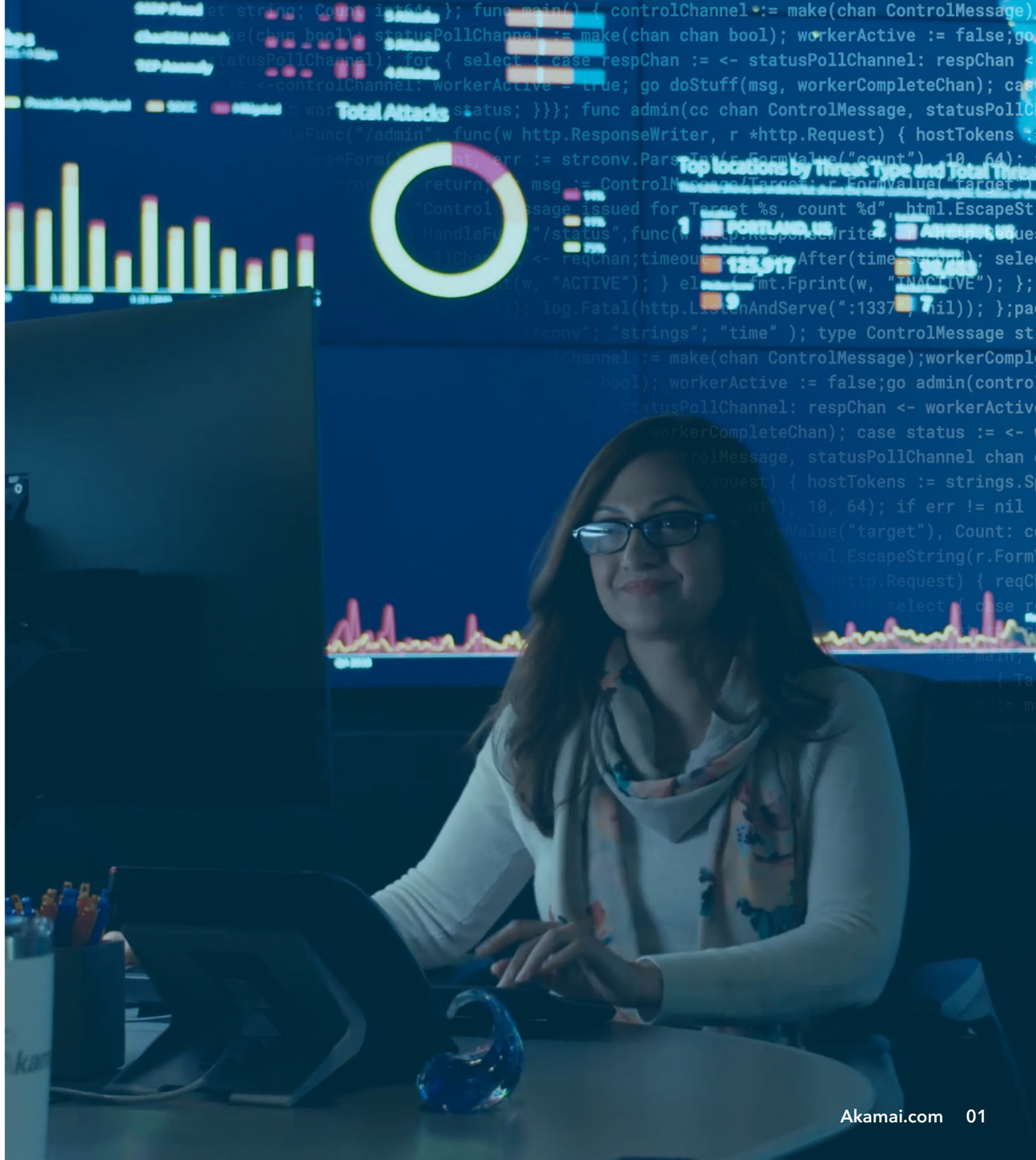
Protection contre les attaques DDoS dans un environnement de cloud hybride

LIVRE NUMÉRIQUE

Protection contre les attaques DDoS dans un environnement de cloud hybride

Les attaques par déni de service distribué (DDoS) représentent l'un des plus anciens types de cybermenaces et continuent d'être largement utilisées pour entraîner des perturbations massives, impliquant des risques de sécurité pour presque toutes les entreprises, petites et grandes. Selon IDC, les attaques DDoS devraient augmenter de 18 % d'ici à 2023, ce qui indique clairement qu'il est temps d'investir massivement dans des protections efficaces. Certaines entreprises peuvent se croire à l'abri des attaques DDoS. Cependant, la dépendance croissante à Internet pour faire fonctionner les services et les applications stratégiques expose toutes les entreprises à des temps d'arrêt et des performances réduites, si l'infrastructure n'est pas protégée.



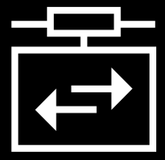
Une menace croissante

La taille des attaques DDoS double tous les deux ans, et leur complexité (le nombre et la combinaison de vecteurs d'attaque) est sans précédent. La disponibilité des applications et du réseau est essentielle à la continuité de l'activité. Les hackers ont donc intérêt à lancer des attaques DDoS volumétriques, de protocole et de couche applicative afin de perturber chaque point de défaillance potentiel, rendant les ressources sur Internet indisponibles pour les utilisateurs finaux.

LES AUTEURS D'ATTAQUES DDOS MÈNENT LEURS OFFENSIVES CONTRE TOUS LES POINTS DE DÉFAILLANCE POTENTIELS :

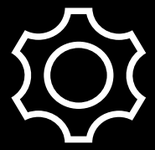
Sites Web

Applications Web et autres services d'entreprise



Concentrateurs VPN pour l'accès à distance aux ressources de l'entreprise

Contrôleurs SD-WAN



API (Application Programming Interfaces)

DNS (Domain Name System) et serveurs d'origine

Infrastructure de réseau et de centre de données

En examinant les environnements, les applications et les espaces IP des victimes, les hackers peuvent déterminer quels vecteurs DDoS peuvent potentiellement infliger le plus de dommages aux services Internet et aux infrastructures d'hébergement d'origine. Aidés par le faible niveau de barrière à l'entrée, ils peuvent utiliser différentes techniques et outils d'attaque (par exemple, think booters, attaques DDoS à la location, etc.) pour identifier les faiblesses ou les vulnérabilités des défenses de l'entreprise.

> Les hackers ont différentes motivations, notamment l'extorsion et la manipulation financière. Akamai a observé des campagnes d'extorsion qui s'étendent au-delà du secteur financier et qui ciblent les services aux entreprises, les jeux vidéo, le tourisme et l'hôtellerie, la haute technologie, la logistique et la vente au détail.
>
> — Roger Barranco, Vice President Global Security Operations, Akamai

Les répercussions des attaques DDoS s'intensifient alors que les entreprises cherchent à faire évoluer et à protéger leurs capacités d'accès à distance, afin de garantir la productivité des employés et d'assurer leurs activités quotidiennes.

Les **conséquences** d'une attaque DDoS

Dans le cas d'attaques de couche réseau (couche 3) et de couche transport (couche 4), les attaques volumétriques et basées sur les protocoles tentent de remplir les canaux Internet, de submerger les serveurs et d'épuiser les entrées de table d'état pour rendre les réseaux et les services indisponibles. Avec les attaques basées sur des applications (couche 7), les hackers visent à perturber les performances Web et l'expérience utilisateur par le biais de vecteurs tels que des attaques de type « low and slow » (de faible puissance et lentes), ainsi que des attaques HTTP, pour occasionner des temps d'arrêt ayant un impact négatif sur les résultats de l'entreprise.

Les répercussions des temps d'arrêt ne s'arrêtent pas à l'indisponibilité des services et des applications ciblés. ***Selon le Ponemon Institute, le coût annuel moyen d'une attaque DDoS pour une entreprise s'élève à 1,7 million de dollars***, à cause de l'augmentation de la charge de travail du service technique, du recours aux ressources de réponse aux incidents, des remontées d'incident en interne, des frais juridiques, des interruptions opérationnelles et de la perte de productivité des employés.

Les enjeux sont donc très importants et ne font qu'augmenter avec la migration accrue vers des infrastructures cloud hybrides.

Le cloud continue de compliquer **les stratégies de sécurité**

À mesure que les entreprises abandonnent les centres de données traditionnels pour migrer leurs applications vers des environnements hébergés dans le cloud, les architectures de sécurité deviennent de plus en plus complexes. De nombreuses entreprises peinent à protéger leurs ressources en ligne avec le même niveau de protection contre les attaques DDoS que celles situées dans le centre de données. En plus de cette complexité, de nombreuses adresses IP hébergées dans le cloud échappent au contrôle direct des entreprises, ce qui les rend vulnérables aux attaques DDOS en cas de protection insuffisante.

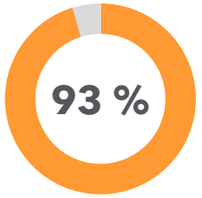
Les hackers sont bien conscients de cette migration accélérée vers les installations de colocation et le cloud public. Ils cherchent à exploiter les faiblesses des architectures et des stratégies de sécurité des entreprises, créées par des règles et des exigences de sécurité manquant de cohérence. De plus, ces entreprises ont du mal à corriger les problèmes au sein d'une infrastructure hébergée dans le cloud hétérogène et fragmentée.

RÉSULTATS :

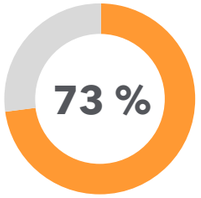
Les entreprises ont besoin de défenses adaptables pour protéger une multitude de ressources et de services Web, quel que soit l'endroit où ils se trouvent. Plus de 93 % des entreprises (< 1000 employés) utilisent une stratégie multicloud. Il est donc grand temps de combler les lacunes défensives causées par la complexité de l'infrastructure.[1]

[1] *https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020*

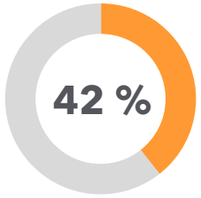
La responsabilité d'assurer la sécurité dans les environnements de cloud public peut varier d'un fournisseur à l'autre et pousser de nombreuses entreprises à se faire de fausses idées les amenant à s'exposer. Par exemple, 73 % des entreprises interrogées dans le cadre d'une enquête IBM estiment que les fournisseurs de services de cloud public (CSP) sont les premiers responsables de la sécurisation des logiciels en tant que service (SaaS), tandis que 42 % estiment que les CSP sont principalement responsables de la sécurisation de l'infrastructure du cloud en tant que service (IaaS). Ce manque de responsabilité en matière de contrôle de la sécurité peut mener à des défaillances des systèmes, un risque qu'aucune entreprise ne devrait accepter.



des entreprises utilisent une stratégie multicloud



des participants à l'enquête pensent que les CSP publics sont responsables de la sécurisation du SaaS



des personnes interrogées pensent que les CSP sont responsables de la sécurisation de l'IaaS dans le cloud

Dans un article récent, Forrester a noté que la plupart des entreprises optent pour une approche stratégique hybride, en utilisant plusieurs fournisseurs de cloud public et en hébergeant des charges de travail sur site. C'est pourquoi le cabinet d'analyse recommande de choisir un fournisseur de protection contre les attaques DDoS capable de mettre en place une protection sur des architectures hybrides.

Toutes les mesures de protection contre les attaques DDoS ne se valent pas

Avec l'augmentation des investissements dans l'infrastructure de cloud, les équipes de sécurité doivent veiller à ce que les contrôles soient homogènes dans les environnements hybrides. Comme les applications déployées sur différentes infrastructures de cloud back-end deviennent de plus en plus difficiles à protéger, de nombreuses entreprises souhaitent disposer d'un point de contrôle unique pour organiser leur défense. Les solutions de technologies de sécurité sont de plus en plus complexes. Beaucoup d'entreprises souhaitent donc disposer d'un panneau de contrôle unique, non seulement pour bénéficier d'une meilleure visibilité, mais également pour obtenir des rapports rationalisés pouvant être transmis via des API aux systèmes de corrélation des données d'événements.

Pour résoudre ce problème, les entreprises se tournent vers des fournisseurs de sécurité DDoS basés dans le cloud qui proposent de déployer, et non de limiter, leurs stratégies de migration vers le cloud hybride. Elles souhaitent des défenses évolutives et réactives, quel que soit l'endroit où sont basés leurs services. Cette demande est la réponse directe à l'augmentation de la complexité opérationnelle requise pour intégrer, déployer et gérer les défenses DDoS au sein de l'environnement unique d'un fournisseur CSP. De plus, la plupart des ressources sur Internet sont réparties sur différents clouds, accentuant encore la complexité de l'architecture.

Enfin, de nombreuses solutions de protection contre les attaques DDoS internes aux fournisseurs CSP ne sont pas efficaces dans des domaines stratégiques tels que la visibilité, les contrats de niveau de service et les rapports, autant de facteurs essentiels pour renforcer les défenses actuelles des entreprises.

Pour les équipes de sécurité, il s'agit d'accroître la visibilité et d'obtenir des informations exploitables, afin d'optimiser la réactivité et la préparation aux incidents. Certaines solutions DDoS des CSP offrent peu ou pas de transparence en termes de rapports, de visibilité et d'analyses post-attaque. Il n'est donc pas étonnant que les CSP soient considérés comme le point noir des analyses et des rapports.

De plus, certains CSP ne proposent pas de contrat de niveau de service assorti d'un délai de protection, mais offrent plutôt des crédits de service à l'entreprise concernée. Lorsque chaque seconde compte, les entreprises doivent être certaines que leur fournisseur s'engage à maintenir le bon fonctionnement et la disponibilité, sans compromettre les performances.

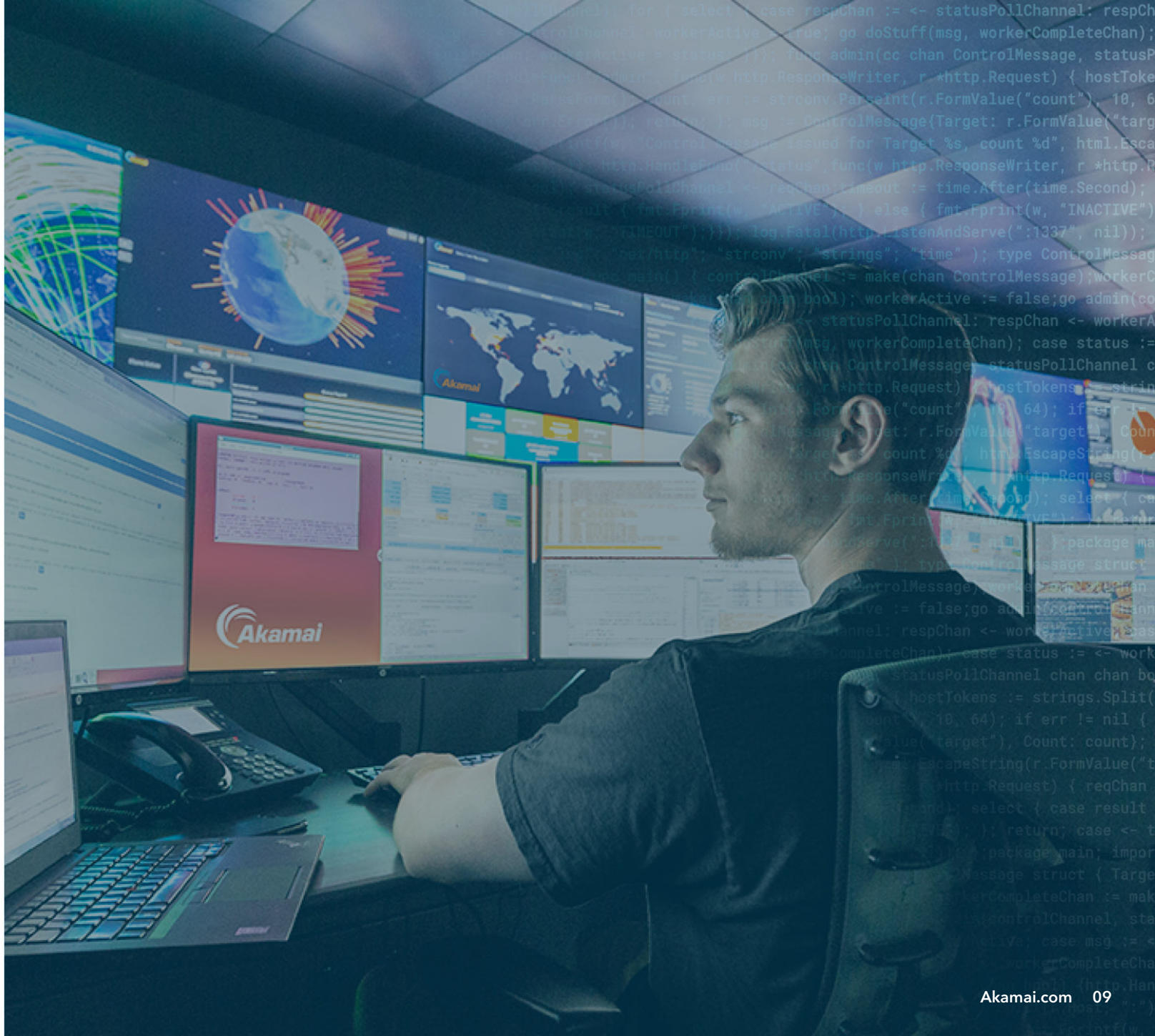
Enfin, de nombreux CSP ne fournissent pas d'accès à la demande 24h/24 et 7j/7 à l'assistance du centre d'opérations de sécurité (SOC) mondial, en plus de l'assistance avant, pendant et après l'attaque proposée par les principaux fournisseurs de solutions de protection contre les attaques DDoS basées dans le cloud. Si cette solution de protection est proposée, c'est souvent à un prix très élevé, généralement plus cher qu'une solution de protection contre les attaques DDoS spécialisée d'un fournisseur de premier plan. Grâce à une solution de protection DDoS entièrement gérée, les fournisseurs de services font office d'extension de l'équipe de réponse aux incidents de l'entreprise et offrent l'expertise nécessaire pour répondre rapidement aux attaques DDoS.

Dans le contexte actuel, il est compréhensible que les entreprises se tournent vers des partenaires de protection contre les attaques DDoS qui prennent en charge une expérience de sécurité rationalisée dans les environnements hybrides, tout en réduisant la complexité de la surface d'attaque.

Un partenaire de protection contre les attaques DDoS doit être un catalyseur de la stratégie cloud, et non un obstacle, et doit aider à soulager la pression liée à la sécurité.

Protection contre les attaques DDoS sur mesure avec Akamai

Les entreprises nécessitent une stratégie cloud de bout en bout, comme elles doivent également envisager une protection DDoS de bout en bout. En adoptant une approche globale, Akamai constitue une première ligne de défense, offrant des stratégies dédiées de protection du cloud, de DNS distribué et en bordure de l'Internet, conçues pour éviter les dommages collatéraux et les points de défaillance uniques. Contrairement aux architectures des autres fournisseurs de sécurité dans le cloud, conçues comme une solution « tout-en-un », les clouds DDoS sur mesure d'Akamai offrent une résilience accrue, une capacité de nettoyage dédiée et une meilleure qualité de protection, adaptés aux exigences spécifiques des applications Web ou des services Internet.



Les solutions de protection contre les attaques DDoS sont conçues pour bloquer les attaques DDoS dans le cloud avant qu'elles n'atteignent vos applications, centres de données et infrastructures.

DÉFENSE EN BORDURE DE L'INTERNET

La solution Akamai Edge (CDN) fournit et accélère le trafic Web à l'aide des protocoles HTTP et HTTPS. Chaque serveur en bordure de l'Internet d'Akamai fonctionne comme un proxy inverse, transférant le trafic HTTP/S légitime sur les ports 80 et 443 et reléguant tout autre trafic en bordure du réseau. Cela signifie que chaque client d'Akamai bénéficie par nature d'une protection instantanée contre toutes les attaques DDoS de couche réseau, intégrée à sa diffusion Web.

DÉFENSE DNS

La même technologie s'applique au service DNS de référence d'Akamai, la solution Edge DNS, qui supprime instantanément tout le trafic ne se trouvant pas sur le port 53. Contrairement à d'autres solutions DNS, Akamai a spécifiquement conçu Edge DNS dans un souci de disponibilité et de résilience contre les attaques DDoS, outre les performances, avec des redondances architecturales à plusieurs niveaux, y compris les serveurs de noms, les points de présence, les réseaux et même les clouds IP Anycast segmentés.

PROTECTION DE NETTOYAGE DU CLOUD

En tant que service de nettoyage du cloud éprouvé, la solution Prolexic protège l'ensemble des centres de données et de l'infrastructure Internet contre les attaques DDoS, sur tous les ports et tous les protocoles. En acheminant à la fois le trafic légitime et le trafic malveillant via Prolexic, nous sommes en mesure de créer des modèles de sécurité positifs et négatifs qui atténuent de manière proactive et instantanée les attaques DDoS avec une haute précision. Les experts du centre de commande des opérations de sécurité d'Akamai (SOCC) assistent l'équipe de réponse aux incidents du client afin d'équilibrer la détection automatisée et les interventions humaines.

Pourquoi choisir Akamai

Akamai dispose des plus grands clouds mondiaux de protection contre les attaques DDoS. Qu'il s'agisse de protéger des applications, des centres de données entiers ou des DNS de référence, Akamai a conçu la protection contre les attaques DDoS bénéficiant de la plus grande capacité, de la résilience la plus élevée et de la protection la plus rapide.

Nous avons contré certaines des plus grandes attaques DDoS lancées dans le monde. Nos contrôles de protection proactifs permettent une véritable atténuation à zéro seconde et un contrat de niveau de service de pointe. De plus, nous pouvons fournir des services de protection DDoS à une multitude de clients et lutter contre différentes attaques DDoS en même temps.

Akamai

Comme les vecteurs d'attaque DDoS ne cessent de changer et que les attaques sont de plus en plus massives, les fournisseurs doivent continuellement investir, ainsi que développer et déployer des outils et des règles pour détecter, organiser et atténuer les attaques. Akamai s'engage à contrer les menaces en neutralisant les attaques avant qu'elles ne commencent.

Votre stratégie de protection contre les attaques DDoS doit renforcer votre stratégie cloud. La plateforme Akamai Intelligent Edge offre les défenses DDoS nécessaires, permettant aux clients d'étendre la protection à l'ensemble de leurs activités, du cloud à la bordure de l'Internet, en minimisant les risques, tout en offrant la flexibilité nécessaire pour prendre en charge les évolutions futures en matière de stratégie cloud.

Contactez-nous pour découvrir comment nous pouvons **protéger** votre entreprise

En savoir plus

*Akamai sécurise et diffuse des expériences digitales pour les plus grandes entreprises du monde entier. L'Intelligent Edge Platform d'Akamai englobe tout, de l'entreprise au cloud, afin d'offrir rapidité, agilité et sécurité à ses clients et à leurs entreprises. Les plus grandes marques mondiales comptent sur Akamai pour les aider à concrétiser leur avantage concurrentiel grâce à des solutions agiles qui développent la puissance de leurs architectures multiclouds. Akamai place les décisions, les applications et les expériences au plus près des utilisateurs, et au plus loin des attaques et des menaces. Les solutions de sécurité en bordure de l'Internet, de performances Web et sur mobile, d'accès professionnel et de diffusion vidéo du portefeuille d'Akamai s'appuient également sur un service client exceptionnel, des analyses et une surveillance 24 h/24 et 7 j/7, 365 jours par an. Pour savoir pourquoi les plus grandes marques internationales font confiance à Akamai, visitez **www.akamai.com**, **blogs.akamai.com** ou **@Akamai** sur Twitter. Vous trouverez nos coordonnées dans le monde entier à l'adresse **www.akamai.com/locations**. Publication 11/20.*