Magic Quadrant for Web Application Firewalls

Published: 7 August 2017 **ID:** G00314552

Analyst(s): Jeremy D'Hoinne, Adam Hils, Claudio Neiva

The WAF market is growing, driven by the adoption of cloud-based WAF service. Enterprise security teams should use this research as part of their evaluation on how WAFs can provide improved security that is also easy to consume and manage, while respecting data privacy requirements.

Strategic Planning Assumptions

By 2020, stand-alone WAF hardware appliances will represent less than 20% of new WAF deployments, down from 40% today.

By 2020, more than 50% of public-facing web applications will be protected by cloud-based WAF service platforms, combining CDN, DDoS protection, bot mitigation and WAF, up from less than 20% today.

Market Definition/Description

The web application firewall (WAF) market is driven by a customer's need to protect public and internal web applications when they are deployed locally (on-premises) or remotely (hosted, cloud-based or as a service). WAFs protect web applications and APIs against a variety of attacks, notably including injection attacks and application-layer denial of service (DoS). They should not only provide signature-based protection, but should also support positive security models and/or anomaly detection.

WAFs are deployed in front of web servers to protect web applications against external and internal attacks, to monitor and control access to web applications, and to collect access logs for compliance/auditing and analytics. WAFs are most often deployed in-line, as a reverse proxy, because historically that was the only way to perform some in-depth inspections. Today, other deployment modes exist, such as transparent proxy or network bridge. Some WAFs can also be positioned out of band (OOB, or mirror mode), and therefore work on a copy of the network traffic. Not every feature can work in all of these deployment choices, and reverse proxy is the most prevalent option for many organizations. In recent years, increased use by web applications of Transport Layer Security (TLS) encryption, based on cipher suites that require in-line traffic interception (man in the middle) to decrypt, have reduced the number of OOB deployments.

In recent years, WAF delivered as a cloud-based service directly by the vendor (cloud-based WAF service) has become a more popular option for a growing number of enterprises, beyond its initial target of midmarket organizations. Cloud-based WAF service combines a cloud-based deployment with a subscription model. The customers might also select a vendor's managed services for its cloud-based WAF service, or be forced to use it because it is a mandatory component of the offering. Some vendors have chosen to leverage their existing WAF solution, repackaging it as SaaS. This allows vendors to have a cloud-based WAF service available to their clients more quickly, and they can leverage the existing features to differentiate from cloud-native cloud-based WAF service offerings. One of the difficulties with this approach is simplifying the management and monitoring console to meet clients' expectations. Cloud-based WAF service, built to be multitenant and cloud-based from the beginning, could avoid costly maintenance of legacy code in the long term. It also provides a competitive advantage with faster release cycles and rapid implementation of innovative features. One of the main challenges for users consuming cloud-based WAF service built separately is the absence of a unified management console to support hybrid scenarios.

When speaking with clients about WAF adoption, Gartner observes occasional confusion with the application control feature (application awareness) present on network firewalls. The primary WAF benefit is protection for custom web applications' "self-inflicted" vulnerabilities in web application code developed by the enterprise, and protection for vulnerabilities in off-the-shelf web application software. These vulnerabilities would otherwise go unprotected by other technologies that guard mainly against known exploits (see "Web Application Firewalls Are Worth the Investment for Enterprises"). Most attacks on these corporate applications come from external attackers.

This Magic Quadrant includes WAFs that are deployed external to web applications and 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")
- Cloud-based WAF service, including WAF modules embedded in larger platforms, such as content delivery networks (CDNs)
- Virtual appliances available on infrastructure as a service (IaaS) platforms, and WAF solutions from IaaS providers

API gateway, bot management (which includes bad-bot mitigation and good-bot whitelisting) and runtime application self-protection (RASP) are adjacent to the WAF market, and might compete for the same application security budget. This motivates WAF vendors to add relevant features from these adjacent markets when appropriate; for example, cloud-based WAF services often bundle web application security with distributed denial of service (DDoS) protection and CDN. The ability of WAFs to integrate with other enterprise security technologies — such as application security testing (AST), database monitoring, or security information and event management (SIEM) — is a capability that supports its strong presence in the enterprise market. Consolidation of WAFs with other technologies, like 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 notably includes how WAF technology:

- Maximizes the detection and catch rate for known and unknown threats
- Minimizes false alerts (false positives) and adapts to continually evolving web applications
- Ensures broader adoption through ease of use and minimal performance impact
- Automates incident response workflow to assist web application security analysts
- Protects public-facing, as well as internally used, web applications and APIs

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

Magic Quadrant

Figure 1. Magic Quadrant for Web Application Firewalls

Source: Gartner (August 2017)

Vendor Strengths and Cautions

Akamai

Akamai moved from the Challengers to the Leaders quadrant. When clients require only cloud-based WAF service, Akamai's WAF appeals to prospective customers for its combination of strong security features and ability to scale.

Based in Cambridge, Massachusetts, Akamai is a CDN provider and employs a staff of more than 5,000. Its network and cloud security services, including its WAF (Kona Site Defender), are built on top of the Akamai Intelligent Platform, its global cloud infrastructure. Kona Site Defender includes DDoS mitigation options, such as Site Shield for origin protection, DDoS fee protection and a compliance management module. Optional add-ons, such as client reputation, bot manager and FastDNS (for DNS security), are frequently bundled with the Kona WAF.

In 2016, Akamai announced both the acquisition of Cyberfend, a company providing bot mitigation services, to enhance its existing bot mitigation offering and the availability of its simplified and lower-priced solution, Web Application Protector. In 2017, Akamai released version 5.0 of Kona Site Defender, which included new API security features and better integration with SIEM.

Kona Site Defender is a good shortlist candidate for all use cases where WAF delivered from the cloud is acceptable, and low price is not the highest priority, especially for existing Akamai CDN customers.

Strengths

- **Marketing strategy:** Akamai leverages a combination of cloud services, making vendor management easier for its client base. New features can be easily subscribed to and deployed, with minimum friction. This allows Akamai to successfully target business application owners, who later become internal sponsors for its solutions.
- **Product strategy:** Akamai's Kona Site Defender offers API and mobile app protections through integration with Akamai's platform. It inspects API calls based on message formats and context for the mobile application front end.
- **Capabilities:** Akamai's managed services help clients through onboarding applications and delivering expertise through rule reviews and threat intelligence. Its security operations center (SOC) can help implement the WAF and maintain it.
- **Capabilities:** Akamai leverages its cloud platform placement and large market share in the CDN market to gain visibility into a substantial share of internet traffic, which continually improves its reputation feeds and statistical analysis.
- **Customer experience:** Several customers scored Akamai very highly for overall customer satisfaction. The main reasons for good customer feedback are DDoS protection and the ability to scale, quality of the attack mitigation techniques, and customer support. Also, clients appreciate good global coverage.

Cautions

- **Market segmentation:** Akamai's WAF is available as a cloud service only. For cases where the organization is simply not comfortable with cloud-based security solutions, or where prospective clients' assessments determine that compliance and regulatory restrictions limit its use, Akamai does not appear on client shortlists.

- **Pricing and contracting:** Clients cite pricing as a barrier. The Web Application Protector offering was supposed to close this gap, but Gartner analysts haven't observed any decline in prospective clients' complaints about Akamai's high prices. The use cases for Web Application Protector seem very limited, as it prohibits the use of some advanced features, such as bot manager.
- **Technical architecture:** Because of its distributed architecture, Kona Site Defender policy changes can take more time than Akamai's direct cloud competitors. Web Application Protector is automated, and does not let customers tune rules provided by the vendor.
- **Capabilities:** Akamai's WAF cannot be managed using an API.
- **Customer experience:** Some clients would like to see better training, and cite a longer-than-expected learning curve to understand what to do in case of suggested policy update. This forces some clients to stick with the first deployed policy, because it is the only one that was validated.
- **Customer experience:** Bot Manager 1.0 had low level of satisfaction from customers. Clients also mention longer than desired delay to get access to consolidated logs.

Amazon Web Services

Amazon Web Services (AWS) is in the Niche Players quadrant. Its AWS WAF offers good integration with other AWS services, and is easily programmable, but it does not offer as many inbuilt security features as other vendors evaluated in this research. Its market reach is currently limited to AWS clients.

Headquartered in Seattle, Washington, Amazon Web Services, a subsidiary of Amazon (AMZN), is a cloud-focused service provider. AWS offers Xen-virtualized multitenant and single-tenant compute (Elastic Compute Cloud [EC2]) with multitenant storage. It also offers extensive additional IaaS and platform as a service (PaaS) capabilities, including object storage with an integrated CDN (Amazon Simple Storage Service [S3] and CloudFront), and a Docker container service (EC2 Container Service [ECS]).

AWS both competes and partners in the WAF market. It allows WAF competitors in the AWS marketplace, and also offers its own solution. AWS WAF can be delivered through AWS Application Load Balancer or through Amazon CloudFront as part of the CDN solution. AWS WAF works by being placed between website viewers and web servers deployed behind Application Load Balancers or CloudFront proxy servers. AWS WAF is not limited to protecting origin servers hosted on Amazon infrastructure. It can be deployed in front of public web applications, too.

Recent news for AWS WAF includes Internet Protocol version 6 (IPv6) support, a template including preconfigured rules for OWASP top vulnerabilities, and rate-based rules.

Prospective customers should consider AWS WAF in their shortlists if they want to protect public-facing web applications from common web exploits and use basic rule conditions at a volume-based cost, especially when the application is also hosted on AWS.

Strengths

- **Customer experience:** Customers rate the vendor highly on ease of deployment of AWS WAF. Teams frequently mention that they like the flexibility they get from the solution, especially the ability to quickly deploy AWS WAF as a temporary or complementary solution, even if there is an ongoing evaluation from the security team.
- **Capabilities:** AWS WAF helps organizations in a DevOps mode of operation with the full-featured APIs and CloudFormation automation. AWS customers can provision a set of WAF rules for each stack, or provision a set of WAF rules and automate the association of those rules with a new stack.
- **Capabilities:** AWS offers internet-scaled infrastructure for all applications. Its WAF service is compliant with the Payment Card Industry Data Security Standard (PCI-DSS) 3.2. In addition, AWS WAF is considered a Health Insurance Portability and Accountability Act (HIPAA)-eligible service.
- **Improvements:** AWS WAF is still a recent effort, launched in late 2015, but the vendor announces new features every other month. Recent releases include DDoS protection, rate-limit rules and IPv6 support. This regular pace of releases helps AWS come closer to what "good enough" would be for many organizations.
- **Sales execution:** Customers that utilize AWS Shield Advanced as a premium service are not charged extra for AWS WAF. For customers not using AWS Shield Advanced, AWS charges per use for AWS WAF based on how many rules customers deploy and how many web requests are inspected. Customers can select the capabilities that are needed for their applications among AWS products.

Cautions

- **Product strategy:** AWS WAF reach is currently mostly limited to AWS workload protection, where it competes with cloud-based WAF services and virtual appliances. It does not appear frequently on Gartner clients' shortlists. Most AWS WAF sales come from existing AWS clients, and the decision to implement AWS WAF is frequently made by the application or IT team, not security.
- **Capabilities:** AWS WAF is not yet feature-complete compared to many other solutions. It lacks API security, and provides basic bot mitigation and malware prevention (IP blacklists for known malware sources) features. Its predefined set of signatures for SQL injection and XSS is still a work in progress. Despite corporate artificial intelligence (AI) capabilities, the use of machine learning for web app security is currently built-in only for DDoS protection.
- **Capabilities:** AWS does not integrate with third-party or in-house application scanning technologies; thus, it complicates the use of the AWS WAF as a virtual patching mechanism.
- **Customer experience:** Security leads from several AWS customers report that using AWS WAF is more labor-intensive than expected. AWS WAF deployment can be fully automated, but configuration of the protections and access control lists remains primarily manual, with a lot of

scripting required to enable add-on features such as threat intelligence feeds. Its management console lacks granular preconfigured roles for administrators.

- **Customer experience:** Clients cite reporting as a weakness, with little capability to drill down or search for historical data. Since AWS lacks integration with SIEM solutions, clients often lack a solution to make AWS WAF part of their security monitoring workflow.

Barracuda Networks

Barracuda Networks is a Challenger. Barracuda is considered a strong contender for deployment in application environments where the primary requirements for selecting a WAF appliance are cost or a virtual appliance on a Microsoft Azure IaaS platform.

Headquartered in Campbell, California, Barracuda Networks (CUDA) is a security and storage vendor that caters primarily to midsize enterprises. Its line of products includes network firewalls, data management, email and web security. Barracuda is also visible in a few enterprise markets, including the WAF market. The vendor delivers its Web Application Firewall line in physical or virtual appliances. It is also available on the Microsoft Azure, AWS and VMware vCloud Air platforms.

Recent news includes the announcement of the expansion of the Barracuda Cloud Ready program, wherein it offers free 90-day licenses for its WAF and network firewalls to use in AWS or Azure migrations. It also announced a free add-on, Barracuda Vulnerability Remediation Service, which provides automated dynamic application security testing (DAST) services and automated mitigation against discovered vulnerabilities.

Barracuda is a good shortlist contender for small and midsize businesses (SMBs) and other value-conscious organizations, in addition to organizations moving applications to public cloud IaaS environments.

Strengths

- **Sales execution:** Barracuda is highly visible among Gartner SMB clients. Barracuda WAF is frequently on enterprise EMEA client shortlists. The vendor WAF appliance revenue grows faster than many competing WAF appliance offerings.
- **Customer experience:** Barracuda customers and partners cite value, ease of use and ease of updates as important differentiators.
- **Offering strategy:** During the evaluation period, Barracuda focused more of its product strategy on developing deeper capabilities and greater presence in the public cloud. The Barracuda Cloud Ready program offers Barracuda's targeted SMB prospects the opportunity to try the WAF product in AWS and Azure for free during the 90-day license. Such efforts, paired with development efforts making its products integrate well with public cloud infrastructures, have given Barracuda significant presence in public cloud. Barracuda customers and partners particularly cite the Azure offering for its high quality.

- **Technical support:** Gartner clients consistently give good marks to Barracuda's post-sale customer support. Barracuda partners cite the vendor's focus on customer satisfaction as a reason they choose to sell Barracuda WAF.
- **Capabilities:** Barracuda's offer of the free WAF add-on Vulnerability Remediation Service is very attractive to Barracuda's targeted SMB customers, who often have neither the time, money nor expertise to support an in-house application scanning program.

Cautions

- **Cloud-based WAF service:** Barracuda offers integration on IaaS platforms, but lacks a cloud-based WAF service, which is a deployment and licensing option that many of its direct competitors offer.
- **Management:** Gartner clients give mixed feedback on Barracuda management interface's ease of use for daily tuning of WAF configuration. Some of the feedback is that the UI is nonintuitive and disorganized. Some customers note that exporting configuration settings across multiple appliances can be very time-consuming and manual. Barracuda WAF lags behind its direct competitors in ease of integration and automation with tools typically seen in DevOps environments.
- **Customer experience:** Barracuda customers note that logs can sometimes load slowly, and that the lack of alert aggregation slows down incident response handling. They also mention that product documentation accuracy could stand improvement.
- **Capabilities:** Automatic policy learning lags behind the vendor's direct competitors and receives poor feedback from Gartner clients. According to customer feedback, lower-end Barracuda WAFs don't support use of automatic learning.
- **Capabilities:** The vendor does not currently offer nor integrate with cloud-based services to provide protection against volumetric DDoS. Its bot mitigation lags behind its leading competitors for the more advanced behavior detection capabilities.
- **Product Strategy:** Barracuda WAF throughput on its top models does not exceed 5 Gbps, making it unsuitable for many enterprise use cases. Gartner rarely sees Barracuda WAF appliances on shortlists for large, complex deployment scenarios.

Citrix

Citrix is a Challenger. It has a long history in the WAF space, mainly focused on delivering web application security as an add-on to its NetScaler deployment. Gartner rarely sees the vendor compete where application security is the highest-weighted requirement.

Citrix (CTXS), co-headquartered in Santa Clara, California, and Fort Lauderdale, Florida, is a global provider with a broad portfolio of virtualization, cloud infrastructure and ADC solutions, with more than 9,000 employees. Citrix has offered WAF functionality (NetScaler AppFirewall) for more than a decade, either as a stand-alone software option or included in the Platinum edition of the NetScaler ADC suite. The Citrix hardware appliance product line (NetScaler MPX) can run a license-restricted

version of the full NetScaler software to act as a stand-alone WAF. In addition, Citrix provides a line of virtual appliances (NetScaler VPX). NetScaler can be bundled in Citrix Mobile Workspace offerings.

In 2016, Citrix released new licenses from NetScaler virtual appliances. In 2017, Citrix has started offering NetScaler Web App Security Services, its cloud-based WAF service, based on AppFirewall and released features and improvements, such as adding ECDHE cipher support for TLS decryption, overall risk score dashboard (Threat Index) and authentication features.

NetScaler AppFirewall is a good choice for existing Citrix clients, or when high-performance WAF appliances are needed.

Strengths

- **Marketing strategy:** For Citrix clients, AppFirewall is a logical option to leverage all investment in the ADC. Due to its ADC, Citrix appears among the top-five vendors on client shortlists for WAF evaluations.
- **Customer experience:** Clients highlight support availability and NetScaler performance as reasons to select AppFirewall. They give good scores to the vendor's threat research team for its ability to release new signatures that can be automatically deployed.
- **Capabilities:** NetScaler AppFirewall applies its strategy for DevOps environments by providing a set of APIs (branded as Nitro API). Nitro exposes its functionality through REST interfaces and other software development kits (SDKs).
- **Capabilities:** NetScaler's ability to scale appeals to large organizations. NetScaler SDX includes multitenant support that consolidates a high number of NetScaler instances on a single hardware appliance. NetScaler integrates with Thales and SafeNet hardware security modules (HSMs), and is recognized for its ability to decrypt SSL at scale.
- **Market responsiveness:** In recent months, Citrix has made progress in releasing improvements to AppWall, partially catching up with its direct competitors on more recent WAF feature requests.

Cautions

- **Product strategy:** Citrix strategy is focused on serving markets other than security. As such, roadmap execution is prioritized to avoid big feature gaps, but typically lags behind the competition when it comes to innovations.
- **Sales execution:** Citrix rarely displace a WAF competitor based on AppFirewall capabilities. The vendor mostly sells AppFirewall as an add-on to customers primarily interested in its ADC features or in high-performance environments.
- **Customer experience:** Some clients indicate that NetScaler AppFirewall has limitations in the areas of automatic policy learning, reporting dashboard and the ability to avoid false alerts (false positive rate). Customers also require additional capabilities, such as support for the ICAP protocol.

- **Customer experience:** Clients cite that documentation needs improvements. Management interface is available in English only. Clients would like a more intuitive way to deploy AppExpert Templates for known applications.
- **Capabilities:** Citrix does not offer a native cloud-based DDoS protection service, although NetScaler appliance has integration with third-party DDoS protection services. The vendor offers basic bot mitigation capabilities.
- **Cloud-based WAF service:** The vendor has just released its cloud-based WAF service, which lacks direct integration with CDN, and no client feedback is available yet.

Cloudflare

Cloudflare is a Challenger. As more web applications move to the cloud, the value proposition of its bundled approach and the regular improvements of its solution appeal to more clients.

Based in San Francisco, California, Cloudflare is well known for its CDN and DDoS protection services. Other services include managed DNS services and WAF. Cloudflare is best known for its free plan and inexpensive self-service Pro and Business plans. Most of its enterprise sales are through the custom Enterprise plan, which starts at $5,000 per month.

The vendor has recently announced a new subscription for load balancing and failover, another subscription (Argo) for performance optimization through improved routing decision between its servers, Internet of Things (IoT) security (Orbit) to secure connections between IoT devices and their origin server, always-on IPv6, a partnership with OpenDNS to improve IPv6 DNS lookup efficiency, and beta version support of TLS 1.3 with performance optimization for resumed connections (0-RTT).

Cloudflare is a good shortlist candidate to protect cloud-native applications, especially for budget-constrained organizations that need bundled WAF and DDoS capabilities for their public-facing web applications, or for organizations willing to secure applications requiring demanding performance.

Strengths

- **Customer experience:** Ease of use, high performance and good value for a lower price than competitors are the most frequent comments Gartner analysts receive from Cloudflare's customers. Clients describe Cloudflare as a reputable organization. They like the transparency of the vendor in case of incidents, and note that these are often quickly solved.
- **Capabilities:** Cloudflare WAF, CDN and DDoS protection is bundled in a way that is easy for customers to deploy and consume. Its WAF can be fully managed using Cloudflare's API. The vendor's ability to mitigate large-scale DDoS, and its custom set of rules for known frameworks and web applications such as CMS, help provide tailored protection for web applications built on third-party modules.
- **Geographic strategy:** Cloudflare has one of the largest-scale back-end infrastructures supporting cloud-based WAF service, with 116 data centers. It has very good presence in North

and South America, Europe, and East Asia, where it is common to see multiple data centers serving the same country.

- **Market responsiveness:** Cloudflare frequently releases new features and improvements that are immediately available at scale. The vendor focuses on new ways to improve overall performance; the most recent examples include the paid option Argo and the partnership with OpenDNS. Surveyed clients and resellers liked the recent addition of the capability to rate limit requests in order to protect against targeted DoS attacks by defining rules for the more sensitive requests, such as failed login attempts.
- **Product strategy:** Cloudflare is instrumental in moving the web toward HTTPS-only and IPv6, with always-on-IPv6 at the edge. The vendor provides an easy option to enable HTTPS and HTTP Strict Transport Security (HSTS) at the edge. Because it is a Certificate Authority, the vendor can help its client deploy a TLS certificate for its origin servers (Origin CA).

Cautions

- **Market segmentation:** Cloudflare is rarely visible in Gartner's clients' enterprise WAF purchase projects led by security teams, if security is weighted the highest. Most of its WAF sales come from clients primarily interested in bundling CDN and DDoS protection, and not in the WAF features only.
- **Marketing strategy:** Gartner believes that Cloudflare plans include a future IPO. Organizations about to become public can be distracted from their previous strategy in order to create a better story for future investors. This can disrupt an organization's plan, influencing roadmap decisions, pricing conditions, recruitments and other areas.
- **Product strategy:** Cloudflare's security roadmap is focused on infrastructure and network security. Its web application security efforts are more targeted at quick reaction in case of a new attack campaign, but the vendor is less proactive than its leading competitors when it comes to using new protection techniques based on in-house threat research.
- **Capabilities:** The Cloudflare WAF lacks an automated positive security model. The vendor does not allow its clients to create custom rules (although clients can submit custom rule requests to the vendor). Its reporting and real-time monitoring solutions could be improved with more customization for reports, and with automated processing of real-time alerts to ease security incident triage and drill-down.
- **Customer experience:** Customers outside North America, especially when in time zones with little North American overlap, rate support experience lower than North American customers do.
- **Capabilities:** Several Gartner clients have reported that Cloudflare's bot mitigation feature did not meet their expectations for efficacy and user experience. As a result, they investigated complementary or replacement solutions for Cloudflare.

Ergon Informatik

Ergon Informatik is a Niche Player. Its market presence is still limited to Europe. Its internationalization efforts do not yet provide the vendor with sufficient visibility. Its WAF appliance benefits from continual improvements, but Ergon still lacks a cloud-based WAF service offering.

Based in Zurich, Switzerland, Ergon Informatik currently employs 270 people, with a quarter of them focused on its Airlock Suite, which includes the Airlock WAF and an IAM solution.

Recent news includes a configuration staging feature, support for HTTP/2, automatic policy learning and integration with IBM Trusteer for fraud prevention.

Ergon Informatik is a viable shortlist candidate for enterprises in need of a WAF appliance, especially European organizations from the financial sector, or those looking for strong integration between WAF and access management.

Strengths

- **Marketing execution:** Ergon Informatik has built a small but faithful channel. New channel partners from countries where Ergon has little presence mention their satisfaction with how they can quickly gain knowledge on the solution, and get adequate help when needed.
- **Vertical strategy:** Ergon has a strong presence in the financial sector, where it frequently wins based on positive peer referrals, especially for Ergon's ability to understand the industry's specialized needs.
- **Capabilities:** Ergon Informatik offers tight integration of its Airlock WAF with its IAM modules, offering flexible integration to provide access control and SSO. It includes a variety of specialized controls, such as URL and cookie encryption, which are actually used by customers.
- **Product offering:** Airlock WAF includes a strong set of access management features and content inspection for the API traffic. The vendor's approach to security for JSON and REST APIs is worth evaluating.
- **Customer experience:** Customers describe Ergon as a trusted brand and a company that is easy to work with. Several clients gave good scores for client support.

Cautions

- **Cloud-based WAF service:** Ergon Informatik does not offer a cloud-based WAF service. Its presence on IaaS is limited to an Amazon Machine Image (AMI) file that can be deployed on AWS, but without any further integration.
- **Geographic strategy:** Ergon is expanding outside of Western Europe, but its local presence is mostly limited to the Germany, Austria and Switzerland (DACH) region. Prospective customers outside of these countries are likely to rely entirely on the channel partner, and therefore should carefully evaluate channel partner skills and experience with the Airlock Suite.

- **Market responsiveness:** Ergon Informatik can be slower than its competitors to release new features, as its roadmap delivery contains a higher mix of continuous improvements of existing features.
- **Capabilities:** Airlock lacks threat intelligence feeds, does not yet offer geo-IP filtering, and does not offer ad hoc and automatically deployed attack signatures to complement its generic rule set. Its bot mitigation feature mostly depends on the integration with IBM Trusteer. Its newly released automatic policy learning has not yet received positive customer feedback. Airlock lacks integration with DDoS protection cloud services for protection against volumetric DDoS attacks.
- **Capabilities:** Role-based access control for the management console and centralized management of Airlock WAF lag behind leading vendors evaluated in this research. Gartner clients have expressed interest in seeing improvements in this area.
- **Customer experience:** Customers would like to see better automation, especially for initial WAF deployment. They report an average time to deploy that is a bit longer than its direct competitors, and would like to see Ergon better leverage the user community.

F5

F5 moved from the Challengers to the Leaders quadrant. It remains one of the most frequently cited vendors in WAF appliance shortlists, and has made progress in cloud-based WAF service. Its renewed efforts in enhancing behavior-based anomaly detections appeals to security-conscious organizations.

F5 Networks (FFIV) is an application infrastructure vendor based in Seattle, Washington, with more than 4,400 employees. F5's WAF offering is a software module called Application Security Manager (ASM) for the F5 Big-IP ADC platform, often sold as a component of F5's bundle of services. The F5 hardware Big-IP appliance product line can also run a license-restricted (yet upgradable) version of the full software to act as a stand-alone security solution (such as a stand-alone WAF). Other F5 security modules include the Access Policy Manager (APM) module for integration with and/or enforcement of identity and access management (IAM), and WebSafe web fraud protection services. F5 also offers managed cloud-based WAF service and a DDoS scrubbing service (F5 Silverline).

Recent news includes the release of Silverline WAF Express, F5's lower-price-tier offering without managed services, and integration between its WAF and DDoS protection cloud services. Big-IP ASM v13 adds improved bot mitigation dashboards, hierarchical policy, better client fingerprinting, and automatic server application framework and language detection.

The vendor is a good shortlist candidate for WAF, especially for large organizations looking for scalable and flexible WAF appliances.

Strengths

- **Marketing strategy:** F5 is among the top-three most visible vendors from client shortlists for WAF. Silverline is starting to be mentioned by clients as a candidate for cloud-based WAF service.
- **Technical architecture:** The large and scalable Big-IP platform portfolio allows F5's customers to bundle WAF with strong access management or load-balancing features, and to build a clean architecture with single-pass decryption. These security appliances offer customization, SSL decryption mirroring to other security solutions, unified learning and policy building. Also, the ability to get central visibility and some configuration of policies within BigIQ central management for WAF helps for large-scale projects.
- **Customer experience:** Reference customers scored F5 very highly for performance and for the quality of the security modules, including protections against injection attacks, DDoS and API security.
- **Product strategy:** F5 already integrates into standard DevOps platforms, with supports for tools such as Chef, Ansible and Kubernetes. It provide an API for WAF configuration management that is feature-complete, and integrates with AWS and Microsoft Azure platforms.
- **Capabilities:** Clients highlight the flexibility of iRules scripting and the possibility it offers for accessing information or changing behavior for ASM. Big-IP ASM provides integration with FireEye malware inspection products via Internet Content Adaptation Protocol (ICAP), Layer 2 (L2), Layer 3 (L3) or through Switched Port Analyzer (SPAN) traffic, which can be useful for file-sharing applications. ASM offers decryption and extraction of files to send over ICAP connections.

Cautions

- **Sales execution:** Gartner estimates that F5's WAF market share has slightly declined, as a result of Silverline growing from a small base, and the WAF appliance-based revenue stabilizing. The vendor's visibility in WAF inquiry is stable, while the visibility of its direct competitors continues to grow. The company's ADC business, its core market, is also suffering.
- **Operations:** F5 has experienced a series of executive changes. Prospective clients should monitor the vendor's communications to anticipate strategic shifts that could impact its web application security solutions.
- **Customer experience:** New clients often report that they get confused with the management interface. They like the flexibility, but the learning curve is quite extensive in order to leverage all capabilities. Customers cite that centralized management console BigIQ needs improvement. Customers complain that BigIQ is not feature-complete, and therefore they need to configure each cluster separately, because BigIQ only allows specification of basic settings across clusters.

- **Sales strategy:** Prospective clients who are not already using F5 and are in search of a WAF only cite cost as a challenge. These comments also apply to WAF Express, which starts as a $29,990 yearly subscription.
- **Capabilities:** Although F5 has built-in integration with Google, Facebook and Ping Identity for open authorization through the on-premises platform, the cloud-based solution does not have the same capability.
- **Customer experience:** Existing customers reported a need to improve the dashboard, reporting and user behavior analysis features. Also, alignment of reporting with Silverline cloud-based and on-premises solutions needs improvement.

Fortinet

Fortinet is a Challenger. Its solid investment in its WAF solution translates into continuous improvements. The vendor experiences better-than-WAF-market-average growth and has become more visible in enterprise shortlists.

Fortinet (FTNT) focuses on network security and network infrastructure. The vendor is headquartered in Sunnyvale, California, and has more than 4,600 employees, including approximately 1,000 R&D employees. The Fortinet portfolio includes a firewall (FortiGate), WAF (FortiWeb), an endpoint protection platform (FortiClient), ADC (FortiADC), SIEM (FortiSIEM), and a sandbox (FortiSandbox). The vendor remains most well-known for its FortiGate firewall, but FortiWeb has become its third-largest non-firewall-related product line, even if WAF R&D remains a relatively small portion of the total R&D team. FortiWeb is available as a physical or virtual (FortiWeb-VM) appliance, and on AWS and Azure IaaS platforms. FortiWeb subscriptions include IP reputation, antivirus, security signature updates, credential stuffing defense and cloud-based sandboxing (FortiSandbox).

In 2016, Fortinet acquired AccelOps; FortiSIEM emerged from this acquisition as part of Fortinet Security Fabric, the vendor's concept of integrating multiple security solutions. Other recent news from Fortinet includes new WAF hardware, an updated management interface, active-active clustering, HTTP/2 support and improved SQL injection detection.

Fortinet's existing customers, as well as organizations looking for a WAF appliance with good value and performance for the price, should include Fortinet's WAF in their competitive assessments.

FortiWeb's management interface is available in English, Chinese and Japanese.

Strengths

- **Sales execution:** Clients cite Fortinet's brand reputation, competitive prices and integration with other products from Fortinet as reasons to purchase FortiWeb.
- **Technical architecture:** Fortinet focuses on developing protection and integration with other elements of the Fortinet Security Fabric. A FortiGate Firewall can forward traffic to the FortiWeb WAF, and FortiWeb can use FortiSandbox for improved malware analysis. A first version of a unified dashboard is available through FortiSIEM or FortiAnalyzer.

- **Capabilities:** Fortinet offers an automated and regularly updated attack signature feed, driven by a large threat research team. With the introduction of syntax-based detection for SQL injection detection, FortiWeb can improve the WAF's detection efficiency and reduce false positives related to this attack vector.
- **Capabilities:** Fortinet uses device fingerprinting to identify traffic sources and to update a reputation or risk score based on the device behavior.
- **Capabilities:** A credential-stuffing detection service is a new subscription for FortiWeb that checks user logins against the stolen credential database. It can help detect credential stuffing on enterprise applications, or warn that legitimate users had their credentials stolen.

Cautions

- **Cloud-based WAF service:** Fortinet does not offer a cloud-based WAF service. Its WAF is available for deployment as a virtual appliance on AWS and Azure IaaS platforms.
- **Marketing strategy:** Fortinet has one of the largest channels in the security industry. However, only a small subset of this channel is fully trained on FortiWeb solutions, a product line that is quickly evolving. Customers indicate FortiWeb is limited in its ease of deployment and the availability of quality third-party resources (integrators or service providers) with sufficient skill to deploy and operate FortiWeb.
- **Market segmentation:** FortiWeb is not as visible in shortlists where security is weighted the highest, compared to leading vendors. The vendor lags behind Leaders in its ability to integrate with DevOps environments and is less frequently visible in this segment.
- **Capabilities:** FortiWeb appliance lacks integration with DDoS protection cloud services and fraud detection solutions.
- **Capabilities:** FortiWeb application policy learning (autolearning) lags behind the leading solutions evaluated in this market.
- **Customer experience:** Clients indicate that FortiWeb should improve its user interface. Clients would like to see features such as better version control and a rollback mechanism. Existing FortiGate clients report frustration with the FortiWeb management console not being as mature as what they get with the FortiGate management console.

Imperva

Imperva is in the Leaders quadrant. The vendor competes and frequently wins on the basis of security features and innovation. Imperva can provide strong WAF functionality as a traditional appliance and cloud-based WAF service, but faces stronger competition for its cloud offering.

Based in Redwood Shores, California, Imperva (IMPV) is an application, database and file security vendor. SecureSphere is Imperva's WAF appliance, and Incapsula is its cloud-based WAF, which is delivered as a service. Imperva also has packages for security monitoring and offers managing service of the SecureSphere and Incapsula WAFs.

Both SecureSphere and Incapsula are deployed mostly in blocking mode. The SecureSphere WAF is available in seven physical and three virtual appliances, with two models each available for AWS and Microsoft Azure. Two models of physical and virtual appliances are also available for dedicated management. ThreatRadar is the family of add-on subscription services available for SecureSphere, available in five offerings: account takeover protection, reputation feed, bot protection, fraud prevention and community defense. Imperva Incapsula can be bundled with other services, including DDoS mitigation and CDN features.

Recent news includes the release of FlexProtect, which allows customers to deploy both SecureSphere and Incapsula with a single subscription, potentially providing more flexibility as customers move workloads to the public cloud. In addition, Imperva has announced enhancements to the Incapsula CDN and has made Incapsula available in the Azure marketplace. SecureSphere has added ThreatRadar Emergency Feed, which provides immediate access to zero-day discoveries, and has new support for HTTP/2 traffic.

Imperva is a good shortlist candidate for many organizations. High-security use cases in larger organizations are addressed with SecureSphere, and organizations that want a cloud-delivered solution to protect public facing web applications should consider Incapsula.

Strengths

- **Product strategy:** The introduction of FlexProtect is lauded by many Imperva customers, who previously pointed to disjointed management and lack of feature parity of SecureSphere and Incapsula as a weakness. This new unified licensing and security view provides Imperva customers with easy deployment options as their application environments shift.
- **Sales and marketing strategy:** With Incapsula, Imperva WAF has found an effective route to serve smaller organizations that previously would not consider the high cost and overhead that come with some SecureSphere deployments. Imperva has done an effective job focusing Incapsula messaging — DDoS-focused to some audiences, WAF-focused to others.
- **Sales execution:** Gartner sees Imperva consistently scoring very high and/or winning competitive assessments done by Gartner clients, with a high success rate when security is the most-weighted criteria.
- **Customer experience:** Gartner clients are highly satisfied with Imperva customer support, citing high-quality, easy ticket resolution.
- **Capabilities:** SecureSphere ThreatRadar feeds go beyond reputation only, and protect against multiple attack profiles. ThreatRadar community sharing, augmented by Imperva's threat research team, can quickly mitigate new attack campaigns.
- **Geographic strategy:** Imperva has strong WAF presence in most geographies, and offers effective support across most regions. Recent presence has been especially strong in the Asia/Pacific region.

Cautions

- **Cloud-based WAF service:** Customers mention that Incapsula bot mitigation could be better in detecting slow and low advanced bots.
- **Cloud-based WAF service:** Some customers that have commissioned advanced security evaluations of both Incapsula and SecureSphere gave higher scores to SecureSphere's ability to protect against advanced injection attacks and to detect evasion attempts.
- **Product strategy:** The Imperva strategy shift to become a cloud security vendor is still a work in progress. The SecureSphere appliances are a secondary component of this cloud security vendor strategy, and Gartner estimates that SecureSphere physical appliance revenue declined in 2016. Prospective customers should ensure that Imperva's investment in SecureSphere's roadmap remains consistent with enterprise expectations of continuous improvement.
- **Pricing:** Gartner clients consistently remark on the relatively high prices of Imperva WAF products and services. This pricing strategy hurts Imperva in competitive situations, especially those in which security is not the highest-weighted evaluation criterion, or in the cloud, even if Incapsula offers more competitive pricing.
- **Customer experience:** SecureSphere customers report that high-availability (HA) configuration is difficult, and that effective baselining of traffic in order to move into blocking mode is a lengthy process.
- **Customer experience:** Incapsula customers indicate that Incapsula lacks high-level executive reports, and that overall, the reporting could be much improved to reach an enterprise-class level.

Instart Logic

Instart Logic is in the Visionaries quadrant. The vendor has quickly gained visibility in WAF shortlists to protect cloud-native web applications due its technology approach and regular release of new features.

Launched in 2010, Instart Logic is based in Palo Alto, California, and employs more than 200 employees. Its portfolio is composed of multiple subscriptions on top of its core CDN infrastructure, including a cloud-based WAF service and DDoS protection, released in 2014. The vendor's core marketing message for its WAF is about being "endpoint-aware," facilitated through a lightweight JavaScript agent (Nanovisor), which gets injected into HTTP traffic and analyzes some aspects of client-side web browser behavior. The vendor also provides performance optimization by dynamically optimizing web object and image delivery. Instart Logic offers rule tunings and 24/7 SOC as an option.

Recent news includes the release of managed services, a new business model for the CDN, better integration with AWS, and two new subscriptions, Bot Defense for bot mitigation and a semi-automated security rule service (Helios) that uses machine learning to generate suggested policies based on log analysis. Instart Logic continues to grow its data center infrastructure that, at the time

of this writing, is composed of 36 points of presence, including 12 in North America, nine in Europe and seven in Asia.

Instart Logic is a good shortlist candidate for organizations that need to quickly protect cloud-native web applications with demanding performance requirements.

Strengths

- **Product strategy:** Instart Logic is part of a new wave of web app security vendors developing an easy-to-deploy, cloud-native solution. Instart Logic's main product development focus is on improving web application performance while implementing strong security by leveraging new techniques, such as machine learning. This appeals to application and infrastructure leaders, who frequently become sponsors of the WAF purchase.
- **Marketing and sales execution:** Because of a competitive price, enterprises frequently first select Instart Logic for Tier 2 applications or newly released, small-scale, cloud-native applications, or complementing a legacy WAF or a more expensive cloud-based WAF service.
- **Vertical strategy:** Instart Logic is very visible in shortlists for small and large e-commerce companies, where its performance optimization, anti-advertisement blocking, and easy-to-deploy security score well.
- **Customer experience:** New customers are satisfied with the ease of deployment. They cite very short time to deploy and good vendor support when onboarding.
- **Capabilities:** Instart Logic management is API-first. Customers can access the dashboard and modify policy using the fully featured management API.

Cautions

- **Product:** Because of Instart Logic's initial positioning on performance optimization, prospective customers rarely conduct in-depth evaluation of the security modules. The vendor also lacks independent testing to demonstrate the efficacy of its detection techniques. Instart Logic does not offer online enrollment, which is available in many of its cloud-based WAF service competitors.
- **Geographic strategy:** The vendor is not yet visible in Asia and Europe. Its channel and presale forces are still developing. Prospective customers, especially outside of North America, should first verify the availability of local skills, and assess their need for support in their native language.
- **Capabilities:** Instart Logic relies heavily on JavaScript code injection to identify bots or to block attacks. This technique does not work well with old browsers and does not apply to mobile applications. Its bot mitigation configurability and traffic visibility are limited. Its WAF lacks integration with AST and SIEM technologies. It does not offer authentication features.
- **Customer experience:** Some clients have reported frustration with the rate-limiting features, and the lack of flexibility in the role-based access control to the management console.

- **Organization:** Instart Logic is a fast-growing company, but its WAF and threat research teams remain comparatively smaller than many of the other vendors evaluated in this research.

NSFOCUS

NSFOCUS is in the Niche Players quadrant. The vendor is a global player, but its WAF sales predominantly come from Chinese clients. Its WAF covers all the basic functionalities, but lacks sophistication for the most advanced use cases.

Based in Beijing, China, and Santa Clara, California, NSFOCUS is a network security vendor with more than 2,000 employees. Its offers IPS and DDoS protection solutions, in addition to WAF (WAF Series).

NSFOCUS has recently added IP reputation, three WAF virtual appliances, new physical appliances with SSL acceleration hardware and a REST API to manage its WAF.

NSFOCUS' WAF is a good contender for organizations in China and East Asia, and for the vendor's current customers in other countries where the vendor has local presence.

Strengths

- **Capabilities:** NSFOCUS' WAF has been successfully deployed in large scale environments, where its clustering capabilities were heavily used.
- **Marketing execution:** NSFOCUS has released a managed service offering for its clients, available in China to start. The vendor continues to grow its staff outside of China to support its internationalization effort.
- **Capabilities:** NSFOCUS has a large threat research team, working for all of its solutions. The vendor leverages this team to issue new protections in case of new attack.
- **Customer experience:** NSFOCUS customers mention the low false positive rate and the ability to perform well when under attack as strong features of the WAF appliances.
- **Technical architecture:** Existing NSFOCUS clients can leverage integration between the WAF and the NSFOCUS DDoS protection and its web application vulnerability scanner.

Cautions

- **Cloud-based WAF service:** NSFOCUS does not offer a cloud-based WAF service. It has only recently released virtual appliances, availability on AliCloud IaaS platform, and announced integration with AWS and Microsoft Azure.
- **Geographic strategies:** NSFOCUS WAF has little visibility in shortlist outside of China. Its channel in other countries is less frequently trained on the WAF product. Prospective clients for the WAF outside of China should expect scarce local technical resources.

- **Customer experience:** For a few years, NSFOCUS customers have consistently requested improvements in the reporting, real-time monitoring and logging modules. They mention a high number of alerts and lack of automated analysis of the generated events.
- **Capabilities:** NSFOCUS lacks authentication features. Its appliances cannot integrate with a HSM to securely store decryption secrets. Its WAF does not use an automated feed to automatically get new protections.
- **Capabilities:** NSFOCUS lags behind competition in centralized management. It provides only a few predefined administrative roles to manage the WAF.

Penta Security Systems

Penta Security Systems is in the Niche Players quadrant. The vendor has a faithful base of customers, and its international expansion in Asian countries is promising.

Penta Security Systems is based in Seoul, Republic of Korea, and has 220 employees. Its product portfolio includes WAFs (Wapples appliances and Cloudbric cloud-based WAF service), a database encryption platform (D'Amo) and authentication/SSO (ISign+). Penta Security emphasizes Wapples' "logic detection" technology, which does not require regular signature updates.

Recent corporate and WAF news from Penta Security includes Wapples version 5.0, with a change in operating system; support for TLS 1.2 and new centralized management solution.

Penta Security Systems is a good choice for organizations looking for an easy-to-operate WAF, and especially for organizations in East Asia.

Strengths

- **Geographic strategy:** Penta Security has expanded beyond its home market, and has good presence in several countries in the Asia/Pacific region.
- **Sales execution:** Cloudbric, Penta Security's cloud-based WAF service, is free for up to 4GB of data per month. Several inexpensive paid plans are also available.
- **Cloud-based WAF service:** Cloudbric infrastructure includes data centers in nine different countries across Asia, Europe and North America.
- **Customer experience:** Penta Security's clients give high scores to Wapples' ease of use and performance. They cite the low rate of false positives as the main reason why operational workloads for the WAF is lower than what they experienced with competing products.
- **Improvements:** Wapples offers a REST API to automate management and better integrate with third-party tools. It can send logs in Common Event Format (CEF) to integrate with SIEM solutions.

Cautions

- **Market segmentation:** Gartner estimates that more than 60% of Penta Security clients are midsize organizations. It is less visible than Leaders in this market, and is not frequently part of shortlists for DevOps use cases.
- **Market responsiveness:** Gartner has observed that the pace of release for Wapples has slowed down compared to previous years, and that version 5.0 includes more refactoring of existing modules than new features.
- **Customer experience:** Clients mentioned they would like to see improvements in the real-time event view, and expressed frustration with the delay in the release of the new web-based UI to replace the existing solution.
- **Customer experience:** Several clients have mentioned that they would like to see improvements in DDoS protection, specifically when using Wapples appliances.
- **Capabilities:** Wapples is not yet available on Microsoft Azure, and lacks integration with the AWS platform. Wapples appliances cannot embed an HSM module to securely store server secrets, and remote HSM is not supported in Cloudbric.
- **Capabilities:** Wapples lacks authentication and API security features. It does not include automatically deployed attack signatures to complement its generic engine. Its bot mitigation lags behind competition.

Positive Technologies

Positive Technologies is in the Visionaries quadrant. The vendor's investments in sales and marketing have not yet translated into global visibility. Its WAF appliance continues to attract new customers based on its strong anomaly detection capabilities.

Positive Technologies is co-headquartered in Moscow, London and Boston, and has more than 700 employees. The vendor's main product lines are MaxPatrol, a vulnerability management solution, and PT Application Inspector, which combines static, dynamic and interactive code analysis techniques. Positive Technologies' WAF (PT Application Firewall, or PT AF) product was initiated in 2013. It is currently available as a dedicated appliance, as a software version that can run on a third-party appliance and as a virtual machine that is predominantly installed on-premises.

In 2016, Positive Technologies introduced a few new appliance models for SMBs. Recent feature releases include user tracking, integration with Check Point Software Technologies' firewall and a new transparent proxy deployment option.

Organizations that are looking for high-security WAF appliances should consider adding Positive Technologies to their shortlists.

Strengths

- **Product strategy:** Positive Technologies has been an early adopter of machine learning on a WAF technology, not only for initial application learning, but also for anomaly detection. The vendor uses a cloud infrastructure to share threat intelligence gathered from its anomaly detection modules.
- **Improvements:** The vendor has extended the scope of its supervised machine learning, from positive security model only (whitelisting), using hidden Markov models, to also improving its negative security model (blacklisting), by using neural networks.
- **Customer experience:** Customers rate PT Application Firewall well on technical capabilities. Customer satisfaction is high with SQL injection protection and cross-site scripting (XSS) protection.
- **Customer experience:** Advanced users like the flexibility of the rule editor and the ability to drill down from the top view to detailed security events.
- **Capabilities:** PT Application Firewall integrates with other solutions from Positive Technologies including its vulnerability scanner and source code analyzer to automatically create virtual patches based on the vulnerability assessment.

Cautions

- **Cloud-based WAF service:** PT Application Firewall is only available on-premises or on Microsoft Azure. It does not provide a cloud-based WAF service option, nor integration with the AWS platform.
- **Geographic strategy:** Positive Technologies currently mostly sells in the EMEA market. Its channel is growing quickly, which means that many resellers are still new to PT Application Firewall. Prospective clients should evaluate the availability and quality of local skills.
- **Product:** PT Application Firewall lacks any third-party certification, such as Common Criteria and ICSA Labs, or independent testing to demonstrate the efficacy of its detection techniques.
- **Customer experience:** Recent customers cite a significant learning curve required to fully leverage the management console. They also cite upgrade procedures as areas for improvement.
- **Customer experience:** Clients cite that reporting and dashboards are too complex, and built only for seasoned security analysts. They mention that documentation needs improvement, and that it is difficult to find a service provider to outsource web application security monitoring.
- **Capabilities:** PT Application Firewall does not support HSM. It lacks support or integration with DDoS cloud-based protection services and lags behind many of its competitors in authentication features.

Radware

Radware moved from the Niche Players to the Visionaries quadrant. The vendor has strong market understanding, and its pace of innovation is accelerating. It is increasingly relevant for security managers who add cloud-based WAF service solutions and look for solutions to manage hybrid delivery models. However, Radware does not appear in enterprise shortlists as frequently as some competitors.

Radware (RDWR) is an application delivery and security vendor co-headquartered in Tel Aviv, Israel and Mahwah, New Jersey. Its main product is its ADC, called Alteon. Its security solutions include a DDoS mitigation appliance (DefensePro), a DDoS protection virtual appliance (DefenseFlow), a cloud-based DDoS mitigation service (Cloud DDoS Protection) and a WAF (AppWall), which can be purchased individually or bundled together in Radware's Attack Mitigation Service (AMS) offering. AppWall may be deployed as a physical or virtual appliance, as a module on top of Radware's ADC appliance (Alteon). AppWall is also available as a vendor-managed cloud-based WAF service (called Cloud WAF Service), based on the same technology than the AppWall appliance.

Recent announcements include the acquisition of Seculert, which adds machine learning, big data analytics and sandboxing capabilities to the Radware portfolio, and also enhances Radware's malware detection capabilities. Radware also announced a partnership to provide security services, including Radware Cloud WAF Service, to Chinese Tencent cloud customers. One of the significant features released during the evaluation period is DefenseMessaging, which enables Radware WAF customers with Radware's DDoS products to use AppWall to signal an attacker's source IP information to DefensePro DDoS to prevent further malicious activity.

Radware is a good shortlist candidate for most organizations, especially those that desire strong positive security and wish to deploy the same security levels across hybrid environments. Prospective customers should still verify the efficacy of the solutions for their environments, using third-party or in-house skilled security staff.

Strengths

- **Capabilities:** Radware has strong in-house threat research, driven by a large team with 24/7 coverage. The vendor also has an internal SOC team to support its offering.
- **Innovation:** Radware's deep integration with Hewlett Packard Enterprise's (HPE's) WebInspect product enables its WAF to be more relevant in DevOps environments. Using the continuous security delivery service, the WAF automatically invokes scans of altered parts of an app when the applications are modified, and automatically generates updated policy for those changed areas, and virtual patches when vulnerabilities are uncovered.
- **Customer experience:** Radware customers frequently cite security, ease of deployment for the automated positive security model (with negative security approaches also available) and a good appliance price as primary reasons for selecting the vendor.
- **Geographic strategy:** Radware's customers are divided roughly evenly in EMEA, North America and Asia/Pacific, and Radware provides pre- and postsale resources across regions.

- **Sales strategy:** Radware has focused on building a value-based pricing strategy that lowers total cost of ownership (TCO) for Radware customers, especially those who use Radware Cloud WAF Service, which is consumption-based and offers up to 1 GB of cloud-delivered DDoS for free. Extra capacity is available for purchase as it becomes necessary.

Cautions

- **Customer experience:** Some customers and partners are not satisfied with AppWall's Java-based graphical user interface (GUI). AppWall's native management interface is available in English only. Users note that Radware does not integrate with third-party reputation feeds.
- **Marketing execution:** The pace of innovation in Radware WAF solutions should make them appealing to U.S. customers. While Radware is well-known in some regions, especially EMEA, its security brand in North America is less well-known.
- **Product strategy:** IaaS platform support and some features are only available on the WAF module of the Alteon ADC platform, but not on dedicated AppWall appliances, IPv6 and HTTP 2.0 support.
- **Sales execution:** Radware has lost market share in 2016. Its newly released Cloud WAF Service is not yet visible in competitive shortlists for cloud-based WAF service.
- **Customer experience:** Radware stakeholders note that customer training and product documentation can become out-of-date and less relevant to new features and releases.

Rohde & Schwarz Cybersecurity (DenyAll)

Rohde & Schwarz Cybersecurity is in the Niche Players quadrant. Its approach to WAF management is praised by its customers, and the vendor bundles several innovations in its core platform to improve efficacy of the detection and avoid false positives. The vendor has limited market reach outside of Western Europe and grows below market average, and its cloud-based WAF service offering is not fully mature yet.

Rohde & Schwarz Cybersecurity is a Germany-based electronics group. The vendor has acquired several vendors to build its cybersecurity division. It has more than 500 employees, including 90 in the DenyAll business unit, resulting from the acquisition in 2017 of DenyAll, a French vendor. DenyAll operates as an independent entity. In addition to DenyAll web application security products, Rohde & Schwarz Cybersecurity's portfolio includes a multifunction firewall product line (following the acquisition of gateprotect in 2014), endpoint security and encryption management products.

A key concept in the DenyAll WAF is the use of graphical workflow to configure traffic processing and inspection. Workflow view is a diagram, where administrators can drag and drop controls, response modification and other actions. The DenyAll WAF is available on AWS and Microsoft Azure. Cloud Protector is the cloud-based WAF service solution.

In addition to the DenyAll acquisition, recent news includes the release of versions 6.3 and 6.4, with the addition of three new security engines from legacy DenyAll rWeb, a new log management stack and integration of HSM.

Rohde & Schwarz Cybersecurity is a good shortlist contender for organizations looking for a WAF appliance, combining ease of use and in-depth security features, especially those located in Europe.

Strengths

- **Customer experience:** Some clients cite DenyAll WAF workflows as a key differentiator from competition. In the past, they mentioned the need for a better learning curve, but the vendor has recently made available many more workflow examples in the default configuration.
- **Capabilities:** DenyAll WAF includes multiple analysis engines and leverages user session risk scoring to ensure accurate detection and low false-positive rate.
- **Capabilities:** Rohde & Schwarz Cybersecurity enables a correlation between its WAF and vulnerability scanner to increase the accuracy of detection. It offers strong web access management features, tightly integrated with the WAF.
- **Customer experience:** Customers indicate excellent support — specifically, the vendor's rapid answers to customer questions, the willingness to find a customized solution and the ability to fix issues.
- **Improvements:** Rohde & Schwarz Cybersecurity has achieved the upgrade of its reporting solution relying on the Elasticsearch, Logstash and Kibana (ELK) stack, which now offers noticeably improved dashboards. The vendor also regularly runs "bug bounties," where security professionals are rewarded when they find a bug or a way to bypass DenyAll WAF security modules.

Cautions

- **Market responsiveness:** DenyAll is finalizing the merge of features from its two WAF platforms, following its 2014 acquisition of BeeWare, and Gartner expects that DenyAll's acquisition by Rohde & Schwarz Cybersecurity will further impact its market responsiveness, in part due to the efforts to integrate with other solutions from the vendor's portfolio.
- **Capabilities:** DenyAll WAF does not include ad hoc and automatically deployed attack signatures to complement its generic rule set. Before acquisition, the vendor had one of the smallest threat research teams for vendors evaluated in this research.
- **Geographic Strategy:** DenyAll mainly focuses on the French and European markets, which limits its visibility and adoption in other geographies. The vendor has direct presence only in France and Germany. Prospective clients outside of these countries should first verify the availability of local skills, and assess their need for support in their native language.
- **Customer experience:** Many customers give low scores to the real-time log view, due to insufficient aggregation of alerts. Some of them complain that the Java console is not as reactive as other management consoles they use.

- **Cloud-based WAF service:** Despite being based on the same software as DenyAll WAF, Cloud Protector, its cloud-based WAF lacks several features, including an automated positive security model, bot mitigation and access management. It relies on a single data center, based in Europe.
- **Capabilities:** DenyAll WAF lacks fully featured web management. DenyAll WAF lags behind its competitors in modern application payload analysis and bot mitigation.

Venustech

Venustech is in the Niche Players quadrant. Its WAF sales are limited to China, and the vendor has not tackled international markets yet. Its WAF technology covers all the basics, but offers limited integrations.

Venustech is a well-known security brand in China. The vendor is headquartered in Beijing, China, and has more than 3,000 employees. The vendor also offers penetration testing services.

Recent news includes WAF virtual appliances and large physical appliances, geo-IP blocking, and improvements against evasion techniques.

Venustech is a good shortlist candidate for existing Venustech clients in China and Japan.

Strengths

- **Marketing execution:** Venustech has good visibility in public sector use cases.
- **Capabilities:** The vendor has a large range of WAF appliances, ranging from 350 Mbps to 30 Gbps. It has recently added virtual appliances.
- **Customer experience:** Clients mention top-notch presale and postsale support as an important reason to continue with Venustech WAF.
- **Customer experiences:** Resellers and clients report that Venusense WAF delivers high performance in production environments.
- **Sales execution:** Venustech frequently manages to win WAF deals based on value.

Cautions

- **Geographic strategy:** Venustech is not visible in WAF shortlists outside of China. The management interface is available in English and Chinese only.
- **Market segmentation:** The vendor has a WAF appliance product line to address larger deployment, but has not penetrated the enterprise segment yet. Gartner estimates that more than 85% of Venustech WAF customers are midsize organizations, not enterprises.
- **Capabilities:** Venustech does not offer a cloud-based WAF service. It lacks integration with IaaS platforms. Venusense WAF appliances do not integrate with DDoS protection cloud services to protect against volumetric attacks.

- **Capabilities:** Venusense WAF lacks authentication features, and has limited predefined role-based access for WAF administrators.
- **Technical architecture**: Venustech WAF appliances cannot embed an HSM module to securely store server secrets. The vendor does not offer managed services for its WAF.
- **Customer experience**: Customers would like to see improvement in SQL injection protection. They also mention centralized management and reporting as solutions that lag behind competing products.

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

- Amazon Web Services, Instart Logic and Venustech have been added.
- DenyAll has been acquired by Rohde & Schwarz Cybersecurity

Dropped

- AdNovum, Trustwave and United Security Providers did not meet this year's updated inclusion criteria.
- DenyAll has been acquired by Rohde & Schwarz Cybersecurity.

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 PCI DSS Requirement 6.6 (which covers Open Web Application Security Project [OWASP] Top 10 threats, in addition to others).
- They provide physical, virtual or software appliances, or cloud instances.
- Their WAFs were generally available as of 1 January 2016.
- Their WAFs demonstrate features/scale relevant to enterprise-class organizations:

  - $10 million in WAF revenue during 2016; able to demonstrate that at least 200 enterprise customers use its WAF products under support as of 31 December 2016.
  - $7 million in WAF revenue during 2016; at least 50% growth compared to 2015.
- Gartner has determined that they are significant players in the market due to market presence or technology innovation.
- 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 not actively providing WAF products to enterprise customers, or has minimal continued investments 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 that provide 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 a host-based WAF, WAM, RASP or API gateway (these are considered distinct markets).

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, including A10 Networks, Alert Logic, Array Networks, Beijing Chaitin Technology, Brocade, DBAppSecurity, DB Networks, ditno., Indusface, Kemp Technologies, Limelight, Microsoft, ModSecurity, Nginx, Piolink, Qualys, Sangfor, SiteLock, Sucuri, Verizon, Wallarm and Zenedge.

The adjacent markets focusing on web application security continue to be innovative. This includes the RASP market and other specialized vendor initiatives. Those vendors take part in web application security, but often focus on specific market needs, or take an alternative approach to web application security. Examples include Cleafy, Distil Networks, Signal Sciences and Shape Security.

Evaluation Criteria

Ability to Execute

- **Product or Service:** This includes the core WAF technology offered by the technology provider that competes in/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-based options) with real-time transaction demands, are weighted heavily. Product evaluation also considers adjacent security functions, such as (but not limited to) DDoS protection services, bot management (which includes bad-bot mitigation and good-bot whitelisting), fraud detection, API security and threat intelligence feeds, which might be bundled or integrated with WAFs. Integration with other markets, such as cloud access security brokers (CASBs) and AST, is evaluated too, but more lightly.
- **Overall Viability:** This 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 to invest in WAF, offer WAF products and advance the state of the art within the organization's portfolio of products.
- **Sales Execution/Pricing:** This is 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 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, changes (such as the relative importance of PCI compliance). 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 that are designed to deliver the organization's message in order 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 buyers' minds. 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 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:** This is the organization's ability 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.

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 (August 2017)

Completeness of Vision

- **Market Understanding:** This is the technology provider's ability to understand buyers' wants and needs, and to translate them 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 them with their added vision. They also determine when emerging use cases will greatly influence how the technology has to work. Vendors showing a better understanding of how the changes in web applications impact security will get higher score. 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.
- **Sales Strategy:** This is the strategy for selling products that 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 machine learning 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 new protocols and standards (such as JavaScript Object Notation [JSON], HTML5, HTTP/2, IPv6 and WebSockets), as well as remaining efficient against the changes in how older web technologies (such as Java, JavaScript and Adobe Flash) are used
  - Providing dedicated protection techniques on emerging web application use cases, such as mobile and IoT applications
  - Bot mitigation not limited to reputation-based controls
  - API security
  - User behavioral analysis
  - Countering evasion techniques actively

  This criterion includes the evaluation of the depth of features, especially features that ease the management of the solution, and the integration with other solutions, including DDoS protection services and emerging technologies like CASB.
- **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 markets. Vendors focusing on a single vertical get lower scores; vendors having differentiated vertical strategies and the ability to reproduce success across several verticals get higher scores.
- **Innovation:** This refers to the direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes. It includes product innovation and quality differentiators, such as:
  - New methods for detecting web attacks and avoiding false positives

- 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 — either directly or through partners, channels and subsidiaries — as appropriate for those 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	Medium
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Medium

Source: Gartner (August 2017)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors that have the ability to 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 to ensure 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 to current customer requirements, Leaders also show evidence of superior vision and execution for anticipated requirements and evolution in web applications that will require paradigm changes.

Challengers

Challengers in this market are vendors that have achieved a sound customer base, but they 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 does not address (and may not be interested in addressing) the entire market.

Visionaries

The Visionaries quadrant is composed of vendors that have provided key innovative elements to answer web application security concerns. They devote more resources on security features that help protecting 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 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 that have a limited geographic reach. The WAF market includes several European and Asian vendors that serve clients in their regions well, with local support and an ability 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 SMB and smaller enterprises' needs.

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 this 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, but with a small share of their revenue coming from their WAF offerings. Product selection decisions should be driven by organization-specific requirements in areas such 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 who are 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 and cloud services
- SSL decryption/re-encryption and other scalability requirements

For more information on WAF technology selection and deployment challenges, see "Web Application Firewalls Are Worth the Investment for Enterprises."

Market Overview

Gartner estimates that the WAF market totaled about $626 million in 2016, representing a growth of 21.3% compared to 2015. The Americas represent 43% of the total market, EMEA accounts for 27% of the market and the Asia/Pacific region accounts for 29%.

WAF Market Trends

Gartner has observed three big trends in the WAF market:

1. Gartner estimates that both physical appliance sales and WAF sales from ADC vendors are declining, with most vendors experimenting a decline or a low-single-digit growth.
2. Cloud-based WAF service grows steadily. Gartner estimates that it now represents more than 30% of the total market in 2017. Cloud-native solutions increasingly compete with the more mature vendors. IaaS providers are not yet as visible in inquiries, but they also offer a WAF.
3. As in previous years, little innovation has occurred during the last 12 months. Use of machine learning is rare and often still unproven. Most WAF solutions still lack the more advanced analytics that Gartner analysts observe in other security markets.

> 2018 could mark a tipping point in the WAF market evolution, as the growth of cloud-based WAF service now manages to support the global market, despite declining appliance revenue.

The complexity of large-scale deployment is a competitive disadvantage against cloud services, but broader choice in vendors, plus the perceived security of on-premises deployment, currently give appliances and virtual appliances an advantage in enterprise client evaluations.

The Future of WAF Could Be Healthy

Based on Gartner's customer research survey (which aligns with Gartner inquiry; see Note 1), the most common applications protected by a WAF include:

- Corporate website (78%)
- E-commerce component (66%)
- Customer portal (63%)

The potential for future growth of the WAF market is still there. According to participants in Gartner's recent survey on web application security (see Note 2), WAF remains the most frequently used security control to protect web applications (84%), followed by enterprise IPS (61%) and use of application security testing (58%). Large enterprises might classify their public-facing web applications in tiers, where the most business-critical applications (Tier 1) require more stringent security controls and benefit from larger budgets, whereas other applications (Tiers 2 and 3) are more likely to suffer from constrained security budgets and resources. Gartner analysts more rarely see WAFs deployed in front of internal web applications.

When asked to rank their top-three most effective technologies and processes to protect enterprise web applications, WAF comes in first position (73%), followed by application security testing (53%). Industry reports, such as Verizon Data Breach Investigations Reports, continue to highlight the pattern of attacking web applications as the most prevalent entry point for data breaches, increasing general awareness of web application security risks in the market.[1]

But WAF Is Shifting From Physical Appliance to Cloud-Based WAF Service

When looking forward, the future is not as bright for WAF appliances. Still, WAF generally does poorly against the use of stolen credentials, which is the No. 1 attack technique against web applications, involved in a third of the identified breaches.[1]

> A growing number of remotely hosted applications and improvements in security controls offered by cloud-based WAF service vendors reduce the advantage that WAF appliances once had.

In Gartner's enterprise application security study, participant's most commonly used deployment methodology for enterprise web applications remains on-premises (51%), with other options closing in: private cloud already accounts for 26%, IaaS for 16% and SaaS for 7% (see Note 2).

Development methodologies are changing, too. A growing number of applications are developed leveraging agile methodologies (see Note 3). Sixty percent of survey participants are commonly using agile methodology for mobile application back-end development. This is also confirmed by Gartner's recent DevOps survey with IT professionals, in which only 28% of surveyed organizations have no plans to use DevOps.

Internal factors aggravating the decline of WAF appliances include the lack of innovation in this space. Some vendors are trying to divide their research and development resources to update the legacy appliance technology to support the more recent standards (HTTP 2.0, JSON payload analysis), while launching a cloud-based WAF service initiative.

One of the most frequent challenges reported by clients about WAF appliance is the deployment and operational workload. When participating value-added resellers were asked about future scenarios for WAF (see Note 1), 60% of the resellers noted they are very likely to sell more WAF cloud services than today, and 54% say they are very likely to sell more managed services for WAF technology. During Gartner client inquiries, security managers confirm increased interest in cloud-based WAF service, frequently as a way to reduce workload related to WAF deployment and operations. They like the idea of using managed services, but express concerns about the related costs and about the complexity of dealing with multiple managed security service providers.

Gartner application security leaders report frustration over the fragmentation of the web application security space. Cloud-based WAF service is one of the potential solutions to these challenges, as they can be easier to deploy, often bundle several of these features together in a subscription-based business model and are catching up in terms of security efficacy.

> Newer use cases like mobile application security and the nascent Internet of Things are excellent fits for cloud-based WAF services. But IoT, single-page and mobile applications have a lot of the application intelligence in the client. WAF won't grow in these areas if it does not evolve its approach.

Cloud-based WAF service offerings will face growing competition from specialized vendors, such as Distil Networks and Shape Security for bot mitigation. It will also compete with alternate approaches to exploit detection and/or protection from new vendors, such as Signal Sciences.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"How Markets and Vendors Are Evaluated in Gartner Magic Quadrants"

"Web Application Firewalls Are Worth the Investment for Enterprises"

"Magic Quadrant for Application Delivery Controllers"

Evidence

[1] Verizon 2017 Data Breach Investigations Report:

Figure 33: Web app attack is the most prevalent attack vector involved in data breaches (29.5%).

Figure 52: Use of stolen credential: used in 33% of breaches, excluding botnet.

Note 1 Customer and Reseller Survey

In addition to hundreds of end-user inquiries about firewall that Gartner analysts conduct every year, Gartner surveys its clients as well as end-user references and reseller references submitted by vendors.

In March 2017, Gartner surveyed 79 resellers currently actively selling web application firewalls as a part of their portfolio: 87% of the resellers have been reselling WAF for more than a year, and 36% for more than five years; 54% of the surveyed resellers sell more than one brand of WAF.

During the same period, 105 WAF end users were surveyed; 53% came from the Americas, 40% from EMEA and 34% from the Asia/Pacific region.

Note that the data shown in this report is included when self-reported data and other marketwide data seem to be aligned. End-user and customer survey data may be subject to self-reporting bias and do not necessarily reflect the market as a whole.

Note 2 Application Security Trends Study

Gartner's 2017 Application Security Trends Study was conducted via an online survey in January 2017 among Gartner Research Circle Members — a Gartner-managed panel composed of IT and business leaders. In all, 108 IT leaders with insight into their enterprise's web application security landscape participated.

Objectives: To understand the enterprise web application security landscape and to identify the trends organizations are facing in meeting their digital business objectives.

Note 3 Enterprise DevOps Survey

The Gartner Enterprise DevOps Survey Study was conducted via an online survey from 9 May 2016 to 13 May 2016 among Gartner Research Circle Members — a Gartner-managed panel composed of IT and business leaders.

Objectives: To learn how organizations are adopting DevOps as a means to accelerate enablement (that is, to go faster while improving quality). It also aims to inform on topics such as starting a DevOps approach, pitfalls to avoid, scaling efforts, integrating information security, pursuing this in a regulated environment and quantifying benefits.

In all, 252 IT and business leaders participated, with 95 members qualified by indicating they are already using DevOps.

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.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

© 2017 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the Usage Guidelines for Gartner Services posted on gartner.com. 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 and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity."