Magic Quadrant for Web Application and API Protection

Published 20 September 2021 - ID G00738149 - 48 min read

By Jeremy D'Hoinne, Rajpreet Kaur, **and 3 more**

The web application and API protection market is composed of two main segments: WAAP services and WAAP appliances. Security and risk management leaders should favor WAAP that provides easy-to-consume controls and more specialized protections against advanced bots and evolving API attacks.

Strategic Planning Assumptions

By 2026, 40% of organizations will select their WAAP provider based on advanced API protections, as well as web application security features — up from less than 10% this year.

By 2026, more than 40% of organizations with consumer-facing applications that initially relied only on their WAAP for bot mitigation will seek additional anomaly detection technology from specialized providers — up from less than 10% today.

By 2024, 70% organizations implementing multicloud strategies for web applications in production will favor cloud WAAP services over WAAP appliances and IaaS-native WAAP.

Market Definition/Description

Gartner defines web application and API protection (WAAP) as the evolution of the web application firewall market (WAF), expanding WAF capabilities to four core features (see Defining Cloud Web Application and API Protection Services):

- WAF
- Distributed denial-of-service (DDoS) protection
- Bot management
- API protection

WAAP is primarily delivered as a cloud service (WAAP service). While WAAP services have a clear advantage when it comes to DDoS protection, WAAP appliances can also deliver volumetric DDoS

mitigation by integrating with a cloud service for the volumetric component of DDoS protection.

The WAAP appliance segment is closer to its WAF roots and many of the existing providers developed their WAAP service with their appliance technology at its core. Some organizations select WAAP appliances to ensure a unified management and reporting console across multiple data center locations, or advanced capabilities (e.g., a positive security model) that WAAP service competitors don't yet offer.

The WAAP service is composed of a mix of WAAP appliance providers, building their cloud presence by leveraging infrastructure as a service (IaaS) ("cloud-rented") and offerings from content delivery network (CDN) and IaaS providers ("cloud-owned").

This Magic Quadrant considers WAAP services that are deployed externally in front of or alongside web applications and are not integrated directly on web servers:

- WAAP appliances — purpose-built physical, virtual or software appliances
- WAAP modules embedded in application delivery controllers (ADCs)
- WAAP services, including WAF modules, embedded in larger cloud platforms, such as CDNs, and delivered directly from IaaS platform providers

The primary use case for WAAP is to protect public-facing web applications and APIs. Organizations sometimes deploy WAAP in front of partner-facing or employee-facing applications, but this is rare.

Stand-alone bot mitigation solutions, API gateway and specialized API protection solutions, and runtime application self-protection (RASP) are adjacent to the WAAP market, even though they can compete for the same security budgets. This motivates WAAP vendors to add relevant features from these markets, when appropriate.

Gartner scrutinizes these features and innovations for their ability to improve web application security beyond what a network firewall, intrusion detection and prevention systems (IDPS) or an open-source/free WAF (e.g., ModSecurity) would do by leveraging a rule set of generic signatures.

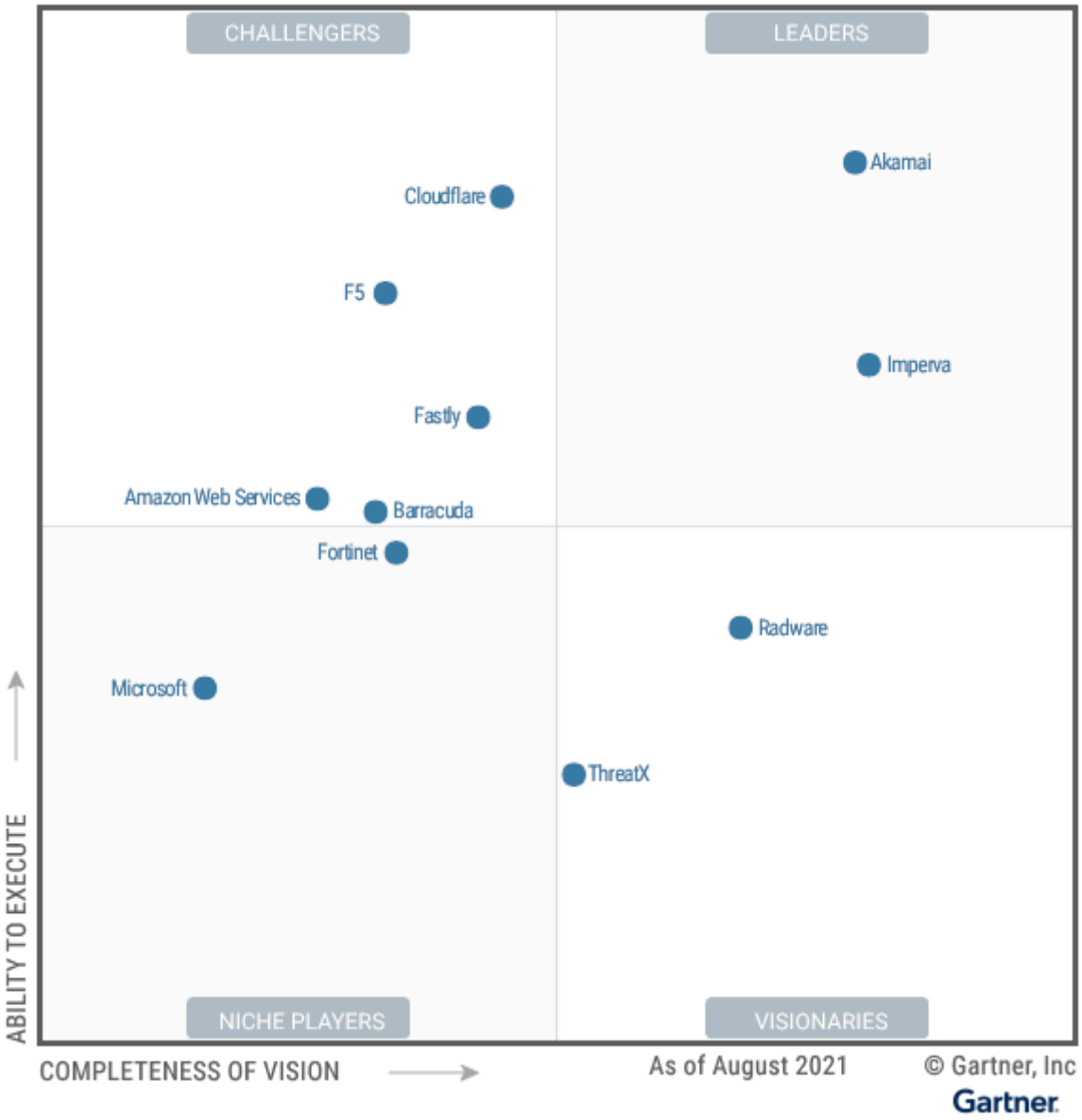
Because many local or platform providers might wrap a ModSecurity engine, and use one of the available rule sets, a large number of legacy WAF solutions are available and compete with WAAP offerings. These products are not evaluated in this Magic Quadrant.

Gartner 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 its WAAP service. This has inevitably led to the exclusion of some of the smaller or more regional vendors.

Please see the Market Overview section for the recent trends in the WAAP market.

Magic Quadrant

Figure 1: Magic Quadrant for Web Application and API Protection



Source: Gartner (September 2021)

Vendor Strengths and Cautions

Akamai

Akamai is a Leader in this Magic Quadrant. This vendor is well-suited to appear on WAAP service shortlists to protect business-critical, web-scale applications, especially for organizations that have a broad and diverse portfolio of web applications and APIs.

Akamai is a global CDN provider with more than 8,800 employees, headquartered in Cambridge, Massachusetts. It has two WAAP offerings: Kona Site Defender (KSD) and Web Application Protector (WAP). WAP is a less-featured, lower-priced and easier-to-manage version of KSD.

Recent updates include: an improved onboarding wizard; the release of Adaptive Security Engine (ASE) to replace the Kona Rule Set (KRS) and Automated Attack Groups (AAG); a free tier for Page Integrity Manager client-side protections, enhancements to bot detection and prevention, such as adding cryptographic challenges; and a new dedicated managed services for Bot Manager Premier.

Strengths

- **Capabilities:** Akamai offers API security features that are more mature than most of its competitors, such as applying behavior anomaly detections for API usage. Its portfolio includes an available API gateway that allows for tighter integration with its API security features.
- **Product offering:** Akamai is willing to disrupt its product and provide improved features. For example, the introduction of ASE to replace the KRS and AAG with a single engine will reduce human error and improve automation of applications and API security.
- **Geographic strategy:** Akamai continues to enhance its global presence and leads competitors in point of presence (POP) scale for many regions by a wide margin. It owns and manages its POPs with no reliance on IaaS vendors.
- **Customer experience:** Akamai's customers give the vendor high marks for customer support experience, including the expertise and assistance they receive from both technical support and managed services.

Cautions

- **Market segmentation:** Like its CDN competitors, Akamai lacks a physical appliance offering, which can cause its exclusion from some WAAP shortlists with hybrid deployment. Akamai KSD tends to appeal most to large and very large enterprises due to complexity and pricing.
- **Pricing strategy:** Gartner continues to see negative customer feedback about the high price of the KSD solution. Price is often the sole disqualifier when Akamai is struck from shortlists, because other enterprise-class WAAP providers sometimes offer lower price points. Prospective clients should get a cost estimate early in the evaluation process.
- **Capabilities:** ASE is promising but as yet unproven. The recommendation engine does not automatically enforce changes, and tends to suggest coarse-grained exceptions to the policy. WAAP analytics capabilities are fragmented over multiple consoles, which create friction in the incident response workflow. Akamai lags behind several competitors for dedicated mitigation controls to detect human click farms.
- **Customer experience:** Gartner analysts received some negative feedback on Bot Manager's efficacy. Prospective customers should test the efficacy against recent bots and the user experience at scale when considering Bot Manager.

Amazon Web Services

Amazon Web Services (AWS) is a Challenger in this Magic Quadrant. Its WAAP service provides basic security and DDoS mitigation, but continually improves and benefits from serving a large number of organizations.

AWS is a cloud service provider (CSP) subsidiary of Amazon, headquartered in Seattle, Washington. The vendor offers several security products, including a network firewall (AWS Network Firewall), managed DDoS and WAF (AWS Shield Advanced). AWS WAF is primarily available through Application Load Balancer (ALB) or through Amazon CloudFront (AWS CDN).

Over the evaluation period, AWS released its bot mitigation feature, AWS WAF Bot Control. It is supported by a dedicated threat research team and is configured through AWS Managed Rules. AWS WAF can now parse JSON and extract key pairs. It has also improved the ability to create exceptions in the policy with its “scope down” feature, and to create custom responses when blocking the traffic.

Strengths

- **Technical architecture:** AWS provides a robust cloud infrastructure worldwide for its WAAP offering, containing 25 AWS regions and more than 225 Amazon CloudFront edge nodes. In fact, several other vendors in this Magic Quadrant deploy their cloud WAAP in AWS, leveraging its cloud edge architectures.
- **Customer experience:** Customers value the complete integration that AWS WAF has with the underlying infrastructure, especially when deploying AWS WAF. They like the ability to choose between CDN-based (Amazon CloudFront) and gateway WAF (ALB). They also value the more flexible WAFv2 API, which eases automation of WAF deployment.
- **Capabilities:** AWS has invested a lot in its bot mitigation feature, with a free bot monitoring feature, Amazon CloudWatch metrics, and labels to use bot status in custom rules. While the efficacy is still unproven because the feature is recent, it is evident that the vendor takes the challenge seriously.
- **Capabilities:** AWS Managed Rules (AMR) rule sets remain a strong asset, especially when cloud operation teams need to convince the security team that AWS WAF can be more than a temporary solution. The ability to use tags in AWS Firewall Manager to limit the scope of a policy provides additional flexibility when deploying multiple rule sets.

Cautions

- **Capabilities:** AWS WAF lags behind many competitors in API security. AWS has just released the ability to parse JSON requests, but does not offer API discovery or behavioral anomaly detection.
- **Marketing strategy:** Gartner analysts do not see AWS WAF in shortlists when multicloud and high security carry a heavy weight in the overall evaluation score. Its primary use case remains existing

AWS customers.

- **Roadmap strategy:** AWS releases regular improvements to its WAAP product, but most releases provide capabilities that other leading competitors already offer.
- **Customer experience:** AWS customers continue to complain about the difficulty to tune the rule set and to write custom rules, especially when protecting a large number of applications. False positive rate is frequently cited as a reason to select another provider.

Barracuda

Barracuda is a Challenger in this Magic Quadrant. The vendor continues to develop its WAAP hardware and virtual appliance product lines, and to grow its WAAP service from a smaller base than its competitors.

Based in Campbell, California, with over 1,500 employees, Barracuda is a security vendor with roots in midsize businesses. The vendor maintains a dedicated team to develop its WAAP appliance (Barracuda Web Application Firewall) and WAAP service (Barracuda WAF-as-a-Service). Barracuda CloudGen is its WAAP virtual appliance, available on IaaS. In July 2021, Barracuda acquired SKOUT Cybersecurity, a managed security service provider (MSSP).

Recent updates include the introduction of machine-learning-based bot protection and API protection features, support for reCAPTCHA v.3, and support for external hardware security modules (HSMs). Barracuda is also moving from a virtual-machine-based to a containerized approach for the back-end infrastructure of its WAAP service.

Strengths

- **Technical architecture:** Barracuda WAAP is available on multiple IaaS platforms. Today, the vendor offers support for AWS, Google Cloud Platform and Microsoft Azure through its CloudGen product line. It also offers virtual WAAP with support for Oracle Cloud, Alibaba Cloud and Huawei Cloud.
- **Capabilities:** Barracuda WAAP management portal offers easy and modular administration capabilities with multiple built-in features, hidden until used. Features such as validating false positive alerts from the logging interface make fine tuning easier. It also comes with a mature risk scoring feature offering the option to customize risk levels and threshold values.
- **Customer feedback:** Customers often score the vendor high for its easy onboarding process. They have also rated the ability to create custom roles as easy to select and configure.
- **Product strategy:** Barracuda has recently introduced its containerized WAAP. The vendor is migrating its WAAP service back end to this model. This architecture change intends to enable future unified management for the WAAP service and WAAP appliances.

Cautions

- **Product offering:** Although it has recently introduced checkbox integration with Azure CDN, the vendor itself lacks comprehensive CDN services. Barracuda does not offer managed security services (MSS) or managed security operation center (SOC) services.
- **Marketing execution:** Gartner has seen Barracuda WAAP more visible in the shortlists of midsize enterprises. Gartner estimates that Barracuda does not lead with innovation. Feature releases are often limited to catching up with Leaders and other Challengers in this Magic Quadrant.
- **Customer feedback:** Larger enterprise customers often express their dissatisfaction about the technical support. Gartner received reports that the support quality and time to resolve is deteriorating gradually. Sometimes, customers express it as a reason to move to a different vendor.
- **Capabilities:** Barracuda WAF-as-a-Service lacks in-depth security incident response and configuration roll-back and versioning, desired by large enterprise clients. It also lacks behavior-based API discovery and DNS security.

Cloudflare

Cloudflare is a Challenger in this Magic Quadrant. It is evaluated as a serious contender in many WAAP deals, including from large enterprises, but continues to suffer sometimes from brand association with its historic SMB roots.

Cloudflare is a cloud infrastructure vendor, headquartered in San Francisco, California. The vendor continues to expand its security portfolio and now employs over 2,000 employees. In addition to its DDoS and CDN platform, Cloudflare now provides cloud-hosted VPN, DNS filtering and secure web gateway (Cloudflare for Teams).

Over the evaluation period, Cloudflare rebuilt its WAF engine. It also released API Shield, with Schema Validation and an early access version of API Discovery. Other features released include Page Shield, a client-side security module, improvements to bot management, and a log encryption option to prevent unwanted access to sensitive information. Cloudflare also introduced Account Takeover Protection as an extra layer of defense against credential stuffing attacks.

Strengths

- **Sales execution:** Cloudflare already owns sizable market share and is one of the fastest-growing vendors represented in this Magic Quadrant, reporting 51% revenue growth across all product lines in fiscal 2020.
- **Scalability:** Cloudflare continues to expand its infrastructure and, as a global player, has a strong multiregion presence, including in countries such as China and Russia, where most competing vendors lack presence.

- **Capabilities:** Cloudflare remains one of the few WAAP providers that supports remote HSMs. The vendor has improved API security over the past year with the launch of API Shield, which centralizes configuration and support for mutual Transport Layer Security (mTLS), schema validation and gRPC.

- **Customer experience:** Customers continue to give Cloudflare good scores for ease of deployment and use. Technical acumen from Cloudflare's team is rated high and is frequently cited by Gartner clients as the reason why Cloudflare wins in competitive evaluations.

Cautions

- **Capabilities:** Cloudflare's WAAP is trying to catch up with leading competitors in terms of API security features. For example, Cloudflare only recently announced API Discovery and anomaly detection techniques.

- **Market segmentation:** Cloudflare is rarely selected in high-security use cases, even when advanced functionality exists. Like its CDN competitors, it lacks a physical appliance offering, which can cause its exclusion from some WAF shortlists with hybrid deployment requirements.

- **Capabilities:** Cloudflare WAF role-based management lacks custom role creation, as well as an easy way to assign roles per application or per group of applications.

- **Capabilities:** Cloudflare lacks some security features seen in other services, such as malware inspection to protect file uploads, native HTTP/2 support connections to origin servers outside of gRPC, and client-side protections such as a mobile software development kit (SDK).

F5

F5 is a Challenger in this Magic Quadrant. F5 continues its transformation from a WAAP appliance vendor to a hybrid and multicloud provider. Its cloud strategy has become clearer, but the underlying fundamental architecture evolution takes time.

Headquartered in Seattle, Washington, F5 is a large application delivery controller vendor. It employs more than 6,000 staff, including a large web application security team. F5's WAAP portfolio includes multiple solutions, with a prevalence of software modules on top of cloud-hosted (Silverline) and appliance-based (F5 Advanced WAF) BIG-IP platforms. NGINX App Protect is a more lightweight module, deployed on the NGINX platform.

In recent months, F5 has acquired the Volterra SaaS platform and has begun to transform it into its future WAAP product. The vendor has added integration of its bot mitigation module (Shape Enterprise Defense) into more of its WAAP products (Silverline and NGINX), and has added POPs for Silverline.

Strengths

- **Geographic presence:** F5 remains one of the most visible WAAP vendors, especially in the Asia/Pacific and EMEA regions, and on WAAP appliance shortlists globally.
- **Product strategy:** The acquisition of SaaS vendor Volterra is a tangible strategic move that, long term, can bring F5 closer to its cloud-native WAAP competitors.
- **Capabilities:** The BIG-IP platform brings mature and reputable features to F5's customers: a flexible rule engine (iRules), a comprehensive set of application and API protections, and session security.
- **Capabilities:** Gartner analysts received positive feedback on noticeably improved bot detection capabilities coming from the addition of Shape. The Shape engine focuses on detecting malicious behaviors, not only due to automation, but also based on various behavioral characteristics.

Cautions

- **Product offering:** F5 is still in the middle of its consolidation strategy for its WAAP service products. Today's customers are more likely to select Silverline, as it is a natural counterpart of BIG-IP appliances, but F5's strategy leans toward the Volterra platform, which creates questions about the future evolution of the current Silverline offering.
- **Capabilities:** Organizations looking for a sustainable hybrid WAAP deployment should anticipate F5's management console evolution. VoltConsole is likely to become the future centralized management console, but does not manage BIG-IP- or NGINX-based WAAP today. These transitions are never seamless. Management relying too much on the current console might have a short life span.
- **Capabilities:** F5 Silverline lacks support for HSMs and full TLS 1.3 cipher suites. It does not provide single sign-on (SSO) features for the back-end application, but can integrate with third-party identity providers. F5 Silverline does not inspect files for malwares and does not offer advanced CDN features.
- **Customer experience:** Gartner customers continue to complain about F5 Silverline. They report that the deployment is more cumbersome than many other shortlisted vendor offerings. High prices are also often cited. Existing, happy BIG-IP customers in EMEA and Asia/Pacific reluctantly look at other cloud WAAP providers because of the poor number of Silverline POPs in their respective regions.

Fastly

Fastly is a Challenger in this Magic Quadrant. In October 2020, it completed the acquisition of Signal Sciences, and has been slowly combining the company's platform capabilities with its own.

Headquartered in San Francisco, California, Fastly is a CDN and DDoS provider. The acquisition of Signal Sciences provides it with a WAAP platform that can be deployed across various form factors. The vendor calls its solution Fastly Next-Gen WAF, which can be deployed as a runtime agent, on top of an NGINX proxy and as a WAAP service. The solution is available for deployment on major IaaS platforms.

Over recent months, Signal Sciences has benefited from integration with Fastly to improve its DDoS mitigation and scalability beyond the limited set of POPs and IaaS partners on which it was dependent in the past. It has also introduced protection and support for integration with service meshes, including Envoy and Istio.

Strengths

- **Product strategy:** Customers often shortlisted Signal Sciences when looking to move away from a WAF appliance to a cloud-delivered model that could operate across a diverse landscape of applications. By acquiring Signal Sciences, Fastly promises its existing customer base an easy-to-use WAAP on top of their CDN infrastructure.
- **Customer experience:** Customers continue to give Fastly high scores for its ability to enable blocking shortly after deployment, with lower-than-expected false positive rates. Clients rate Fastly and Signal Sciences high for overall sales and support, especially when the buying center is part of a cloud-native application initiative. DevOps teams value Signal Sciences' ability to protect dynamically developed applications.
- **Technical architecture:** Fastly supports a wide variety of deployable form factors to add WAAP services, such as service mesh integration, serverless platform integrations, containers and as-a-service offerings.
- **Capabilities:** The foundation of Fastly's technology is a flexible policy engine, with three levels of rules: vendor rules; templated rules, with some customization; and custom rules ("power rules").

Cautions

- **Roadmap execution:** Fastly's pace of new feature releases has been slow, relative to that of leading competitors. This hurts its ability to not only maintain differentiation, as some competitors improve their monitoring and reporting capabilities, but also to reduce the feature gaps with leading competitors for some of the core capabilities.
- **Geographic strategy:** Fastly is primarily seen in North America and currently has limited sales and support presence for Fastly Next-Gen WAF in other geographies. The vendor provides support primarily in English and Japanese, and an English-only management interface.
- **Capabilities:** Fastly continues to lag behind peers for API security and bot mitigation. It lacks automatic application behavior learning and API discovery, and supports securing web

applications and APIs through Signal Sciences' SmartParse engine, which inspects traffic to apply protections. Fastly still lacks capabilities such as human behavior detections and forcing bots to solve cryptographic challenges, rather than presenting a CAPTCHA.

- **Capabilities:** By relying on its proprietary generic engine to automatically block new attacks, Fastly releases a limited number of dedicated protection signatures when a new vulnerability is made public. This might limit the ability of an enterprise's SOC team to use Fastly's console when investigating attack campaigns.

Fortinet

Fortinet is a Niche Player in this Magic Quadrant. While it also sells a WAAP service (FortiWeb Cloud), the Fortinet WAAP appliance product line (FortiWeb) is shortlisted more by existing network firewall customers who want to consolidate on a single vendor.

Headquartered in Sunnyvale, California, Fortinet is an established infrastructure and security vendor with around 8,000 employees. Its primary product line remains its firewall appliances (FortiGate).

Recent updates to the WAAP appliance product line include new client tracking design, rapid sample detection for machine learning (ML), ML deep learning and cross-site scripting (XSS) syntax-based detection. Updates to the WAAP service include global templates, action per security policy, cloud connectors, SQL injection (syntax-based detection), and Oracle Cloud Infrastructure support.

Strengths

- **Product strategy:** Fortinet continues to focus on its WAAP appliance product line, making it a favorable shortlist candidate for enterprises in need of an appliance form factor because of data localization or privacy constraints.
- **Geographic presence**: Fortinet has an established global presence, including in emerging regions where many other WAAP vendors lack a direct presence and sometimes even lack direct channel presence. Hence the vendor has a strong customer base in emerging markets such as Colombia, UAE and India, where it offers direct professional services and local support.
- **Customer experience**: Fortinet's WAAP offers easy onboarding steps and easy initial configuration options, such as autolocation discovery during the first set-up to use the closest POP automatically. Customers like that they can manage both WAAP (FortiWeb) and network firewall (FortiGate) from the FortiManager console.
- **Capabilities:** FortiWeb's risk scoring view includes a trend-level history view, where organizations can compare their threat level with the average threat level within Fortinet's customer base.

Cautions

- **Sales execution:** FortiWeb is not visible in WAF shortlists when the client is not already using at least one other Fortinet product. FortiWeb Cloud is growing nicely, but its market share is one of the smallest of evaluated vendors.
- **Market segmentation:** Fortinet is more often shortlisted by midsize enterprises from the EMEA and Asia/Pacific regions looking for a WAAP appliance.
- **Capabilities:** Fortinet's WAAP still lacks multiple features offered by its competitors. The vendor only recently introduced API discovery and FortiWeb Cloud lags behind competition in terms of behavior-based bot mitigation. Fortinet does not offer direct MSS or managed SOC services.
- **Customer experience:** Clients using FortiWeb have reported that ML-based policy configuration is not intuitive and requires a steep learning curve to configure the policies. Clients are often dissatisfied with their basic logging feature of FortiWeb Cloud and would like to see improvements. Today, the vendor doesn't offer real-time access to traffic logs and incident response capabilities. Customers also would like to see faster improvements in the number of POPs for FortiWeb Cloud.

Imperva

Imperva is a Leader in this Magic Quadrant. It provides strong security for hybrid and cloud-only organizations, but is challenged to differentiate from leading CDN competitors with its cloud offering.

Based in San Mateo, California, Imperva is a privately held application security vendor. Its portfolio includes data security products, RASP (Imperva RASP), a WAAP as an appliance or virtual appliance (Imperva WAF Gateway), and a cloud WAAP service (Imperva Cloud WAF).

Over the past few months, Imperva has completed the acquisition of CloudVector, an API security company, and reinstated a free trial for Imperva Cloud WAF. It has launched a new product to secure AWS Lambda serverless functions (Imperva Serverless Protection) and client-side protection. The vendor has also announced its unified management and monitoring initiative (Imperva Sonar) and improved the scale of its management console for the Imperva WAF Gateway. It has added a managed DNS service and advanced reporting to App Protect plans. Proactive monitoring is also available selectively.

Strengths

- **Product offering:** Imperva has released a first version of API discovery, which shows API endpoints and includes additional insights such as when the API transports sensitive PII. The recent acquisition of CloudVector shows the vendor's willingness to make API security a major component of Imperva Cloud.
- **Product strategy:** Imperva announced its intent to build Sonar, a unified cloud-delivered management and monitoring console, for all of its application security products. In the meantime,

the vendor has completely revamped its management UI for Imperva Cloud, making more visible security- and performance-related insights.

- **Customer experience:** Customers noted the recent improvement in the management and monitoring interfaces. They gave good scores to the vendor's product capabilities, both for the Gateway and Cloud products.
- **Capabilities:** The Imperva Account Takeover (ATO) module includes several interesting features, such as the detection of credential stuffing, but also malicious intent from successful logins. Users can choose different actions based on the risk level (low, medium, high) associated with the account login.

Cautions

- **Sales execution:** While Imperva remains one of the largest vendors for WAAP services in terms of market share, its visibility has grown slower than its competitors during the last few months. Gartner estimates that Imperva Cloud slightly lost market share in this segment.
- **Product offering:** As yet, Imperva does not offer a containerized WAAP, or the ability to deploy its WAAP as a Kubernetes sidecar.
- **Customer experience:** Imperva's customers would like to see the vendor be more responsive when it comes to supporting features regarded as "low hanging fruits." They mentioned late support for TLS 1.3, lack of SSO for back-end applications, and expect better certificate management. With the exception of the bot mitigation engines, Imperva Cloud is very signature based, and lags behind some competitors for ML-based capabilities.
- **Geographic strategy:** Imperva's presence in the Asia/Pacific region continues to lag behind its direct competitors. The cloud service does not have local POPs in China and only has two in India. Overall, worldwide POPs are limited, compared with other CDN providers.

Microsoft

Microsoft is a Niche Player in this Magic Quadrant. Azure Web Application Firewall's capabilities are more limited compared with those of most competitors, but the service remains attractive for organizations with workloads on Azure.

Microsoft is a well-known IT and cloud provider, based in Redmond, Washington. Its IaaS and PaaS offering, Microsoft Azure, includes a WAF (Azure WAF) built on top of its CDN (Azure CDN), which is also available with its application delivery solution (Azure WAF on Azure Application Gateway). Microsoft offers other security products, including DDoS protection (Azure DDoS Protection), API security (Azure API Management), network firewall (Azure Firewall) and a security information and event management (SIEM) tool (Azure Sentinel).

In recent months, Microsoft has released a limited number of major new features for its Azure WAF, with improved integration with Sentinel, more granular scope for WAF policy, and updated bot protection rule sets.

Strengths

- **Sales execution:** Azure WAF is gaining market share and growing much faster than the market average, especially within the Azure customer base. Customers needed to scale their Azure footprint during the pandemic and liked the ability to easily purchase Azure WAF when subscribing to other Azure services.
- **Scalability:** With more than 170 POPs and 60 Azure regions supporting Azure WAF, Microsoft's global infrastructure is an asset for organizations looking to protect global web applications.
- **Capabilities:** Recent improvements for Azure WAF's integration with Azure Sentinel confirmed the importance of Microsoft's SIEM tool in Azure WAF's value proposition. Gartner analysts observe that large organizations using Sentinel report higher satisfaction with Azure WAF overall.
- **Customer experience:** Azure WAF users have noticed improvements made to the onboarding wizard. Many of them like that Microsoft offers a predefined policy with blocking enabled, since it shortens the initial setup.

Cautions

- **Marketing strategy:** Azure WAF remains mostly visible in Azure deployments. Although its architecture provides technical options for the use case, organizations with a multicloud strategy do not consider Azure WAF in their shortlists.
- **Customer experience:** Customers point to insufficient documentation, especially when trying to customize Azure WAF protections or when the protected applications require more advanced tuning.
- **Capabilities:** Azure WAF's capabilities lag behind those of many competitors. Its rule set remains primarily based on generic signatures without ad hoc signatures related to vulnerabilities covered by Common Vulnerabilities and Exposures (CVEs). Its security engine still lacks behavior-based detections and API discovery.
- **Capabilities:** Despite recent improvements, Azure WAF's bot mitigation capabilities remain limited compared with those of most competing services evaluated in this research. The lack of behavior-based bot detection or account takeover protection are the primary gaps to fill.

Radware

Radware is a Visionary in this Magic Quadrant. Its differentiated approach to application security, combining ML techniques and rules, is more successful in the appliance segment than in cloud today,

but the vendor continues to experiment with innovative approaches.

Radware is an infrastructure and security provider, primarily known for its DDoS protection (DefensePro and Cloud DDoS Protection Service) and application delivery (Alteon ADC), based in Tel Aviv, Israel, and Mahwah, New Jersey. Radware offers WAAP in various form factors, including appliances, in a containerized envelope (KWAF), or as a cloud WAAP service (Cloud WAF Service).

In the last 12 months, Radware has added API security features to its cloud WAAP, including more fine-tuned bot mitigation and the ability to import OpenAPI schema. The vendor has also finalized the integration of the ShieldSquare bot management, released improved role-based access control (RBAC) and TLS 1.3 support, and refreshed its onboarding wizard.

Strengths

- **Innovation:** Radware's roadmap continues to include a significant portion of features intended at solving web application security problems in an innovative way. Recent examples include: new uses of ML for real-time classification of SQL injection attacks; a new approach to CAPTCHA to defeat CAPTCHA-solving bots; and multiple options for deploying WAAP in the most efficient way when protecting applications in Kubernetes environments.

- **Capabilities:** Radware's risk scoring for source, leveraging "penalties," offers a good combination of easy-to-understand and easy-to-tune abnormal activity detection. The feature and penalty weights have matured over time to provide a more balanced default configuration.

- **Capabilities:** Radware's cloud monitoring portal includes clean views for its IP analytics module, a good set of features in the application analytics, including smart aggregation of events, and an easy way to add an exception in case of false alert. Users can also create custom notifications triggered by the threshold of selected alerts.

- **Customer experience:** Gartner received good feedback from existing Radware customers who have transitioned to the new bot mitigation modules. They reported meaningful improvements in bot detections and more actionable dashboards than for other categories of threats.

Cautions

- **Sales execution:** Radware's success in cloud WAAP services is limited for now. Gartner estimates Radware Cloud WAF Service lost market share in the last 12 months due to a lower-than-market-average growth.

- **Marketing execution:** Radware struggles to build brand awareness for its WAAP product line. This is more likely to position the vendor as an outlier in shortlists, making it more difficult to convince nontechnical decision makers during the product evaluation.

- **Customer experience:** Users of the Radware WAAP appliances report that the UI could be improved, that a steep learning curve is required, and that advanced options are sometimes

difficult to find.

- **Organization:** Radware's relatively small threat research team is focused mainly on the data science aspects of the product. The vendor's direct support team for WAAP supporting the Asia/Pacific region is also relatively small.

ThreatX

ThreatX is a Visionary in this Magic Quadrant. The vendor is gaining traction thanks to its risk scoring engine and its use of shared threat intelligence to provide better visibility and protection on the threats to its customer applications.

ThreatX is a cloud-native security startup, launched in 2015, with its main headquarters in Louisville, Colorado. Its fully managed WAAP platform (ThreatX WAAP Platform) comprises containerized processing units that 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.

In the last 12 months, ThreatX has announced API traffic monitoring for threat detection, which complements the previously existing API protection features, showing discovered API endpoints. It has also made available a bot activity dashboard and new threat detection capabilities.

Strengths

- **Innovation:** ThreatX real-time dashboards are centered around the notion of risk for the protected applications. The risk score, associated with the client ("user" in ThreatX terminology) leverages insights gained from any connection by the same fingerprinted client across the vendor's customer base. It helps categorize malicious sources, even if they never connected to the application before.
- **Capabilities:** ThreatX WAAP offers three options for blocking: risk-based, per request, or manual (detection only). Most clients combine risk-based and per-request blocking to minimize the risk and impact of false positives.
- **Product strategy:** ThreatX's management console includes multitenancy by design, which makes it really easy to manage multiple entities, such as applications belonging to different business units or projects. The multitenancy approach is also integrated into the "top targets" view of the monitoring console.
- **Customer experience:** ThreatX receives high marks from customers for its ease of deployment and excellent customer support, including fast responses for rule customization requests.

Cautions

- **Operations:** ThreatX is the smallest vendor evaluated in this research. Its threat research and managed SOC teams are small. Prospective enterprise clients should evaluate the vendor's ability

to support their needs and offer personalized services.

- **Geographic strategy:** ThreatX primarily operates from the U.S. Its management console is only available in English, and support is delivered from U.S.-based locations. Even if the containerized-based architecture makes it easy to deploy new POPs in theory, ThreatX has yet to maintain a strong set of POPs outside of North America.

- **Product:** ThreatX defends a different approach to risk scoring, not messaging around ML capabilities. Differentiated approaches demand strong customer support. Prospective customers in need of a high-security solution must get feedback from peers with similar applications before considering a POC.

- **Capabilities:** As expected from a smaller provider focused on some key differentiations, ThreatX lacks features that its competitors offer. It offers limited API discovery and does not provide a dedicated set of signatures for API threats. It also lacks client-side protection. ThreatX does not use HSMs to secure TLS secrets, nor does it work with remote HSMs.

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

Fastly acquired Signal Sciences and therefore appears for the first time in this report.

ThreatX appears for the first time in this report.

Dropped

Fastly acquired Signal Sciences and therefore Signal Sciences no longer appears in this report.

Inclusion and Exclusion Criteria

Each WAAP vendor that met Gartner’s market definition/description was considered for this Magic Quadrant under the following conditions:

- 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 OWASP Top 10 threats, in addition to others.

- It provides physical, virtual or software appliances, or a cloud WAAP service.
- Its WAAP service was generally available as of 1 January 2020.
- Its WAAP service demonstrates global presence, and features/scale relevant to enterprise-class organizations:
  - It generated $20 million in WAAP revenue during 2020 and had at least 200 enterprise customers use its WAAP products under support as of 31 December 2020, including:
    - At least 40 paying customers for its cloud WAAP service product
    - At least 30 net new enterprise WAAP customers in 2020
  - Or, $3 million in WAAP revenue during 2020, and two years of compound annual revenue growth (CAGR) of at least 50%
- The vendor must demonstrate at least minimum signs of a global presence — i.e., Gartner needed to see strong evidence that more than 10% of the vendor's customer base is outside its home region (the Americas, EMEA or Asia/Pacific region).
- The vendor offers 24/7 support, including phone support — in some cases, this is an add-on, rather than being included in the base service.
- Gartner has determined that the vendor is a significant player in the market due to market presence, competitive visibility or technology innovation.
- The vendor is a top provider by Gartner-estimated market share or mind share for the relevant segments of the overall WAF market.
- The vendor appears in Gartner client inquiries, has competitive visibility, client references and local brand visibility.
- The vendor's WAF technology provides more than a repackaged ModSecurity engine and signatures.
- The vendor must provide evidence to support meeting the above inclusion requirements.

WAAP and WAF companies that were not included in this research may have been excluded for one or more of the following reasons:

- The vendor primarily has a network firewall or IPS with a nonenterprise-class WAAP.

- The vendor is primarily an MSS provider and WAF/WAAP sales mostly come as part of broader MSS provider contracts, or is a service provider leveraging third-party WAF or WAAP technology.
- 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 (ISPs) 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, WAM, RASP or API gateway (these are considered distinct markets).

Honorable Mention

Vendors to Watch

In addition to the vendors included in this Magic Quadrant, Gartner tracks other vendors that did not meet our inclusion criteria because of a specific vertical market focus and/or WAAP revenue and/or competitive visibility levels in WAAP projects.

Other vendors include A10 Networks, Alert Logic, Alibaba Cloud, Array Networks, Brocade, Cequence Security, Citrix, DBAPPSecurity, DB CyberTech, ditno, Ergon Informatik, Google, Huawei, Imvision, Kemp, L7 Defense, Limelight Networks, Link11, ModSecurity, NSFOCUS, Oplon, Oracle, Penta Security Systems, PIOLINK, Positive Technologies, Qualys, Reblaze, Rohde & Schwarz, Sangfor Technologies, SiteLock, Salt Security, StackPath, Sucuri, Templarbit, Tencent, Total Uptime, Trustwave, Venustech, Verizon, VMware, and Wallarm.

Evaluation Criteria

Ability to Execute

Product or Service: This criterion includes the core 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/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 WAAP core security functions. These include DDoS protection services, bot management (e.g., bad-bot mitigation and good-bot management) and API security, which might be bundled or integrated with WAF features. Integration with other markets, such as cloud access service brokers (CASBs) and application security testing (AST), is evaluated as well, but more lightly.

Overall Viability: This includes an assessment of the organization's overall financial health, and the financial and practical success of the business unit. It also involves the likelihood that individual business units will continue to invest in WAAP, offer WAAP products and advance the state of the art in the organization's portfolio of products.

Sales Execution/Pricing: This 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 applications or e-commerce. Low pricing will not guarantee high execution or client interest. Buyers want good results even more than they want bargains. Buyers balance WAAP security requirements and pricing, and don't consider best pricing only.

Market Responsiveness/Record: This is 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 higher 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 assesses the relationships, products and services/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. But it can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups and service-level agreements (SLAs) that enable the organization to operate effectively and efficiently on an ongoing basis.

Operations: This is the organization's ability to meet its goals and commitments. Factors include the quality of the organizational structure.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	***Weighting*** ↓
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (September 2021)

Completeness of Vision

Market Understanding: This is the technology provider's ability to understand buyers' wants and needs, and translate them into products and services. Vendors that show the highest degree of vision listen to and understand buyers' requirements, and can shape or enhance them with their added vision. 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 will receive higher scores. Trends include cloud, IaaS, agile methodologies, web services and microservices, continuous integration, and the growing importance of APIs.

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

Sales Strategy: This strategy for selling products uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates to extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base. The ability to attract new customers in need of web application security only has a strong influence on this criterion.

Offering (Product) Strategy: This is the technology provider's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets, as they map to current and future requirements. As attacks change and become more targeted and complex, we highly weight vendors that move their WAAP beyond rule-based web protections that are limited to known attacks. For example:

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

This criterion also includes the evaluation of the depth of features, especially features that ease the management of the solution, and integration with other solutions, such as SIEM tools, API gateways and other technologies (e.g., CASBs).

Business Model: This is the soundness and logic of a technology provider's underlying business proposition.

Vertical/Industry Strategy: This is the technology provider'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 get lower scores. Vendors with differentiated vertical strategies and the ability to reproduce success across several verticals receive higher scores.

Innovation: This refers to 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 process and tooling
- Integration with companion security technologies, which improves overall security

Geographic Strategy: This is the technology provider's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography. This can happen directly or through partners, channels and subsidiaries, as appropriate for the geographies and markets.

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	Low
Vertical/Industry Strategy	Low

Evaluation Criteria ↓	Weighting ↓
Innovation	High
Geographic Strategy	Medium

Source: Gartner (September 2021)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors that can shape the market by introducing additional capabilities into their offerings, raising awareness of the importance of those features and being the first to do so. Leaders also meet the enterprise requirements for the different use cases of web application security.

We expect Leaders to have strong market share and steady growth, but these alone are not sufficient. Key capabilities for Leaders in the WAAP market are ensuring high-level security and smooth integration in the web application environment. They also include: advanced web application behavior learning; a superior ability to block common threats (such as SQLi, XSS and CSRF), protect custom web applications and avoid evasion techniques; and strong deployment, management, real-time monitoring and extensive reporting. Leaders should also provide and regularly improve DDoS protection, bot mitigation and API security capabilities. In addition to providing technology that is a good match with customer requirements, Leaders exhibit superior vision and execution for anticipated requirements, and evolution in web applications that require paradigm changes.

Challengers

Challengers in this market are vendors that have achieved a sound customer base, but are not leading on security features. Many Challengers leverage existing clients from other markets (e.g., CDN, ADC) to sell their WAAP technology, rather than competing with products to win deals. A Challenger may also be well-positioned and have good market share in a specific segment of the WAAP market (e.g., appliance or cloud service), but not address (and may not be interested in addressing) the entire market.

Visionaries

The Visionaries quadrant comprises vendors that have provided key innovative elements to answer web application security concerns. Visionaries devote many resources to security features that help

protect critical business applications against targeted attacks. However, they lack the capability to influence a large portion of the market. They either haven't expanded their sales and support capabilities on a global basis, or they lack the funding to execute with the same capabilities as vendors in the Leaders and Challengers quadrants. Visionaries also have a smaller presence in the WAAP market, as measured by the installed base, revenue size or growth, smaller overall company size or long-term viability.

Niche Players

The Niche Players quadrant is composed primarily of smaller vendors that provide WAAP technology that is a good match for specific WAAP use cases (such as PCI compliance), or vendors with a limited geographic reach. The WAAP market includes several European and Asian vendors that serve clients in their regions well with local support, and are able to quickly adapt their roadmaps to specific needs. However, they do not sell outside their home countries or regions. Many Niche Players, even when making large-scale products, offer features that would suit only the needs of SMBs and smaller enterprises.

Niche Players may also have a small installed base, or may be limited, according to Gartner's criteria, by a number of factors. These factors may include limited investments or capabilities, or other inhibitors to providing a broader set of capabilities to enterprises now and during the 12-month planning horizon. Inclusion in the Niche Players quadrant does not reflect negatively on a vendor's value in the more narrowly focused service spectrum.

Context

Gartner generally recommends that client organizations consider products from vendors in every quadrant of this Magic Quadrant, based on their specific functional and operational requirements. This is especially true for the WAAP market, which includes a large number of relatively small vendors, or larger vendors that have only a small share of their revenue coming from WAAP offerings. Product selection decisions should be driven by organization-specific requirements. These involve such areas as deployment constraints and scale, the relative importance of compliance, the characteristics and risk exposures of business-critical and custom web applications, and the vendor's local support and market understanding.

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

- Their tolerance for a full, in-line reverse proxy with blocking capabilities in front of the web applications
- The benefits and constraints of the different WAAP delivery options:
  - Appliances

- Cloud services

- TLS decryption/re-encryption and other scalability requirements
- Requirement to protect applications hosted on multiple cloud and on-premises locations.

Market Overview

The web application and API protection (WAAP) market remains dynamic, with many providers claiming strong, double-digit growth for their cloud WAAP. Gartner observed a 15% growth in WAAP inquiries in 2020 compared with the previous year, impacted less by the pandemic and attributed to the expansion of organizations' digital transformation initiatives adding more applications and APIs to their portfolios.

WAAP development started with cloud-delivered WAF services that were easier to deploy, and from the start bundled WAF with application-layer DDoS protection. Slowly, the WAF market evolved to offer more than basic capabilities for bot management and API protection. 2019 marked a turning point, with four vendors acquiring specialized bot mitigation providers. During 2020, Gartner observed improvements related to the availability of API security features, but also more stringent enterprise requirements related to the four core WAAP features: WAF, DDoS protection, bot management and API protection.

Last year, we noted that **the WAAP appliance segment remains the silent majority,** with most existing WAAP deployments in the form of physical or virtual appliances. This remains true even if a growing number of organizations in EMEA and in the Asia/Pacific region start to incorporate cloud WAAP as an option, or even cloud-first for the new web applications also deployed in the cloud.

Cloud WAAP vendors are sharpening their API security strategy. Leading vendors are adding API discovery and dedicated controls, but the market's average for API security remains behind the specialized API security vendors.

Machine learning (ML) primarily for bot management and false positives could be used to help the management UIs to scale. Cloud WAAP services have been leveraging ML to build reputation scores, better differentiate bots from humans and, more recently, discover APIs. While there is still much progress to be made for combining ML with other detection techniques to better detect attacks, ML could also apply to a lesser known issue of WAAP — management at scale.

Generic default configurations cannot scale to every enterprise's application portfolio. Many enterprises have hundreds of applications and APIs. Most cloud-delivered WAAP services' user interfaces (UIs) are not capable of being efficient at this scale. Most security teams are forced to stick to a generic configuration and handle exceptions, ending up with a list of exceptions they can neither track nor understand, and a diminished security posture.

This is an area where the WAAP market could make the biggest progress. Unfortunately, because of the inherent complexity of the attack landscape, the vendors that have invested in their UI have narrowed the scope to keeping the basic configuration simple, and providing good security dashboards, which appeal to buyers during vendor shortlist demos. They do not address the more complex challenge of managing WAAP configuration at scale while providing the right combination of change workflow management, reliable configuration audit and change traceability, and a good mix of global, per-group and per-application settings.

Is distributed WAAP the future of WAAP? Modern application architectures are a moving target for WAAP products. Vendors are expanding reach with new WAAP components, such as host agent or Kubernetes sidecar. But these emerging architectures, while becoming more popular, have not yet reached broad market adoption. Most security teams remain in favor of a cloud-delivered WAAP deployed before the IaaS infrastructures, which can easily support web applications deployed across multicloud and hybrid environments.

For the WAAP to move closer to the web applications, providers will have to demonstrate the ability of these new deployment options to:

- Gather better context from the application and who or what is accessing the microservice, which could help reduce the false positive rate.
- Classify and protect against new categories of threats to the microservices environment through dedicated unsupervised ML techniques.
- Allow application development teams to programmatically declare application context and let the WAAP automatically enforce or modify the correct security rules at runtime.

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.