



Les acheteurs sont confrontés à des choix difficiles alors que le marché de la sécurité des applications Web et des API se développe et évolue

Gartner nomme Akamai leader dans son rapport Gartner® Magic Quadrant™ for Cloud Web Application and API Protection 2022

Les professionnels de la cybersécurité sont soumis à une pression intense, alors que les attaques d'applications Web et par déni de service distribué (DDoS) se multiplient et que les ransomwares prolifèrent. La sécurité des applications Web et des API, en particulier, a pris de l'importance ces dernières années avec l'augmentation des attaques ciblées. Dans ce contexte, les équipes de sécurité sont mises à rude épreuve et doivent faire face à un écosystème applicatif de plus en plus complexe, les applications Web reposant sur un environnement multicloud.

Le secteur des services financiers est un bon exemple pour illustrer à quel point les attaques contre les applications Web et les API sont devenues pernicieuses. En novembre 2022, une étude d'Akamai a révélé que [les attaques Web et API contre les entreprises de services financiers](#) avaient augmenté de 257 % au cours des 12 mois précédents, les attaquants continuant à exploiter les failles Zero Day.

Cette recrudescence des attaques peut être attribuée à plusieurs vecteurs, notamment l'inclusion de fichiers locaux et le cross-site scripting, que les attaquants utilisent pour pénétrer dans le réseau. La sécurisation des applications Web et des API est donc plus importante que jamais, car une fois que les attaquants ont exploité ces failles, elles peuvent être utilisées comme point d'entrée pour s'introduire dans les organisations cibles. En réponse à cette situation, les professionnels de la cybersécurité se tournent de plus en plus vers les fournisseurs qui proposent une offre unique pour répondre à toutes leurs exigences en matière de sécurité des applications Web et des API. Nous pensons que le rapport 2022 Gartner® Magic Quadrant™ for Cloud Web Application and API Protection est une ressource précieuse pour aider ces professionnels de la sécurité à prendre des décisions d'achat.

Lorsqu'il s'agit d'évaluer le marché des technologies de protection des applications Web et des API (WAAP), les entreprises ont désormais des besoins plus complets et plus complexes en matière de WAAP. Les acheteurs doivent désormais considérer des fournisseurs qui, au minimum, offrent quatre fonctionnalités de base : un pare-feu d'application Web, une protection DDoS, une gestion des bots et une protection des API.

Toutefois, il ne s'agit là que d'un point de départ. La plupart des organisations devraient élargir leurs exigences pour inclure un ensemble de fonctionnalités beaucoup plus large. Dans son rapport, Gartner recommande aux acheteurs de prendre également en compte les fonctionnalités suivantes :

- Protection côté client
- Analyse des failles
- Sécurité des applications pour mobile
- Services et sécurité DNS
- Réseau de diffusion de contenu (CDN), équilibrage de la charge, gestion des accès, et d'autres fonctionnalités
- Protection contre le détournement de sites Web

Le marché évolue

Alors que les achats WAAP ont historiquement eu tendance à se concentrer sur les équipements, et que même aujourd'hui certaines organisations achètent des équipements en remplacement, les déploiements de la WAAP dans le cloud sont devenus prédominants. Selon Gartner, cette tendance va se poursuivre.

« D'ici 2024, 70 % des entreprises qui mettent en œuvre des stratégies multicloud pour les applications Web dans des environnements de production privilégieront les services de plateforme de protection des API et des applications Web (WAAP) dans le cloud plutôt que les dispositifs WAAP et la WAAP native IaaS », prévoit Gartner dans son rapport.

Évaluation Gartner® Peer Insights™. Soumise le 7 avril 2022 :

« Akamai AAP est un WAF complet, comprenant la détection des attaques Web, la protection DDoS, la gestion des bots et la protection des API. En plus de la production exceptionnelle, l'équipe de service est professionnelle et apporte des réponses rapides. »

— Professionnel de la sécurité informatique et de la gestion des risques dans le secteur des services informatiques

Gartner® nomme Akamai leader dans son rapport WAAP Magic Quadrant™

Dans le Magic Quadrant™ for Cloud Web Application and API Protection, Gartner a évalué 11 fournisseurs différents selon 15 critères et a placé Akamai dans son Leaders Quadrant™. Les années précédentes, Gartner a publié un rapport similaire, le Magic Quadrant™ for Web Application Firewalls. Entre les deux rapports, Akamai a été nommé leader six fois de suite.

Dans le rapport Gartner 2022, Akamai a été positionné le plus haut pour sa « capacité d'exécution » et le plus loin pour sa « vision exhaustive ».

« Avec Akamai, nous avons accès aux dernières technologies plus rapidement et à moindre coût, tout en prenant moins de risques que si nous avions investi pour leur développement en interne. »

— Russ Soper, Directeur informatique chargé des technologies et des opérations client chez Finastra

La position d'Akamai sur le marché WAAP

App & API Protector d'Akamai offre une suite complète de produits WAAP (pare-feu d'application Web, atténuation des bots, sécurité des API et protection contre les attaques DDoS) qui fonctionnent en étroite collaboration, offrant aux clients une vue globale de leur posture de sécurité. Et ce, depuis des années. La position de leader d'Akamai dans les rapports [d'autres cabinets d'analystes](#) témoigne de l'expérience éprouvée d'Akamai sur le marché.

Par exemple, les équipes de sécurité doivent rester vigilantes face aux attaques DDoS et la protection contre celles-ci reste une compétence essentielle de la suite Akamai. Dans [Comment répondre à l'écosystème des menaces en 2022](#), Gartner prévient que les organisations doivent s'attendre à ce que les attaquants « combinent les ransomwares avec d'autres techniques, telles que les attaques par déni de service distribué (DDoS), pour mettre hors ligne les services publics jusqu'à ce que les organisations paient une rançon ».

De même, nous pensons qu'Akamai simplifie la maintenance des API grâce à des fonctionnalités API avancées qui découvrent automatiquement une gamme complète d'API connues, inconnues et changeantes dans le trafic Web, y compris leurs points de terminaison, leurs définitions et leurs profils de trafic.

Les points forts d'Akamai vont toutefois au-delà de ses principaux produits WAAP de base. L'envergure et la longue histoire d'Akamai sur le marché, avec des dizaines d'entreprises clientes, lui confèrent un avantage par rapport à ses concurrents de niche, en lui permettant de réagir rapidement aux menaces émergentes, à la fois par le lancement de produits et par son expertise interne. En particulier, l'Intelligent Edge Platform d'Akamai est le plus grand réseau de diffusion de contenu au monde. Ses milliers de serveurs périphériques répartis dans 134 pays donnent à Akamai une visibilité énorme sur les menaces mondiales émergentes. Grâce à ces ressources, Akamai est en mesure d'analyser 300 To de données d'attaques par jour. L'entreprise compte également plus de 330 experts en sécurité des données qui se consacrent à la protection des clients. Cela permet à Akamai de fournir des services dans un plus grand nombre de lieux et de détourner les menaces plus près de leur point d'origine.

Parallèlement, [l'Akamai Adaptive Security Engine](#), qui alimente les produits WAF d'Akamai, analyse automatiquement les modifications de l'environnement, les modèles de trafic Internet et l'écosystème mondial des menaces. Adaptive Security Engine calcule ensuite un score de menace pour apporter ou recommander des modifications aux paramètres de réglage de l'organisation. Les clients peuvent ensuite personnaliser les ensembles de règles en fonction des besoins de leur entreprise.



Téléchargez le rapport complet, offert par Akamai

Le marché des API continue d'évoluer à mesure que les entreprises ajoutent des applications et des API pour soutenir leurs besoins en matière de cybersécurité.

Pour ce rapport, Gartner a évalué 11 fournisseurs répondant à ses critères d'inclusion. Si vous êtes un professionnel de la sécurité, en savoir plus sur ces critères et découvrir les évaluations de ces 11 fournisseurs vous sera très utile. Nous pensons qu'il peut s'agir d'un point de départ important dans votre recherche d'un fournisseur de WAAP capable de répondre à vos besoins.

« D'ici 2026, 40 % des entreprises choisiront leur fournisseur WAAP en fonction de ses fonctionnalités avancées de protection des API et de sécurité des applications Web, contre moins de 15 % en 2022. »

— Gartner® Magic Quadrant™ for Cloud Web Application and API Protection 2022

Obtenir le rapport

Visitez akamai.com

Gartner

Gartner n'apporte son soutien à aucun vendeur, produit ou service présenté dans ses études et ne conseille aucunement aux utilisateurs de technologies de ne choisir que les vendeurs les mieux évalués ou autrement désignés. Les études publiées par Gartner représentent l'opinion de l'organisation de recherche Gartner et ne sauraient être considérées comme des déclarations de fait. Gartner rejette toute garantie, expresse ou tacite, concernant cette étude, y compris toute garantie de caractère commercial ou d'adéquation à un usage particulier. GARTNER est une marque déposée et une marque de service de Gartner, Inc. et/ou de ses affiliés aux États-Unis et dans le monde. MAGIC QUADRANT et PEER INSIGHTS sont des marques déposées de Gartner, Inc. et/ou de ses affiliés et sont utilisées ici avec autorisation. Tous droits réservés.

Le contenu de Gartner Peer Insights reflète les opinions des utilisateurs finaux d'après leur expérience avec les fournisseurs répertoriés sur la plateforme. Il ne doit pas être considéré comme des déclarations de fait, et ne représente pas les opinions de Gartner ou de ses filiales. Gartner ne soutient aucun fournisseur, produit ou service décrit dans ce contenu et ne fournit aucune garantie, expresse ou implicite, à son sujet quant à son exactitude ou son exhaustivité, y compris toute garantie de qualité marchande ou d'adéquation à un usage particulier.