CLOUDFLARE

Présentation de solution

Dites adieu aux boîtiers

Remplacez vos équipements traditionnels par une solution de sécurité des applications agile et évolutive, déployée en tant que service.

Les problèmes des équipements de sécurité

Les équipements physiques de sécurité sont peu adaptés pour répondre aux attaques modernes et sophistiquées sur les applications. Ces appareils sont coûteux à entretenir et à gérer, nécessitent un temps d'arrêt et ne sont pas équipés pour faire face aux pics de trafic provenant d'attaques ou de périodes de forte demande. Les entreprises doivent acheter de nouveaux équipements tous les 3 à 7 ans pour suivre l'évolution de leurs besoins en matière de débit, à mesure que la technologie avance et que les entreprises se développent. En outre, lorsque le matériel doit subir une mise à niveau ou une session de maintenance, les services de sécurité doivent être mis hors ligne, avec pour résultat des failles dans la protection. Les appareils doivent également être dimensionnés à la taille adéquate pour faire face aux pics de attendus, sous peine d'être soit sous-utilisés, soit incapables de gérer le trafic au-delà des niveaux prévus, et donc de laisser les applications sans défense.

Le passage à une sécurité basée sur le cloud aide non seulement les entreprises à rationaliser leur infrastructure et leurs opérations, mais peut également conduire à des économies considérables, en éliminant les frais de renouvellement du matériel, en diminuant la prolifération des fournisseurs et en réduisant les frais généraux des datacenters.

La différence Cloudflare

Le réseau mondial de serveurs de périphérie (Edge) de Cloudflare réduit la latence, tout en améliorant les performances et la sécurité de votre site web. Cloudflare propose toute une gamme de fonctionnalités de sécurité conçues pour vous aider à vous protéger contre une diversité d'attaques basées sur le web, avec notamment une protection contre les attaques DDoS, un pare-feu d'applications web (WAF) et une protection contre les bots. Grâce à notre architecture cloud-native, nous sommes bien équipés pour faire face aux menaces émergentes. Pour prendre un exemple, dès que notre équipe d'ingénieurs publie une nouvelle règle WAF pour notre corpus de règles gérées, les utilisateurs Cloudflare bénéficieront de ces protections dans leur environnement de production en 10 à 15 secondes. Cloudflare constitue un guichet unique pour déployer des mesures consolidées d'amélioration de la sécurité et des performances : notre solution à panneau de contrôle unique aidera ainsi les équipes de sécurité à identifier les incidents et à y répondre rapidement.

Évolutive et facile à utiliser

La plateforme Cloudflare permet aux entreprises de consommer des ressources selon leurs besoins et peut absorber de vastes attaques DDoS sans affecter les performances.

Elle permet la mise en place d'actions automatiques, plus rapides, tant en termes d'investigation sur les menaces que de réponse aux incidents, tout en minimisant les opérations manuelles de configuration et de gestion.

Protections rapides contre les attaques émergentes

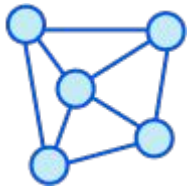
Fondée sur des informations sur les menaces provenant d'un vaste réseau mondial, la pile de sécurité cloud-native de Cloudflare aide les entreprises à répondre de front à ces attaques, sans devoir attendre la publication de nouveaux correctifs de sécurité ou de mises à jour d'équipements.

Efficace

Cloudflare réduit les précieuses heures d'ingénierie consacrées à la configuration et à la gestion, afin de vous permettre de vous concentrer sur vos initiatives prioritaires.

Nous permettons une croissance efficace, car vous ne payez que pour les ressources dont vous avez besoin, lorsque vous en avez besoin, plutôt que de devoir vous acquitter de coûts initiaux pour les équipements physiques.

Pourquoi l'évolutivité est-elle si importante pour la sécurité ?



Cloudflare permet aux utilisateurs de faire appel à des ressources selon leurs besoins, afin de répondre aux pics de trafic pendant les moments d'affluence, par exemple, lors d'une attaque DDoS ou du lancement d'un produit très demandé. Nous disposons également de solutions illimitées de protection contre les attaques DDoS et de limitation du débit, afin que vous n'ayez pas à vous soucier de devoir vous acquitter d'une tarification spéciale en cas de pics de trafic ni de faire face à des difficultés pour allouer les ressources nécessaires à la défense de vos applications.

Notre réseau peut absorber toutes les attaques DDoS, même les plus vastes, afin de préserver la présence en ligne de votre entreprise.

Découvrez le comparatif entre les fournisseurs d'équipements de sécurité et Cloudflare

	Équipements de sécurité traditionnels	Solution de sécurité des applications de Cloudflare
Coûts d'équipement	Coûts d'équipement, y compris le renouvellement et les frais généraux des datacenters.	Pas de coûts d'équipement.
Heures d'ingénierie	Les coûts d'ingénierie peuvent être élevés, avec de nombreuses heures consacrées à la gestion de scripts complexes et à la maintenance, y compris la gestion des cycles de vie matériel et logiciel.	Un produit facile à utiliser implique moins d'heures d'ingénierie consacrées à la gestion d'un fournisseur, libérant ainsi les ingénieurs pour des projets à plus fort impact.
Sécurité	Sécurité des applications proposée par des fournisseurs d'équipements : • Peut être robuste et personnalisable, mais pas très agile. • Les temps d'arrêt pour maintenance impliquent que les applications sont laissées sans protection. • Incapacité à absorber ou à répondre aux plus vastes attaques DDoS sur Internet ou à gérer les pics de trafic.	Avantages de Cloudflare en matière de sécurité par rapport aux fournisseurs d'équipements : • Réduction de plus de 50 % du temps moyen nécessaire pour détecter les attaques. • Notre échelle et notre réseau mondial nous permettent de réagir rapidement aux menaces et de détecter 30 à 40 % de tentatives d'intrusion supplémentaires. • Nous réduisons généralement le temps moyen de correction de ces attaques de plus de 90 %.
Prise en compte des répercussions	Les équipements physiques sont des immobilisations : • Ils nécessitent des coûts d'acquisition initiaux et peuvent perdre de la valeur au fil des ans. • Les entreprises ont besoin d'acquérir du matériel pour gérer les besoins en période de pic, mais les équipements sont sous-utilisés en dehors de ces épisodes.	Les dépenses d'exploitation éliminent les dépenses en immobilisations et la baisse de valeur : • Les avantages de Cloudflare en termes de comptabilité sont plus immédiats. • Le modèle de dépenses d'exploitation de Cloudflare implique que les clients peuvent facilement faire évoluer leur environnement afin de répondre à leurs besoins spécifiques, sans coûts initiaux.
Délai de mise en œuvre	• Délai d'approvisionnement en matériel (allongé par les problèmes sur la chaîne logistique). • Long processus de configuration. • La gestion centrale doit souvent être scriptée afin que les configurations puissent être déployées de manière cohérente sur l'ensemble des appareils.	• Gestion centrale de la sécurité facilitée sur l'ensemble de vos domaines. • Cloudflare présente un délai de rentabilité au moins 10 fois plus rapide par rapport aux fournisseurs d'équipements, même une fois les équipements physiques déployés et en place.