Défense contre les attaques DDoS dans un environnement de cloud hybride

Table des matières

Les attaques DDoS continuent d'évoluer 3

Une menace grandissante 5

Les conséquences d'une attaque DDoS 7

Les environnements hybrides et multicloud continuent de compliquer la gestion de la sécurité 8

Tous les services de protection contre les attaques DDoS ne sont pas identiques 10

Protection sur mesure contre les attaques DDoS avec Akamai 13

Akamai Prolexic offre une protection DDoS hors pair, adaptée à la posture de sécurité proactive et positive d'une entreprise 14

Akamai Edge DNS et **Akamai Shield NS53** sécurisent et renforcent l'infrastructure DNS critique 17

Akamai App & API Protector sécurise les applications et les API contre les attaques DDoS 18

Pourquoi choisir Akamai ? 19

Les attaques DDoS continuent d'évoluer

Le déni de service distribué (DDoS), l'un des types de cybermenaces les plus anciens, a continué d'évoluer pour devenir un outil hautement sophistiqué entre les mains des cybercriminels et des hacktivistes motivés par des raisons idéologiques. En effet, les attaques DDoS posent des risques de sécurité non seulement aux petites et grandes entreprises, mais aussi aux infrastructures publiques critiques dans des domaines tels que la santé, l'énergie et les services publics, ainsi que l'éducation.

L'adoption croissante de ressources de Cloud Computing par les institutions publiques et privées complique encore davantage cette dynamique. Lorsque ces organisations combinent le cloud avec leurs ressources sur site préexistantes, l'environnement hybride qui en résulte devient beaucoup plus complexe. Les applications, les interfaces de programmation d'applications (API), les données, les microservices et les charges de travail doivent désormais traverser un environnement fragmenté. Les différentes architectures de ces environnements créent de nouvelles vulnérabilités et une surface d'attaque fracturée, qui peuvent être exploitées par les cybercriminels pour lancer des attaques DDoS de plus en plus sophistiquées et invalidantes.

Les organisations s'efforcent de s'assurer que leur infrastructure digitale est protégée. Elles ont besoin d'une plateforme de protection DDoS intégrée et hybride capable de protéger leur infrastructure sur site (cloud privé) contre les attaques DDoS courtes mais précises, mais également de tirer parti de l'échelle et de la capacité du nettoyage du cloud pour les attaques DDoS volumétriques de grande envergure.

Les tendances semblent indiquer que les attaques DDoS continueront à être plus puissantes et plus fréquentes. En février 2023, Akamai a contré la plus grande attaque DDoS jamais lancée contre un client Prolexic d'Akamai basé dans la région Asie-Pacifique (APAC), avec un trafic d'attaque culminant à 900,1 Gbit/s et 158,2 Mpps (millions de paquets par seconde). Cela s'est produit quelques mois seulement après la plus grande attaque DDoS jamais commise contre un client Prolexic d'Akamai en Europe, avec un trafic d'attaque qui a brusquement atteint 704,8 Mpps lors d'une tentative agressive de blocage des opérations commerciales de l'entreprise. Celle-ci s'ajoute à la plus grande attaque DDoS qu'Akamai a atténuée à ce jour : une attaque distribuée à 1,44 Tbit/s et 385 Mpps qui a duré près de deux heures. De fait, en se basant sur sa connaissance des schémas de trafic et d'attaque, Akamai a déterminé qu'au cours de l'année 2023, les attaques DDoS sont devenues plus fréquentes, plus longues, plus sophistiquées (avec de multiples vecteurs) et se sont concentrées sur des cibles horizontales (attaquant plusieurs IP de destination au cours du même événement d'attaque).

Une menace grandissante

Aujourd'hui, la plupart des attaques DDoS sont des attaques multivectorielles, employant souvent plus de dix vecteurs d'attaque pour submerger les systèmes et plateformes de protection DDoS rudimentaires. En effet, selon les informations internes d'Akamai sur les menaces, le nombre d'attaques DDoS multidestination ou horizontales a doublé entre 2022 et 2023. Par ailleurs, l'envergure, l'échelle et la durée globales des attaques DDoS volumétriques ont atteint les plus hauts niveaux jamais enregistrés en 2023.

L'évolution d'un certain nombre de tactiques utilisées par les pirates en conjonction avec les attaques volumétriques traditionnelles complique encore la planification de la sécurité pour les entreprises.

Les auteurs d'attaques DDoS conduisent leurs offensives contre tous les points de défaillance potentiels et ils peuvent être nombreux :

- Sites Web
- Applications Web et autres services d'entreprise
- Concentrateurs VPN pour l'accès à distance aux ressources de l'entreprise
- Contrôleurs SD-WAN
- Interfaces de programmation d'applications (API)
- Système de noms de domaine (DNS) et serveurs d'origine
- Infrastructure du réseau et du centre de données

Infrastructure DNS

Les attaques DDoS contre l'infrastructure DNS d'une organisation sont devenues de plus en plus courantes, en particulier les attaques NXDOMAIN (également connues sous le nom d'attaques par sous-domaine pseudo-aléatoire, attaques DNS Water Torture ou attaques par épuisement des ressources DNS). Plus de 60 % des attaques DDoS atténuées par Akamai en 2023 comportaient un composant DNS, les attaques NXDOMAIN constituant environ la moitié de ces attaques DDoS DNS. Ces menaces représentent un risque important pour le chiffre d'affaires et la réputation d'une entreprise, car si le DNS d'une société tombe en panne, sa présence en ligne disparaît.

Les attaques au niveau de la couche applicative

Les attaques DDoS au niveau de la couche applicative (couche 7) sont devenues plus sophistiquées, car les pirates font évoluer leurs tactiques pour exploiter une logique et des flux de travail apparemment bénins. Une vulnérabilité HTTP/2 découverte en 2023 a conduit à la plus grande attaque DDoS de couche 7 jamais enregistrée.

DDoS en tant que service

Des groupes cybercriminels organisés comme Anonymous Sudan et Killnet proposent des attaques DDoS en tant que service. Dans ce scénario, les groupes offrent leurs services, généralement un botnet, moyennant paiement, et commettent des attaques pour le compte d'un client. Ces services DDoS-for-hire peuvent être extrêmement rentables pour les groupes motivés.

Ransomware + DDoS = RDDoS

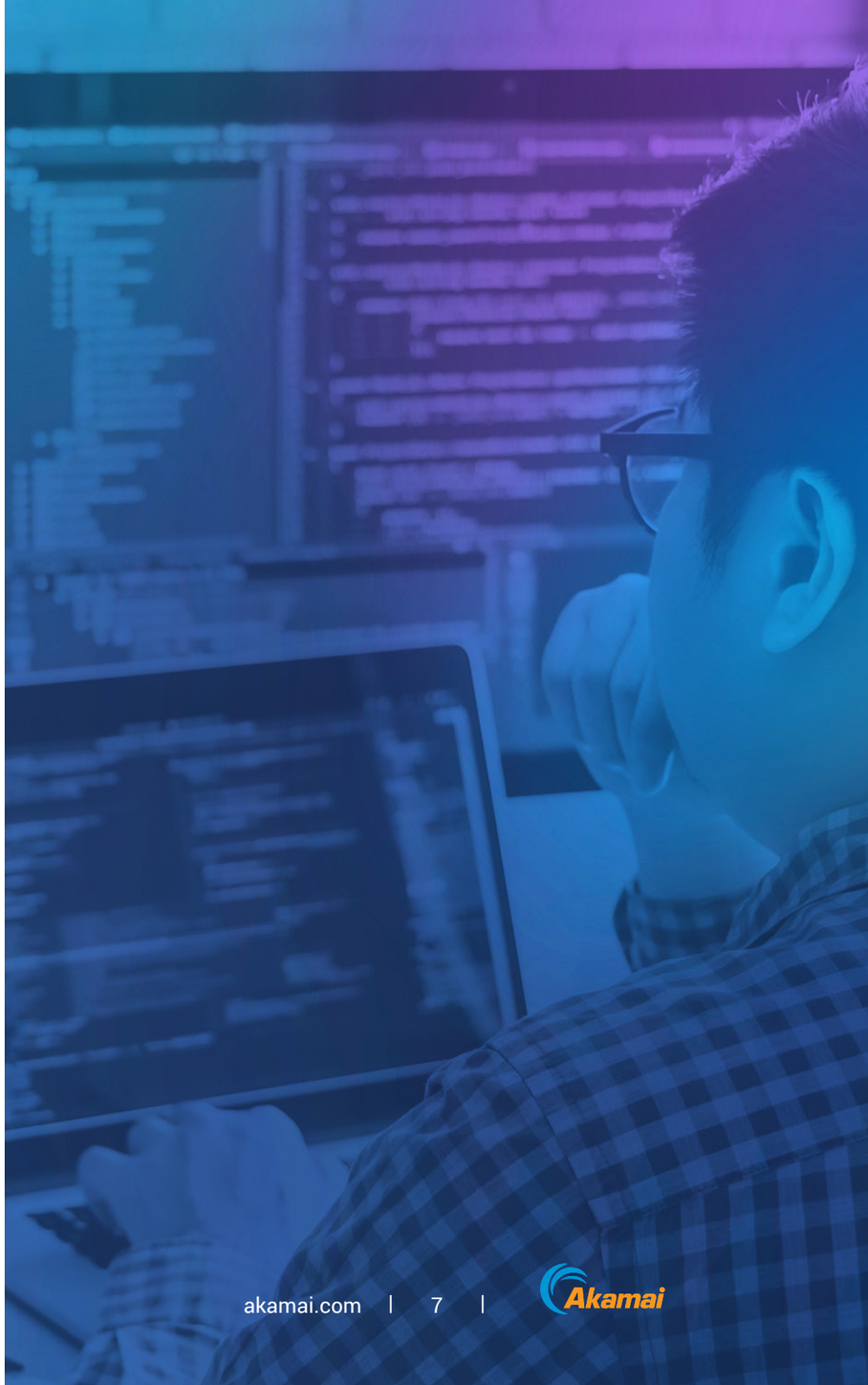
La disponibilité de tactiques telles que les DDoS en tant que service permet également aux attaquants d'utiliser plus facilement les attaques DDoS comme écran de fumée pour détourner l'attention des équipes de sécurité. Pendant ce temps, ils lancent une attaque par ransomware simultanée ou une attaque à triple extorsion. Ces attaques sont appelées attaques DDoS avec demandes de rançon (RDDoS).

Les conséquences d'une attaque DDoS

Avec les attaques DDoS sur les couches réseau (couche 3) et transport (couche 4), les attaques volumétriques et basées sur les protocoles tentent d'obstruer les réseaux de diffusion sur 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 de couche 7, les acteurs malveillants visent à perturber les performances Web et l'expérience utilisateur par le biais de vecteurs tels que les attaques low-and-slow et les floods HTTP afin de provoquer des temps d'arrêt qui ont un impact sur les résultats. Les attaques DDoS sur DNS peuvent être un peu plus complexes : selon le type d'attaque, elles peuvent affecter différentes couches du réseau d'une organisation. Par exemple, les attaques DDoS par réflexion et amplification DNS peuvent générer du trafic sur les couches 3 et 4 du réseau d'une entreprise, alors que les types de DDoS NXDOMAIN ou DNS Flood attaquent souvent la couche applicative d'un réseau.

Les répercussions des temps d'arrêt n'affectent pas seulement le coût des services ciblés et des applications indisponibles. Selon le Ponemon Institute, le coût moyen d'une attaque DDoS contre une organisation s'élève à 1,7 million de dollars par an, en raison de l'augmentation du recours au support technique, de la consommation de ressources de réponse aux incidents, des remontées internes, des coûts juridiques, des perturbations opérationnelles et de la perte de productivité des employés. En outre, pour les entreprises en contact avec les utilisateurs telles que les institutions de services financiers, les entreprises de jeux vidéo et de médias, et les sociétés de commerce électronique, la mise hors ligne risque non seulement de provoquer des dommages financiers, mais aussi, et surtout, des atteintes irréparables à la réputation.

Il est clair que les enjeux sont élevés et ne font qu'augmenter avec la migration accrue vers les infrastructures cloud hybrides.

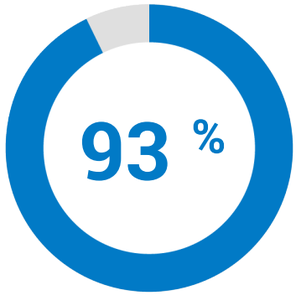


Les environnements hybrides et multicloud continuent de compliquer la gestion de la sécurité

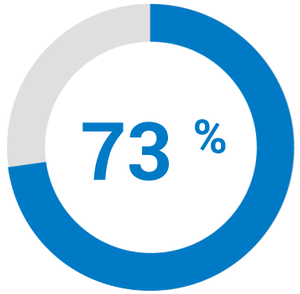
Les organisations conservent certaines charges de travail dans des centres de données sur site ou des clouds privés, et déplacent d'autres applications vers des environnements hébergés dans des clouds publics. Avec une telle approche hybride de l'infrastructure, il est extrêmement compliqué de garantir une sécurité robuste. De même, les entreprises disposent souvent d'une infrastructure DNS hybride dans laquelle certaines de leurs zones DNS faisant autorité sont gérées dans le cloud, les autres zones étant gérées par des serveurs de noms sur site et des équilibreurs de charge pour serveur globaux (GSLB). Il existe des raisons pour lesquelles les entreprises peuvent continuer à maintenir une infrastructure DNS sur site. Par exemple, elles ont peut-être déjà réalisé des investissements importants dans la mise en place d'une infrastructure sur site pour répondre aux exigences de conformité. La migration de tous les DNS vers le cloud peut ne pas être financièrement viable en raison de sa complexité.

Les acteurs malveillants, bien conscients des vulnérabilités qui découlent d'un environnement aussi fragmenté, sont impatients d'exploiter les failles de l'architecture et de la posture de sécurité d'une entreprise, qui résultent de l'incohérence des politiques et des exigences de sécurité. Ils cherchent à tirer parti des difficultés à résoudre les problèmes dans une infrastructure hébergée dans le cloud disparate et fragmentée.

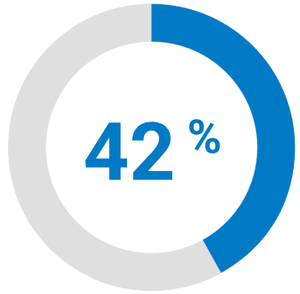
Malheureusement, la responsabilité en matière de sécurité dans les environnements de cloud public peut être incohérente d'un fournisseur à l'autre, ce qui conduit de nombreuses entreprises à faire des suppositions erronées qui risquent de les exposer. Par exemple, 73 % des entreprises interrogées dans le cadre d'une enquête IBM pensent que les fournisseurs de services de cloud publics (CSP) sont les principaux responsables de la sécurisation des logiciels en tant que services (SaaS), tandis que 42 % pensent que les CSP sont principalement responsables de la sécurisation des infrastructures cloud en tant que services (IaaS). Ce manque de connaissance concernant la responsabilité du contrôle de sécurité peut conduire à la compromission, un risque qu'aucune organisation ne devrait être disposée à accepter.



utilisent une stratégie multicloud



pensent que les CSP publics sont responsables de la sécurisation du SaaS



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

Pour résoudre ce problème, elles se tournent vers des fournisseurs de sécurité DDoS qui offrent une plateforme de protection DDoS intégrée, hautement évolutive et complète, capable de protéger leurs applications, leurs API, leur DNS et l'infrastructure sous-jacente qui les alimente.

Tous les services de protection contre les attaques DDoS ne sont pas identiques

Dans un contexte où les entreprises continuent d'investir dans l'infrastructure cloud, garantir des contrôles cohérents couvrant les environnements hybrides sera un véritable enjeu pour les équipes de sécurité. Et comme les applications déployées sur plusieurs infrastructures cloud back-end deviennent de plus en plus difficiles à protéger, de nombreuses entreprises recherchent un point de contrôle unique pour orchestrer les défenses.

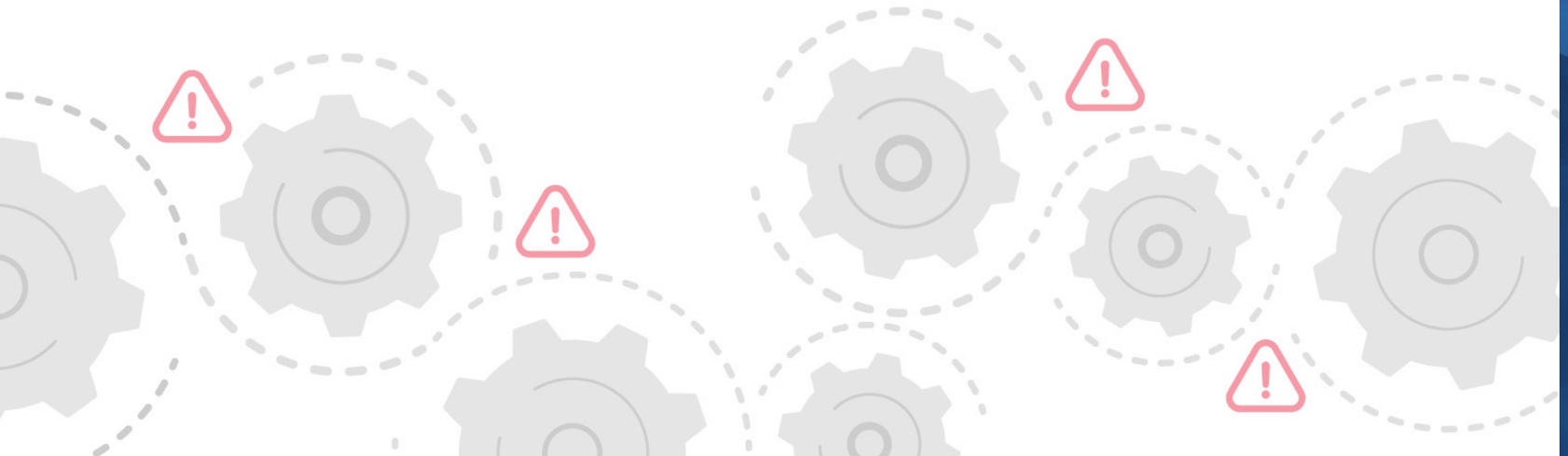
À mesure que la pile technologique de sécurité devient de plus en plus complexe, bon nombre d'entreprises souhaitent bénéficier d'une vue consolidée de leur environnement, non seulement pour optimiser la visibilité, mais aussi pour simplifier les rapports qui peuvent être alimentés par des API dans les systèmes de corrélation des données d'événements.

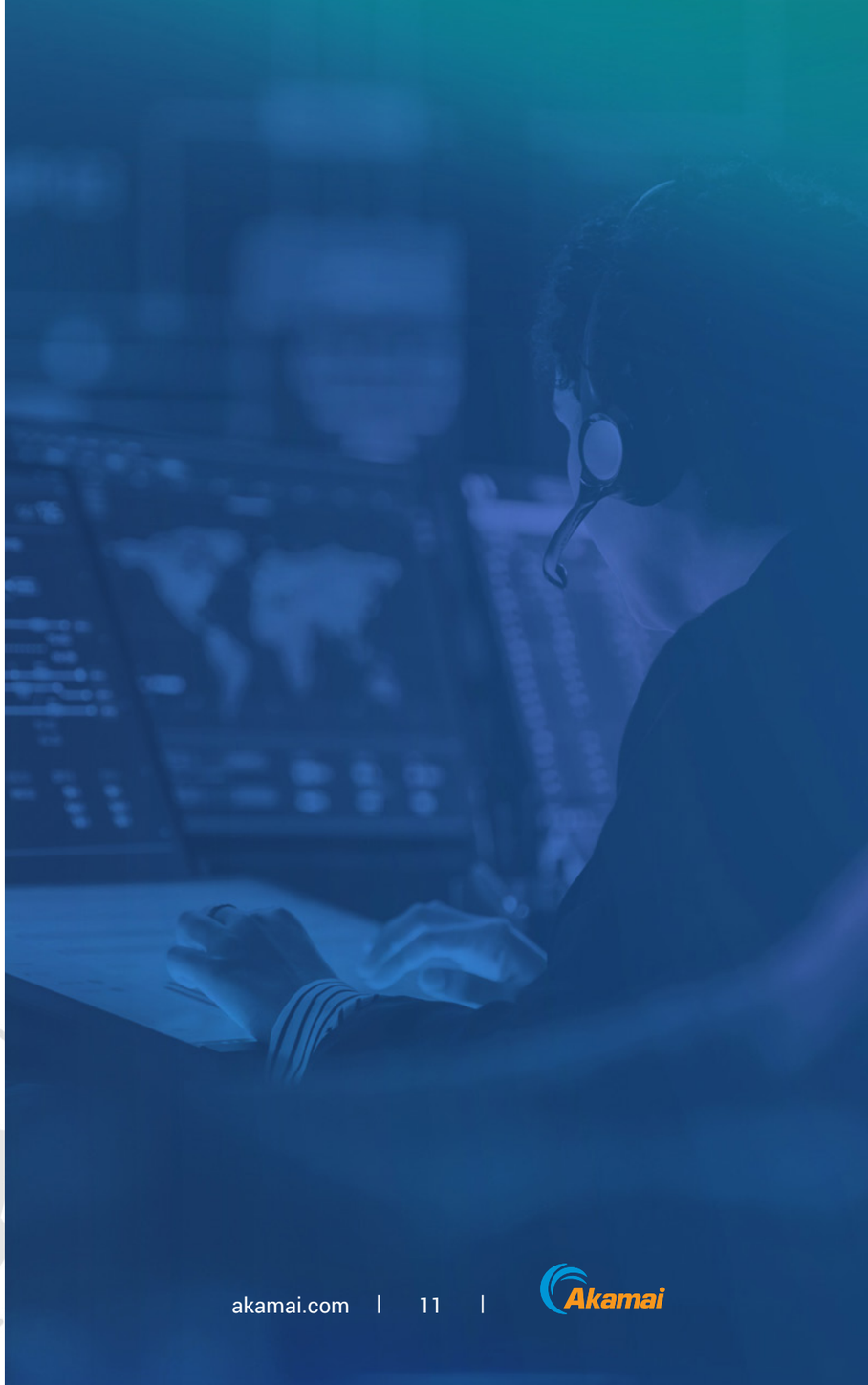
Pour résoudre ce problème, elles se tournent vers des fournisseurs de sécurité DDoS qui offrent une plateforme de protection DDoS intégrée, hautement évolutive et complète, capable de protéger leurs applications, leurs API, leur DNS et l'infrastructure sous-jacente qui les alimente. Elles veulent des défenses évolutives et réactives — quel que soit l'endroit où résident les services d'entreprise — sur site, dans le cloud ou dans un environnement hybride. Il s'agit d'une 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 CSP. Et la grande quantité d'actifs connectés à Internet situés sur plusieurs clouds privés et publics complique encore les choses.

Pour ajouter à la pression, de nombreuses solutions internes de protection contre les attaques DDoS de CSP ne fournissent pas la visibilité, les accords de niveau de service (SLA) et les rapports nécessaires pour donner aux défenseurs des entreprises d'aujourd'hui les moyens suffisants pour agir.

Pour les équipes de sécurité, il est essentiel de bénéficier d'une bonne visibilité et d'obtenir des informations exploitables afin d'optimiser la réponse aux incidents et la préparation. Certaines solutions DDoS de CSP n'offrant que peu ou aucune transparence en termes de rapports, de visibilité et d'analyse post-attaque, il n'est pas étonnant que de nombreuses équipes considèrent les CSP comme la bête noire des analyses et des rapports. Bien que certains CSP permettent à l'équipe de sécurité d'une entreprise de définir leurs propres contrôles et de maintenir la souveraineté sur les environnements spécifiques aux clients, ils rejettent généralement toute responsabilité en matière de trafic DDoS et finissent par facturer aux clients le volume astronomique de trafic malveillant associé à une attaque DDoS, qu'il s'agisse ou non d'une attaque de la couche applicative, d'une attaque de la couche réseau ou d'une attaque DDoS DNS.

De plus, certains fournisseurs de services de sécurité et CSP n'offrent pas d'accord de niveau de service (SLA) clair en termes de temps d'atténuation (TTM), au lieu de quoi ils proposent des crédits de service à l'organisation affectée. Il est important de comprendre si la clause TTM inclut le temps nécessaire à l'identification d'une attaque. S'il faut plusieurs minutes, voire plusieurs heures, à une plateforme pour identifier une attaque DDoS avant que ses protocoles d'atténuation ne s'activent, une organisation victime peut rester hors ligne pendant une période prolongée. Lorsque les secondes comptent, les organisations ont besoin d'être certaines que leur fournisseur s'engage à maintenir la disponibilité sans compromettre les performances.





En outre, il est tout aussi important (voire plus important) pour les équipes de sécurité ou les acheteurs de déterminer si les fournisseurs de services de sécurité DDoS et les CSP offrent **une capacité de défense DDoS dédiée** ou si la capacité de défense est partagée avec leur réseau de diffusion de contenu (CDN). La défense DDoS dédiée est une sorte d'équipe d'intervention spéciale qui se concentre exclusivement sur la lutte contre les attaques DDoS et ne partage pas les ressources ou l'infrastructure avec d'autres aspects de l'entreprise, comme la diffusion de contenu, garantissant ainsi un impact minimal même en cas d'attaque DDoS d'une ampleur inédite. Les entreprises qui évaluent la protection contre les attaques DDoS doivent comprendre que les fournisseurs eux-mêmes seront parfois confrontés à des attaques DDoS et doivent accorder une grande importance au fait que le fournisseur offre un SLA de disponibilité ou non.

Enfin, de nombreux CSP et fournisseurs de services de sécurité ne fournissent pas d'accès à la demande au support du centre mondial d'opérations de sécurité (SOC) 24 h/24, 7 j/7 en plus de l'assistance avant, pendant et après l'attaque. Et s'ils proposent ce service, son coût est souvent plus élevé qu'une solution spécialisée dans l'atténuation des attaques DDoS hybrides d'un fournisseur de premier plan. Avec une solution entièrement gérée de protection contre les attaques DDoS hybrides, les fournisseurs de services agissent comme une extension de l'équipe de réponse aux incidents d'une organisation et offrent l'expertise nécessaire pour répondre rapidement aux événements DDoS.

Au vu de l'écosystème des menaces actuel, il est clair que les entreprises d'aujourd'hui se tournent vers des partenaires de protection contre les attaques DDoS qui garantissent une expérience de sécurité rationalisée dans les environnements hybrides et réduisent la complexité de la surface d'attaque. Votre partenaire de protection contre les attaques DDoS doit pouvoir promouvoir votre stratégie hybride ou multicloud, et non pas l'entraver, et s'aligner sur vos objectifs commerciaux.

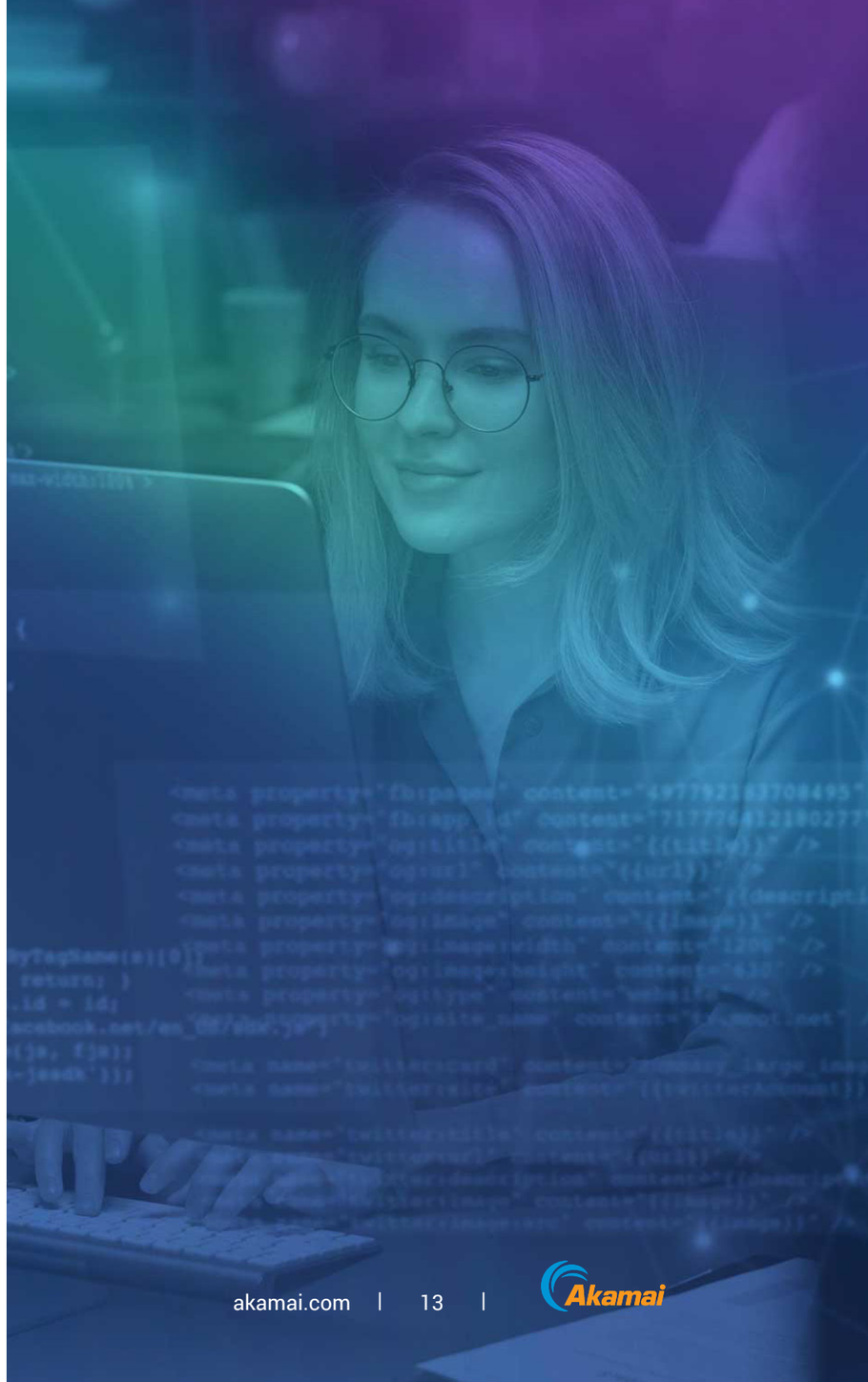
Protection sur mesure contre les attaques DDoS avec Akamai

Tout comme les entreprises ont besoin d'une stratégie d'infrastructure digitale de bout en bout qui inclut des environnements hybrides et multicloud, elles doivent également envisager une protection DDoS de bout en bout. En adoptant cette approche globale, Akamai agit comme une première ligne de défense, offrant une protection avec des stratégies dédiées en bordure de l'Internet, de DNS distribué et d'atténuation hybride. Celles-ci sont conçues pour éviter les dommages collatéraux et les points de défaillance uniques. Contrairement aux autres architectures CSP, conçues comme une solution tout-en-un, les solutions DDoS d'Akamai offrent une résilience accrue, une capacité de défense DDoS dédiée et une meilleure qualité d'atténuation, adaptée aux exigences spécifiques des applications Web ou des services Internet. La défense contre les attaques DDoS d'Akamai est disponible là où les clients en ont besoin (sur site, dans le cloud, dans des environnements hybrides) et comme ils en ont besoin (toujours active ou à la demande). Cette protection complète repose sur trois grands produits.

Capacité de défense DDoS dédiée

DNS distribué

Atténuation hybride



Akamai Prolexic offre une protection DDoS hors pair, adaptée à la posture de sécurité proactive et positive d'une entreprise

Une architecture nouvelle génération et évolutive

Akamai Prolexic utilise une architecture entièrement définie par logiciel qui peut s'adapter à l'évolution des tendances réseau liées à l'Edge Computing, à la 5G/6G et à la virtualisation réseau. Avec la transition vers des environnements logiciels virtualisés, Prolexic a supprimé toute dépendance à l'égard du matériel spécialisé. Cette standardisation du déploiement permet à Akamai de répondre plus rapidement aux besoins en constante évolution des clients, de faciliter les déploiements modulaires pour l'extension de capacité, de fournir une meilleure couverture régionale grâce à des liaisons à faible latence et d'améliorer la redondance de la plateforme. En outre, l'architecture accélère les capacités avancées d'apprentissage comportemental de Prolexic pour apprendre à partir des signatures d'attaques, s'adapter aux vecteurs de menaces émergents et construire de manière proactive des postures résilientes aux DDoS pour les clients. Prolexic Cloud est alimenté par plusieurs **centres de nettoyage répartis dans 32 zones métropolitaines mondiales et une capacité de défense dédiée de plus de 20 Tbit/s**. Pour mettre en perspective la capacité de défense de Prolexic, même les plus grandes attaques DDoS connues des couches 3 et 4 ne représentent pas 10 % de la capacité disponible pour les clients Prolexic.

Une protection DDoS complète, flexible et fiable

Akamai Prolexic est disponible dans les versions Prolexic Cloud, Prolexic On-Prem et Prolexic Hybrid.

Prolexic Cloud est le pionnier du secteur de la protection DDoS basée sur le cloud et offre aux clients des SLA d'atténuation instantanée et de disponibilité permanente de la plateforme. Les contrôles d'atténuation permettent une adaptation dynamique de la capacité en vue d'empêcher les attaques sur les flux de trafic IPv4 et IPv6. Les ressources de calcul peuvent être allouées de manière dynamique à tous les contrôles d'atténuation devant être étendus.

Prolexic On-Prem fournit une protection DDoS permanente, physique ou logique, en ligne et sur le chemin de données, qui s'intègre nativement avec les routeurs de périphérie pour arrêter automatiquement plus de 98 % des attaques en bordure du réseau d'un client, sans nécessiter de transfert de trafic. Cette solution est idéale pour la grande majorité des petites attaques rapides et pour les entreprises qui ont besoin d'une protection DDoS à très faible latence.

Prolexic Hybrid combine la puissance, l'automatisation et les performances de Prolexic On-Prem avec l'évolutivité et la capacité de pointe de Prolexic Cloud à la demande, pour protéger les origines des clients contre les attaques DDoS volumétriques les plus importantes.

La sécurité au-delà des attaques DDoS

Akamai Prolexic est livré avec Prolexic Network Cloud Firewall, une fonctionnalité entièrement en libre-service et configurable par l'utilisateur qui permet aux clients de définir, de déployer et de gérer facilement leurs propres listes de contrôle d'accès (ACL) et les règles qu'ils souhaitent appliquer en bordure de leur réseau. C'est un pare-feu qui se place devant tous les autres pare-feux. Network Cloud Firewall recommande également des ACL pour bénéficier de la meilleure position de défense proactive basée sur les données de veille sur les menaces d'Akamai, et le pare-feu fournit des analyses exploitables des règles existantes. Comme pare-feu en tant que service de nouvelle génération, Network Cloud Firewall permet aux clients :

- de définir des défenses proactives pour bloquer instantanément le trafic malveillant ;
- d'alléger l'infrastructure locale en déplaçant les règles en bordure de l'Internet ;
- de s'adapter rapidement aux changements du réseau via une nouvelle interface utilisateur.

Akamai Edge DNS et **Akamai Shield NS53** sécurisent et renforcent l'infrastructure DNS critique

Akamai Edge DNS offre une protection complète contre un large éventail d'attaques DNS sur votre infrastructure DNS, qu'elle soit sur site, dans le cloud ou dans des environnements hybrides. Cette solution offre également un haut niveau de performances DNS, de résilience et de disponibilité. Construite sur un réseau mondial distribué Anycast, Edge DNS peut être implémentée en tant que service DNS principal ou secondaire en vue de remplacer ou de renforcer l'infrastructure DNS existante, selon les besoins.

Akamai Shield NS53 est une solution de proxy DNS inverse bidirectionnel qui protège l'infrastructure DNS sur site et hybride, y compris les GSLB, les pare-feux et les serveurs de noms, contre les attaques par épuisement des ressources (alias NXDOMAIN). Les clients peuvent configurer, administrer, gérer et appliquer eux-mêmes leurs propres règles dynamiques en temps réel. Les requêtes DNS illégitimes et les flux d'attaques DNS sont éliminés à la périphérie du réseau Akamai pour protéger l'infrastructure DNS critique contre les attaques DDoS DNS.

Akamai App & API Protector sécurise les applications et les API contre les attaques DDoS

Reconnue comme une solution de protection des applications Web et des API (WAAP) incontournable sur le marché, App & API Protector élimine instantanément les attaques DDoS au niveau de la couche réseau en bordure de l'Internet (pour les propriétés hébergées sur Akamai Connected Cloud) et fournit des stratégies approfondies de défense contre les attaques DDoS au niveau de la couche applicative.

Pourquoi choisir Akamai ?

Akamai propose les solutions de protection contre les attaques DDoS les plus fiables au monde. Que vous protégiez des applications individuelles, des centres de données entiers ou une infrastructure DNS critique, Akamai a conçu une stratégie de protection contre les attaques DDoS présentant la plus grande capacité, la meilleure résilience et l'atténuation la plus rapide.

Nous avons atténué certaines des plus grandes attaques DDoS lancées dans le monde. Nos contrôles d'atténuation proactifs offrent une capacité de neutralisation immédiate et un accord de niveau de service (SLA) de pointe. Et nous pouvons fournir des services de protection DDoS à plusieurs clients tout en luttant simultanément contre plusieurs attaques DDoS.

En raison de l'évolution permanente et de l'augmentation de l'envergure des vecteurs d'attaque DDoS, une plateforme DDoS fiable doit continuellement innover, se développer et déployer de nouvelles capacités pour détecter les menaces de manière proactive, orchestrer les stratégies d'atténuation et minimiser les impacts. Akamai s'emploie à garder une longueur d'avance sur les menaces en atténuant les attaques avant leur lancement.

Votre stratégie de protection contre les attaques DDoS doit renforcer votre stratégie hybride et multicloud. Les solutions DDoS de nouvelle génération d'Akamai protègent votre infrastructure réseau digitale, vos applications et vos DNS (sur site, dans le cloud ou les deux), et offrent les avantages combinés de l'apprentissage machine et de l'intelligence humaine.

En savoir plus

 | Publication 10/24