Gartner Magic Quadrant for Web Application Firewalls (2018)

Back to Web Application Firewall (WAF)

Summary

The WAF market is growing, driven by the adoption of cloud WAF services. Enterprise security teams should use this research as part of their evaluations of how WAFs can provide improved security that's easy to consume and manage, while respecting data privacy requirements.

Strategic Planning Assumptions

By 2020, stand-alone web application firewall (WAF) hardware appliances will represent fewer than 20% of new WAF deployments, which is a decrease from today's 35%.

By 2023, more than 30% of public-facing web applications will be protected by cloud web application and API protection (WAAP) services that combine distributed denial of service (DDoS) protection, bot mitigation, API protection and WAFs. This is an increase from fewer than 10% today.

Market Definition/Description

This document was revised on 3 September 2018. For more information, see the Corrections page.

The web application firewall (WAF) market is being driven by customers' needs to protect public and internal web applications. WAFs protect web applications and APIs against a variety of attacks, including automated attacks (bots), injection attacks and application-layer denial of service (DoS). They should provide signature-based protection, and should also support positive security models (automated whitelisting) 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 exist in the form of physical or virtual appliances, and, increasingly, are delivered from the cloud, as a service (cloud WAF service). WAFs are most often deployed in-line, as a reverse proxy, because, historically, that was the only way to perform some in-depth inspections. There are other deployment options. The rise of cloud WAF services, performing as reverse proxies by design, and the adoption of more-recent transport layer security (TLS) suites that require in-line traffic interception (man in the middle) to decrypt, have reinforced the use of reverse proxy.

Cloud WAF service combines a cloud-delivered as-a-service deployment with a subscription model. Cloud WAF service providers may offer a managed service, and, for some, it is a mandatory component of using the WAF. Some vendors have chosen to leverage their existing WAF solutions, repackaging them as SaaS. This enables vendors to have a cloud WAF service available to their clients more quickly, and they can leverage the existing features to differentiate from cloud-native WAF service offerings with a more limited feature set. One of the difficulties with this approach is simplifying the management and monitoring console, inherited from the comprehensive WAF appliance feature set to meet clients' expectations for ease of use, without shrinking security coverage. Gartner defines cloud web application and API protection (cloud WAAP) services as the evolution of existing cloud WAF services (see "Defining Cloud Web Application and API Protection Services"). In the long term, cloud WAF services, which were built from the beginning to be multitenant and cloud-centric, avoid costly maintenance of legacy code. They also provide a competitive advantage, with faster release cycles and rapid implementation of innovative features. Some organizations consuming cloud WAF services built from WAF appliances do it to acquire a unified management and reporting console.

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 WAF service, including WAF modules embedded in larger cloud platforms, such as content delivery networks (CDNs), and cloud WAF services delivered directly from infrastructure as a service (IaaS) platform providers
- Virtual appliances available on IaaS platforms, as well as WAF solutions from IaaS providers

API gateway, and runtime application self-protection (RASP) are adjacent to the WAF market, and might compete for the same application security budgets. This motivates WAF vendors to add relevant features from these markets, when appropriate. For example, cloud WAF services often bundle web application security with DDoS protection and CDN. The ability of WAFs to integrate with other enterprise security technologies -- such as application security testing (AST), web access management (WAM), 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, such as ADCs, CDNs or DDoS mitigation cloud services, brings its own benefits and challenges. However, this market evaluation focuses more heavily on the buyer's

security needs when it comes to web application security. This includes how WAF technology:

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

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

Gartner has strengthened this year's inclusion criteria for the web application Magic Quadrant, to reflect enterprises' changing expectations when selecting WAF providers (see Inclusion Criteria). Updated criteria include a requirement to get minimal revenue outside of a vendor's home region, which led to the exclusion of some of the more local vendors.

Magic Quadrant

Imperva

Imperva is in the Leaders quadrant. The vendor is one of the most visible in both the appliance and cloud WAF service segments. Imperva frequently wins on the basis of security features and innovation. Imperva can provide strong WAF functionality as a traditional appliance and cloud WAF service, but faces stronger competition for its cloud offering.
Imperva is an application, database and file security vendor, with headquarters in Redwood Shores, California. Its portfolio includes database security products (SecureSphere Data Protection and Database Audit and CounterBreach), a WAF appliance (SecureSphere WAF), and a cloud WAF service (Incapsula). Imperva also offers managed security services and managed SOC.

SecureSphere can be delivered as physical and virtual appliances. It is also available on AWS and Microsoft Azure marketplaces. The vendor also offers managed rule sets for AWS WAF.

In recent months, Imperva saw changes in its executive team, including a new CEO and CFO, followed by an internal reorganization to refocus on a cloud-first strategy. The company recently announced the acquisition of Prevoty, a RASP vendor. The vendor continued its investment in Incapsula infrastructure with new points of presence, refreshed some SecureSphere hardware appliances, and released Attack Analytics, a new real-time event management solution for Imperva SecureSphere and Incapsula.
Imperva is a good shortlist candidate for all kind of organizations, especially large enterprises looking for high-security WAF appliances, or organizations planning to transition their applications from on-premises to the cloud.

STRENGTHS

- Marketing Strategy: Imperva's offers a flexible licensing for organizations with a mix of on-premises and cloud-hosted applications. It allows the vendor to target a wider range of use cases and organizations, and to better manage the transition from WAF appliance to cloud WAF service.
- Sales Execution: Imperva is one of the only vendors providing both WAF appliances and cloud WAF service to achieve strong visibility in shortlists and large customer bases for both segments.
- Customer Experience: Gartner clients using SecureSphere continue to praise customer support. They've noted some improvements in Incapsula's bot mitigation.
- Capabilities: Incapsula and SecureSphere benefit from the shared threat intelligence from ThreatRadar.
- Capabilities: Imperva has recently released attack analytics to get unified and improved monitoring for SecureSphere and Incapsula. The vendor has also made available a first version of role-based administration for Incapsula.
- 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 APAC region.

CAUTIONS

- Market Responsiveness: Imperva is experiencing a lot of organizational changes, which could be the source of a slower pace of release, especially for the SecureSphere product line.
- Cloud WAF Service: Customers wish that Incapsula supported single sign-on (SSO) features, such as SAML 2.0. They also would like better and more-flexible canned reports.
- Capabilities: Customers considering Incapsula to replace SecureSphere often notice the lack of feature parity. The cloud WAF service cannot yet match the depth and breadth of security function covered by the appliance product line.
- Pricing: SeveralGartner clients cited higher-than-competitive prices for Imperva WAF SecureSphere, and to a lesser extent for Incapsula.
- Cloud WAF Service: Incapsula's infrastructure does not include any point of presence in China, and its infrastructure lags behind other cloud-native WAF services in South America and Africa.
- Customer Experience (WAF Appliance): SecureSphere customers report that the management console remains complex when using the more advanced capabilities. Customers frequently mentioned that deployment often requires professional services to effectively implement the offerings at scale. They also would like to see closer integration between Attack Analytics and the WAF management consoles, and more-unified management capabilities between SecureSphere and Incapsula.
- Customer Experience (Cloud WAF Service): Some customers complain about Incapsula's limited cross-sites and multidomain management and reporting, especially when multiple applications share the same IP address. Surveyed customers and resellers indicated that they did not get the same quality of support for Incapsula, compared with what they are accustomed to with Securesphere. They cite too many canned and not necessarily helpful answers as a first response when contacting support.

Barracuda Networks

Barracuda Networks is in the Challengers quadrant. Barracuda has good visibility for its WAF deployment over IaaS, and for existing Barracuda customers, but focuses on catching up with market leaders.

Barracuda Networks (CUDA) is based in Campbell, California. Barracuda is a known brand in security and backup markets, especially for midsize enterprises. In addition to network firewalls, its product portfolio includes email security and a user awareness training tool (acquired from Phishline in January 2018). The vendor also offers DDoS protection. The vendor delivers its WAF line in physical or virtual appliances. It is also available on the Microsoft Azure, AWS and Google Cloud Platform (GCP) platforms.

In November 2017, Barracuda agreed to be acquired by private equity firm Thomas Bravo. The acquisition was completed in February 2018. Barracuda has recently released Barracuda WAF-as-a-Service, its self-service cloud WAF. This release follows its DDoS protection service (Barracuda Active DDoS Prevention Service). The

vendor has improved its integration on Microsoft Azure for better scalability, and made its virtual appliances available on Google Cloud Platform. It has also worked on its ability to work with continuous integration tools, and has made significant updates of its management API, improving the ability for Barracuda WAF to be deployed programmatically.

Barracuda is a good shortlist contender for midsize enterprises and existing Barracuda customers. It offers interesting solutions for organizations in North America and Europe, developing a multicloud strategy.

STRENGTHS

- Offering Strategy: Barracuda remains one of the most visible WAFs on Microsoft Azure. Customers are then more likely to select Barracuda in multicloud strategy for unified management.
- Pricing Strategy: Barracuda Cloud WAF as a Service includes DDoS protection at no additional charge.
- Product Offering: With the release of the WAF appliance 1060, Barracuda now supports throughput as high as 10 Gbps.
- Technical Support: Gartner clients across multiple regions give excellent scores to Barracuda's customer support. Barracuda partners cite the vendor's focus on customer satisfaction as the reason they choose to sell Barracuda WAF.
- Capabilities: Barracuda's offer of the free WAF add-on Vulnerability Remediation Service is attractive to Barracuda's targeted small or midsize business (SMB) customers, which often lack the time, money and expertise to support an in-house application scanning program.

CAUTIONS

- Sales and Marketing Execution: Barracuda struggles to adapt to the multiplication of meaningful competitors. Its visibility in shortlists is shrinking, and the vendor has lost market share during the past 12 months.
- Customer Experience: Many customers have complained about Barracuda's WAF appliance user interface (UI). They cite a long learning curve, difficulties locating features buried in submenus and longer-than-necessary amounts of time spent updating the configuration.
- Market Responsiveness: Barracuda has been late to the market in providing cloud WAF as a service. Prospects should scrutinize the vendor's infrastructure and point-of-presence availability across regions, as well as investigate the vendor's ability to meet enterprise-class SLAs for availability, because the solution remains a recent addition.
- Capabilities: Despite recent improvements, Barracuda WAF lags behind the leaders in bot mitigation and advanced analytics for anomaly detection. Its predefined list of good bots is limited to a few search engines.
- Capabilities: Barracuda WAF lacks access management features and support for Oauth.
- Capabilities: Barracuda WAF lags behind the leaders in security monitoring. It lacks automated alert aggregation in the real-time log view, and users report that they would like to see more improvements.

Amazon Web Services

Amazon Web Services (AWS) is in the Niche Players quadrant. It serves almost exclusively AWS clients, and invests significantly in continuous improvements to its WAF solution.

AWS is a subsidiary of Amazon, based in Seattle, Washington. It is a cloud-focused service provider. It offers a large portfolio of cloud workloads (EC2), online storage (S3, EBS and EFS), database, and artificial intelligence (AI) frameworks. Its security portfolio is not as well-known, but includes identity and access management (IAM; Cognito), managed threat detection (GuardDuty) and HSM (AWS Cloud HSM). AWS Shield provides managed DDoS protection, and its WAF product is simply called AWS WAF.

AWS WAF can be delivered through AWS Application Load Balancer or through Amazon CloudFront as part of the CDN solution. AWS WAF is not limited to protecting origin servers hosted on Amazon infrastructure. AWS also partners with WAF vendors and offers their solutions in the AWS marketplace.

In recent months, AWS has released managed rules, a feature that allows clients to deploy sets of rules managed by third-party WAF vendors. The vendor has also recently released AWS Firewall Manager, which allows it to centralize the deployment of WAF policies and managed rules set. Also, AWS Config, the vendor's configuration monitoring service, can monitor AWS WAF rule sets (RuleGroup).

AWS customers looking for an easy way to add runtime protection in front of their applications hosted on AWS should consider deploying AWS WAF, especially when combined with AWS Shield, and with one, or multiple, set of managed rules.

STRENGTHS

- Capabilities: With managed rulesets, AWS customers have access to more than a dozen sets of rules from established WAF or managed security service (MSS) vendors that are automatically updated. Because they can deploy multiple rulesets simultaneously, it is easy, even if it comes at a cost, to provide multiple layers of defense, or to test multiple providers.
- Customer Experience: Existing AWS customers appreciate being able to quickly deploy and enable AWS WAF. Customers give good scores to the autoscaling and built-in integration with Cloudfront.
- 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.
- Roadmap Execution: AWS continues to regularly improve its WAF, releasing relevant features to close existing gaps, such as the recent firewall manager, at the time they are announced.
- Sales Execution: AWS WAF is integrated in AWS Shield Advanced. For customers not using AWS Shield Advanced, AWS charges per use for AWS WAF are based on how many rules customers deploy and how many web requests are inspected.

CAUTIONS

- Marketing Strategy: AWS WAF's reach is mainly limited to AWS workload protection, where it competes with cloud WAF services and virtual appliances. As more clients consider a multicloud strategy, AWS WAF is less likely to be on WAF shortlists.
- Capabilities: AWS WAF lacks bot detection techniques, relying on reputation-based controls. Customers need to deploy AWS API Gateway to get dedicated API security features, because AWS does not parse JavaScript Object Notation (JSON) or XML. The vendor does not offer managed SOC for AWS WAF as part of its SiteShield managed services offering. Its DDoS Response Team (DRT) focuses on DDoS response only.
- Product Strategy: Despite numerous corporate security initiatives, the WAF product remains mostly a siloed product. The vendor does not yet have a dedicated threat research team to add new protections to the WAF. AWS WAF does not leverage AWS AI capabilities, the use of machine learning for web app security is built-in only for DDoS protection.
- Customer Experience: Customers would like to be able to whitelist a specific rule from the managed ruleset. Currently, they can only disable the entire ruleset, and have trouble identifying why a rule was triggered.
- Customer Experience: Clients cite logging and reporting as a weakness. They cannot get detailed logging, aggregated events and mention occasional delays in getting the logs. Some clients also request integration with SIEM.

Information is gathered from https://www.gartner.com/doc/reprints?id=1-5ELTARA&ct=180904&st=sb