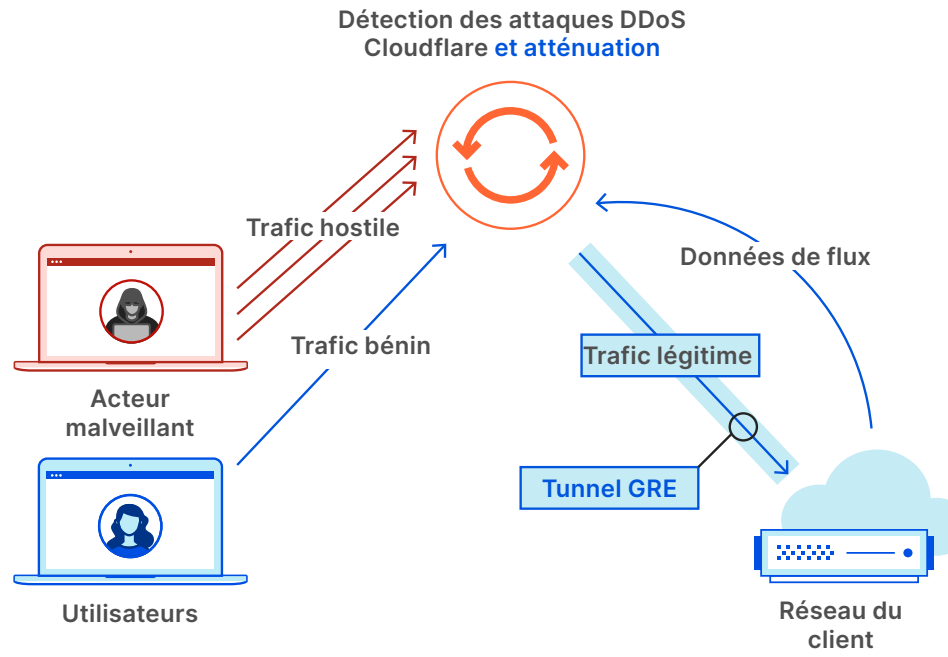
Menaces et attaques DDoS avec demande de rançon, répartition trimestrielle
Pourcentage des personnes interrogées ayant déclaré avoir été menacées ou été la cible d'une attaque DDoS avec demande de rançon



Fin 2020, avant de se tourner vers Cloudflare pour ses besoins d'atténuation DDoS, une grande entreprise classée au Fortune Global 500 a été prise pour cible par une tentative d'attaque RDDoS provenant de diverses parties se revendiquant comme le Lazarus Group (un groupe de cybercriminels censément soutenu par le gouvernement de Corée du Nord). Les acteurs malveillants ont initialement envoyé un e-mail exigeant une somme en Bitcoin et lui ont accordé une semaine pour « payer », sans quoi l'entreprise ferait à nouveau les frais d'une attaque (plus puissante) et la rançon augmenterait.

Après avoir reçu la demande de rançon et constaté une augmentation significative du trafic destiné à l'un de ses datacenters mondiaux, l'entreprise a contacté son centre de nettoyage à la demande. Il lui a fallu plus de 30 minutes pour activer le service du prestataire et rediriger le trafic vers le centre de nettoyage. L'activation du service à la demande a également provoqué des défaillances du réseau et entraîné plusieurs incidents.

Après l'attaque initiale et face aux défis rencontrés avec son fournisseur de protection à la demande, l'entreprise a décidé d'intégrer Cloudflare Magic Transit, la solution active en permanence de Cloudflare pour la protection contre les attaques DDoS sur la couche réseau. Bien que les acteurs malveillants aient menacé leur cible d'une seconde attaque, plus puissante, celle-ci ne s'est jamais produite.



Cloudflare Magic Transit, la protection anti-DDoS au niveau de la couche réseau

« Les données d'analyse sur les attaques et le trafic constituent l'un des facteurs de différenciation principaux. Notre prestataire précédent ne pouvait pas nous les fournir. Nous voyons maintenant des attaques dont nous n'avions aucunement connaissance auparavant être atténuées automatiquement. »

Équipe d'intervention et d'analyse post-incident
Une entreprise classée au Fortune Global 500

Conclusion

Face à l'augmentation de la fréquence et de la complexité des attaques DDoS dans le contexte post-pandémique, il est important d'assurer la circulation du trafic légitime afin de vous aider à protéger vos revenus. Grâce à la possibilité de se protéger rapidement et sans effort contre les attaques (sans les problèmes de latence ou de coût élevé couramment retrouvés chez les autres fournisseurs), Cloudflare simplifie la décision d'adoption d'une stratégie cloud active en permanence.

Pour en savoir plus concernant la protection contre les attaques DDoS sur la couche réseau avec Cloudflare, n'hésitez pas à demander une démo.

Pour en savoir plus sur notre réseau mondial unique disposant de fonctionnalités intégrées en matière de Zero Trust, d'atténuation des attaques DDoS, de pare-feu réseau et d'accélération du trafic, cliquez ici.

Sources

1 Langrock, Sam. « The Cloud has Complicated Attack Surface Management » (Le cloud dispose d'une gestion de la surface d'attaque compliquée). Recorded Future, 3 avril 2023, https://www.recordedfuture.com/the-cloud-has-complicated-attack-surface-management

2 « Uptime Institute's 2022 Outage Analysis Finds Downtime Costs and Consequences Worsening as Industry Efforts to Curb Outage Frequency Fall Short » (L'analyse des défaillances 2022 compilée par l'Uptime Institute révèle que les coûts et les conséquences des interruptions de service empirent face à l'échec des efforts du secteur pour réduire la fréquence des pannées). Uptime Institute, 8 juin 2022, https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening

3 Cimpanu, Catalin. « Bandwidth.com expects to lose up to $12M following DDoS extortion attempt » (Bandwidth.com s'attend à perdre jusqu'à 12 millions de dollars après une tentative d'extorsion à l'attaque DDoS). The Record, 1er novembre 2021, https://therecord.media/bandwidth-com-expects-to-lose-up-to-12m-following-ddos-extortion-attempt

4 Holmes, David and Blankenship, Joseph, et al. « The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021 » (The Forrester Wave™: solutions d'atténuation des attaques DDoS, premier trimestre 2021). Forrester, 3 mars 2021

5 Didio, Laura. « The Cost of Enterprise Downtime » (Le coût des interruptions de service pour les entreprises). TechChannel, 30 septembre 2021. https://techchannel.com/IT-Stratgy/09/2021/cost-enterprise-downtime

6 « The Cost of Downtime for the Top US Ecommerce Sites » (Le coût des interruptions de service pour les principaux sites d'e-commerce américains). Gremlin, dernier accès le 8 mai 2023, https://www.gremlin.com/ecommerce-cost-of-downtime

7 Crets, Stephanie. « Most consumers abandon a slow-loading ecommerce site » (La plupart des consommateurs quittent un site d'e-commerce lent). DigitalCommerce360, 21 août 2020. https://www.digitalcommerce360.com/2020/08/21/most-consumers-abandon-a-slow-loading-ecommerce-site

8 Duperre, Mathieu. « 44 percent of gamers respond to latency by quitting their games — what can we do to stop this? » (44 % des joueurs quittent leur jeu en cas de latence. Que faire pour mettre fin à ce problème ?) PocketGamer.biz, 24 octobre 2022, https://www.pocketgamer.biz/asia/comment-and-opinion/79974/44-per-cent-of-gamers-respond-to-latency-by-quitting-their-games-what-can-we-do-to-stop-this

9 « Infinity Data and the battle to conquer latency » (Infinity Data et la bataille pour conquérir la latence). Hazelcast and Intel, novembre 2019. https://hazelcast.com/resources/infinity-data-report

+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

CLOUDFLARE