Gartner

Magic Quadrant for Web Application Firewalls

17 June 2014 ID:G00259365

Analyst(s): Jeremy D'Hoinne, Adam Hils, Greg Young, Joseph Feiman

VIEW SUMMARY

The WAF market is growing quickly from a small base; it is composed of pure players, application delivery controller vendors, cloud service providers and network security vendors. Buyers should evaluate how WAFs can provide high security, minimize false positives and sustain performance.

Market Definition/Description

The Web application firewall (WAF) market is defined by a customer's need to protect internal and public Web applications when they are deployed locally (on-premises) or remotely (hosted, "cloud" or "as a service"). WAFs are deployed in front of Web servers to protect Web applications against hackers' attacks, to monitor 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 it was the only way to perform some in-depth inspections. Other deployment modes exist, such as transparent proxy, bridge mode, or the WAF being positioned out of band (OOB) and, therefore, working on a copy of the network traffic.

The primary WAF benefit is providing protection for custom Web applications that would otherwise go unprotected by other technologies that guard only against known exploits and prevent vulnerabilities in off-the-shelf Web application software (see "Web Application Firewalls Are Worth the Investment for Enterprises").

WAFs also integrate with other network security technology, such as vulnerability scanners, distributed denial of service (DDoS) protection appliances, Web fraud detection and database security solutions. In addition, WAFs sometimes include performance acceleration, including content caching, and might be packaged with Web access management (WAM) modules to include authentication features — notably to provide single sign-on (SSO) for legacy or distributed Web applications.

Gartner estimates that the WAF market grew in 2013 at a rate of approximately 30% from $259 million to $337 million, and most of the growth was driven by a handful of vendors. Demand in North America has been strong, with 45% of the total market. EMEA accounts for 29% of the market, while Asia/Pacific accounts for 26%. The Middle East demonstrated the highest growth rate, while Europe was the least dynamic region.

To be considered for this Magic Quadrant, vendors must actively sell and market WAF technology to end-user organizations. The technology should include protection techniques that have been designed for Web security, beyond signatures that can be found in next-generation firewalls and intrusion prevention systems (IPSs). WAF products should support single and multiple Web server deployments. This Magic Quadrant includes WAFs that are deployed in front of Web applications and are not integrated directly on Web servers. This includes:

- Purpose-built physical, virtual or software appliances provided by pure players or network security vendors
- WAF modules embedded in application delivery controllers (ADCs; see "Magic Quadrant for Application Delivery Controllers")
- Cloud services

How WAFs integrate other network security technologies — like static application security testing and dynamic application security testing (DAST) or security information and event management (SIEM) — is often one of the indicators that reflect a strong presence in the enterprise market. Consolidation of WAFs with other technologies, like ADCs or anti-DDoS cloud services, brings its own benefits and challenges, but this market evaluation primarily focuses on the buyer's security needs when it comes to 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

In particular, Gartner scrutinizes these features and innovations for their ability to improve Web application security beyond what a next-generation firewall, IPS or open-source WAFs — which are available for free (such as ModSecurity and IronBee) — would do.

STRATEGIC PLANNING ASSUMPTIONS

At the end of 2018, less than 20% of enterprises will rely only on firewalls or intrusion prevention systems to protect their Web applications — down from 40% today.

By year-end 2020, more than 50% of public Web applications protected by a WAF will use WAFs delivered as a cloud service or Internet-hosted virtual appliance — up from less than 10% today.

EVIDENCE

[1] "Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures, Version 1.2," October 2008; and "PCI Security Standards Council — Information Supplement: Application Reviews and Web Application Firewalls Clarified, Version 1.2" October 2008

NOTE 1 TYPE A, B AND C ENTERPRISES

Enterprises vary in their aggressiveness and risk-taking characteristics:

- Type A enterprises seek the newest security technologies and concepts, tolerate procurement failure, and are willing to invest for innovation that might deliver lead time against their competition. This is the "lean forward" or aggressive security posture. For Type A enterprises, technology is crucial to business success; of course, they also have skilled and dedicated security teams.
- Type B enterprises are "middle of the road." They are neither first nor last to bring in a new technology or concept. For Type B enterprises, technology is important to the business and security teams are often understaffed.
- Type C enterprises are risk-averse for procurement, perhaps investment-challenged and willing to cede innovation to others. They wait, let others work out the nuances and then leverage the lessons learned. This is the "lean back" security posture that is more accustomed to monitoring rather than blocking. For Type C enterprises, technology is critical to the business and is clearly a supporting function. These enterprises might not have dedicated security teams.

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

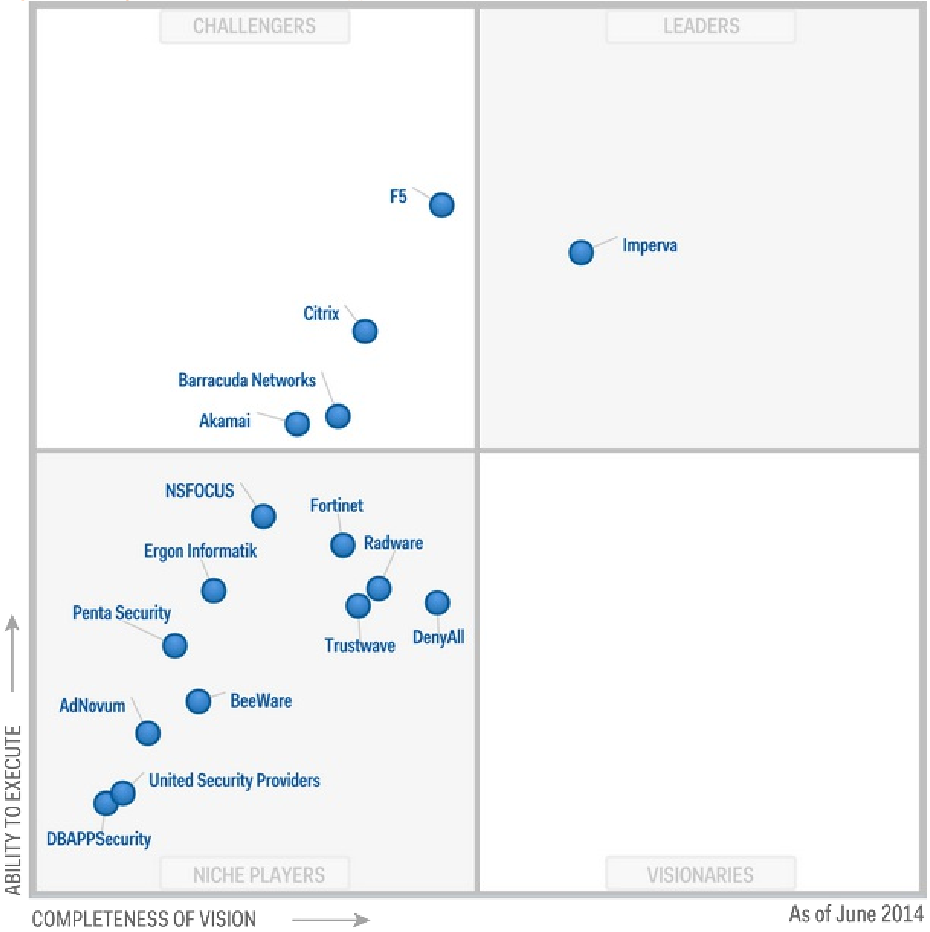
Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

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

Magic Quadrant

Figure 1. Magic Quadrant for Web Application Firewalls



Source: Gartner (June 2014)

Vendor Strengths and Cautions

AdNovum

Switzerland-based AdNovum is a long-established provider of application development, IT and security services. It recently started its expansion beyond this home market, and had its first successes in Singapore. AdNovum's product offering, under the cover name Nevis Security and Compliance Suite, includes WAF (nevisProxy), authentication, identity management and document signing, and was first shipped in 1997. The nevisProxy WAF is delivered as a software appliance and does not yet have third-party evaluations, but provides some features beyond signatures with support for a positive security model, URL encryption and protection against cross-site request forgery (CSRF).

Swiss enterprise buyers in need of a combined WAM and WAF solution to protect custom application should consider AdNovum in their competitive shortlists.

Strengths

- AdNovum has proven experience with large financial institutions in Switzerland, and is able to quickly develop to specific customer requirements.
- Nevis Suite includes robust authentication and SSO features. Its centralized management ("nevisAdmin") supports a large number of WAF instances, and is multitenancy-capable.
- AdNovum provides free licensing for test servers and unlimited flat-rate agreements for very large deals.

Cautions

- AdNovum's WAF is one component of a software suite that serves primarily WAM purposes; consequently, the R&D investment in pure WAF development is more limited.
- AdNovum does not appear on Gartner customer shortlists for WAF outside of Switzerland.
- AdNovum lacks hardware appliance offerings that many of its competitors provide.
- Protections against SQL injection and cross-site scripting (XSS) are focused primarily on ModSecurity open-source signatures, with no complementary internal or third-party threat research.
- nevisProxy does not offer virtual patching based on the results of a vulnerability scanner, or dedicated security and compliance reports.

Akamai

Akamai (AKAM) is based in Cambridge, Massachusetts, and provides a leading content delivery network (CDN). Its network and security cloud services, including its WAF (Kona Site Defender),

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.

are built on top of the Akamai Intelligent Platform, its global cloud infrastructure. The Kona WAF has been available since 2009, and received significant improvement in 2013. The Kona WAF management and monitoring consoles (Luna Control Center and Security Monitor) are also delivered as Web portals.

Akamai's WAF is delivered as a service with a monthly fee, based on performance requirements for up to 10 sites. Additional subscriptions are available to limit the extra costs in case of volumetric DDoS attack (DDoS Fee Protection), to get assistance with Web security rule updates and tuning (Rule Update Service), or to reduce the scope of PCI compliance assessment with tokenization of client credit credentials (Edge Tokenization).

In the first quarter of 2014, Akamai completed the acquisition of DDoS protection service Prolexic Technologies. Gartner analysts expect future integration between Kona and the Prolexic offering.

The Kona WAF is a good choice for existing Akamai customers as an extension to deployed Akamai solutions, and for large public websites looking for simple WAF deployment.

Strengths

- Gartner clients cite the combination of DDoS protection and Web application security as a differentiator when comparing Akamai with most competitors.
- Akamai leverages its visibility into a substantial share of Internet traffic to tune security signatures in order to avoid false alerts and improve detection, with multiple steps for anomaly detection that feed a scoring mechanism.
- Akamai's subscription model makes it easy for enterprises to purchase and enable Web application security. This is especially true for existing Akamai CDN clients, and for owners of very large hosted Web applications.
- The transparency and professionalism demonstrated in Akamai's reaction to the recent Heartbleed vulnerability inspires trust in its ability to handle security-related challenges.

Cautions

- Akamai's WAF is available as a cloud service only. Akamai does not provide an on-premises appliance option that many of its competitors offer to protect internal applications, or to maintain Secure Sockets Layer (SSL) secrets on the client's corporate network.
- Akamai lacks lower-price WAF subscriptions to reach smaller enterprises and midsize organizations.
- Kona Site Defender security still relies primarily on signatures and reputation scoring. It lags behind competitors in other capabilities, such as an automatic learning engine and the degree of custom configuration of Web application behavior.
- Akamai is growing the customer base for its WAF offering mainly from existing clients of other cloud services in the U.S., but Gartner does not see the vendor winning deals on Web application security needs.

Barracuda Networks

Barracuda Networks (CUDA), which is based in Campbell, California, provides a wide variety of information security and storage products that are largely targeted at small or midsize businesses (SMBs). Barracuda offers its Web Application Firewall line in a variety of form factors, including as a physical or virtual appliance, and also as a cloud-based service that can be deployed on the Microsoft Azure and Amazon Web Services (AWS) cloud platforms.

SMB buyers and resource-strapped security teams that require a low-cost solution and attentive vendor support should consider this product.

Strengths

- Barracuda's WAF provides strong IP reputation, cookie protection and client fingerprinting capabilities. It also combines embedded authentication features and integration with several third-party authentication solutions.
- Barracuda has a broad range of hardware appliances to support a wide variety of scalability and performance requirements, especially for SMBs; it is also one of the only vendors to offer a WAF on the Microsoft Azure platform.
- Barracuda customers rate its geographically distributed support capabilities quite highly.
- Barracuda offers a wide range of foreign language support in its management interface, including Mandarin, Cantonese and Korean.

Cautions

- Barracuda's WAF lags behind its leading competitors in enterprise-level automation. It integrates with a low number of established vulnerability scanners for virtual patching, and the scanning results must be imported manually. Automatic learning capabilities are disabled by default.
- Customers note that the management graphical user interface (GUI) looks a bit dated, which can make it difficult to use in some situations.
- Barracuda heavily relies on a relatively small set of generic signatures to protect against XSS and SQL injection.

BeeWare

France-based BeeWare has been marketing its technologies since 2003. Its products, which include WAF, Web services firewall and WAM, have been integrated into its i-Suite platform, which can be deployed as a physical or virtual appliance. The i-Suite solution also offers ADC features, such as load balancing, content caching, compression and traffic rewriting. BeeWare is one of the smaller vendors in the WAF space, and predominantly sells its WAF to the French market. In May

2014, it was acquired by DenyAll.

Midsize and large French enterprises in financial, government and manufacturing sectors that have WAF and authentication needs should consider BeeWare on their shortlists, but also take into account the acquisition by DenyAll.

Strengths

- BeeWare offers an i-Suite version for the protection of applications hosted on AWS, Microsoft Azure and other clouds (although deployment of this WAF cloud version is very low).
- Its i-Suite has strong protection for Web services and SSO features.
- BeeWare's WAF flow-based policy management interface may be attractive to customers that like an event-based graphical representation of a security policy.

Cautions

- BeeWare's revenue and growth are low and lag behind most players in the WAF market.
- It has low visibility and does not appear on Gartner customer shortlists outside France.
- Its technology has limited anti-evasion techniques. It offers only generic SQL injection (SQLi) and XSS protection capabilities.
- Its non-Web Java client GUI, although graphical and rich, is not in-line with the general trend of Web-based GUIs.
- Its WAF has integration with only one DAST vendor, Qualys, and with only two SIEM vendors, Splunk and RSA, The Security Division of EMC.

Citrix

U.S.-based Citrix (CTXS) is a global provider with a broad portfolio of virtualization, cloud infrastructure and ADC solutions. Citrix has offered WAF functionality (NetScaler AppFirewall) for more than a decade as a software option, or included in the "Premium" bundle of the NetScaler Application Delivery Controller suite. The Citrix hardware appliance product line (NetScaler MPX) can also run a license-restricted version of the full NetScaler software to act as a stand-alone WAF. In addition, Citrix provides virtual appliances (NetScaler VPX). The NetScaler SDX platform allows several instances of Citrix solutions, including ADC and NetScaler AppFirewall software in a single hardware appliance. NetScaler can also be bundled in Citrix Mobile Workspace offerings.

Citrix NetScaler AppFirewall is a good choice for large enterprise clients that are looking for an easy way to add WAF functionalities to their existing Citrix infrastructures.

Strengths

- NetScaler AppFirewall includes mature features for Web security, and can be bundled with SSL VPNs for remote access of internal applications.
- Citrix NetScaler's ability to scale appeals to large organizations, especially when massive SSL offloading is required.
- Citrix has a compelling ecosystem of partnerships with third-party solutions.
- Citrix offers an extensive range of hardware (MPX/SDX) and virtual (VPX) appliances.

Cautions

- Like most ADC vendors, Citrix primarily targets enterprise clients with ADC solutions and does not focus its efforts on pure-play security use cases.
- Despite good visibility historically, Citrix recently has appeared less often on client shortlists than its direct competitors have.
- Citrix NetScaler's physical appliance price tag starts at $15,000 and lacks a price-competitive WAF offering for midsize organizations. Citrix's virtual appliance and NetScaler on AWS might offer less expensive alternatives.
- Citrix does not offer or collaborate with cloud-based DDoS protection services.
- Gartner does not see Citrix's WAF displacing the competition based on its security capabilities, but rather sees it as an accompanying sale for ADC placements.

DBAPPSecurity

DBAPPSecurity, which is headquartered in Hangzhou, China, is a vendor of Web application and database security solutions. Its product offering includes a WAF (DAS-WAF) that was first released in 2007. DBAPPSecurity also provides a Web application vulnerability scanner (DAS-WebScan) and database audit platform (DAS-DBAuditor) that can collaborate with its WAF product.

DBAPPSecurity is a good shortlist candidate in China for SMBs and large enterprises in financial and government sectors.

Strengths

- DBAPPSecurity has a firm base of faithful clients in China that praise the benefits of having a Chinese provider. Those benefits include good resident support and local certifications.
- DAS-WAF includes automatic policy learning and Web application caching, and it can operate in transparent proxy or monitoring mode.
- Of all the vendors evaluated in this Magic Quadrant, DBAPPSecurity offers the lowest support cost relative to the WAF appliance price.

Cautions

- DBAPPSecurity lags behind several competitors' WAFs in areas such as role-based management, detailed activity reports and authentication features.

- DBAPPSecurity has very limited market visibility and does not appear on Gartner customers' WAF shortlists outside of China.
- DBAPPSecurity's recent strategic focus moved toward its security scanners, and the DAS-WAF is not promoted on the international version of the vendor's corporate website.

DenyAll

DenyAll is based in France and has marketed its WAF technology (rWeb) since 2001. Later, it added sProxy (a plug-in to rWeb with predefined policies for email, SharePoint and SAP) and rXML (a Web services firewall). DenyAll's rWeb WAF product was developed to secure HTTP(s), SOAP and XML traffic, and is currently available as a tool that is predominantly installed on enterprise's premises. Its technology can be deployed as software or appliance (physical or virtual). DenyAll is in the process of developing and testing its WAF cloud offering, and rWeb is already available via AWS and Microsoft Azure.

DenyAll mostly focuses on the French market, and then on the European market, where it primarily targets midsize and large enterprises in financial and government sectors. It is a relatively small vendor in the WAF market, but is able to sustain a focus on technology innovation. In May 2014, DenyAll announced the acquisition of WAF vendor BeeWare.

European organizations that are looking for high security first should consider adding DenyAll to their shortlists.

Strengths

- DenyAll's technology includes several advanced protection techniques, including JavaScript Object Notation (JSON) traffic analysis/protection, code leakage detection and a browser lightweight agent.
- It also offers a comprehensive list of anti-evasion techniques and a scoring list feature (a weighted scoring approach in addition to signatures) for protection against attacks, such as SQLi and XSS.
- The WAF technology combines security detection/protection features with caching, load balancing and high availability (with active-passive and active-active modes) features.
- DenyAll enables correlation between its WAF and DAST to increase the accuracy of detection and protection.
- The DenyAll rWeb offering is available via AWS to support Web protection for AWS-specific infrastructure-as-a-service customer deployments.

Cautions

- DenyAll mainly focuses on French and EU markets, which limit its visibility and adoption in other geographies.
- The acquisition of BeeWare will be a big challenge for DenyAll in the next 12 months. It could divert DenyAll from executing on its road map, but maintaining two product lines for too long would annihilate much of the benefits from the increased R&D size.
- Its revenue and growth are low compared with the Leaders, Challengers and even some Niche Players in this Magic Quadrant.
- It has certified integration with only one SIEM vendor, Splunk, and does not have integration with reputation vendors' technologies.
- DenyAll's WAF correlation process between WAF and DAST mainly focuses on WAF integration with its own DAST, but not DAST from other application security testing vendors.

Ergon Informatik

Ergon Informatik, which is headquartered in Zürich, has been shipping its WAF technology (Airlock) for more than 15 years. Ergon also develops other software solutions, including an authentication platform (Medusa) and mobile payment solutions. The Airlock WAF can be deployed as a reverse proxy, is available as a software and virtual appliance, and can run on Amazon Elastic Compute Cloud (EC2). Its pricing is primarily based on the number of protected Web applications and additional modules, such as SSL VPNs, XML security or graphical reports, which are available for an additional one-time fee. Airlock 5, which was released in January 2014, introduced a major operating system change and the full integration of an identity and access management (IAM) solution. Ergon will continue to support the previous versions of Airlock for 18 months.

Ergon's Airlock is a good contender for European organizations' WAF projects, especially large banking and insurance enterprises from the DACH countries (Germany, Austria and Switzerland) and the Middle East region that have access management needs.

Strengths

- Airlock includes extensive techniques for Web application parameters, with URL encryption, various cookie protections (including a cookie store) and form parameter integrity checks.
- Airlock's integration of a full IAM solution adds comprehensive authentication and SSO features.
- Ergon gets good marks from users for its security expertise, the efficiency of its support, and its understanding of the needs and constraints of large financial institutions.

Cautions

- Airlock does not offer centralized management, automatic Web application behavior learning or automated security signature updates, and it does not integrate with vulnerability scanners for virtual patching.

- Airlock lacks hardware appliance models. Instead, Ergon provides multiple ways to facilitate the installation of the software appliance.
- For SIEM integration, Airlock provides only a Splunk App, but Ergon reports that its customers have integrated with other SIEM technologies.
- Airlock has very low visibility in Gartner's customer base.

F5

Seattle-headquartered F5 (FFIV) is an application infrastructure vendor that is focused on ADCs. The primary WAF offering is a software module for the F5 Big-IP ADC: the Application Security Manager (ASM). Other F5 security modules include the network firewall Advanced Firewall Manager (AFM) and the WAM Access Policy Manager (APM) module. ASM is also available on the virtual edition of Big-IP. 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).

F5 is a good shortlist candidate, especially for large organizations that own or are considering ADC technology.

Strengths

- As a leading ADC vendor with a large installed base of clients, F5 leverages the scalability of its ADC Big-IP platforms and the strength of its ADC sales as the entry point for add-on WAF licenses. F5's WAF is an easy upgrade for existing F5 clients.
- F5's corporate teams and channels provide logistic capabilities and support that are larger and have more geographic coverage than many WAF vendors.
- ASM utilizes the same management software that is familiar to F5 administrators. iRules scripting enables the creation of custom policies that complement the predefined rule sets.
- F5 has been active in adding new WAF features, and messaging well on overall security.

Cautions

- Like other ADC-based WAFs, F5's WAF buyers must also select or have selected the accompanying ADC in reverse proxy mode. This might place F5 at a potential disadvantage versus pure-play WAFs.
- F5 does not have an as-a-service option, and its on-premises appliance line lacks low-end appliances. Its acquisition of Defense.Net in May 2014 could lead to future integration.
- Some Gartner clients have commented that ASM support can be challenging until escalated.

Fortinet

Based in California, Fortinet (FTNT) is a significant network security and network infrastructure vendor. It started as a unified threat management vendor in 2000. It later expanded its portfolio to include multiple security offerings, including a WAF (FortiWeb, released in 2008), an ADC (FortiADC) and a database protection platform (FortiDB). The vendor remains most well-known for its FortiGate firewall product line, and it keeps adding new products, such as the recent sandboxing appliance FortiSandbox.

FortiWeb provides multiple deployment options with a physical or virtual appliance (FortiWeb-VM), and acts as a reverse/transparent proxy or not in-line. It is also available on AWS. FortiWeb can be purchased with individual software options that can be bundled together for better overall costs. Subscriptions include IP reputation, antivirus and security signature updates.

Fortinet's existing customers and midsize organizations should include Fortinet's WAF in their competitive assessments.

Strengths

- FortiWeb includes an integrated vulnerability scanner, OOB deployments and predefined reports that clients seeking PCI compliance score positively.
- FortiWeb has a good set of features, including recently released automatic policy learning, cookie signing, SSL acceleration, Web application caching and bot detection.
- The security expertise offered through Fortinet's FortiGuard threat labs and the competitive price/performance points are often cited as differentiators by Fortinet's clients.
- Gartner sees FortiWeb doing best in selections from midsize businesses.

Cautions

- Fortinet does not offer WAF functionalities on top of its ADC and does not provide WAF as a cloud service.
- Despite a considerable sales channel, Fortinet's revenue in the WAF market is low compared with most other vendors. Enterprises should carefully assess the experience of its partners, because FortiWeb may be a new or unknown solution.
- FortiWeb has limited integration with other Fortinet solutions, thereby limiting the benefits for existing Fortinet customers to a common log reporting solution (FortiReporter).
- Gartner does not see the Fortinet WAF appearing on enterprise shortlists where security is highly weighted.

Imperva

California-headquartered Imperva (IMPV) is a data center security vendor with a long WAF legacy. Other Imperva products are focused on data and security, including products for database audit and protection as well as file activity monitoring. Early on, Imperva positioned itself primarily as a transparent bridge deployment. This aligned Imperva with enterprises, because deployments could more easily be made behind ADCs without introducing a second proxy, and "try before you buy" was easier with the transparent yet in-line mode. As most pure-play competitors were acquired or disappeared, Imperva continued to grow its share of the WAF market. Incapsula is the Imperva-owned, off-premises or as-a-service WAF that is bundled with other services, including DDoS mitigation.

Gartner sees a good attach rate level for Imperva's WAF with its database security offering. Imperva has a good third-party ecosystem, which includes data loss prevention, anti-fraud, SIEM and vulnerability scanners.

Imperva is a good shortlist contender for organizations of all sizes, especially those with high security requirements or those looking for an easy-to-deploy, cloud-based WAF.

Strengths

- Gartner sees Imperva consistently scoring very high and/or winning competitive assessments done by Gartner clients when security, reporting and protection are the most weighted criteria. Postsale, Gartner client commentaries usually are also very positive.
- Imperva has continually led the WAF market in new features that forced competitors to react; it also includes several advanced techniques for better efficiency of protection that its competitors lack. Thus, it is a good shortlist contender when protection is foremost and having a different vendor for WAFs and ADCs is an acceptable scenario.
- Imperva has consistently and effectively messaged on and delivered WAF features in response to changes in the data center and the application threat landscape.
- Having as-a-service Incapsula and on-premises SecureSphere options gives Imperva access to a larger addressable market in the enterprise and SMBs. This provides a transition path for clients whose application security needs change, and Incapsula is a good source to feed SecureSphere's threat intelligence (ThreatRadar Reputation Services).
- Like the on-premises SecureSphere, Incapsula continually scores high in Gartner client feedback.

Cautions

- As a premium enterprise product, Imperva SecureSphere is usually too advanced for SMBs, or for projects where the WAF is being deployed only as a "check the box" measure to meet compliance requirements.
- Some Gartner clients express concerns about Imperva's ability to maintain its security leadership because of the challenges it faces as a public company that is focused on a narrow market, but is still not profitable — versus larger data center infrastructure players.

NSFOCUS

NSFOCUS is a network security vendor headquartered in Beijing. It started in 2000 as a provider of an anti-DDoS solution (ADS Series), and then introduced new product lines for intrusion prevention (NIPS Series) and a vulnerability scanner (RSAS Series). NSFOCUS's WAF (WAF Series) offering was first released in 2007. It is delivered as a physical appliance and can perform in reverse or transparent proxy mode. NSFOCUS also offers centralized management software (Enterprise Security Manager) along with managed services for WAF. In January 2014, it announced an initial public offering (IPO) to accelerate its internationalization and launch new products.

NSFOCUS's WAF is a good shortlist candidate SMBs and larger organizations in China. Buyers from other regions should first verify local channel and support presence.

Strengths

- NSFOCUS has a larger R&D and support team dedicated to WAF than many other Niche Players.
- Clients selecting NSFOCUS WAF often report competitive price/performance as being a decisive factor.
- The WAF can redirect incoming Web traffic to NSFOCUS's anti-DDoS cloud service when congestion is detected, and then switch back to normal.
- The WAF has a good mix of local and global product certification, including ICSA WAF certification.

Cautions

- NSFOCUS's WAF lags in some enterprise-class features, such as limited role-based management, active-active clusters restricted to two appliances, and no SSL acceleration or hardware security module (HSM).
- NSFOCUS's WAF does not provide user session tracking or authentication features.
- NSFOCUS's WAF integrates with NSFOCUS's vulnerability scanner (RSAS); however, to date, there are no integrations with third-party SIEM or vulnerability scanners.

Penta Security

Penta Security is a network security vendor that was created in 1997 and is based in Seoul, South Korea. Its product portfolio includes WAFs (Wapples), database encryption (D'Amo) and authentication/SSO (ISign Plus). Wapples is offered as a physical or virtual appliance (Wapples V-Series), and centralized management appliances (Wapples MS) are also available. Penta Security emphasizes Wapples' "logic detection" technology, which does not require regular signatures updates. The vendor is accelerating its international presence in 2014 through the acquisition of channel partners.

Enterprise buyers in the Asia/Pacific region should consider Penta Security for WAF selection.

Organizations from other regions should check its local presence first.

Strengths

- The availability of transparent proxy and monitoring modes, combined with Wapples' logic detection approach to SQL injection and XSS protection, concurs to reduce the operational workload to install and maintain Penta Security's WAF.
- Wapples is the only WAF evaluated in this research with Common Criteria EAL4 certification.
- Wapples includes parameter and cookie security features, and it can create whitelists from IP reputation feeds. Its audit logs provide good traceability of configuration changes.
- Penta Security has a noticeable presence in the Asia/Pacific region, and other WAF vendors see it as a competitive threat in this region.

Cautions

- Wapples does not include any advanced automation features to create its security policy from Web application behavior. Instead, it relies on customizable templates, including one for PCI compliance and one for detection only.
- To date, there are no integrations with third-party SIEM or vulnerability scanners.
- Penta Security does not appear on Gartner customer shortlists outside the Asia/Pacific region.

Radware

Headquartered in Mahwah, New Jersey, Radware (RDWR) delivers a variety of application delivery and security products. These security products include a DDoS mitigation tool (DefensePipe), an IPS (DefensePro) and a WAF (AppWall), which can be bundled together in Radware's Attack Mitigation System (AMS) offering. Radware has been shipping the AppWall WAF, which it acquired from Protegrity, since 2010. AppWall may be deployed as a physical or virtual appliance. Radware also provides a solution for the centralized management, monitoring and reporting of its own products (APSolute Vision).

Radware's WAF predominantly serves the vendor's existing customer base of midsize and large enterprise clients. It is a good fit in security environments that use other Radware security or ADC products.

Strengths

- Among other deployment scenarios, AppWall can be deployed in transparent bridge mode while providing reverse proxy capabilities to specific traffic. Combined with automatic policy learning, this enables AppWall to be deployed easily, with no configuration changes to the network.
- Radware has announced software-defined networking partnerships with IBM, Cisco and NEC.
- Radware's WAF console includes strong service-provider-focused multitenancy capabilities, and integrates authentication and SSO modules.
- Radware has executed well on its road map for the past two years.
- AppWall is attractive to budget-constrained midsize organizations.

Cautions

- No reporting is available without the additional Radware APSolute Vision Reporter, which adds cost and complexity for organizations using a SIEM solution, or for those unwilling to invest specifically in a fully fledged reporting solution.
- AppWall lacks integration with third-party dynamic vulnerability scanners and database monitoring solutions.
- Radware has been slow to integrate AppWall as a module with Radware Alteon ADC (it was added in June 2014), thereby putting the vendor at a competitive disadvantage with fully integrated ADC/WAF competitors.
- Radware's market share is still lower than its direct competitors.

Trustwave

Based in Chicago, Trustwave (TWAV) provides managed services around its comprehensive portfolio of network security solutions. The Trustwave WAF (formerly WebDefend) was first available in 2006 as a physical appliance (TX Series), and then in 2013 as a virtual appliances (VX Series) for VMware hypervisors. Trustwave also provides managed services for its WAF offering. Trustwave's WAF works with other solutions from the vendor, including the SIEM and vulnerability scanner. Trustwave also supports the open-source ModSecurity WAF, and provides a commercial signature package that is maintained by SpiderLabs, its threat research team.

Trustwave is a good choice for organizations in North America that are seeking PCI compliance.

Strengths

- Trustwave's support of ModSecurity gives its threat research team access to feedback from a large community, which is useful for improving the quality of its WAF.
- In addition to in-line deployment methods, Trustwave's WAF offers a well-crafted OOB deployment mode, with multiple types of blocking capabilities and the ability to decrypt SSL connections using a copy of the network traffic.
- Trustwave recently acquired two companies that could contribute to tight integration with Trustwave's WAF in the future: Application Security, which provides database monitoring, and Cenzic (with its Hailstorm technology) for application security testing.
- Clients report that they have confidence in the SpiderLabs team's expertise to provide

accurate signatures against known attacks.

Cautions

- Except for compliance-driven projects, Gartner very rarely sees Trustwave in competitive evaluations for WAF procurement.
- Trustwave's high-end appliance performance may not meet the scalability requirements of larger enterprises, and active-active high availability is only planned for release in 2014.
- Trustwave lags its competitors in several areas, including authentication, protection against application DDoS, integration with third-party SIEM and Web application delivery optimization.
- OOB deployment of WAF, which is used by a majority of Trustwave clients, does not permit all the protection techniques that we see in competitors' WAF in-line modes, including decryption of Transport Layer Security (TLS) traffic when used with perfect forward secrecy, which can be an issue for some organizations.

United Security Providers

United Security Providers, which is headquartered in Bern, Switzerland, provides a WAM solution (USP Secure Entry Server) that includes a tightly integrated WAF, authentication server and XML gateway. It also offers managed security services, including products from other vendors. The WAF is available as a physical, software or virtual appliance, and as a cloud service, and it can be deployed as a reverse proxy only.

United Security Providers has been selling its WAF product as a component of WAM projects for more than 15 years, primarily to Swiss and German organizations. The WAF best serves Swiss and German organizations with authentication and security needs to protect internal Web applications or applications with restricted access.

Strengths

- The integration with the WAM solution offers a lot of flexibility for authentication and SSO, which can be factored into the WAF security decisions.
- United Security Providers' WAF includes URL encryption, protection against CSRF, cookie security and Web client fingerprinting.
- Clients like the flexibility of the WAF solution and the reactivity of vendor's support team.

Cautions

- United Security Providers focuses primarily on the WAM market. Buyers seeking Web application security only should verify the vendor's commitment to its WAF offering.
- Clients indicate that the management and reporting console could be improved with more intuitive configuration and additional security reports.
- The WAF does not provide integration with vulnerability scanners or SIEM, with the exception of a Splunk App.
- United Security Providers does not appear on Gartner competitive shortlists for WAF, and it has one of the smallest R&D teams dedicated to WAF development.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor's appearance in a Magic Quadrant or MarketScope 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

This is the first Magic Quadrant for the WAF market.

Dropped

This is the first Magic Quadrant for the WAF market.

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 Data Security Standard (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 2013.
- Their WAFs demonstrate features/scale that is relevant to enterprise-class organizations.
- They have achieved $3 million in revenue from the sale of WAF technology.
- Gartner has determined that they are significant players in the market due to market presence or technology innovation.

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

- The company primarily has a network firewall or IPS with a non-enterprise-class WAF.
- The company has minimal or negligible apparent market share among Gartner clients, or is not actively shipping products.
- The company 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 company has a host-based WAF or API security gateway (these are considered distinct markets).

In addition to the vendors included in this report, 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, including: A10 Networks, Alert Logic, CloudFlare, Positive Technologies, Qualys, Riverbed, Sangfor, Sucuri, Venustech and Verizon.

The different markets focusing on Web application security continue to be highly innovative. The vendors included in this Magic Quadrant participate, as do others that are not included. These 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 Juniper Networks (with its WebApp Secure product), Foresight Security 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 are weighted heavily, such as the ability to support complex deployments for on-premises or cloud-hosted public and internal applications with real-time transaction demands.
- ***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.
- ***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 weights its responsiveness during the most recent product life cycle higher.
- ***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 is 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 (June 2014)

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.
- ***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 product 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.
- ***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
  - Using a weighted scoring mechanism based on a combination of techniques
  - Providing updated security engines to handle new protocols and standards (such as JSON, HTML5, SPDY, 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
  - Actively countering evasion techniques
- ***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. This criterion is not rated this year.
- ***Innovation:*** This is 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
  - Integration with companion security technologies, which improves the 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	Not rated
Innovation	High
Geographic Strategy	Medium

Source: Gartner (June 2014)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors that have the ability to shape the market by introducing additional capabilities in their offerings, by raising awareness of the importance of those features and by 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. 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 also strong deployment, management, real-time monitoring, and extensive reporting. 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.

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 on 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. 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 quadrant vendors 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 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 road maps to specific needs; however, they do not sell outside their home countries or regions. Many Niche Players, even when making large products, offer features that would suit only SMB and smaller enterprises' needs.

Vendors in this quadrant may also have a small installed base or 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 also 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 or 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

Despite recent acceleration in adoption of the technology, many organizations have not yet deployed WAFs. That's especially true outside the North America region, where a majority of WAF sales target new clients, even if this varies based on the vertical industry. Large financial and e-commerce organizations already have a high adoption rate. WAF technology is also strongly implemented in government, especially in the Asia/Pacific region. Other vertical industries and a large portion of the European market often lack awareness of their need for WAF technology, which leaves good potential for future growth.

The WAF market includes different categories of vendors. In 2013, dedicated WAF offerings from pure players and network security vendors dominated the market with more than 50% of the WAF revenue. Large ADC vendors that were the first to add WAF capabilities have good market shares, leveraging their existing client base. They offer lower costs than dedicated technology, and emphasize easy integration and high performance to win WAF deals. Various CDN and anti-DDoS cloud providers now offer WAF subscriptions, growing quickly and from a small base.

Open-source module ModSecurity and the more recently released IronBee are also considered cost-effective competition for commercial WAFs.

Compliance Is Not the Primary Motivation for WAF Adoption, but It Remains Prevalent

In 2008, the PCI Security Standards Council released the PCI DSS Version 1.2 with an updated Requirement 6.6, which allowed WAFs as a viable alternative to Web application vulnerability assessments, and marked the beginning of a second stage in the evolution of the WAF market.[1] The PCI requirement was the root cause of many new WAF projects, thereby helping the WAF market to expand beyond niche use cases, especially in financial and banking organizations. It also convinced a lot of new ADC and network security vendors to add WAFs to their portfolios. Today, WAFs often protect more than public Web applications. For example, they might also be deployed in front of a mix of internal application and Web services. PCI and other compliance are still mentioned as the primary reasons for WAF purchases in 25% to 30% of inquiries with Gartner clients, especially in midsize organizations and smaller enterprises.

WAFs Will Continue to Integrate, Absorb and Be Integrated in Adjacent Technologies

WAFs integrate with several other technologies, including vulnerability scanners, database monitoring, Web fraud detection and DDoS protection. Gartner expects tighter integration or even inclusion for some of these technologies. Some WAFs already provide integrated vulnerability scanners in addition to integration with third-party vendors. Other WAFs use code injection and fingerprinting to gain knowledge about user behaviors that could lead them to include many of the features that currently fall under the Web fraud detection category.

Conversely, other technologies (such as network firewalls, IPSs, ADCs and cloud services for DDoS protection) integrate WAF modules in their offerings. While the offer from network firewalls and IPSs doesn't yet compare with WAFs, ADCs and cloud services are serious competitors.

Historically, WAFs have been leading in the protection against denial-of-service attacks, relying on vulnerabilities in the network and application stacks. In enterprises, with the growing presence of next-generation firewalls that include protections against network DDoS, and with the availability of dedicated appliances and services for DDoS protection, the relevance of DDoS features in WAFs is limited to DDoS attacks at the application layer. However, some network security vendors that offer DDoS protection and WAFs highlight collaboration between both technologies for better protection. Dedicated DDoS protection, WAFs and next-generation firewall technologies overlap for protocol attacks, provide very limited synergies and are not fully efficient against volumetric attacks.

Gartner believes that successful collaborations will happen between WAFs and cloud-based DDoS protection services, but that other partnerships will remain limited to niche use cases.

The Ability to Scale Is the Key to WAF's Market Future

Gartner already sees Type A organizations (see Note 1) with mature risk evaluation methodologies adopting WAFs for their public and internal Web applications, even when there are no compliance constraints.

Now, if WAF vendors want to sustain their growth in the future, they need to reach not only Type B and Type C enterprises, but also upper midsize organizations. The ability of WAF technologies to scale down for these organizations and adapt their offerings to SMB needs through ease of use, competitive pricing, and good channel support is challenging. Organizations that handle very large public Web applications will also require better automation during the staging as well as optimized operational costs, with larger appliances replacing complex cluster architectures. In addition, security for mobile Web applications, cloud hosting and cloud services implies new security measures and an alternative deployment setup that could impact how the WAF market evolves in the future.

The WAF market is in early mainstream phase, on the eve of the most critical period in its recent history; however, the overall dynamic is good, fed by steady growth of the number and size of Web applications, as well as by new, unexplored areas, such as the security of management servers for industrial control systems (ICSs) and mobile Web applications. Gartner estimates that the compound annual growth rate through 2017 will be in the range of 20%, but with increasing discrepancies between vendors and the growing importance of WAF delivered as an off-premises (hosted) virtual appliance, or as a cloud service.

Successful WAF vendors will manage to:

- Evolve their marketing message from education on Web application security to the unique capabilities offered by their technology.
- Provide easy integration in existing Web application infrastructure with low operational maintenance.
- Enforce high security against well-known and emerging threats.
- Maintain an extremely low rate of false positives without compromising their ability to detect attacks, and provide quick analysis and remediation when false positives happen.

- Consistently win competitive evaluations based on the quality of WAFs, rather than on good prices.
- Maintain high satisfaction from existing clients to ensure more than a 90% renewal rate, and provide unique value to new market segments.
- Provide good price and performance to organizations that don't give a premium score to security.

Increased visibility into well-known Web application behavior, better security against targeted attacks and ease of use will continue to be highly weighted in competitive evaluations; however, incremental improvements alone won't be sufficient to maintain a long-term high-growth rate. WAF vendors must also find new ways to provide high value to client organizations, and adapt to new methods of delivery and consumption for Web applications and services.