DELL Technologies

DDoS : renforcement de la cybersécurité et de la résilience avec Dell Technologies

La menace croissante des attaques DDoS

Les attaques par déni de service distribué (DDoS) sont désormais l'une des menaces les plus répandues et les plus perturbatrices de l'ère numérique. Les attaques DDoS exploitent de vastes réseaux d'appareils compromis pour submerger les systèmes, les serveurs ou les réseaux ciblés avec un énorme volume de trafic. Cette pression incessante ralentit les opérations ou les interrompt, et aboutit souvent à la paralysie de l'entreprise.

Aucune entreprise, qu'il s'agisse d'une start-up ou d'une multinationale, n'est à l'abri de la menace croissante des attaques DDoS. Compte tenu de la dépendance croissante des entreprises vis-à-vis des infrastructures numériques, les attaques ont des conséquences dévastatrices qui vont de la perte financière à l'atteinte à la réputation. Consciente de l'importance de ce défi, Dell Technologies propose des solutions innovantes et évolutives qui aident les entreprises à renforcer leurs défenses et à affronter les menaces.

En quoi consistent les attaques DDoS ?

Les attaques DDoS visent à perturber le fonctionnement normal d'un réseau, d'un service ou d'un serveur en le submergeant d'un volume de trafic massif provenant de plusieurs sources. Elles sont exécutées à l'aide de botnets.
Il s'agit de réseaux d'appareils infectés contrôlés à distance par des pirates.

Fonctionnement des attaques DDoS

1. **Recrutement de botnets :** les cybercriminels infectent des milliers ou des millions d'appareils avec des logiciels malveillants. Le botnet ainsi obtenu leur permet de réaliser une attaque afin de mettre votre entreprise à l'arrêt.
2. **Inondation du trafic :** les pirates donnent l'ordre aux botnets d'envoyer un flot de requêtes au serveur ciblé, après quoi le système ralentit, se bloque ou devient indisponible pour les utilisateurs légitimes.
3. **Surcharge du système :** le système, submergé par un trafic illégitime, devient incapable de répondre aux demandes légitimes, ce qui entraîne des pannes de service ou des retards importants.

Techniques courantes

- **Les attaques basées sur le volume** exploitent le volume de trafic pour épuiser la bande passante d'un réseau.
- **Les attaques basées sur le protocole** exploitent les vulnérabilités des protocoles tels que TCP/IP pour consommer des ressources.
- **Les attaques de la couche applicative** ciblent des applications spécifiques, telles qu'un site Web ou une base de données, afin de perturber leur fonctionnement.

Ces attaques évoluent constamment, ce qui en fait un défi redoutable pour les entreprises qui tentent de protéger leurs opérations.

L'impact sur les entreprises

Perte financière

Une seule attaque DDoS peut coûter des millions de dollars en pertes de chiffre d'affaires, en interruptions de service et en frais de récupération. Une indisponibilité de service, même si elle ne dure que quelques minutes, peut avoir un impact considérable sur les entreprises qui dépendent des transactions en temps réel, telles que les plates-formes d'e-commerce et les services financiers.

Interruption opérationnelle

Les interruptions causées par une attaque DDoS réduisent la productivité, retardent les processus stratégiques et entravent l'accès aux services essentiels. Dans des secteurs tels que la santé ou la fabrication, les interruptions de service peuvent avoir des conséquences majeures.

Atteinte à la réputation

Lorsque les clients subissent des interruptions de service, leur confiance diminue. Des incidents prolongés ou répétés peuvent nuire durablement à la réputation d'une entreprise, entraînant une perte de clients et une diminution de la confiance du marché.

Exemple concret

En 2020, une institution financière de premier plan a été victime d'une attaque DDoS de grande envergure qui a paralysé ses services bancaires en ligne pendant plusieurs heures. Les pertes directes de chiffre d'affaires, combinées à une réputation entachée, ont causé des dommages dépassant les **50 millions de dollars.**

Statistiques alarmantes

Selon le rapport DDoS Insights de Zayo Group (février 2024), les entreprises non protégées ont enregistré un coût moyen de **6 000 $** par minute. En 2023, le coût moyen s'est élevé à environ **408 000 $** par incident. En outre, la fréquence de ces attaques augmente : plus de **10 millions sont signalées chaque année**. Ces statistiques mettent en évidence le besoin urgent de mettre en œuvre des mécanismes de prévention solides.

20,5 millions

attaques DDoS ont été bloquées au cours du 1er trimestre 2025

Source : rapport Cloudflare sur les menaces DDoS (2024)

Lutte contre les attaques DDoS avec Dell Technologies

Dell Technologies propose une suite avancée de solutions pour aider les entreprises à anticiper les incidents DDoS, à les détecter et à assurer la récupération.

Points de terminaison renforcés avec Dell Trusted Devices

Les points de terminaison sont des points d'entrée essentiels pour les menaces liées aux attaques DDoS. Dell Trusted Devices offre des fonctionnalités de sécurité robustes intégrées au matériel, telles que Secure BIOS et SafeID, qui assurent la protection contre les accès non autorisés et préservent l'intégrité du système.

Sécurité des serveurs

Solutions de serveur Dell, équipées de mesures de sécurité intégrées telles que la technologie Dell Trusted Server, qui comprend les éléments suivants :

- **Racine de confiance matérielle :** cette fonctionnalité garantit que les composants matériels du serveur sont vérifiés au démarrage, fournissant ainsi une couche de sécurité fondamentale contre les altérations ou modifications non autorisées.
- **Fonctionnalités de sécurité intégrées :** les serveurs Dell intègrent des disques à autochiffrement et la vérification du démarrage de bout en bout, qui assurent la protection contre les accès non autorisés et renforcent la confiance dans l'intégrité des données.
- **Cyberrésilience :** cette approche inclut des fonctionnalités de détection des anomalies, des violations et des opérations non autorisées, permettant ainsi aux entreprises d'assurer une récupération rapide en cas de cyberincidents.
- **Protection complète des données :** les solutions Trusted Server de Dell intègrent des mécanismes de sécurité qui protègent les données au repos et en transit. Il s'agit notamment de techniques de chiffrement avancé et d'options de récupération automatisée conçues pour assurer la continuité de l'activité.

Ces fonctionnalités garantissent la résistance des serveurs face aux pics de trafic tout en assurant la stabilité opérationnelle. Les solutions de stockage protègent la disponibilité et l'intégrité des données stratégiques lors d'une attaque, réduisant ainsi les interruptions.

Sécurité stockage

Dell Storage vous protège contre les attaques DDoS grâce à diverses mesures de sécurité intégrées et à des technologies avancées conçues pour minimiser les vulnérabilités, détecter les menaces à un stade précoce et assurer une récupération rapide en cas d'attaque. Les méthodes clés incluent :

- **Détection proactive des menaces :** les solutions de stockage Dell utilisent une surveillance intelligente et une détection des anomalies basée sur l'IA pour identifier les schémas d'accès inhabituels susceptibles de correspondre à une attaque DDoS. Ces outils fournissent des informations de sécurité en temps réel et peuvent déclencher des réponses automatisées aux menaces afin d'atténuer l'impact d'une attaque.
- **Architecture de racine de confiance :** intégrée aux contrôleurs de stockage, cette architecture garantit l'authenticité du firmware et empêche les modifications non autorisées, ce qui améliore la sécurité du matériel de stockage tout en réduisant les risques de compromission lors d'une attaque DDoS.
- **Authentification multifacteur et contrôles d'accès :** la mise en œuvre de l'authentification multifacteur et du contrôle d'accès basé sur les rôles (RBAC) permet d'empêcher les accès non autorisés aux systèmes de stockage, ce qui renforce la protection contre les menaces associées aux attaques DDoS.
- **Microsegmentation et isolation du réseau :** en isolant les systèmes de stockage et en limitant l'accès entre les charges applicatives, Dell minimise les vecteurs d'attaque potentiels et protège les systèmes de stockage des mouvements latéraux en cas de violation.
- **Snapshots sécurisés et journaux immuables :** les solutions de stockage Dell fournissent des snapshots sécurisés et des journaux immuables qui garantissent l'intégrité des données et aident les entreprises à assurer une récupération rapide en cas d'attaques DDoS. Ces fonctionnalités facilitent l'analyse approfondie et les enquêtes sur les incidents, permettant ainsi aux équipes IT de détecter et d'analyser les vecteurs d'attaque.
- **Cyber Recovery Vault :** des solutions telles que Dell PowerMax et PowerProtect Cyber Recovery Vault créent des sauvegardes isolées, immuables et protégées contre les rançongiciels et autres attaques. Ces sauvegardes peuvent être restaurées pour assurer la continuité de l'activité sans risque de réinfection.

En intégrant ces fonctionnalités et technologies de sécurité complètes, Dell Storage et Cyber Resilience aident les entreprises à se défendre efficacement contre les attaques DDoS tout en assurant la résilience et la sécurité des environnements IT.

Surveillance proactive avec CrowdStrike

La surveillance en temps réel et l'analyse avancée sont indispensables pour détecter les anomalies dans les schémas de trafic avant qu'elles ne s'aggravent. CrowdStrike s'intègre à l'écosystème Dell pour utiliser l'analyse comportementale et les informations optimisées par l'IA afin de différencier l'activité légitime du trafic des attaques, ce qui permet une correction rapide.

Dell PowerProtect pour l'intégrité des données

Dell PowerProtect garantit la sécurité et l'accessibilité des données stratégique en cas d'attaque DDoS. Des fonctionnalités de sauvegarde immuable et des environnements de récupération isolés permettent aux entreprises de restaurer leurs systèmes et de minimiser les interruptions de service après un incident.

Sécurité réseau avancée et microsegmentation avec Dell PowerSwitch Networking et SmartFabric OS

Renforcez la défense contre les attaques zero-day grâce à une segmentation avancée du réseau, des contrôles d'accès stricts et une analyse du trafic en temps réel sur l'ensemble de votre infrastructure.

Mise en œuvre concrète

Une plate-forme d'e-commerce mondiale a récemment tiré parti des solutions PowerProtect de Dell ainsi que des fonctionnalités de détection proactive pour repousser une attaque DDoS sophistiquée. En isolant les systèmes stratégiques et en déployant des processus de récupération d'urgence, l'entreprise a relancé l'intégralité de ses opérations en un temps record, réduisant ainsi les pertes financières et préservant la confiance des clients.

Approche de la sécurité multicouche

La réussite contre les attaques DDoS repose sur des défenses multicouches et adaptatives. Pour compléter ses offres technologiques, Dell préconise les stratégies suivantes :

Étapes clés pour améliorer la défense

- **Architecture Zero-Trust** Implémentez un modèle « ne jamais faire confiance, toujours vérifier » pour examiner chaque utilisateur et appareil.
- **Chiffrement avancé** Chiffrez la communication sur toutes les couches pour protéger les données sensibles transmises lors d'éventuelles tentatives d'attaque.
- **Formation des employés** Formez les employés à l'identification des activités suspectes et au respect des protocoles sécurisés afin d'éviter les violations accidentelles.
- **Tests réguliers du système** Effectuez des évaluations de routine, y compris des tests d'intrusion et de charge, afin d'évaluer la préparation du système à des volumes de trafic élevés.

Ces actions, associées aux solutions Dell Technologies, permettent de créer un mécanisme de défense robuste et efficace contre les menaces sophistiquées.

Cybersécurité renforcée via des partenariats

Pour étendre ses fonctionnalités, Dell Technologies collabore avec des leaders du secteur tels que **Microsoft**, **CrowdStrike** et **Secureworks**. Ces partenariats offrent des couches de protection supplémentaires en intégrant les meilleures méthodologies d'intelligence sur les menaces et de détection avancée dans le cadre complet de Dell.

Utilisation de Dell Professional Services

Au-delà de la technologie, Dell Professional Services permet aux entreprises confrontées à des défis DDoS de recevoir les conseils d'experts. De la réponse aux incidents aux consultations personnalisées sur l'architecture de sécurité, l'équipe Dell veille à ce que les entreprises puissent assurer une récupération rapide et renforcer leurs défenses futures.

Construisez un avenir meilleur

Dell Technologies est bien plus qu'un fournisseur de technologies. Nous sommes un partenaire engagé à protéger votre entreprise contre l'évolution des menaces liées aux attaques DDoS. En combinant des technologies de pointe, des partenariats étroits et des informations exploitables, Dell aide les entreprises à protéger leurs opérations, à maintenir la confiance de leurs clients et à poursuivre activement leur croissance.

Faites le premier pas vers la résilience dès aujourd'hui. Contactez Dell Technologies pour défendre votre entreprise contre les menaces DDoS et sécuriser votre avenir.

Dell Technologies permet aux entreprises de relever les défis de la cybersécurité DDoS, prouvant ainsi qu'une base sécurisée est la clé de la réussite dans un monde interconnecté.

Découvrez comment relever certains des défis actuels majeurs en matière de cybersécurité sur **Dell.com/SecuritySolutions**

En savoir plus sur Solutions Dell

Contacter un expert Dell Technologies

Consulter d'autres ressources

Prenez part à la discussion avec #hashtag

DELL Technologies