Gartner

Licensed for Distribution

# Magic Quadrant pour la protection des applications Web et des API cloud

30 août 2022 - ID G00759361 - 53

Par **et 2 autres**Jeremy D’Hoinne, Adam Hils,

Le marché de la protection des applications Web et des API dans le cloud connaît une croissance rapide. Ce Magic Quadrant vous aidera à identifier les fournisseurs WAAP cloud qui offrent des contrôles faciles à utiliser et des protections spécialisées contre les bots avancés et les attaques d’API en évolution.

## Hypothèses de planification stratégique

D’ici 2024, 70 % des organisations mettant en œuvre des stratégies multicloud pour les applications Web dans les environnements de production privilégieront les services WAAP (Web Application and API Protection Platform) cloud par rapport aux appliances WAAP et WAAP natives IaaS.

D’ici 2026, 40 % des organisations choisiront un fournisseur WAAP sur la base de ses protections avancées des API et de ses fonctionnalités de sécurité des applications Web, contre moins de 15 % en 2022.

D’ici 2026, plus de 40 % des organisations disposant d’applications destinées aux consommateurs qui ne dépendaient initialement que d’un WAAP pour l’atténuation des bots chercheront à obtenir une technologie de détection d’anomalies supplémentaire auprès de fournisseurs spécialisés, contre moins de 10 % en 2022.

## Définition/description du marché

Les applications Web cloud et les plates-formes de protection des API (WAAP) atténuent un large éventail d’attaques d’exécution, notamment le top 10 de l’Open Web Application Security Project (OWASP) pour les menaces d’applications Web, les menaces automatisées et les attaques spécialisées sur les API. Les WAAP cloud sont des services fournis dans le cloud qui protègent principalement les applications Web et les API publiques.

Les principales fonctionnalités des WAAP cloud sont les suivantes :

- **Pare-feu applicatif Web (WAF) : Un WAF** combine des modèles de sécurité positifs, des signatures, des heuristiques et la détection d’anomalies pour détecter et empêcher l'exploitation des vulnérabilités des applications.

- **Protection contre le déni de service distribué (DDoS)** : elle peut atténuer les attaques volumétriques et « faibles et lentes » en offrant une bande passante suffisante, des limites de débit et une détection des anomalies. Il offre également des points de présence distribués (POP) pour atténuer les attaques plus proches de leurs sources.
- **Gestion des bots :** détecte les comportements malveillants provenant de sources automatisées grâce à des techniques basées sur la réputation, les empreintes digitales, l'heuristique et l'apprentissage automatique. Il fournit également l'assurance que les robots autorisés peuvent passer.
- **Protection des API** : permet de découvrir, de catégoriser et d'appliquer des contrôles spécialisés au trafic d'API. Il peut également extraire des stratégies de schémas d'API.

Les fonctionnalités facultatives des WAAP cloud incluent :

- Protection côté client.
- Protection contre la dégradation de la toile.
- Analyse des vulnérabilités.
- Sécurité des applications mobiles.
- Services DNS et sécurité DNS.
- Réseau de diffusion de contenu (CDN), équilibrage de charge, gestion des accès et autres fonctionnalités.

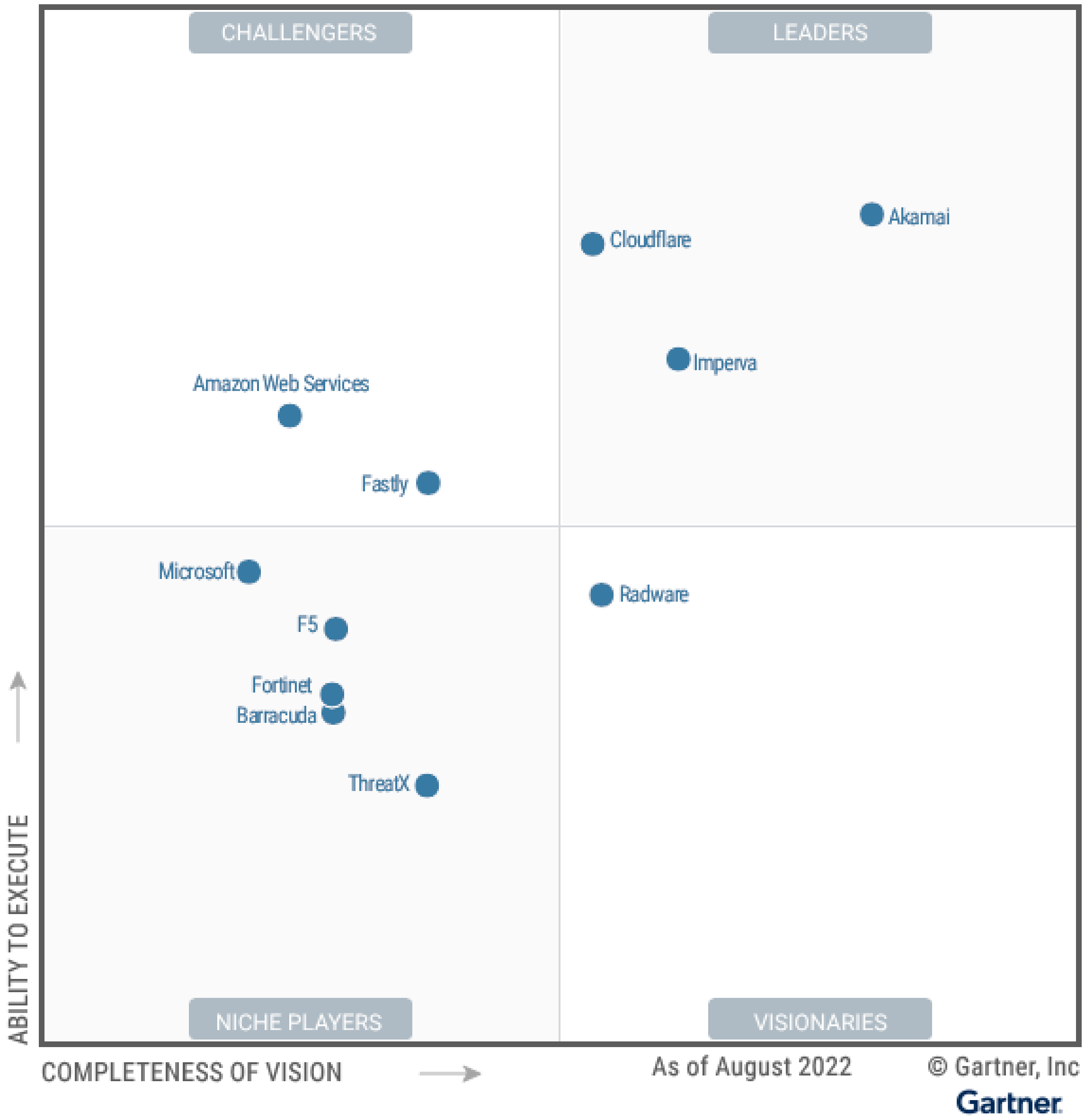
Les WAAP Cloud peuvent s'intégrer aux fournisseurs d'infrastructure, aux outils d'exploitation de sécurité et aux pipelines d'intégration continue/livraison continue (CI/CD).

La section Contexte de ce Magic Quadrant explique le changement dans la portée de cette édition et l'impact de ce changement, en particulier sur les fournisseurs qui proposent des appliances WAAP en plus des services WAAP cloud.

La section Aperçu du marché plus loin dans ce document met en évidence certaines des tendances récentes du marché WAAP.

## Magic Quadrant

Figure 1 : Magic Quadrant pour la protection des applications Web et des API



Source : Gartner (août 2022)

### Forces et mises en garde des fournisseurs

### Akamai

Akamai est l'un des leaders de ce Magic Quadrant. Il est bien adapté pour figurer sur les listes restreintes des services cloud WAAP des organisations qui souhaitent protéger les applications critiques à l'échelle du Web. C'est particulièrement le cas pour les organisations qui disposent d'un portefeuille large et diversifié d'applications Web et d'API.

Akamai est un fournisseur mondial de cloud et de sécurité comptant près de 10 000 employés. Son siège social est situé à Cambridge, dans le Massachusetts, aux États-Unis. Les principales offres d'Akamai comprennent un CDN et des services de sécurité des applications et des applications. Il a continué d'élargir son portefeuille de sécurité, notamment avec l'acquisition du fournisseur de microsegmentation Guardicore en octobre 2021.

En novembre 2021, Akamai a mis à jour son offre en fusionnant Web Application Protector (WAP), son offre simplifiée pour les entreprises du Midmarket, avec Kona Site Defender. Le nouveau produit, App & API Protector, inclut une atténuation de base des bots. Plusieurs modules complémentaires sont disponibles, y compris un abonnement avancé de gestion de la sécurité.

Depuis l’édition 2021 de ce Magic Quadrant, le changement le plus important dans le WAAP d’Akamai a été ce reconditionnement des capacités. Akamai a également lancé Account Protector pour se protéger contre la prise de contrôle de compte, une version mise à jour de son moteur de sécurité adaptatif (ASE) et la prise en charge des déploiements Terraform.

*Forces*

- Avantage de la plate-forme : en combinant et en intégrant un large éventail de fonctionnalités de sécurité des applications Web et des applications Web, la plate-forme mondiale d’Akamai séduit les grandes entreprises qui cherchent à mettre à disposition un ensemble complet de fonctionnalités devant toutes leurs applications Web.

- **Fonctionnalités avancées** : Akamai offre des fonctionnalités de pointe en matière de renseignement sur les menaces grâce à sa fonctionnalité de réputation client, et publie souvent de nouveaux contrôles avant le reste du marché. Cela est évident en termes de capacités de protection contre les menaces d’API d’Akamai, car il améliore ses capacités de découverte et de classification existantes à un moment où de nombreux autres fournisseurs n’ont même pas publié de fonctionnalités de découverte d’API.

- **Commentaires sur** le support : les clients d’Akamai continuent d’accorder une grande importance à son support, ce qui constitue une réalisation remarquable pour un grand fournisseur de plates-formes. Un support client toujours solide crée la confiance et favorise l’adoption d’Akamai lorsque des clients potentiels demandent des références à leurs pairs.

- **DDoS** : Akamai obtient des notes élevées pour l’évaluation de ses fonctionnalités DDoS. Bien qu’il soit relativement rare que les clients potentiels considèrent la protection DDoS comme un facteur de différenciation, les pics d’activité DDoS, en particulier contre les API, nécessitent toujours de solides défenses applicatives et volumétriques, fournies par Akamai.

*Précautions*

- **Prix** : Gartner continue d’entendre des clients potentiels pour qui le prix global élevé facturé par Akamai est l’une des principales raisons pour lesquelles ils élargissent leurs listes restreintes de fournisseurs ou réduisent la portée des déploiements Akamai. Les entreprises du marché intermédiaire préfèrent souvent une alternative moins coûteuse.

- **Confusion concernant la transition du portefeuille** : Gartner a reçu des commentaires de clients selon lesquels Akamai ne sait pas toujours clairement si App & API Protector remplace ou complète Kona Site Defender. Certains perçoivent le remaniement des abonnements comme un moyen de les faire payer plus ou de souscrire à plus d’options.

- **Faux positifs** : Akamai a investi dans la réduction des faux positifs grâce à son ASE amélioré, mais les clients continuent de noter un taux élevé de faux positifs, en particulier pour les détections de bots.

- **Complexité de l’interface utilisateur** : Akamai a simplifié son processus d’intégration, mais doit toujours faire face à la difficulté de combiner de nombreuses fonctionnalités et modules : pour une variété de cas d’utilisation WAAP, le déploiement devrait être plus simple. Les utilisateurs ont salué l’amélioration de la prise en charge de Terraform, mais ils restent plus susceptibles d’utiliser l’interface utilisateur et signalent que l’ASE d’Akamai et la gestion traditionnelle des politiques pourraient être plus intégrées.

**Amazon Web Services**

Amazon Web Services (AWS) est un challenger dans ce Magic Quadrant. AWS WAAP convient aux clients à la recherche de contrôles natifs, d’une approche de plateforme et d’une consolidation des fournisseurs. Les services professionnels haut de gamme pour les développeurs et l’intégration avec les outils DevOps en font un candidat de présélection populaire pour les équipes d’application.

AWS est une filiale de fournisseur de services cloud (CSP) d’Amazon. Son siège social est situé à Seattle, Washington, États-Unis. Il propose plusieurs produits de sécurité applicative et API, notamment un pare-feu réseau (AWS Network Firewall), un DDoS géré et un WAF (AWS Shield Advanced). Le WAF d’AWS est principalement disponible sur Application Load Balancer (ALB) ou Amazon CloudFront (AWS CDN).

Depuis l’édition 2021 de ce Magic Quadrant, AWS a apporté des améliorations de fonctionnalités à son offre WAAP et étendu son infrastructure CDN et WAAP en Asie/Pacifique. Les mises à jour des fonctionnalités liées au WAAP incluent des améliorations de l’atténuation des attaques DDoS de la couche application et de l’atténuation des bots, l’ajout de la fonctionnalité de gestion des versions et de restauration pour les règles gérées.

*Forces*

- **Infrastructure** : AWS se concentre sur l’augmentation de la disponibilité mondiale de son infrastructure. Le WAF d’AWS est déployé sur tous les POPs CloudFront. Il est disponible dans 25 régions AWS (disponibilité générale) et plus de 310 nœuds périphériques CloudFront avec plus de 310 POP. En 2021, AWS a ajouté plus de 80 POP, y compris en Asie/Pacifique.

- **Atténuation** des attaques DDoS : AWS propose une offre complète d’atténuation des attaques DDoS via AWS Shield et le service AWS WAF. AWS offre une atténuation pour les volumes de trafic très élevés, y compris les attaques de bots. AWS Shield protège contre les attaques DDoS volumétriques et basées sur les applications des couches 3, 4 et 7. La protection DDoS AWS Shield est disponible sous forme standard et avancée. La protection Shield Standard est incluse sans frais supplémentaires pour tous les clients AWS.

- **Tarification** : AWS utilise un modèle de tarification transparent, basé sur la consommation, facile à comprendre et à gérer ; il est clairement publié sur son site Web. AWS propose des fonctionnalités de sécurité facultatives, telles que le contrôle des bots, CAPTCHA et la prévention de la prise de contrôle de compte en tant que modules complémentaires payants au service WAF de base. Il offre également un niveau gratuit pour le contrôle des bots et la

prévention de la prise de contrôle de compte, avec un plafond d'utilisation. Shield Standard est également proposé à tous les clients AWS en tant que service d'atténuation DDoS de base.
- **Ensemble de règles géré :** AWS Managed Rules (AMR) est une fonctionnalité WAAP puissante. De nouvelles améliorations de fonctionnalités, telles que la protection contre la prise de contrôle de compte et la configuration WAF CAPTCHA basée sur le débit, les attributs et les étiquettes d'AMR, améliorent l'administration et le déploiement du produit. Un SDK JavaScript/mobile permet à la fonctionnalité AMR de protéger la page de connexion de l'application contre les attaques de bourrage d'informations d'identification et autres activités de connexion anormales.

*Précautions*

- **Sécurité des API :** AWS est à la traîne en termes de protection contre les menaces d'API, par rapport à de nombreux fournisseurs WAAP. Il offre uniquement une prise en charge directe des charges utiles JSON et prend en charge GraphQL via l'intégration AWS AppSync. Il manque également des fonctionnalités d'apprentissage automatique (ML) pour la protection contre les menaces d'API et la découverte automatique basée sur ML pour catégoriser les points de terminaison d'API.

- **Personnalisation insuffisante :** certains clients AWS trouvent que le manque de possibilité de personnaliser les règles WAF est un inconvénient. Ils regrettent également le manque relatif d'alertes de journalisation et de surveillance détaillées sur le tableau de bord.

- **Stratégie de rattrapage :** le WAAP d'AWS manque d'innovation. Pour combler les lacunes en matière de fonctionnalités, AWS continue d'ajouter régulièrement des fonctionnalités déjà proposées par les principaux concurrents. Par conséquent, les clients pour lesquels l'atténuation des bots et la protection contre les menaces des API sont des critères clés choisissent souvent d'autres fournisseurs.

- **Cas d'utilisation cloud unique :** le WAAP d'AWS est un candidat approprié pour les équipes applicatives à la recherche de contrôles natifs, mais il manque de visibilité pour les équipes de sécurité réseau et les entreprises avec des environnements hybrides et multicloud, par rapport aux offres de nombreux autres fournisseurs WAAP.

**Barracuda**

Barracuda est un joueur de niche dans ce Magic Quadrant. Son siège social est situé à Campbell, en Californie, aux États-Unis. Il fonctionne bien pour les clients existants de Barracuda et les entreprises relativement petites, mais fait face à une forte concurrence pour les contrats WAAP cloud pure-play des grandes entreprises.

Barracuda Cloud Application Protection comprend des produits et services de sécurité des applications Web, les plus importants étant les appliances cloud WAAP (Barracuda WAF-as-a-Service) et WAAP (Barracuda Web Application Firewall) de Barracuda. Le fournisseur propose également des services de gestion des bots (Barracuda Advanced Bot Protection), de DDoS et de renseignement sur les menaces. Au cours des derniers mois, Barracuda a ajouté une première version de découverte automatisée des API et de support pour GraphQL.

En avril 2022, la société d'investissement KKR a annoncé son intention d'acquérir Barracuda. Dans le passé, Barracuda a changé de mains plusieurs fois, sans impact négatif notable sur son portefeuille de produits WAAP ou sa feuille de route.

*Forces*

- **Interface utilisateur modulaire** : l'approche modulaire de Barracuda en matière de sécurité permet aux organisations de faire progresser leur déploiement WAAP en ajoutant de nouvelles catégories de contrôles au fur et à mesure de leur progression.

- Améliorations des contrôles **accessibles :** Des moteurs pratiques de notation des risques et de recommandation facilitent l'amélioration des contrôles après un déploiement initial.

- **Protection contre les menaces** d'API : Barracuda continue d'améliorer sa découverte et ses contrôles d'API. Il a introduit de nouvelles fonctionnalités telles qu'un « niveau de confiance » lors de la découverte d'API et une configuration dédiée pour graphQL. Gartner a cependant des commentaires limités sur ces nouvelles capacités.

- **Sécurité** pour les téléchargements de fichiers : Le WAAP de Barracuda offre une bonne combinaison d'inspection des logiciels malveillants et de protection des formulaires pour les applications qui nécessitent des téléchargements de fichiers sécurisés (par exemple, les applications qui reçoivent les CV des candidats).

*Précautions*

- **Visibilité en liste restreinte** : le WAAP cloud de Barracuda lutte pour une visibilité au-delà des clients existants de Barracuda en Amérique du Nord. Lorsque les clients évaluent Barracuda, Gartner a tendance à recevoir des commentaires indiquant que le produit est assez bon mais ne se démarque pas.

- **Atténuation** des bots : Barracuda, qui a acquis un fournisseur d'atténuation des bots en 2019, n'innove pas en matière de fonctionnalités avancées de gestion des bots aussi rapidement que ses principaux concurrents sur le marché WAAP. Le réglage de l'atténuation des bots est principalement une activité back-end, qui n'est pas transparente pour les utilisateurs finaux. Les options de réponse sont moins flexibles que celles des principaux concurrents et, jusqu'à récemment, les fonctionnalités avancées dédiées à la protection des informations d'identification faisaient défaut.

- **Incident response:** Barracuda's real-time incident response depends too much on external integrations. Native event views are basic and lack some reports that security operations centers (SOCs) use for external communication about their activities.

- **Support quality:** Feedback from Barracuda customers about its support varies greatly. Many express concern about the time it takes to get a precise answer when an issue concerns more than a basic configuration.

**Cloudflare**

Cloudflare is a Leader in this Magic Quadrant. It is based in San Francisco, California, U.S. It has quickly become very visible on cloud WAAP shortlists seen by Gartner, and has developed a set of security features to compete with other Leaders.

Cloudflare has more than 3,000 employees, who are building its portfolio of cloud-delivered application and security services. Its application security portfolio includes a cloud WAAP offering (Cloudflare WAF), and DDoS and client-side protection (Cloudflare Page Shield).

In recent months, Cloudflare has continued to expand beyond application protection and delivery. Recent WAAP features include API discovery, scheme ingestion and semiautomated rate limiting. The vendor also improved its bot mitigation module.

*Strengths*

- **Threat intelligence:** Cloudflare's large base of small and midsize business (SMB) and personal customers helps feed its global threat intelligence in order to detect new attacks more quickly. The vendor combines its own analysis with third-party feeds, and recently acquired Area1 Security, which further diversifies its sources.

- **Expanding presence in Asia/Pacific:** Cloudflare's infrastructure in Asia/Pacific is already one of the most developed in the WAAP market. The vendor continues to invest in this region, as is shown, for example, by a recent increase in its hiring.

- **Pervasive presence:** Cloudflare has a strong ecosystem of channel and technical partnerships. These make Cloudflare an extremely common choice by organizations in their infancy. They also mean that its technology is an important one to work with for application platforms.

- **Platform advantage:** By making security service edge (SSE) features available, Cloudflare has increased the chance of it being selected for enterprise platform and consolidation projects. This has considerably increased its attractiveness to large enterprises.

*Cautions*

- **Lack of hybrid deployment:** Cloudflare is a pure-play cloud-delivered WAAP provider. Its offering lacks the option to run as an agent, a Kubernetes sidecar or a containerized WAAP. The lack of these hybrid deployment options might deter organizations deploying API architecture and looking for a way to monitor east-west traffic.

- **Support:** Although there have been some improvements to Cloudflare's presales support, Cloudflare's larger enterprise customers continue to expect more consistent and better postsale support. Gartner observes discrepancies in phone support quality and occasional failures to follow up requests consistently.

- **Forensic analysis:** Large enterprises with in-house SOCs continue to complain about Cloudflare's basic reporting capabilities and insufficient embedded features for incident response drill-down, although these have improved recently.

- **User interface:** Gartner continues to receive comments from users stating that Cloudflare's management interface can appear cluttered and confusing. Although they like its embedded dashboards, they would like to see easier ways to perform custom security configuration from the UI. Cloudflare has, however, recently updated its WAAP UI, based on customer feedback.

### F5

F5 is a Niche Player in this Magic Quadrant. Headquartered in Seattle, Washington, U.S., F5 is a large vendor, with roots in the application delivery controller market, that now provides a portfolio of application delivery and security products. It employs more than 6,500 staff, including a large web application security team. F5's WAAP portfolio includes multiple solutions. Its main cloud-based WAAP offering is Distributed Cloud WAAP, built by combining its BIG-IP Advanced WAF, Volterra and Shape Security acquisitions. It also offers managed services (Silverline Web Application Firewall), Silverline DDoS Protection, Silverline Shape Defense, and a new cloud-managed Distributed Cloud Account Protection service for fraud prevention. F5 also offers an appliance-based WAF (BIG-IP Advanced WAF) and a lightweight module for NGINX called App Protect.

F5 launched its Distributed Cloud WAAP product in February 2022, combining Shape, Volterra and F5 WAAP technology into a single cloud-based WAAP platform. This is an important milestone in F5's strategic transition to a cloud-native platform. F5 has also acquired Threat Stack to improve its ability to provide cloud security and compliance for infrastructure and applications.

*Strengths*

- **Ease of reporting:** Distributed Cloud WAAP's management console includes useful reporting features out of the box. These include the ability to view the health of microservices through a service mesh view and transactions of APIs through a service graph and API endpoint reports.

- **Flexibility of pricing model:** F5 offers a free tier to enable organizations to get started with load balancing and very basic WAF policies for its Distributed Cloud WAAP, which appeals to small and midsize organizations.

- **Managed-service and support team investment:** F5 invests heavily in its support capability and keeps a good number of personnel in both its managed service and support teams. Customer feedback about Distributed Cloud WAAP is limited because of this offering's recent release, but F5 has a strong reputation for support.

- **Product strategy:** Consolidating into a distributed cloud platform backed by many modules shows good vision from F5 in responding to the market trend for consolidation of WAAP features.

*Cautions*

- **Distributed WAAP is new and maturing:** Early feedback from clients indicates that F5's new Distributed Cloud WAAP is still a work in progress and does not have feature parity with Silverline at the time of writing. F5 has, however, announced progress in reaching feature parity with the June 2022 version of Distributed Cloud WAAP.

- **Disjointedness of WAAP portfolio:** F5 continues to invest in separate WAAP products, which leads to feature disparities. For example, the iRules feature is not carried over into the Distributed Cloud WAAP offering (it is replaced by Service Policies). Organizations that adopt multiple F5 WAAP products for hybrid WAAP scenarios need to evaluate the operational complexity of managing different WAAP policies.

- **Complexity of configuration:** Within Distributed Cloud WAAP, every origin pool and WAAP instance is tied to a load balancer configuration and requires configuration for load balancers in addition to WAAP policies.

- **Roadmap execution:** The shift from on-premises WAF appliance vendor to cloud WAAP provider is proving challenging for F5. Distributed Cloud WAAP remains a work in progress, and the UI reproduces configuration workflows that sometimes mimic an appliance form factor. F5 has made slower progress than its leading competitors in terms of key capabilities such as bot mitigation, application security and API threat protection, as it has focused its efforts on rebuilding features for its new platform.

### Fastly

Fastly is a Challenger in this Magic Quadrant. Headquartered in San Francisco, California, U.S., Fastly is a CDN and DDoS provider that offers a cloud-based WAAP through integration of its Signal Sciences acquisition. The Fastly Next-Gen WAF solution can be deployed as a runtime agent on top of an NGINX proxy and as a WAAP service. The foundation of Fastly's technology places minimal focus on traditional signatures. It relies on its proprietary SmartParse engine, which uses a proprietary mix of rules to parse requests: vendor rules; templated rules, with some customization; and custom rules ("power rules").

Since the 2021 edition of this Magic Quadrant, Fastly has introduced edge rate limiting and a managed service called Response Security Service (RSS). It has also added support for GraphQL inspection and HTTP/3.

#### *Strengths*

- **Flexibility of deployment model:** Fastly's deployment model lets customers deploy its WAAP in multiple environments, such as the Fastly edge cloud. They can also deploy it in various ways, such as within a traditional application, as a reverse proxy, or integrated with containers and platform as a service (PaaS) environments.

- **Sales and support experience:** Customers give Fastly high scores for its lower-than-expected false-positive rates, after tuning. Clients rate Fastly highly for overall sales and support, praising both the timeliness of its responses and the quality of its support team.

- **Native DevOps support:** Fastly supports native integration with containers. It also offers support for Terraform, as well as a variety of other DevOps tools for integration, such as Ansible. Additionally, there is integration with Slack for alerting. Customers praise Fastly's capabilities, with integration for DevOps teams being the reason that many choose Fastly over other WAAP vendors.

- **Ease of onboarding:** Fastly customers frequently identify ease of onboarding in blocking mode as a strength of Fastly's product, especially when they are migrating from a legacy WAF that required a large number of tuning policies.

*Cautions*

- **Slowness of roadmap execution:** Fastly introduces new features more slowly than many vendors in this market. This results in a widening capability gap between Fastly and its competitors in areas such as API and application security features.

- **International presence:** Although Fastly has invested in expanding its sales staff outside North America, it still derives most of its revenue from U.S. customers. Clients outside North America looking to utilize Fastly's edge should verify how it is supported in their country.

- **Bot management features:** Fastly continues to lag behind its main competitors in terms of bot mitigation capabilities, and client feedback indicates that its bot reporting is weak. Fastly lacks a curated credential-stuffing database and still offers only basic blocking techniques, such as blocking based on velocity.

- **Native reporting:** Fastly customers frequently complain that integration with a third party is required for richer and more flexible reporting capabilities.

### Fortinet

Fortinet is a Niche Player in this Magic Quadrant. Fortinet sells a WAAP service called FortiWeb Cloud. It also offers a WAAP appliance product line called FortiWeb, which is shortlisted mainly by existing network firewall customers who want to consolidate on a single vendor.

Headquartered in Sunnyvale, California, U.S., Fortinet is an established infrastructure and security vendor with over 10,000 employees. Its primary product line remains its range of FortiGate firewall appliances, but it has developed a large portfolio of security products and is slowly expanding into cloud services.

During the evaluation period for this Magic Quadrant, Fortinet acquired Sken.ai, a DevSecOps application security vendor, which could enhance the ability of Fortinet's WAAP to integrate with dynamic DevSecOps teams or pipelines and processes. Feature updates to Fortinet's WAAP service include a new threat analytics service, ML for anomaly detection updates, and ML-based API discovery and protection.

*Strengths*

- **Market dynamics:** FortiWeb Cloud's presence is growing faster than the average for offerings in this market, albeit from a small base. Fortinet is able to benefit from its large global customer base by adding its cloud WAAP offering to existing deployments of Fortinet solutions.

- **Geographic presence:** Fortinet has an established global presence and a large sales channel. Its strong direct presence in EMEA and high number of local support centers helps with initial presale and postsale interactions.

- **Investment in machine learning techniques:** Fortinet has advanced its ML techniques over the past few years. It provides clear ML dashboards with detailed explanations of the use of ML.

- **Threat intelligence:** FortiWeb's risk-scoring view includes a trend-level history view that enables users to compare their organization's threat level with the average threat level within Fortinet's customer base.

*Cautions*

- **Hybrid deployment:** Fortinet's cloud WAAP cannot be managed from FortiManager, Fortinet's central management platform. Fortinet customers with hybrid deployments (appliances and cloud WAAP) must manage their appliances using FortiManager and FortiWeb Cloud from a portal. This limits Fortinet's supposed advantage for central management of hybrid WAAP deployments.

- **Architectural limits:** When competing with CDN-based WAAP providers, Fortinet's architectural limitations, such as the lack of a tunnel mode, the absence of remote hardware security module (HSM) support and inability to run custom code at the edge, reduce its appeal.

- **Bot mitigation:** Despite recent improvements, FortiWeb Cloud's bot mitigation features are not yet on a par with those of many of its competitors. This is especially true for advanced response capabilities and when managing authorized bots. Prospective customers should seek peer feedback on this feature, as most improvements are recent.

- **Customer experience:** Clients often express dissatisfaction with the basic logging features of FortiWeb Cloud. Although the number of FortiWeb cloud POPs has increased, customers continue to request more POPs for FortiWeb Cloud, especially outside the Americas.

### Imperva

Imperva is a Leader in this Magic Quadrant. It is headquartered in San Mateo, California, U.S. Imperva has a long history in application security, and is well known for making advanced features available in a cloud WAAP form factor. Imperva is a privately held application and data security vendor, part of Thoma Bravo's portfolio of security vendor equity investments.

Imperva Cloud WAF is the vendor's cloud WAAP service offering. It is part of the "Imperva Anywhere" portfolio, which also includes a WAAP gateway (the Imperva Web Application Firewall Gateway), database security (Imperva Data Security) and other security services, including DNS security and runtime application self-protection (RASP).

In the past year, noticeable changes have included improved Imperva's CDN and caching features, support for external HSMs, and numerous improvements to the advanced bot protection service, including a new tarpit action.

*Strengths*

- **Product maturity:** Longtime Imperva customers appreciate the stability and incremental improvement of the UI, and the additional security controls. They trust the results of the threat intelligence feeds and consider that the overall product gives good protection out of the box.

- **Event analytics:** Imperva relies on multiple ML approaches for bot mitigation and for event aggregation that shows promise for simplifying the management and incident response process.

- **Account takeover detection:** The Imperva Account Takeover Protection module includes several interesting features, such as detection of credential stuffing, and is designed to determine malicious intent from successful logins or impossible logins.

- **Application security portfolio:** The "Imperva Anywhere" strategy resonates with security teams willing to centrally manage WAAP enforcement points in different form factors and to consider adjacent application security approaches, such as RASP and database security.

*Cautions*

- **Executive churn:** Over the past few years, Imperva's leadership has changed a lot, especially in its sales and distribution channel teams. Although its product strategy remains consistent, Gartner has observed some adverse impact on Imperva's roadmap execution and overall market presence in the past 12 months.

- **DevOps deployment:** Imperva's cloud WAAP offering can be deployed as a sidecar proxy on Envoy, but is not available as a containerized WAAP offering. Imperva lags behind other vendors in supporting this deployment use case.

- **Global infrastructure:** Imperva often struggles against its CDN competitors due to direct comparisons of distributed infrastructure and presence. Imperva's presence in Asia/Pacific lags behind that of its direct competitors. Its cloud service does not have local POPs in China and has only two in India.

- **Customer experience:** Imperva's customers would like to see it be more responsive when it comes to supporting features regarded as "low-hanging fruit." They highlight its late support for TLS 1.3 and lack of single sign-on (SSO) for back-end applications, and they expect better certificate management.

### Microsoft

Microsoft is a Niche Player in this Magic Quadrant. Its Azure Web Application Firewall (WAF) remains basic, compared with the majority of competing offerings, but the desire to consolidate on fewer vendors remains a key reason why organizations choose it.

Microsoft is a large IT and digital workplace vendor, based in Redmond, Washington, U.S. It has a large product portfolio. Its infrastructure as a service (IaaS) and PaaS offering, Microsoft Azure, includes a WAF (Azure WAF) built on top of its CDN (Azure Front Door), which is also available with its application delivery solution (Azure WAF on Azure Application Gateway). Microsoft also offers other security products, notably DDoS protection, API security and a security information and event management (SIEM) tool (Microsoft Sentinel).

In the past 12 months, Microsoft has added multiple features. These include a new proprietary WAF engine, updated bot classification and Default Rule Set 2.0, based on Microsoft threat intelligence, which adds anomaly-based scoring and support for JSON and XML through Azure Front Door.

*Strengths*

- **Infrastructure:** Microsoft is expanding its global Azure infrastructure to increase its presence in different regions of the world. Microsoft Azure now has 179 POPs and over 60 Azure regions. In the past 12 months, Microsoft has added 25 POPs.
- **Breadth of security portfolio:** Microsoft has a huge product portfolio. In addition to Azure products, it offers multiple security, compliance and identity applications, artificial intelligence and other product lines. Many of its product lines have a huge market share, which makes Microsoft a desirable vendor for organizations seeking to consolidate their technology vendors.
- **Customer feedback:** Azure WAF customers praise its integration with Azure Front Door CDN and other native Azure tools. Microsoft also offers WAF integration with Microsoft Sentinel, which many customers recommend.
- **Volumetric DDoS:** Microsoft offers volumetric DDoS protection to mitigate the impact of large numbers of attacks. It has a highly distributed infrastructure to protect against distributed volumetric DDoS attacks. Microsoft also offers a subscription to its DDoS rapid response team for help with configuration or forensic investigation.

*Cautions*

- **Bot mitigation:** Azure WAF offers only basic bot mitigation and lacks features offered by the majority of WAAP vendors. It lacks features such as fingerprinting, JavaScript challenges, and ML capabilities to detect good and bad bots. This makes it less desirable for enterprises seeking mature bot mitigation within their WAAP solution.
- **API security:** Azure WAF offers only basic API threat protection. It lacks features such as autodiscovery and categorization of APIs, which are being offered by many WAAP competitors. This makes it a less desirable candidate for mature API threat protection integrated as a WAAP feature.
- **Pace of execution:** Azure WAF lacks many of the standard features offered by the majority of WAAP vendors. Microsoft's execution timelines for closing security feature gaps in its WAAP products are longer than those of other competitors.
- **Customer feedback:** Azure WAF customers find its logging and monitoring feature to be basic and its integration with third-party SIEM products to be challenging. Azure WAF also lacks native incident response alerts for the OWASP API top 10 threats.

### Radware

Radware is a Visionary in this Magic Quadrant. It is trying to apply its differentiated approach to application security, which combines ML techniques and rules, to the cloud WAAP segment.

Radware is also heavily invested in providing innovative WAAP form factors for DevOps environments.

Radware is based in Tel Aviv, Israel and Mahwah, New Jersey, U.S. It is primarily known for its DDoS protection (DefensePro and Cloud DDoS Protection Service). Radware offers WAAP in various form factors, including appliances, in a containerized envelope (Kubernetes Web Application Firewall [KWAF]) and as a cloud WAAP service (Cloud WAF Service).

Since the 2021 edition of this Magic Quadrant, Radware has added API threat protection features to its cloud WAAP, including API discovery and automated detection of API changes. It has also introduced a feature that automatically detects potential false positives and notifies customers of potential signature changes to minimize false positives.

*Strengths*

- **Suitability for DevOps environments:** SecurePath, a fully managed, out-of-band cloud WAF deployment mode with connectors to NGINX and Amazon CloudFront, appeals to cloud architects and DevOps teams looking for nonintrusive third-party web app security.
- **Innovation:** Radware's recent roadmap includes advances in application security. Examples include automated false-positive detection and the introduction of SecurePath.
- **Security techniques:** Gartner clients value the automated learning approach that Radware takes, even if they are using it only on a "trust but verify" basis.
- **Threat research team:** Radware effectively packages its threat research with support from its emergency response team (ERT). It also provides detailed technical blog posts that demonstrate the depth of its knowledge in this area.

*Cautions*

- **Transition strategy:** Radware is continuing with its transition from appliance-based application delivery controllers to cloud and application security. Radware's success in selling cloud WAAP services is not yet on par with that of the large platform and CDN providers.
- **Fragmentation of management consoles:** Radware's cloud portal can only manage its cloud WAAP. Radware's appliance management console handles appliances and Kubernetes containers. Hybrid use cases therefore require the use of at least two management consoles, which limits the advantage of using the same vendor. The most frequent complaint Gartner hears from Radware customers is about the weakness of its management capabilities.
- **Solution architecture:** Radware's ad hoc attack signature set is less extensive than those of the leading vendors in the market. This causes some non-Radware WAF users to question the efficacy of its solution.
- **Bot mitigation:** Over the past 12 months, customer feedback about Radware's bot mitigation module's ease of use has worsened. This is often due to configuration options that are less granular and intuitive than those of Radware's leading competitors.

### ThreatX

ThreatX is a Niche Player in this Magic Quadrant. This cloud-native security startup vendor, which was launched in 2015 and has its main headquarters in Boston, Massachusetts, U.S., is expanding its operations around the world. It relies on its automated, risk-based classification of events to differentiate itself from other WAAP providers.

The ThreatX WAAP Platform comprises containerized processing units, which can be deployed in various environments, and a cloud-hosted analysis engine. ThreatX offers managed security services, including a 24/7 managed SOC supported by a small team and automated procedures.

Since the 2021 edition of this Magic Quadrant, ThreatX has introduced API discovery, schema ingestion and support for GraphQL, which complement its API protection features by showing discovered API endpoints. It has also made available a modernized Attack Dashboard.

*Strengths*

- **API discovery:** ThreatX has introduced intuitive API autodiscovery, and is increasingly being shortlisted for API protection-centric use cases.
- **Capabilities:** ThreatX's WAAP offers three options for blocking: risk-based, per request and manual (detection only). Most clients like the ability to combine the risk-based approach with the per-request blocking option as it ensures limited risk and limited impact in the event of false positives.
- **Product strategy:** ThreatX's container-driven product strategy gives it early traction in the distributed WAAP space, and could be useful for monitoring east-west API traffic.
- **Customer experience:** ThreatX receives high marks from customers for its ease of deployment and customer support, which, among other things, responds quickly to requests for rule customization.

*Cautions*

- **Geographic strategy:** ThreatX operates primarily from the U.S. Its management console is available only in English, as is its product documentation. Support is delivered from U.S.-based locations and Estonia. ThreatX has yet to introduce many POPs outside North America.
- **Size of team:** Although ThreatX's platform can be used without managed services, the vendor strongly encourages use of these services, which are included in the cost of its WAAP platform. Given the small size of ThreatX's support team, large organizations should check whether ThreatX can support them with these included services.
- **Learning curve:** ThreatX has a relatively small, but growing, customer base. It takes a proprietary approach that relies on detecting attacker behavior and lacks good explainability and fine-grained configuration options. Organizations that do not use its managed services may require additional training to make full use of the platform for optimal protection.

- **Bot mitigation:** ThreatX lacks some features that its competitors offer. It offers only a limited number of the bot mitigation features often requested in customers' RFIs, such as bot farm detection, mouse and keyboard analytics, and a predefined set of good bots. It also lacks client-side protection.

### Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

#### Added

None.

#### Dropped

None.

## Inclusion and Exclusion Criteria

Each vendor of a cloud WAAP corresponding to the description in the Market Definition/Description section of this Magic Quadrant was considered for inclusion if:

- Its offering(s) can protect applications and APIs running on different types of host environments, such as web servers, service containers and PaaS.
- Its WAF technology is known to be approved by qualified security assessors as a solution for Payment Card Industry Data Security Standard (PCI DSS) Requirement 6.6, which covers the OWASP top 10 threats, in addition to others.
- It offers a cloud WAAP as a service.
- Its cloud WAAP service was generally available as of 1 January 2021.
- Its data centers are in at least two metropolitan areas, separated by a minimum of 250 miles, on separate power grids.
- It offers an SLA, with a minimum of 99.9% availability, with committed financial penalties in case of failure to meet the SLA.
- Its cloud WAAP service demonstrates global presence, features and scale relevant to enterprise-class organizations. It must have **either:**
  - Generated $20 million in cloud WAAP revenue during 2021 and had at least 80 enterprise customers use its cloud WAAP products under support as of 31 December 2021, including:
    - At least 25 net new enterprise cloud WAAP customers in 2021.

    - **Or** generated $5 million in annual recurring revenue (ARR) for its cloud WAAP, for the 12 months of 2021, and had two years of compound annual revenue growth (CAGR) of at least 50%.
- It demonstrates at least the minimum signs of global presence by:
    - Presenting Gartner with strong evidence that more than 10% of its cloud WAAP service's customer base is outside its home region (the Americas, EMEA or Asia/Pacific).
    - Offering a POP in at least two of the following regions: North America, EMEA and Asia/Pacific.
- It offers 24/7 support, including phone support — in some cases, this is an add-on, rather than being included in the base service.
- It is a significant player in the market, as determined by Gartner on the basis of its market presence, competitive visibility or technology innovation.
- It is a top provider in terms of Gartner-estimated market share or mind share for relevant segments of the overall WAAP market.
- It is the subject of inquiries from users of Gartner's client inquiry service, and has competitive visibility, client references and local brand visibility.
- Its WAF technology provides more than a repackaged ModSecurity engine and signatures.
- It provides evidence to show that it meets the above inclusion requirements.

WAAP and WAF vendors not included in this Magic Quadrant may have been excluded for one or more of the following reasons:

- The vendor primarily has a network firewall or IPS with a non-enterprise-class WAAP.
- The vendor is:
    - Primarily a managed security service (MSS) provider and its WAF/WAAP sales are mostly part of broader MSS provider contracts.
    - A service provider using third-party WAF or WAAP technology.
    - A WAAP provider offering a cloud WAAP in the form of WAAP virtual machines (VMs) managed by third parties.
- The vendor offers only a fully managed WAAP, with no self-service.
- The vendor is not actively providing WAAP products to enterprise customers, or has minimal continued investment in the enterprise WAAP market.

- The vendor has minimal or negligible apparent market share among Gartner clients, or is not actively shipping products.
- The vendor is not the original manufacturer of the firewall product. This includes hardware OEMs, resellers that repackage products that would qualify from their original manufacturers, and carriers and internet service providers that offer managed services. We assess the breadth of OEM partners as part of the WAAP evaluation, and do not rate platform providers separately.
- The vendor has only a host-based WAF, WAAP, web access management (WAM), RASP or API gateway (these are considered distinct markets).

## Honorable Mentions

In addition to the vendors included in this Magic Quadrant, Gartner tracks vendors that did not meet our inclusion criteria because of a specific vertical market focus and/or shortcomings in terms of WAAP revenue and/or competitive visibility in WAAP projects. The following merit mention here:

- **Alibaba Cloud** is a large cloud service provider based in China. It offers the Alibaba Cloud Web Application Firewall (with built-in bot management and API protection features) and Alibaba Anti-DDoS products as part of its cloud service offering. It appeals to customers who are implementing cloud services from Alibaba. Alibaba Cloud did not qualify for inclusion in this Magic Quadrant due to its more regional presence and the lack of feature parity for WAF and DDoS protections outside its home region.
- **Citrix** is a large infrastructure and security vendor based in the U.S. In 2020, it launched Citrix Web Application and API Protection (CWAPP), a cloud-based WAAP service. While expanding CWAPP, Citrix continues to be successful at selling its WAF as an add-on to its application delivery controllers (ADCs). Citrix did not qualify for inclusion in this Magic Quadrant primarily because it did not meet the customer thresholds for cloud WAAP service.
- **Cloudbric** is a cloud-native web application security vendor based in South Korea. It is a spinoff from Penta Security Systems, which offers WAAP appliances (called WAPPLES). Cloudbric's WAAP as a service is primarily available in the vendor's home region. Cloudbric did not qualify for inclusion in this Magic Quadrant due to insufficient presence outside its home region.
- **Google** is a large cloud service provider headquartered in the U.S. Google is investing in WAAP-related services, including Cloud Armor for DDoS protection and a web application firewall, reCAPTCHA Enterprise to combat automated bots and detect online fraud, and Apigee for API protection. Google is not included in this Magic Quadrant because it did not have a generally available cloud WAAP offering as of 1 January 2021.
- **Indusface** is a WAAP vendor based in India. It sells the AppTrana WAAP solution primarily bundled with managed services. It continues to attract positive feedback from customers who use its product and like its managed-services approach to WAAP. Indusface did not qualify for

inclusion in this Magic Quadrant because it offers a primarily managed solution and lacks sufficient presence outside its home region.

- **NSFOCUS** is a security vendor based in China. It offers a cloud WAAP service and a range of appliance and WAAP service offerings that appeal to clients looking for a WAAP in China, and it continues to grow its presence in other regions. NSFOCUS did not qualify for inclusion in this Magic Quadrant because it did not meet the thresholds for cloud WAAP service and had insufficient presence outside its home region.

## Evaluation Criteria

### Ability to Execute

**Product or Service:** This criterion includes the core cloud WAAP technology offered by the technology provider that competes in and serves the defined market. It also includes current product or service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements and partnerships, as defined in the Market Definition/Description section. Strong execution means that a vendor has demonstrated to Gartner that its products or services are successfully and continually deployed in enterprises. Execution is not primarily about company size or market share, although these factors can considerably affect a company's Ability to Execute. Some key features, such as the ability to support complex deployments (including on-premises and cloud options) with real-time transaction demands, are weighted heavily. Product evaluation also considers other cloud WAAP core security functions. These include DDoS protection services, bot management (such as bad-bot mitigation and good-bot management) and API threat protection, which might be bundled or integrated with WAF features.

This year's evaluation increases the importance of delivering specialized controls when protecting APIs. Integration with other markets, such as those for cloud access service brokers (CASBs) and application security testing (AST), is evaluated as well, but more lightly.

This year's evaluation increases the importance of delivering specialized controls when protecting APIs.

**Overall Viability:** This criterion assesses the organization's overall financial health, and the financial and practical success of the business unit. Also assessed are the likelihood that individual business units will continue to invest in a cloud WAAP, offer cloud WAAP products and advance the state of the art within the organization's portfolio of products.

**Sales Execution/Pricing:** This criterion encompasses the technology provider's capabilities in all presales activities and the structure that supports them. It includes deal management, pricing and negotiation; presales support; and the overall effectiveness of the sales channel. It also includes deal size, and the use of the product or service in large enterprises with critical public web applications, such as banking and e-commerce applications. Low pricing will not guarantee strong execution or client interest. Buyers want good results even more than they want bargains. Buyers balance cloud WAAP security requirements and pricing; they do not consider best pricing only.

For cloud WAAP providers with multiple security products, or a WAAP appliance offering, this criterion also evaluates the ability to craft a pricing model adapted to a cloud WAAP. This model should not inherit characteristics from pricing models used for other product offerings that are unsuitable for a cloud WAAP.

**Market Responsiveness/Record:** This criterion assesses the ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, and security trends and customer needs evolve. It includes a vendor's responsiveness to new or updated web application frameworks and standards, as well as its ability to adapt to market dynamics (such as the relative importance of PCI compliance) and changes. This criterion also considers the provider's history of releases, but gives greater weight to its responsiveness during the most recent product life cycle.

**Marketing Execution:** This criterion assesses the clarity, quality, creativity and efficacy of programs designed to deliver the organization's message. It is aimed at influencing the market, promoting the brand and business, increasing product awareness, and establishing positive identification with the product, brand and organization among buyers. This mind share can be driven by a combination of publicity, promotional activities, thought leadership, word of mouth and sales activities.

**Customer Experience:** This criterion assesses the relationships, products, services and programs that enable clients to be successful with the products that are being evaluated. Specifically, it includes the ways in which customers receive technical support or account support. It can also include ancillary tools, customer support programs (and the quality thereof), the availability of user groups, and SLAs that enable the organization to operate effectively and efficiently on an ongoing basis.

**Operations:** This criterion evaluates the organization's ability to meet its goals and commitments. Factors include the quality of the organizational structure. For vendors with multiple WAAP form factors (such as appliances), this criterion evaluates the organization's alignment with the offer of a cloud-delivered WAAP. For vendors with a broad security portfolio, it also evaluates the ability to maintain focus on the cloud WAAP service offering.

Table 1: Ability to Execute Evaluation Criteria

| ***Evaluation Criteria*** ↓ | ***Weighting*** ↓ |
|---|---|
| Product or Service | High |
| Overall Viability | Medium |

| *Evaluation Criteria* | *Weighting* |
|---|---|
| Sales Execution/Pricing | High |
| Market Responsiveness/Record | High |
| Marketing Execution | Medium |
| Customer Experience | High |
| Operations | Medium |
| | |

Source: Gartner (August 2022)

## Completeness of Vision

**Market Understanding:** This criterion assesses the vendor's ability to understand buyers' wants and needs, and to translate that understanding into products and services. Vendors with the most vision listen to and understand buyers' requirements, and can shape or enhance them. They also determine when emerging use cases will greatly influence how the technology has to work. Vendors that better understand how changes in web applications affect security receive higher scores. Trends include cloud, IaaS, agile methodologies, web services and microservices, continuous integration, and the growing importance of APIs.

**Marketing Strategy:** This criterion looks for a clear, differentiated set of messages that is consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements. Assessment includes the vendor's ability to communicate effectively about how its solution is a good fit for emerging use cases.

**Sales Strategy:** This criterion looks for a strategy that uses an appropriate network of direct and indirect sales, marketing, service and communication affiliates to extend the scope and depth of a vendor's market reach, skills, expertise, technologies, services and customer base. The ability to attract new customers who need web application security only is weighted heavily.

Compared with the 2021 edition of this Magic Quadrant, this criterion has been revised to reflect strategies adapted to cloud-delivered WAAP and "as a service" offerings.

**Offering (Product) Strategy:** This criterion assesses a vendor's approach to product development and delivery, with an emphasis on differentiation, functionality, methodology and feature sets, in relation to current and future requirements. As attacks change and become more targeted and complex, we give heavy weightings to vendors' efforts to move their WAAPs beyond rule-based web protections that are limited to known attacks by, for example:

- Combining rules, heuristics and ML to detect abnormal behaviors.
- Using a weighted scoring mechanism based on a combination of techniques to shape the WAAP's responses.
- Providing updated security engines to handle all protocols and standards updates, and remaining efficient in relation to changes in how older web technologies are used.
- Providing dedicated protection techniques for emerging web application use cases, such as mobile and Internet of Things (IoT) applications.
- Offering bot mitigation that is not limited to reputation-based controls.
- Providing API protection.
- Analyzing user behavior.
- Countering evasion techniques actively.
- Enabling a positive security model with automatic and efficient policy learning.

In this year's Magic Quadrant, we have increased the weighting for delivery of differentiated security controls when protecting APIs, including automated discovery and anomaly detection.

This criterion also evaluates the depth of features provided, especially features that ease management of the solution, and its integration with other solutions, such as SIEM tools, API gateways and other technologies (CASBs, for example).

**Vertical/Industry Strategy:** This criterion assesses the vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical industries. Vendors focusing on a single vertical receive lower scores. Vendors with differentiated vertical strategies and the ability to reproduce success across several verticals receive higher scores.

**Innovation:** This criterion examines the direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or preemptive purposes. It includes product innovation and quality differentiators, such as:

- New methods for detecting web attacks and avoiding false positives.
- Resistance to evasion and detection of new attack techniques.

- A management interface, monitoring and reporting that contribute to easy web application setup and maintenance, better visibility, and faster incident response.
- Automated delivery of detection and protection.
- Ability to integrate with DevOps processes and tools.
- Integration with companion security technologies, which improves overall security.

**Geographic Strategy:** This criterion assesses a vendor’s strategy to direct resources, skills and offerings to meet the specific needs of geographies outside its “home” country or region. This can happen directly or through partners, channels and subsidiaries, as appropriate for the geography and market. This criterion considers a vendor’s infrastructure (POPs), but is not limited to technical components. It also considers how the vendor adapts its strategy to local cloud demands and privacy requirements.

Table 2: Completeness of Vision Evaluation Criteria

| ***Evaluation Criteria*** ↓ | ***Weighting*** ↓ |
|---|---|
| Market Understanding | High |
| Marketing Strategy | Medium |
| Sales Strategy | Low |
| Offering (Product) Strategy | High |
| Business Model | NotRated |
| Vertical/Industry Strategy | Low |
| Innovation | High |
| Geographic Strategy | Medium |

Source: Gartner (August 2022)

## Quadrant Descriptions

### Leaders

Leaders can shape the market by introducing additional capabilities to their offerings, raising awareness of the importance of those features and being the first to do so. Leaders also meet enterprises' requirements for different uses of web application security.

Leaders have strong market shares and steady growth, but these alone are not sufficient to qualify as a Leader. Leaders in the cloud WAAP market require strong distributed infrastructure and must ensure high-level security and smooth integration into a web application environment. They also require advanced web application behavior learning; superior ability to block common threats (such as SQL injection [SQLi], cross-site scripting [XSS] attacks and cross-site request forgery [CSRF]), protect custom web applications and avoid evasion techniques; strong deployment, management and real-time monitoring; and extensive reporting. Leaders should also provide, and regularly improve, DDoS protection, and be ahead of the market in terms of bot mitigation and API security capabilities.

In addition to providing technology that is a good match for customers' requirements, Leaders exhibit superior vision and execution for anticipated requirements, and drive evolution in web applications that requires changes to the security paradigm.

### Challengers

Challengers have a sound customer base, but do not lead in terms of security features. Challengers draw on existing clients from other markets (such as the IaaS and CDN markets) to sell their cloud WAAP technology, rather than competing to win deals through product differentiation. Challengers may be well-positioned and have good market shares in a specific segment of the WAAP market (such as a specific cloud infrastructure segment), but do not address the entire market (and may not be interested in doing so).

### Visionaries

Visionaries provide key innovations to address web application security concerns. They devote many resources to security features that help protect critical business applications against targeted attacks. However, they lack the ability to influence a large portion of the market. They either have not expanded their sales and support capabilities on a global basis, or they lack the funding to execute with the same capabilities as Leaders or Challengers. They also have a smaller presence in the cloud WAAP market, as measured by installed base, revenue size or growth, or in terms of overall company size or Gartner's assessment of long-term viability.

### Niche Players

The Niche Players quadrant primarily includes vendors of cloud WAAPs that are a good match for specific use cases (such as PCI compliance) or vendors with a limited reach in relation to cloud WAAP deployments. The cloud WAAP market includes several European and Asian vendors that serve clients in their regions well with local support, and that can quickly adapt their roadmaps to specific needs, but that do not sell outside their home countries or regions.

Even when selling large-scale products, some Niche Players offer features that only suit the needs of SMBs.

Niche Players may also have a small installed base because their cloud WAAP products are recent, in transition, or limited, according to Gartner's criteria, by various factors. These factors may include limited investment or capabilities, and other inhibitors to providing a broader set of capabilities to enterprises both now and during the next 12 months.

Niche Players may be in the early stages of building a broader product. Inclusion in the Niche Players quadrant does not reflect negatively on a vendor's value within its more narrowly focused service spectrum.

## Context

This Magic Quadrant evaluates vendors of WAAP offerings that are delivered as cloud services (WAAP services), in contrast to previous editions that covered vendors of both appliances and cloud WAAP technologies. This change alters the customer expectations we have considered and the relative positions of evaluated vendors.

WAAP vendors with an existing appliance portfolio are now evaluated primarily for their cloud WAAPs. Vendors are now evaluated against other cloud WAAP vendors only. This changes their positioning, as WAAP appliances are not weighted as in the previous Magic Quadrant.

Gartner's inclusion and exclusion criteria include a requirement to derive meaningful revenue from outside a vendor's home region, as well as a requirement for a minimum number of customers for the WAAP service. This has led to the exclusion of some smaller or more regional vendors (see the Honorable Mentions section).

The adjacent WAAP appliance market is closer than the cloud WAAP market to its WAF roots and many of the vendors evaluated in this Magic Quadrant have their appliance technology at the core of their cloud WAAPs. Some organizations continue to select WAAP appliances, instead of cloud WAAPs, to ensure a unified management and reporting console across on-premises and cloud data centers. Additional reasons to use WAAP appliances include insufficient, or a complete lack of, cloud WAAP POPs in a particular country, other local data residency regulations, and discomfort with the consumption-based licensing of cloud WAAPs.

The cloud WAAP market includes historical WAAP appliance providers that are building a cloud presence by using infrastructure as a service (IaaS) and offerings from CDN and IaaS providers. Because many local or platform providers might wrap a WAF around a ModSecurity engine, and use one of the available rule sets, many legacy WAF solutions are available and compete with WAAP offerings. These products are not evaluated in this Magic Quadrant.

Gartner generally recommends that clients consider products from vendors in every part of a Magic Quadrant, based on their specific functional and operational requirements. This is especially true for the cloud WAAP market, which includes many relatively small vendors, as well as larger vendors that derive only a small share of their revenue from cloud WAAP offerings. Product selection decisions should be driven by organization-specific requirements. These relate to factors such as deployment constraints and scale, the relative importance of compliance, the characteristics and risk exposure of business-critical and custom web applications, and vendors' local support and market understanding.

Security managers considering cloud WAAP deployments should first define their deployment constraints, especially their:

- Tolerance for a full, in-line reverse proxy with blocking capabilities in front of web applications.
- TLS decryption/re-encryption and other scalability requirements.
- Detailed needs for bot management, especially advanced and nonintrusive responses.
- Requirements to protect applications hosted on multiple cloud and on-premises locations.
- Ability to secure the more recent API architectures (such as Microservices architectures).

## Market Overview

The overall cloud WAAP market is mature, though some segments are quite dynamic, such as bot management and API threat protection. Unlike the WAAP appliance market, which is dominated by replacement purchases, the cloud WAAP market continues to experience double-digit growth, thanks to new customers, new applications to protect, and shifts from appliances to cloud-delivered security.

In the past 12 months, cloud WAAP has been the dominant form factor for new deployments in the Americas and EMEA. The remaining WAAP appliance deployments continue to fuel many renewal purchases, especially in the form of virtual appliances. The WAAP appliance form factor is also a serious contender for hybrid deployments.

API security is becoming a key part of WAAP evaluations in situations where WAAP providers compete against more specialized API threat protection vendors. Gartner has observed noticeable improvements in some API protection offerings from vendors evaluated this year. However, API protection features integrated into cloud WAAPs often look like initial versions and tend to lack depth, especially in terms of providing context relevant to API specialists in alerts and business context management for discovery modules. More vendors have introduced decent API discovery capabilities in the past year.

Providers of the more mature bot mitigation modules face reinvigorated competition from the remaining bot mitigation specialists, and have focused their efforts on a few differentiators:

- Fine-grained categorization of malicious and authorized bots.
- Better controls against human-operated bots ("hu-bots"), especially CAPTCHA- solving services.

- Alternatives to traditional intrusive CAPTCHA services.
- Ability to distinguish between good and bad human actors, particularly to mitigate account takeovers.

Growth in the use of ML to detect and reduce false positives has leveled off in the past year, with no noticeable improvements and a slight de-emphasization from vendors that reflects general market fatigue about “ML hype.” ML could still be useful to overcome the more complex challenge of managing WAAP configurations at scale, while providing the right combination of change workflow management, reliable configuration auditing and change traceability, and a good mix of global, per-group and per-application settings. However, Gartner has not observed any noticeable improvement in this area.

### Distributed WAAP Emerges as a Separate Segment of the WAAP Market

A growing number of cloud WAAP vendors are adding deployment options for the more automated cloud applications: Kubernetes sidecars, containerized WAAPs and WAAP agents. The future of this segment remains unclear, however. But embedded WAAPs cannot replace cloud-delivered WAAPs for every use case and requirement such as DDoS protection or the ability to deploy quickly in front of hundreds of applications hosted on various environments.

Distributed WAAPs are intended to improve DevSecOps practices to secure newly developed applications through “shift left” techniques, but they do not address the “shift right” needs of legacy and third-party applications. In future, large enterprises with mature DevOps practices will demand a combination of cloud gateway WAAPs and distributed WAAPs to enable DevSecOps and better protect existing applications.

WAAP controls, deployed closer to the applications they protect, could provide benefits such as:

- Gathering of better contextual information from applications and details of who or what is accessing a microservice, which could help reduce the false-positive rate.
- Classification of, and protection against, new categories of threats to microservices environments through the use of dedicated, unsupervised ML techniques.
- Enabling application development teams to declare application context programmatically and WAAPs to automatically enforce or modify the correct security rules at runtime.

The most likely scenario for the coming months is that WAAP agents, containers and VMs will be components of an integrated network and distributed WAAP. Centralized but flexible management and monitoring remains one of the biggest challenges for distributed WAAPs to overcome if they are to become a reality at scale. Vendors must also identify which features are most suitable for distributed WAAPs, such as specific, targeted protections for certain workloads, and which should be enforced at the network level, such as API discovery and bot mitigation.

## Evaluation Criteria Definitions

## Ability to Execute

**Product/Service:** Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

**Overall Viability:** Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

**Sales Execution/Pricing:** The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

**Market Responsiveness/Record:** Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

**Marketing Execution:** The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

**Customer Experience:** Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

**Operations:** The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

## Completeness of Vision

**Market Understanding:** Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

**Marketing Strategy:** A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

**Sales Strategy:** The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

**Offering (Product) Strategy:** The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

**Business Model:** The soundness and logic of the vendor's underlying business proposition.

**Vertical/Industry Strategy:** The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

**Innovation:** Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

**Geographic Strategy:** The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.