Akamai

LIVRE BLANC

# Protégez votre entreprise contre les attaques avancées

Au fur et à mesure que les environnements informatiques se complexifient, les cyberattaques évoluent pour tirer parti des nouveaux points de défaillance. Les applications, les API, les microservices et les composants ne cessent d'augmenter et changent en permanence la façon dont les entreprises mènent leurs activités en ligne. Malheureusement, elles créent également de nouvelles vulnérabilités et de nouvelles surfaces de menaces que les attaquants peuvent exploiter. Les solutions de cybersécurité doivent répondre à la fois aux menaces internes (sécurisation de vos propres données) et externes (blocage des attaques par ransomware, DDoS, épuisement des ressources, etc.).

Nous le savons bien, car les chercheurs d'Akamai analysent en moyenne 788 To de données chaque jour. Nous innovons continuellement en nous appuyant sur les connaissances acquises, afin de vous protéger, vous et vos utilisateurs, contre les attaques les plus dangereuses et les campagnes avancées, même si les attaques continuent d'évoluer.

Quelles sont les attaques les plus dangereuses auxquelles votre entreprise pourrait faire face et comment pouvez-vous vous y préparer ?

## Les ransomwares sont en plein essor

La perte d'accès à vos données (et à celles de vos clients) est l'une des plus grandes menaces pour votre entreprise. Entre le premier trimestre 2022 et le premier trimestre 2023, le nombre d'attaques par ransomware a augmenté de 143 % dans le monde, les attaquants tirant parti des vulnérabilités Zero Day et One Day, selon le rapport Les ransomwares évoluent d'Akamai. Mais vous pouvez réduire la probabilité et l'impact des attaques avancées grâce à la segmentation.

Si la segmentation est une approche architecturale qui divise un réseau en segments plus petits dans le but d'améliorer les performances et la sécurité, la microsegmentation est une technique de sécurité qui vous permet de diviser logiquement un réseau en segments de sécurité distincts jusqu'au niveau de la charge de travail individuelle. Les contrôles de sécurité et la prestation de services peuvent alors être définis pour chaque segment unique.

Akamai Guardicore Segmentation, qui fait partie de la plateforme Akamai Guardicore pour une sécurité Zero Trust, agit pour contenir les attaques sur tous vos systèmes critiques, les empêcher de se propager à travers vos ressources (ce que l'on appelle la circulation est-ouest), puis favoriser l'intervention et la récupération. Il en résulte une protection contre les dommages à la réputation, la perte de données et la perte de revenus qui accompagnent une violation réussie.

La plateforme Akamai Guardicore est une solution sans agent pour la microsegmentation. Elle peut donc être déployée rapidement et facilement, sans avoir à apporter de modifications physiques à votre réseau ni à vous soucier de l'emplacement de vos serveurs et de vos terminaux. Elle génère un visuel interactif de toutes les connexions de votre réseau, vous aidant à surmonter l'un des principaux obstacles au déploiement : le manque de visibilité. En outre, Akamai a développé des moyens actifs pour résoudre les problèmes liés aux éventuels goulets d'étranglement des performances et aux exigences de conformité, ainsi qu'à l'application de règles pouvant couvrir de nombreux types d'infrastructures. Vous bénéficiez ainsi d'une visibilité étendue et d'un contrôle granulaire, sur tous les environnements, le tout depuis une plateforme unique.

Akamai dispose d'une visibilité inégalée sur le trafic en ligne sur l'ensemble de son réseau mondial massivement distribué. La plateforme Akamai Guardicore s'en sert pour vous donner une visibilité approfondie sur votre environnement, vos ressources, vos accès et vos flux réseau. Avec ces informations en temps réel, vous avez l'assurance que votre entreprise ne connaîtra pas de perturbations.

## Applications et API prises pour cible

Combien d'applications votre entreprise utilise-t-elle ? Le chiffre auquel vous pensez est presque certainement en-deçà de la réalité. Une entreprise moyenne utilise plus de 1 000 applications. La forte dépendance aux API pour presque toutes les transactions en ligne, et l'adoption croissante d'architectures reposant sur les microservices, induisent également une complexité accrue des applications. Malheureusement, la pression pour se développer rapidement grâce à l'innovation conduit souvent les entreprises à publier des applications avant qu'elles n'aient pu être rigoureusement testées pour détecter d'éventuels problèmes de sécurité, ce qui introduit davantage de risques pour l'ensemble de l'écosystème applicatif.

Le récent rapport État des lieux d'Internet d'Akamai a révélé que 29 % des attaques mondiales ciblaient les interfaces de programmation d'applications (API), qui sont au cœur de la plupart des transformations digitales. Dans la région Europe, Moyen-Orient et Afrique, cette part était légèrement supérieure à 47 %. Les API sont un vecteur d'attaques courant pour les cybercriminels, qui utilisent aussi bien des techniques traditionnelles que spécifiques aux API. Les bots, les attaques par déni de service distribué (DDoS) et les attaques multivectorielles doivent tous être pris en compte.

Protéger vos applications Web avec Akamai App & API Protector préservera votre workflow, vos utilisateurs et votre entreprise des activités malveillantes et de la fraude. Cette solution fournit des protections de pare-feu configurables qui peuvent absorber les attaques visant la couche applicative, y compris celles lancées via des API. Grâce à la visibilité en temps réel sur le trafic des bots, vous pouvez étudier les analyses Web biaisées, empêcher la surcharge de l'origine et personnaliser les autorisations pour permettre l'accès aux bots tiers et partenaires, sans obstruction.

Mais, pour revenir à la question initiale, que se passe-t-il si vous ne connaissez pas toutes vos applications et API ? La visibilité est, une fois de plus, la clé : Akamai API Security identifie toutes vos API, évalue leur niveau de risque et réagit aux attaques. Elle empêche les attaquants d'accéder à vos données, de charger des fichiers malveillants sur les serveurs ou de submerger les serveurs avec des pics de trafic.

**Le saviez-vous ?**

Les attaques DDoS ont augmenté de 50 % entre 2021 et 2023

Plus de 60 % du total des attaques DDoS en 2023 comportaient un composant DNS

## Défendez-vous contre les attaques DDoS et par épuisement des ressources

Les attaques par déni de service distribué figurent parmi les menaces en ligne les plus répandues. Elles sont apparues dès les premières heures d'Internet et leur impact n'a fait que suivre la courbe exponentielle du développement du Web. Ces dernières années, les attaques DDoS ont augmenté en taille, en durée et en sophistication avec des vecteurs d'attaque et des destinations multiples. Le nombre d'attaques DDoS hautement volumétriques a augmenté de 50 % entre 2021 et 2023. Et plus de 60 % du total des attaques DDoS en 2023 comportaient un composant DNS.

Même les plus grandes entreprises peuvent être mises à mal par ces botnets hostiles, perturbant alors le service de millions de clients en paralysant leurs activités. Les cybercriminels dotés de très nombreuses ressources, les acteurs étatiques et les hacktivistes motivés par la situation géopolitique exploitent les botnets volumineux et distribués, non seulement pour mettre à mal les plus grandes entreprises, mais aussi les institutions publiques critiques, allant des écoles et des hôpitaux aux aéroports et aux fournisseurs de services publics. Les attaques DDoS dévastatrices et les attaques par épuisement des ressources visent toutes les couches, les ports, les protocoles et même le DNS des entreprises et des institutions.

Protéger votre infrastructure contre les attaques DDoS nécessite une veille stratégique en temps réel. Les données que nous recueillons sont utilisées pour alimenter Prolexic, notre solution de protection contre les attaques DDoS et d'atténuation. Capable de protéger l'infrastructure digitale sous-jacente qui alimente les applications et expériences digitales d'une entreprise, elle bloque les attaques sur tous vos ports et protocoles (dans le cloud, sur site ou les deux) avant qu'elles n'affectent votre entreprise.

Ces dernières années, nous avons pu observer une résurgence significative des attaques par épuisement des ressources visant l'infrastructure DNS des entreprises. Le DNS est l'élément fondamental de la présence en ligne d'une entreprise. Si le système DNS tombe en panne, alors il n'y a plus de présence en ligne. Edge DNS et Shield NS53 d'Akamai bloquent le trafic des attaques par épuisement des ressources DNS en bordure de l'Internet, et autorisent uniquement les requêtes DNS légitimes à atteindre l'origine d'un client.

La protection DDoS est depuis longtemps un enjeu de taille pour les entreprises en ligne, le volume des attaques doublant tous les deux ans avec une augmentation concomitante de leur complexité. Sécuriser tous les points de défaillance potentiels contre ces attaques est nécessaire pour éviter de perdre des revenus et la confiance des clients.

## Que se passe-t-il en cas d'attaque ?

On peut affirmer sans risque que la présence digitale de n'importe quelle entreprise sera, un jour ou l'autre, ciblée par une attaque. L'un des objectifs d'une stratégie de sécurité est de vous protéger avant l'attaque ; vous éviter d'être pris pour cible en protégeant vos actifs critiques, en vous donnant de la visibilité sur votre réseau et en détectant les attaques dès qu'elles commencent.

Mais que se passe-t-il en cas d'événement tel qu'une attaque Zero Day ? C'est là qu'intervient l'analyse comportementale, qui est au cœur de solutions telles qu'Akamai App & API Protector.

Akamai associe des solutions hautement automatisées, l'apprentissage machine et l'intelligence humaine de plus de 225 intervenants de première ligne travaillant dans son centre de commande des opérations de sécurité (SOCC) mondial, afin de protéger les données, l'infrastructure et les expériences digitales de ses clients.

Akamai examine plus de 13 000 milliards de requêtes DNS chaque jour et contre plus de 12 milliards d'attaques de WAF chaque trimestre. Avec toutes ces observations effectuées auprès de nos clients, nous avons transformé nos analyses des attaques en véritable force. En effet, Akamai utilise toutes ces informations sur les menaces pour accroître la réactivité et l'efficacité de ses solutions.

Même si vous n'utilisez pas encore les solutions de sécurité d'Akamai, si vous êtes victime d'une attaque, vous pouvez nous contacter via notre centre d'assistance contre les cybermenaces. Un expert en sécurité vous appellera pour vous indiquer les étapes à suivre pour atténuer les attaques en cours.

## La sécurité partout où votre entreprise se connecte au monde

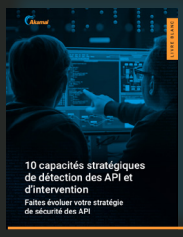
Comme la mort et les impôts, les cyberattaques figurent parmi les choses auxquelles il est impossible d'échapper. Mais vous pouvez protéger votre entreprise et vos clients grâce à des solutions de sécurité qui utilisent des informations à jour sur les menaces, offrent une excellente visibilité sur vos applications et réseaux et évoluent en fonction de l'écosystème des menaces.

Akamai protège votre expérience client, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous concevez, quel que soit l'endroit où vous le développez et où vous le diffusez. Tirant parti de la visibilité sur les menaces de notre plateforme mondiale, notre vaste portefeuille de solutions offre une fiabilité de pointe, vous permettant de garder une longueur d'avance sur les menaces et de vous adapter rapidement à l'évolution de l'écosystème de la sécurité.

## Plus de ressources


**Découvrez les cinq étapes que vous devez entreprendre pour briser la chaîne d'attaque des ransomwares**


**Soutenez votre stratégie de cloud hybride en vous protégeant contre les attaques DDoS**




**Défendez les composants de votre entreprise avec une sécurité des API renforcée**

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous créez, dans toutes vos conceptions et diffusions. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre stratégie de sécurité (activer Zero Trust, bloquer les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS), vous donnant ainsi la confiance nécessaire pour innover, prospérer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 06/24.