Gartner.

Licensed for Distribution

Magic Quadrant for Web Application Firewalls

Published 19 October 2020 - ID G00458445 - 52 min read

By Analysts Jeremy D'Hoinne, Adam Hils, Rajpreet Kaur, John Watts

The web application firewall market's growth continues to be driven by cloud-delivered web application and API protection services. Security and risk management leaders must assess how WAFs can provide improved, easy-to-consume and easy-to-manage security that respects data privacy demands.

Strategic Planning Assumptions

By 2023, more than 30% of public-facing web applications and APIs will be protected by cloud web application and API protection (WAAP) services, which combine distributed denial of service (DDoS) protection, bot mitigation, API protection and web application firewalls (WAFs). This is an increase from fewer than 15% today.

By 2024, most organizations implementing multicloud strategies for web applications in production will use only cloud WAAP services.

Market Definition/Description

The WAF market is driven by customers' need to protect public and internal web applications. WAFs protect web applications and APIs from a variety of attacks, including automated (bots), injection and application-layer denial of service (DoS). They should provide signature-based protections, and should also support positive security models (automated allow lists) and/or anomaly detection.

WAFs are deployed to protect web applications against external and internal attacks, monitor and verify access to web applications, and collect access logs for compliance/auditing and analytics. WAFs can take the form of physical or virtual appliances. Increasingly, they are delivered from the cloud as WAAPs. WAFs are most often deployed in-line, as a reverse proxy. This is the easiest way to perform full inspection and policy enforcement. Other deployment options include WAF plug-ins on the top of reverse proxies and load balancers, or network tap deployment. The rise of WAAP services performing as reverse proxies by design — as well as the adoption of more-recent transport layer security (TLS) suites that require in-line traffic interception (e.g., man in the middle) to decrypt — has reinforced the use of reverse proxies.

Gartner defines WAAP services as the evolution of cloud WAF services (see Defining Cloud Web Application and API Protection Services). WAAP services combine cloud-delivered, as-a-service deployment of WAF, bot mitigation, DDoS protection and API security, with a subscription model. WAAP providers may offer a managed service, and, for some, it is a mandatory component of such a product. WAAP originated as WAF vendors expanding to the cloud, and CDN vendors adding WAF. More recently, these vendors have built or acquired bot mitigation capabilities, and are working to expand their API security capabilities. Many vendors offer multiple versions of their WAAPs, often divided into a simple-to-use offering and a highly configurable version.

Some organizations selecting WAAP built from WAF appliances do it to acquire a unified management and reporting console, or advanced capabilities (e.g., a positive security model) that cloud-native WAAP services don’t yet offer.

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

- Purpose-built physical, virtual or software appliances
- WAF modules embedded in application delivery controllers (ADCs; see Magic Quadrant for Application Delivery Controllers)
- WAAP, including WAF modules embedded in larger cloud platforms, such as content delivery networks (CDNs), and cloud WAF services delivered directly from infrastructure as a service (IaaS) platform providers
- Virtual appliances available on IaaS platforms, as well as WAF solutions from IaaS providers

Stand-alone bot mitigation solutions, API gateway and specialized API protection solutions, and runtime application self-protection (RASP) are adjacent to the WAF market, and might compete for the same security budgets. This motivates WAF vendors to add relevant features from these markets, when appropriate. For example, WAAP might bundle web application security CDNs.

The ability of WAFs to integrate with other enterprise security technologies — e.g., application security testing (AST), web access management (WAM), or security information and event management (SIEM) — supports WAF's strong presence in the enterprise market. Consolidation of WAFs with such technologies as ADCs, CDNs or DDoS mitigation cloud services brings its own benefits and challenges. However, this market evaluation focuses more heavily on the buyer's security needs when it comes to web application security. This includes how WAF technology:

- Maximizes the detection and catch rate for known and unknown threats
- Minimizes false alerts (i.e., false positives) and adapts to continually evolving web applications
- Differentiates automated traffic from human users, and applies appropriate controls for both categories of traffic
- Ensures broader adoption through ease of use and minimal performance impact
- Automates incident response workflow to assist web application security analysts
- Protects public-facing, partner-facing, as well as internally used web applications and APIs

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

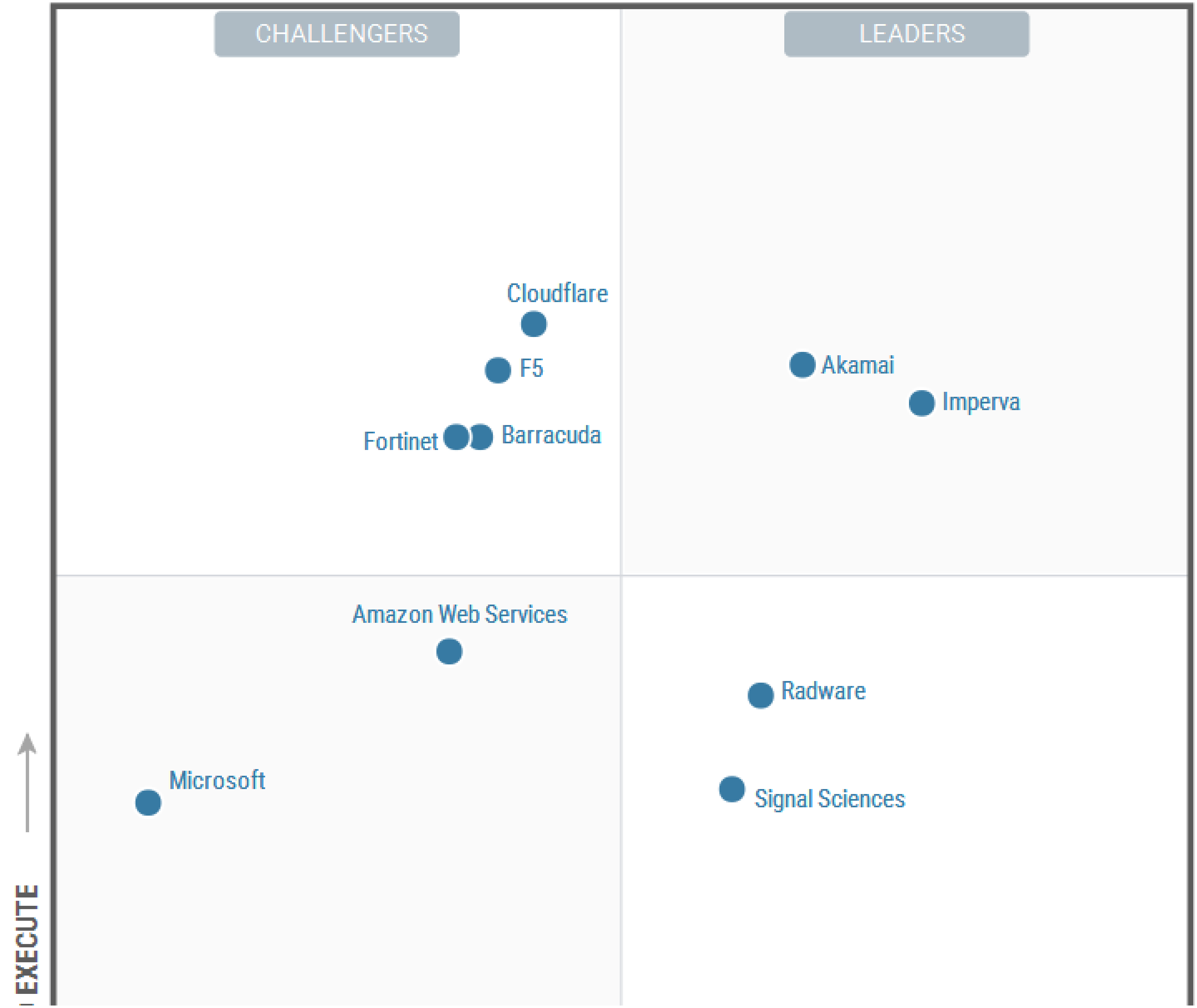
Because many local security providers, CDNs and ADCs might wrap a ModSecurity engine, and use one of the available rule sets, a large number of WAF solutions are available in the market today.

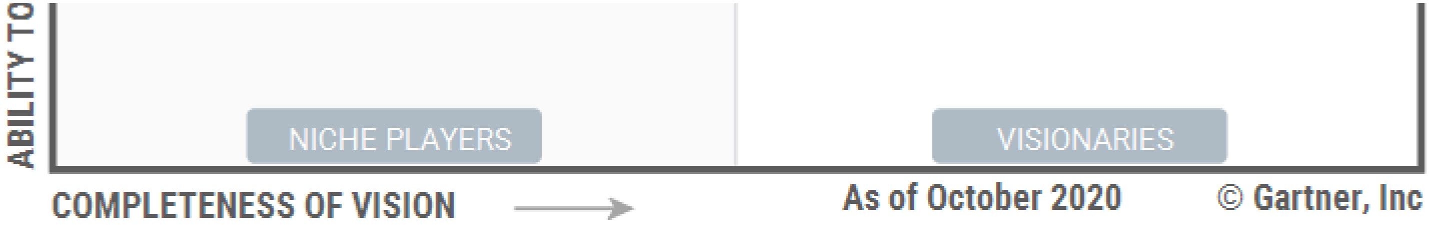
Gartner inclusion and exclusion criteria include a requirement to derive minimal revenue from outside a vendor's home region, as well as a requirement for a minimum number of customers for a cloud WAF service.

This has inevitably led to the exclusion of some of the smaller or more-regional vendors.

Magic Quadrant

Figure 1: Magic Quadrant for Web Application Firewalls





Source: Gartner (October 2020)

Vendor Strengths and Cautions

Akamai

Akamai is in the Leaders quadrant. This vendor is well-suited to appear on WAAP service shortlists to protect business-critical, web-scale applications, especially for organizations that want to deploy several high-quality, adjacent security capabilities.

With its headquarters in Cambridge, Massachusetts, Akamai is a global CDN provider with more than 8,000 employees, including a sizable group devoted to web application security. Akamai has two WAF 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 the release of Page Integrity Manager, Akamai's entry into client-side security. A central management user interface (UI) redesign and overhaul is intended to improve ease of administration and the user experience. There is also new zero overage pricing to lower customer costs, and enhanced API discovery and security. The vendor has also begun offering a new managed service on top of Bot Manager subscriptions.

KSD is a good shortlist candidate for use cases in which a premium WAAP solution is required, and adjacent application security features are desired, especially for Akamai CDN customers.

Strengths

- **Roadmap Execution:** Akamai has consistently delivered two major web application security releases each year that contain meaningful capabilities and products. Its large R&D group and its Threat Research team drive consistent product evolution.

- **Product Offering:** The broad portfolio of Akamai’s cloud services continues to expand. Akamai continues to expand web application security to cover new forms of attacks. The recently introduced Page Integrity Manager (PIM) is intended to protect users from form-jacking attacks, which involve compromised client-side scripts.

- **Product Capabilities:** Akamai has deep capabilities to provide a full spectrum of anti-DDoS services, offering volumetric Layer 2 through Layer 4 DDoS prevention (Prolexic), Layer 7 DDoS (KSD) and Authoritative DNS (Edge DNS).

- **Geographic Strategy:** Akamai continues to enhance its global presence. During this evaluation period, Akamai acquired Exceda, a leading Latin American channel partner, in an attempt to grow its Latin American footprint. The vendor leads competitors in point of presence (POP) scale for many regions.

- **Customer Experience:** Surveyed customers mention the high quality of Akamai’s managed security operations center (SOC) offering and staff.

Cautions

- **Market Segmentation:** Akamai’s WAF remains available as a cloud service only. For organizations uncomfortable with cloud security solutions, or where prospective clients’ assessments determine that compliance and regulatory restrictions limit its use, Akamai does not appear on client shortlists. Organizations with workloads in IaaS clouds sometimes prefer more-traditional virtual appliance approaches.

- **Pricing Strategy:** Gartner continues to get 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 sometimes provide lower price points. Akamai’s contracting model can be quite complex. Prospective clients should get a cost estimate early in the evaluation process.

- **Customer Experience:** According to Gartner clients, KSD is difficult for new users to learn. They have mentioned that technical support for the most recent features could be improved, and also report that extensive use of professional services is mandatory when deploying Akamai WAAP.

- **Capabilities:** Customers complain that error logs are not reported in a structured way, which creates difficulties. Once an error occurs, they struggle to navigate through the event information, making remediation less easy.

- **Technical Architecture:** Akamai lags behind some of its direct competitors in the ability to programmatically update the WAF, because it lacks a full-featured management API.

Amazon Web Services

Amazon Web Services (AWS) is in the Niche Players quadrant. Its WAF provides basic security and DDoS mitigation for web applications hosted inside and outside AWS, and it continues to lag in some capabilities, compared with third-party cloud WAF competitors.

Based in Seattle, Washington, AWS is a cloud service provider (CSP) subsidiary of Amazon. Its security portfolio includes identity and access management (IAM; Cognito), AWS Firewall Manager, and managed threat detection (GuardDuty). Its WAF product is simply called AWS WAF.

AWS WAF can be delivered through AWS Application Load Balancer or through Amazon CloudFront as part of the CDN solution. It is also integrated with the AWS Amazon API Gateway.

In 2020, AWS improved the WAF API (WAFv2) by removing previous limitations and combined the WAF-regional and WAF API into a single API, AWS WAF. Using the latest version, it now offers rules managed by the vendor (“AWS Managed Rules” [AMR]), in addition to the third-party rule sets already available in the AWS Marketplace.

AWS customers looking for an easy way to add security signatures in front of their applications or on the top of the AWS Amazon API Gateway should consider deploying AWS WAF, especially with one, or multiple, sets of managed rules.

Strengths

- **Customer Experience:** Customers cite an overall lower cost in using AWS WAF and ease of integration with other AWS security components as key strengths, compared with competitors’ offerings.

- **Technical Architecture:** AWS provides a robust cloud infrastructure worldwide containing 19 AWS regions and more than 200 Amazon CloudFront edge nodes. In fact, several other vendors in this Magic Quadrant deploy their cloud-based WAF service in AWS, leveraging their cloud edge architectures. Many vendors provide virtual instances of their WAF appliances in the Amazon marketplace.

- **Capabilities:** With AMR rule sets from AWS and other rule sets via subscription, AWS customers have access to automatically maintained rules from various sources, including established WAF or managed security service (MSS) vendors. Because they can deploy multiple rule sets simultaneously, customers can provide multiple layers of defense or test multiple provider rule sets.

- **Capabilities:** Similar to many other AWS services, AWS WAF is a fully programmable, API-first service that uses AWS continuous integration tools. AWS WAF Security Automations uses CloudFormation templates to allow administrators to add automated creation of rules and IP sets based on observed activity protecting against multiple classes of threats, such as SQL injection, cross-site scripting, HTTP floods and IP reputation allow lists.

- **Technical Architecture:** AWS Shield DDoS mitigation is provided at ingress, simplifying the need to route requests to scrubbing centers. AWS Shield DDoS can be applied to third-party WAFs hosted in the AWS Marketplace as well.

Cautions

- **Marketing Strategy:** AWS WAF's visibility is mainly limited to AWS workload protection, where it competes with cloud WAF services and virtual appliances. Gartner observes few clients adding AWS to their shortlists when evaluating WAF vendors.

- **Capabilities:** AWS WAF provides basic bot protection through the AWS-provided managed rule set and infrastructure protection capability. However, it lacks many application-specific, advanced bot protection features found in competitors, such as device fingerprinting, user behavior detections and JavaScript challenges.

- **Capabilities:** Customers need to deploy AWS Amazon API Gateway to get advanced API management features, such as the enforcement of JSON and XML traffic, based on definition files. In addition, AWS WAF does not support mobile security and relies on AWS Amplify or Amazon API Gateway for mobile security.

- **Customer Experience:** Customers cite challenges with the false-positive rates of the WAF rules, and with the granularity and features found in the reporting provided by Amazon CloudWatch, compared with other WAF vendors, which offer more comprehensive and detailed reporting.

- **Technical Architecture:** AWS WAF is deployed only in AWS and cannot be integrated directly with third-party CDN providers, unless the CDN is in front of AWS or Amazon API Gateway.

Barracuda

Barracuda is in the Challengers quadrant. Barracuda has good visibility for its WAF deployment on Microsoft Azure, and for existing Barracuda customers. It has significantly enhanced the feature set of its WAAP, named WAF-as-a-Service, and has gained traction with it during the evaluation period.

Headquartered in Campbell, CA, Barracuda is a known brand in security and data protection markets, especially for midsize enterprises (MSEs). Barracuda delivers its WAF line in physical or virtual appliances. It is also available as a virtual appliance (Barracuda CloudGen WAF) on Microsoft Azure, AWS platforms and Google Cloud Platform (GCP), and it has limited presence in Oracle Cloud and Alibaba. WAF-as-a-Service is based on the CloudGen WAF software stack.

In recent months, Barracuda has been expanding its WAAP to 61 POPs leveraging public cloud infrastructure. It has released enhancements of the Barracuda Advanced Bot Protection ML Layer, partially by integrating with the InfiSecure bot detection engine.

Barracuda is a good shortlist contender for organizations looking for WAF virtual appliances deployed on Azure, and for organizations seeking a comprehensive set of features delivered in an easy-to-use, self-service WAAP.

Strengths

- **Product Offering:** Barracuda has expanded the footprint of Cloud WAF-as-a-Service globally. It has seen rapid growth among midsize customers, especially in North America and Australia.

- **Customer Experience:** Customers remark on the ease of onboarding and initial setup, Customers routinely deploy the service without involving Barracuda technical support. They quickly set up the default policy that protects across Open Web Application Security Project (OWASP) Top 10, DDoS and malicious bots.Capabilities: The vendor has full TLS 1.3 capability, with custom cipher control and perfect forward secrecy.

- **Pricing Strategy:** Barracuda WAF continues to be perceived as a high-quality, low-cost solution. Barracuda Cloud WAF-as-a-Service includes DDoS protection and bot mitigation at no additional charge.

- **Technical Support:** Gartner clients continue to make positive remarks about Barracuda’s customer support. Barracuda’s as-a-service offerings may allow support to deal less with tactical issues and more with complex support issues.

- **Capabilities:** Barracuda’s free WAF add-on Vulnerability Remediation Service is attractive to Barracuda’s small or midsize business (SMB) customers, which often lack the time, money and expertise to support an in-house application scanning program.

Cautions

- **Sales and Marketing Execution:** Barracuda’s visibility in shortlists remains low, especially outside its customer base.

- **Customer Experience:** WAF appliances and WAF-as-a-Service use different UIs. Default signatures and customized signatures must be managed separately.

- **Capabilities:** Barracuda lacks DNS security. It also has no mobile software development kit (SDK) or other mobile application security.

- **Technical Architecture:** Barracuda WAF-as-a-Service supports HTTP/2 between the client and WAF, but not between the WAF and the origin server.

- **Product Strategy:** Gartner has noted that Barracuda is investing more effort in enhancing its CloudGen WAF and WAF-as-a-Service. Barracuda WAF customers that need hardware firewalls should ask the vendor what the product roadmap holds.

Cloudflare

Cloudflare is in the Challengers quadrant. Cloudflare is now evaluated as a serious contender in many WAAP deals, but continues to suffer from its brand association with its SMB roots.

Cloudflare is a public company, based in San Francisco. The vendor continues to grow, with more than 1,500 employees. The vendor's primary offering is a combination of DDoS protection and a CDN offering.

In recent months, Cloudflare has released its regional AnyCast group to better control which POPs process the traffic. Firewall rules can now apply to the body of the request, in addition to the header. Bot mitigation improved with the addition of optional JavaScript injection and a list of "verified bots" to avoid blocking legitimate bots. Cloudflare also replaced Google reCaptcha, as the service became a paid option and is now using hCaptcha. The vendor also improved its analytics engine and reduced the latency when exporting logs to the external SIEM solution.

Cloudflare is a viable solution for organizations of all sizes looking for a self-service WAAP, especially international organizations with multiple offices.

Strengths

- **Technical Architecture:** Cloudflare continues to expand its infrastructure and is one of the global players with the best presence across regions, including countries such as China, where other vendors often lack presence. Cloudflare's portfolio of easily integratable features, including CDN or single sign-on (SSO; Cloudflare Access) and edge scripting (Cloudflare Workers) appeals not only to the smaller organizations, but also to more-technical application and operations teams.

- **Capabilities:** Cloudflare offers an easy-to-follow portal for new Cloudflare signature releases, with an optional RSS feed. Cloudflare remains one of the only cloud WAFs that supports remote hardware security modules (HSM).
- **Bot Management:** Cloudflare has improved its bot management coverage with more flexibility in building custom rules for bot detection, and by making the Captcha success rate visible on the rule dashboard. Customers have reported slight improvement in the detection rate, following changes to the detection engine.
- **Roadmap Execution:** Cloudflare continues to regularly release a large number of new features across many of its products. Gartner hasn't observed any distraction or slowdown following the IPO, which sometimes comes as a distraction for vendors in a similar situation.
- **Customer Experience:** Customers continue to give good scores to the application onboarding process. Cloudflare WAF scores higher than average in customer surveys on the performance of the organization with international customer bases.
- **Capabilities:** Cloudflare WAF rules and bot management modules include a rule-testing module, which can show how many times a rule would have been hit in the last 24 hours. Combined with the flexible choices for response action, this is convenient for teams manually deploying the security rules in front of their most-sensitive web applications.

Cautions

- **Product Strategy:** Cloudflare has a “move fast and experiment” approach to product development. It has built enough safeguards to have service-level agreements (SLAs) competing with the other vendors evaluated in this research. However, an occasional outage, even one quickly fixed and followed by transparent postmortem analysis, might happen. This creates a challenge for technical sponsors when they have to explain their choice of Cloudflare to other teams, in organizations with little risk appetite.
- **Capabilities:** The WAF lacks an automated positive security model. It also lags its leading competitors in API security.
- **Market Segmentation:** Cloudflare is more rarely selected in high-security use cases. By continuing to add more advanced features to seduce the larger enterprises, Cloudflare WAF shows early signs of UI clutter.

- **Geographic Strategy:** Cloudflare lacks some of the desired features to support General Data Protection Regulation (GDPR)-compliant requirements, such as the ability to ensure that the traffic is logged only in specified European data centers.

- **Customer Experience:** Customers continue to rate Cloudflare's enterprise support lower than its direct competitors, especially on the timeliness of the answers. The vendor has invested more in its enterprise support during the past 12 months, and customers should expect improvements.

- **Capabilities:** Cloudflare WAF lacks the ability to schedule aggregated reports. Its real-time alert view does not automatically correlate individual alerts into more meaningful incidents. Role-based management still lacks custom role creation, and an easy way to assign roles per application or per group of applications.

- **Capabilities:** Cloudflare lacks some vertical-specific features, such as malware inspection to protect file upload services, or fraud detection capabilities that are sometimes desired by smaller financial institutions.

F5

F5 is in the Challengers quadrant. F5 continues to be challenged to keep up with its competitors, especially in the cloud space, as it tries to close the gaps through acquisitions.

Based in Seattle, Washington, F5 is known for its ADC product lines. F5's WAF is primarily consumed as a software option; Application Security Manager (ASM) is integrated in the F5 BIG-IP platform. Advanced WAF is the most comprehensive bundle. NGINX App Protect is a more lightweight module, deployed on the NGINX platform. Essential App Protect is a simpler version, aimed at protecting simpler web applications.

Under the Silverline brand, F5 delivers cloud WAF and DDoS protection with two offerings: Silverline Managed WAF and its self-service WAF Express, with a threat intelligence (TI) add-on (Silverline Threat Intelligence). All Silverline services rely on BIG-IP technology.

F5 made improvements in its Silverline dashboards and several improvements to the appliance, including enhanced API security policies, improvements in the learning engine, and Layer 7 denial of service (DoS) dashboards. In December 2019, F5 acquired Shape Security to improve bot management and fraud prevention capabilities. The vendor also released NGINX App Protect, its first WAF deployed on the top of the NGINX proxy and added Shape Security bot mitigation subscription on the top of Silverline (Silverline Shape Defense).

F5 is a good shortlist contender for large-scale WAF appliances, and for hybrid application environments, requiring consistent security features across cloud and on-premises deployment.

Strengths

- **Capabilities:** F5 Silverline WAF offers strong application security features, compared with other cloud-based WAAP products, such as cookie security, form protection and cross-site request forgery (CSRF) security. In addition, it provides strong API protections, including JSON and XML parsing and a mobile SDK.

- **Capabilities:** F5 WAF is part of a broader set of capabilities available on BIG-IP. It includes access management, load balancing and, now, more-advanced fraud detection features with Shape Security. Combined with the flexibility of iRules, it enables larger organizations to build strong sets of protections in front of their critical applications.

- **Sales Execution:** F5 remains among the most visible vendors in the WAF market. Organizations deploying WAF in the cloud frequently evaluate F5 virtual appliances when they need load-balancing features.

- **Capabilities:** F5 supports installation of its virtual appliance on IaaS environments and major private cloud vendors, such as Citrix XenServer, KVM, Microsoft Hyper-V and VMware for public cloud.

- **Customer Experience:** Customers like F5’s managed security service offering, which has a strong, dedicated staff to manage the service for customers with 24/7 SOC services located in North America and Europe.

Cautions

- **Product Strategy:** F5 struggles to demonstrate a clear, long-term strategy for the future of its WAAP offering. Its current portfolio is confusing. By owning NGINX with open-source and commercial WAF module options, an on-premises appliance and F5 Silverline cloud service, the company has split its WAF product lines. With the integration of Shape Security in progress, there is a potential to further split capabilities across multiple product sets, confusing existing and potential customers.

- **Capabilities:** Although, F5 Silverline WAF has strong API security features, it still lacks API management features integrated with the product. NGINX offers API management gateway features, but is not integrated with the F5 Silverline WAF.

- **Pricing:** Gartner feedback indicates lower satisfaction with overall Silverline costs, as well as evaluation and contract terms and negotiations, compared with peers in the WAF market.

- **Customer Experience:** Feedback in the past year shows relatively not as good customer experience with F5 than in previous years. Specifically, Gartner has seen higher levels of complaints on the reporting and complexity of the overall product.

- **Sales Execution:** F5 is a large corporation, compared with some of the vendors in the WAF market; however, Gartner estimates that it didn't grow at the market rate, indicating it's ceding share in the WAAP segment.

- **Technical Architecture:** F5 provides only 13 POPs worldwide for its F5 Silverline service, compared with competitors who offer many more. Most regions of the world have three or fewer POPs to cover the entire region, such as the U.S. or Europe, the Middle East and Africa (EMEA). The vendor also relies on third parties to deliver CDN services.

Fortinet

Fortinet is in the Challengers quadrant. FortiWeb continues to be visible in shortlists in the vendor's customer base, but it has not yet caught up in terms of visibility with the offerings from the leading WAAP providers.

Fortinet is based in Sunnyvale, California. The vendor was primarily known for its application-specific integrated circuit (ASIC)-accelerated firewall, but it is now a credible large-network security provider. The vendor has almost 7,500 employees.

Fortinet's portfolio includes a firewall (FortiGate) that constitutes most of the vendor's revenue. The WAF (FortiWeb appliance and FortiWeb Cloud) is available as a physical or virtual (FortiWeb-VM) appliance, and on IaaS, including AWS, Azure and GCP.

During the last year, Fortinet continued its effort to leverage machine learning (ML) to improve its attack detection, including bot detection, and to further reduce false positives. It released the ability to validate API schema and other API security features. Fortinet has also released more-granular, role-based access for FortiWeb Cloud.

FortiWeb is a good WAF appliance shortlist candidate, especially for existing Fortinet customers. WAAP prospects interested in evaluating the potential benefits of ML on attack detection should monitor Fortinet's progress.

Strengths

- **Product Strategy:** Fortinet continually improves and expands its use of ML to refine detections, support new use cases and reduce noise. Recent improvements include what the vendor calls Rapid Sample Collection, which reduces the learning period and bot detection features, such as analytics of keyboard and mouse click.
- **Customer Experience:** Customers give high scores to the modularity of FortiWeb Cloud UI. They like the fact that FortiWeb is available in multiple form factors, including appliances, containers and cloud services.
- **Customer Experience:** Fortinet customers emphasize the benefits of using FortiView, which looks familiar and allows them to integrate FortiWeb as part of its broader incident response workflow.
- **Sales Execution:** Fortinet continues to grow faster than the market in Europe and the Asia/Pacific (APAC) region, where its physical and virtual appliances have gained traction among Fortinet clients.

Cautions

- **Marketing Execution:** FortiWeb is not visible in WAF shortlists, when the client is not already using at least one Fortinet device.
- **Roadmap Execution:** FortiWeb Cloud’s roadmap continues to lag behind FortiWeb’s appliance for new feature release, and is not yet at feature parity.
- **Capabilities:** FortiWeb Cloud lacks ML-based bot mitigation and API discovery. It does not offer granular, role-based access for administrative users.
- **Capabilities:** FortiWeb Cloud lacks a tunnel mode to enforce better origin server security. Traffic log view is limited to a relatively low number of entries on the embedded FortiWeb Cloud log view.
- **Customer Experience:** FortiWeb customers continue to complain about false alerts, despite the vendor’s efforts. Customers outside North America mention support quality discrepancies, which Gartner attributes to inconsistent channel skill levels.

Imperva

Imperva is in the Leaders quadrant. Imperva provides strong security in on-premises and cloud offerings, but is increasingly challenged by competitors of its cloud offering.

Based in San Mateo, CA, Imperva is a privately held application security vendor. Its portfolio includes data security products, RASP (Imperva RASP), from the acquisition of Prevoty, a WAF as an appliance or virtual appliance (Imperva WAF Gateway), and a cloud WAF service (Imperva Cloud WAF). Imperva also offers a subscription for integrated, real-time analytics of the appliances and cloud WAF alerts (Attack Analytics), along with MSS and managed SOC.

In recent months, Imperva has completed integration of the Distil Network bot mitigation product into its Cloud WAF inspection engine and unified central management, and it has released new protections to defend against client-side attacks, such as Magecart. The vendor also revamped its FlexProtect pricing policy. It released support for gRPC and stronger role-based access management for WAAP administrators.

Imperva is a good shortlist candidate for all kinds of organizations, especially large enterprises looking for high-security WAF appliances, and in need of distributed WAAP service.

Strengths

- **Market Segmentation:** Imperva is one of the only vendors to achieve strong visibility in shortlists and large customer bases for WAF appliances and WAAP.

- **Capabilities:** Imperva offers comprehensive API security, including DDoS protections and the ability to parse JSON and XML, websockets, webhooks, GraphQL, gRPC and server-side events (SSE).

- **Customer Experience:** Imperva is often found on the shortlist of Gartner clients and compares favorably with other competitors in the market, especially when considering on-premises and cloud-based WAF requirements.

- **Capabilities:** Imperva has successfully integrated bot mitigation capabilities from Distil Networks, which are now available as a subscription (Advanced Bot Protection [ABP]) on top of the Imperva Cloud. It also remains available as an integrated module for IaaS platforms, and for some of Imperva's competitors. Imperva Cloud is also one of the few WAAP with a rule simulation feature, which helps users anticipate the impact of rules before enabling them.

- **Product Strategy:** Imperva focuses on end-to-end application security with a large portfolio of products, such as RASP, WAAP, file security and database security products, in addition to its WAF products.

Cautions

- **Capabilities:** Unlike some competitors and Imperva Gateway WAF, Imperva's Cloud WAF lacks ML for implementing positive security models, and relies on static rules to implement this approach.
- **Customer Experience:** Some Gartner clients report disappointment in the security of their Imperva Cloud WAF, which may be due to challenges with the default configuration and unintuitive configuration options to improve on that.
- **Product Strategy:** Imperva offers API security features, but lacks API management capabilities. It hasn't shown any intention to include API management features into its offering.
- **Customer Experience:** Customers rate their experience of product evaluation and contract negotiation, as well as service and support with Imperva, lower than with other vendors.
- **Geographic Strategy:** Imperva's presence in India and China remains limited. There is no local support in India. The cloud service does not have local POPs in China itself and only has two in India. Overall, worldwide POPs are limited, compared with other CDN providers.
- **Capabilities:** Imperva does not provide a way to natively inspect files for malware with its Cloud WAF. They only provide integration to third-party sandboxes through application delivery rules.

Microsoft

Microsoft is in the Niche Players quadrant. Azure WAF is integrated with Azure's ecosystem and is easy to deploy.

Based in Redmond, Washington, Microsoft is a one of the most well-known IT brands, with a diversified and broad portfolio. Microsoft Azure, its IaaS and platform as a service (PaaS) include a WAF (Azure WAF) built on the top of its application delivery solution (Azure Gateway WAF) and, more recently, on Azure's CDN (WAF with Front Door service). The vendor's WAF integrates with other Azure products, such as Azure DDoS protection service, Azure Load Balancer (ALB) and Azure Traffic Manager (ATM).

Azure Portal and Security Center are the management solutions for Azure Application Gateway and for Azure WAF.

In recent months, Microsoft has focused on making Azure WAF available in more Azure regions, and on better integrating Azure WAF with other Azure services. It now natively integrates with the AKS ingress controller for the protection of microservices, and can send events to Microsoft's Azure Sentinel for integrated monitoring. Azure WAF also better leverages Microsoft TI to block known bots.

Microsoft Azure WAF is a good shortlist candidate for organizations looking for integrated WAF, while deploying workloads on Microsoft Azure.

Strengths

- **Technical Architecture:** Azure WAF native autoscaling and native integration with the AKS ingress controller greatly simplify the deployment of WAF for web application and microservices.

- **Capabilities:** Azure WAF's integration with Azure Sentinel, Microsoft Azure monitoring and analytic product, brings mature role assignment and investigation capabilities. Early customers see it as a strong value-add, especially when using Azure Sentinel for other Microsoft products.

- **Capabilities:** Microsoft has improved its ability to block volumetric DDoS, and released a first version of bot mitigation capabilities, leveraging TI to block known bots. Azure WAF can parse JSON and XML payloads and apply security rules to this content. Bot mitigation rules can be added as an additional rule set to the WAF policies.

- **Customer Experience:** Surveyed customers continue to give good scores to Azure WAF's scalability. They also mention improvements to the onboarding wizard.

- **Geographic Strategy:** Azure WAF benefits from Microsoft's global infrastructure of data centers, with multiple PoPs in most regions. During the past 12 months, Microsoft has added more regions, and increased its total DDoS mitigation bandwidth.

Cautions

- **Product Strategy:** Microsoft is focused on making the WAF available to all of its clients, and incrementally adding features; however, the pace of new features does not allow Azure WAF to catch up to the competition yet.

- **Marketing Strategy:** Microsoft WAF is only visible in Azure deployments. Although Azure WAF architecture provides technical options for the use case, organizations with a multicloud strategy do not consider Azure WAF in their shortlists.

- **Capabilities:** Azure's management UI still lags behind competition. Although integration with Sentinel is a welcome addition, integrated reporting capabilities remain limited.
- **Capabilities:** Microsoft WAF lags behind the competition for behavior-based detection, and API security remains limited to OWASP signatures.
- **Customer Experience:** False positives and some features lagging behind competition or being unavailable remain the most frequent complaints about Azure WAF.

Radware

Radware is in the Visionaries quadrant. It maintains a differentiated approach through ML techniques devoted to a positive security model and continues to innovate and execute on its roadmap.

Headquartered in Tel Aviv, Israel, and Mahwah, New Jersey, Radware is a DDoS protection and application delivery and security provider. Its WAF, AppWall, may be deployed as a physical or virtual appliance, as a module on top of Radware's ADC appliance (Alteon) or, using the same technology as part of Radware's Cloud WAF Service.

In recent months, Radware released Kubernetes WAF (KWAF), which can natively integrate with Kubernetes as a sidecar container in a Kubernetes Pod. It delivered the integration of the ShieldSquare bot mitigation product as an add-on for the WAF. It also introduced Alteon Cloud Control for application delivery and security services deployed across various environments, such as on-premises data centers and private clouds, as well as various public cloud providers.

Radware is a good shortlist candidate for most organizations, especially those that want a strong positive security model. Organizations with high-security use cases, or applications that are unlikely to be compatible with an allow-list approach should engage in security testing, as part of the evaluation of the technology.

Strengths

- **Innovation:** Radware is regularly the first to invest in emerging architecture and use cases. The vendor now supports Kubernetes natively with the introduction of the Kubernetes WAF (KWAF), including integration with Kibana and Graphana for DevOps reporting and observability.

- **Capabilities:** Radware provides multiple, advanced ML algorithms to implement negative and positive security models for WAF, including automatic policy generation. Onboarding an application can be done in learning mode upfront to build policies or in immediate protection mode using a set of predefined templates based on application type (e.g., PHP).

- **Product Strategy:** Radware bases its Cloud WAF on the AppWall WAF, enabling existing policies to be bidirectionally shared between the two environments, easing transition to and from the cloud. The products are feature-complete between the two, offering a consistent experience in all locations: on-premises, public cloud and WAAP deployments.

- **Innovation:** Radware has fully incorporated ShieldSquare and now offers a complete bot management solution, with many advanced bot mitigation features, including the “Intent-based Deep Behavior Analysis technique,” which is designed to defeat bots that have “humanlike” behaviors to bypass other detection capabilities.

- **Capabilities:** Radware provides vDirect software-based management orchestration product to automate onboarding, configuration changes, and operations management. It hosts scripts in GitHub, supports Ansible scripts and has a Terraform provider.

Cautions

- **Sales Execution:** Based on client inquiries with prospects for cloud WAF services, Gartner analysts observe that Radware continues to be less visible in WAF shortlists than the Leaders and Challengers evaluated in this research.

- **Customer Experience:** Radware customers report slow responses from technical support and difficulties understanding how to integrate with other third-party products, such as a SIEM.

- **Capabilities:** Radware lacks several API security features found in other products, such as OAuth support, API key management, webhook parsing and parsing SSEs.

- **Technical Architecture:** Radware’s Cloud WAF does not support server origin with IPv6 addresses, which is sometimes requested in the APAC region where the vendor is visible. It leverages a partnership with Verizon to provide CDN, because the WAF does not natively include CDN features.

- **Product Strategy:** Radware’s relatively small threat research team is focused mainly on the data science aspects of the product. It relies on its own signatures, plus intelligence feeds from their ERT service to update the WAF for current threats.

- **Geographic Strategy:** Radware lacks vendor support centers in China and Latin America. Overall, worldwide POPs are limited, compared with other CDN providers, particularly in the APAC region.

Signal Sciences

Signal Sciences is in the Visionaries quadrant. The application security startup is gaining momentum, and customers have expressed a great deal of satisfaction with the solution.

Headquartered in Culver City, CA, it is a pure-play application security startup. Its main product is a runtime application security platform with multiple form factors. Signal Sciences competes in the WAF and RASP markets. The vendor calls its solution Signal Sciences Next Generation WAF. It can be deployed in multiple forms, including as a runtime agent, on the top of an NGINX proxy and, more recently, as a cloud WAF service. The solution is available on the main IaaS platforms. The vendor does not yet offer MSS or managed SOC.

Since last year’s evaluation, Signal Sciences has focused on making its WAAP available globally by adding more than 50 POPs, and by leveraging IaaS partners. It released new dashboards, and improved self-service onboarding. In September 2020, Fastly closed the acquisition of Signal Sciences.

Signal Sciences WAF is a good shortlist candidate for securing cloud-native applications. Enterprises considering Signal Sciences WAF should get clarity on agent-based deployment’s future, because Fastly’s main offering is a CDN.

Strengths

- **Customer Experience:** Customers continue to give high scores to Signal Sciences’ ease of use and flexible dashboards. The ability to create views for some specific traffic pattern in a few minutes is a frequent differentiator, especially when trying to convince nonsecurity teams.

- **Technical Architecture:** Signal Sciences has scaled its WAAP on the top of an IaaS infrastructure and now offers a global presence for the “hosted agent” deployment option, the vendor’s name for its WAAP.

- **Capabilities:** The foundation of Signal Sciences technology is a flexible policy engine, with three levels of rules: vendor rules; templated rules, with some customization; and custom rules (“power rules”).

- **Sales Execution:** Signal Sciences' visibility in North American WAF shortlist is higher than what Gartner analysts witness for solutions of the same age.

- **Customer Experience:** Signal Sciences customer base is faithful and extremely positive about the overall experience, especially when the buying center is part of a cloud-native application initiative. They often contrast it with previous unsuccessful and more-resource-intensive WAF deployments.

Cautions

- **Roadmap Execution:** Signal Sciences' pace of new feature release has been slow, when compared to its leading competitors. The vendor needs to demonstrate its ability to maintain its differences, but also close feature gaps if it aims at leading the market.

- **Customer Experience:** Although comments on ease of use are generally positive, some customers report a negative experience with the agent, including initial friction when trying to automate the deployment in various environments, and the cost of maintenance, especially the lack of automated update and relative short life span of agent as they are replaced with newer versions.

- **Support:** Signal Sciences' support team is small, and its ability to provide support in languages other than English is limited. The vendor's support primarily operates from North America. Documentation and management interface are in English only.

- **Product Offering:** Like its CDN competitors, Signal Sciences lacks a physical appliance offering, which can cause its exclusion from some WAF shortlists with hybrid deployment requirements. Deploying the WAAP on more than one IaaS regions requires users to contact the vendor.

- **Marketing Strategy:** Signal Sciences' WAAP lacks strong proof of its security depth. Prospective customers should evaluate the product's ability to detect advanced and custom attacks, beyond the automated scanner tests that some proofs of concept (POCs) rely on.

- **Capabilities:** Signal Sciences lacks automatic application behavior learning. Its bot mitigation capabilities lag behind most vendors evaluated in this research. Creating a positive security model for API traffic requires the manual creation of custom rules.

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.

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 reflect a change in the market and, therefore, changed evaluation criteria, or a change of focus by that vendor.

Dropped

Alibaba Cloud has been dropped, because it did not meet our inclusion criteria.

Oracle was dropped, because it did not meet our inclusion criteria.

Inclusion and Exclusion Criteria

WAF vendors that meet Gartner’s market definition/description are considered for this Magic Quadrant under the following conditions:

- Their offerings can protect applications running on different types of web servers.
- Their 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.
- The product provides physical, virtual or software appliances, or cloud WAF service.
- Their WAFs were generally available as of 1 January 2019.
- Their WAFs demonstrate global presence, and features/scale relevant to enterprise-class organizations:
  - They generated $20 million in WAF revenue during 2019

  - At least 200 enterprise customers use their WAF products under support as of 31 December 2018, including:
    - At least 40 paying customers for its WAAP product
    - At least 40 net new WAF customers in 2019
  - Or, $10 million in WAF revenue during 2019, and two years of compound annual revenue growth (CAGR) of at least 30%
- The vendor must demonstrate minimum signs of a global presence — i.e., Gartner received strong evidence that more than 10% of its customer base is outside its home region (the Americas, EMEA or the APAC region).
- The provider 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 they are significant players in the market, due to market presence, competitive visibility or technology innovation.
- All the providers in this evaluation are among the top providers by Gartner-estimated market share or mind share for the relevant segments of the overall WAF market.
- Vendors appearing in Gartner client inquiries, competitive visibility, client references and the vendor's local brand visibility are considered.
- Gartner analysts assess that 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.

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 non-enterprise-class WAF.
- The vendor is primarily an MSS provider and WAF sales mostly come as part of broader MSS provider contracts, or is a service provider leveraging third-party WAF technology.

- The vendor is not actively providing WAF products to enterprise customers, or has minimal continued investment in the enterprise WAF 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 WAF evaluation, and do not rate platform providers separately.
- The vendor has only a host-based WAF, WAM, RASP or AWS Amazon API gateway (these are considered distinct markets).

Honorable Mention

Vendor to Watch: Google

In May 2020, Google updated Cloud Armor, its WAF and DDoS mitigation service, available on GCP, adding useful features, such as IP control lists and geo-IP filtering, predefined rules for XSS and SQLi blocking, and custom rule creation. Google's WAF is still recent; however, the vendor is showing signs of willingness to expand its capabilities.

Gartner analysts continue to monitor Google's progress with its WAF product, because GCP is a convenient solution to deploy for applications hosted on Google IaaS platform.

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 WAF revenue and/or competitive visibility levels in WAF projects. These include A10 Networks, Alert Logic, Alibaba Cloud, Array Networks, Avi Networks, Beijing Chaitin Technology, Brocade, Citrix, DBAPPSECURITY, DB Networks, ditno., Ergon Software, Fastly, Huawei, Indusface, Kemp Technologies, L7 Defense, Limelight Networks, Link11, ModSecurity, NGINX, NSFOCUS, OPLON, Oracle, Penta Security, PIOLINK, Positive Technologies, Qualys, Rohde & Schwarz Cybersecurity, Sangfor, SiteLock, Sucuri, Templarbit, Tencent, Threat X, Total Uptime, Trustwave, Venustech, Verizon and Wallarm.

Evaluation Criteria

Ability to Execute

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 (October 2020)

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

Product or Service: This includes the core WAF technology offered by the technology provider that competes in and serves the defined market. This 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 related security functions. These include DDoS protection services, bot management (e.g., bad-bot mitigation and good-bot management), fraud detection, API security and TI feeds, which might be bundled or integrated with WAFs. 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 WAF, offer WAF 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, as well as 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 WAF 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. 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 is 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 customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, and service-level agreements (SLAs), including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

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	Medium
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Medium

Source: Gartner (October 2020)

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. This 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 WAFs beyond rule-based web protections that are limited to known attacks. For example:

- Enabling a positive security model with automatic and efficient policy learning
- Leveraging ML to improve the quality of the detection engines
- Using a weighted scoring mechanism based on a combination of techniques
- 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

The following criteria include the evaluation of the depth of features, especially features that ease the management of the solution, and integration with other solutions, such as DDoS protection services 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.

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors that can shape the market by introducing additional capabilities in their offerings, raising awareness of the importance of those features and being the first to do so. They 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 WAF market are ensuring higher 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. They should also provide and regularly improve DDoS and bot mitigation 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 to sell their WAF 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 WAF market, 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. They devote more resources on 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 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 WAF market, as measured by the installed base, revenue size or growth, or by smaller overall company size or long-term viability.

Niche Players

The Niche Players quadrant is composed primarily of smaller vendors that provide WAF technology that is a good match for specific WAF use cases (such as PCI compliance), or vendors with a limited geographic reach. The WAF 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 WAF market, which includes a large number of relatively small vendors, or larger vendors that have only a small share of their revenue coming from WAF 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 WAF 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 WAF delivery options:
  - Dedicated appliances
  - CDNs

- ADCs
- Cloud services
- Secure Sockets Layer (SSL) decryption/re-encryption and other scalability requirements

Market Overview

The WAF market remains dynamic, with many providers claiming strong, two-digit growth. Gartner observed a short period of slowdown during the early days of the pandemic, followed by a quick return to normal with 20% growth in end-user WAF inquiries for the first half of 2020.

- **WAF Appliance Is the Silent Majority:** Most Gartner client inquiries involve selecting a WAAP product. However, Gartner estimates that most existing WAF deployments are in the form of physical or virtual appliances. This is especially true outside North America, and among the more traditional web applications, even when deployed on IaaS. What is changing is that, despite the existing market share, most providers now prioritize the development of their WAAP products. When planning their roadmap, providers favor features that can be delivered in both deployment form factors.

- **WAAP Is the Primary Solution for New Applications:** Gartner has observed the growing importance of WAAP architecture. There is a split between WAAP over IaaS infrastructure (“cloud-rented”), which sometimes looks like a forklift of WAF appliance products, and distributed WAAP built on proprietary infrastructure (“cloud-owned”). The latter architecture style tends to move faster when adding new features and leveraging large-scale data to feed learning algorithms. The single-site (or regional) approach often comes with centralized management expanding beyond WAAP. Customers with hybrid WAF deployments often favor this option. Customers with a larger number of cloud-hosted web applications and API to protect tend to favor the distributed WAAP, which more often comes bundled with a CDN and favorable DDoS protection add-ons.

- **The Next Two Years Will Decide Whether WAAP Can Lead API Security:** 2019 was the year of bot mitigation vendor acquisition: Radware acquired ShieldSquare in January, Imperva acquired Distil Networks in June, Barracuda acquired InfiSecure in August and F5 acquired Shape Security in December. This series of acquisitions significantly moved the market average for bot mitigation capabilities, with bot mitigation subscriptions, leveraging the acquired technologies now broadly available. Gartner anticipates that the next step will be API security, where first versions of schema validation for positive security model, and additional support for API protocol are already available. However, WAF providers will have to face competition from API gateway providers, and also ensure that they can be “good enough” for the discovery, the monitoring and the protection of critical API and service meshes. Enterprises looking for WAF appliances and WAAP solutions do not yet strongly consider API security as part of their evaluations, but Gartner expects that to change during the next two years.

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.

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."

© 2018 Gartner, Inc. and/or its Affiliates. All Rights Reserved.