radware

Fiche technique

La protection DDoS la plus avancée du secteur

Les attaques par déni de service distribué (DDoS) sont de plus en plus fréquentes, puissantes et sophistiquées. Avec l'augmentation de la disponibilité en ligne des outils d'attaque, le nombre d'attaques possibles est plus important que jamais. Le service Cloud DDoS Protection de Radware défend les organisations contre les attaques DDoS les plus avancées, en utilisant une détection comportementale avancée pour les attaques de la couche réseau (L3/4) et de la couche application (L7), la création automatique de signatures en temps réel pour protéger contre les attaques de type " zero-day ", une protection SSL DDoS unique, et des options de déploiement flexibles basées sur le cloud et hybrides qui conviennent à tous les clients.

Protection DDoS de pointe

Protection DDoS complète contre toutes les menaces possibles grâce à la détection basée sur le comportement, à la création automatique de signatures et à l'atténuation unique des attaques SSL.

SLA de premier plan

Engagé à détecter, alerter, détourner et atténuer grâce à une automatisation avancée et à des flux de travail prédéfinis. Large éventail de services et de mesures supplémentaires pour la visibilité et le contrôle.

Modes de déploiement sans friction

Modèles de déploiement à la demande, en continu et hybrides pour s'adapter aux besoins du client, à la topologie du réseau ou au profil des menaces.

Des experts à vos côtés

Une équipe d'intervention d'urgence ; un expert en protection DDoS sert de point focal pour les meilleures pratiques, la stratégie et les alertes pendant toute la durée de l'attaque.

Quadrant Knowledge Solutions
SPARK MATRIX : Atténuation des DDoS, 2022

Quadrant Knowledge Solutions
SPARK MATRIX : Atténuation des DDoS, 2021

FORRESTER®
WAVE LEADER 2020
DDoS Mitigation Solutions

IDC Analyze the Future

Choisir la bonne solution pour vous

À la demande	Toujours en service	Hybride
↗ Pas de latence supplémentaire en temps de paix ; trafic détournement uniquement en cas de détection d'une attaque	↗ Toujours disponible, en temps réel basé sur l'informatique dématérialisée Protection DDoS	↗ Combinaison de dispositifs sur site soutenus par une capacité d'épuration basée sur l'informatique dématérialisée
↗ Permet de réduire les coûts et de simplifier l'accès à l'informatique en nuage déploiement	↗ Offre une protection immédiate mais avec latence minimale ajoutée	↗ Protection en temps réel et temps de latence minimal temps de paix
↗ Convient le mieux à sensible à la latence les applications et les organisations qui sont rarement attaquées	↗ Mieux adapté à l'informatique en nuage applications hébergées et les organisations constamment soumises à des attaques DDoS	↗ Meilleure pratique de sécurité recommandée ; le mieux adapté à la protection des centres de données

Couverture mondiale, capacité massive

Le service Cloud DDoS Protection de Radware est soutenu par un réseau mondial de 21 centres d'épuration, avec une capacité d'atténuation de 15 Tbps (en augmentation). Les centres d'épuration de Radware sont connectés à l'échelle mondiale en mode maillé complet, en utilisant un routage basé sur Anycast. Cela garantit que les attaques DDoS sont atténuées au plus près de leur point d'origine et fournit une atténuation DDoS véritablement globale, capable d'absorber même les attaques volumétriques les plus importantes.

Centre de nettoyage pour l'atténuation des DDoS

Gestion et contrôle faciles

Visibilité totale
Un lieu unique pour les informations pertinentes en matière de
et des informations importantes en temps de paix
la gestion du réseau
et des données. Des détails élaborés sur le trafic
ation à l'analyse avancée qui contribue à l'amélioration de la qualité de vie des citoyens.

Expérience utilisateur améliorée
Avec une interface graphique très intuitive, navi clics. Une expérience e
mode sombre
la préférence de l'utilisateur.
La communication entre les écrans et les interfaces n'est qu'un exemple parmi 'autres, et le mode régulier est disponible pour répondre aux besoins des utilisateurs.

Centré sur l'attaque
L'état de santé du réseau est mis à jour
s'affiche. Une ressource d'attaque d
permet aux utilisateurs de répondre aux prom
L'utilisateur est informé en temps réel lorsqu'il fait l'objet d'une attaque et une indication claire est affichée pour fournir des informations importantes sur l'attaque. Cette
ptly.

Rapports détaillés
Des rapports et des analyses précieux sont fournis, que ce soit en temps de paix ou en cas d'attaque. Les informations sont facilement visualisables à partir d'un seul widget. Ces données peuvent être exportées pour une analyse plus approfondie.

Soutien en gants blancs

- Service géré par des experts grâce à l'équipe d'intervention d'urgence (ERT) de Radware.
- Alertes pré-attaque provenant de la bibliothèque Radware d'avis sur les cybermenaces, recueillis par l'exploration continue de données sur le Web, le darknet et l'analyse médico-légale post-attaque. et des recommandations.
- Un gestionnaire de compte technique dédié (TAM) qui sert de point focal pour tous les aspects de la gestion de l'entreprise.
  y compris la configuration, l'intégration, les mises à jour et l'atténuation des attaques.
- Soutenu par l'accord de niveau de service (SLA) le plus granulaire du secteur, avec des engagements détaillés concernant le temps nécessaire pour atténuer, détecter, alerter et détourner les risques, ce qui permet
  la cohérence des mesures d'atténuation et la disponibilité générale des services.

RW 1204| 03.19.2024