Gartner has just released the 2018 Magic Quadrant for Web Application Firewalls

**Gartner has named Imperva a Magic Quadrant Leader in Web Application Firewalls (WAF) for the fifth year running.**

Gartner has named Imperva as a Leader in their 2018 Magic Quadrant for Web Application Firewalls (WAF) — for the fifth year in a row. The combination of on-premises appliances, cloud WAF, threat intelligence and flexible licensing has solidified Imperva once again as the best choice for companies to protect their websites with complete confidence.

![2018 Magic Quadrant for Web Application Firewalls](image)

= Change from 2017 Placement
Comparison 2017 vs. 2018:

- Imperva is a leader in Gartner Magic Quadrant for Web Application Firewalls for 5 years in a row!!!
- F5 is not a leader in Gartner Magic Quadrant for Web Application Firewalls anymore
- Ability to execute (Y-axis): Both Imperva and Akamai declined while AWS made significant gain
- Completeness of vision (X-axis): Imperva and F5 decreased while Akamai, Fortinet, Cloudflare & Barracuda made slight gains
- In 2018 there were 16 vendors and in 2018 there are 14 vendors in the quadrant
- New additions — Oracle and Microsoft
- Removed — Positive Technologies, NSFOCUS, Venustech and Penta Security Systems

The MQ shows that we are still way ahead of our competition and Gartner specifically cites the following strengths behind the evaluation:

- **Marketing Strategy:** Imperva offers 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 continue to praise Imperva customer support. They’ve noted some improvements in Incapsula’s bot mitigation.
- **Capabilities:** Incapsula and SecureSphere both benefit from the shared threat intelligence from ThreatRadar
- **New Product Releases:** 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 Asia/Pacific region.

Gartner’s recognition for five consecutive years solidifies Imperva as the best choice to protect companies’ websites with confidence. However, competitors may try and use specific points in the MQ to position themselves. The following provides guidance on addressing how some of our main competitors - Akamai, F5 and Cloudflare - will likely position themselves.
Akamai
Akamai remains in the leaders quadrant for two years in a row. However, in both ability to execute and completeness of vision, they lag behind Imperva. Gartner is very clear in its cautions regarding Akamai:

- “Akamai’s WAF is available as a cloud service only.”
- “Akamai Kona is an expensive product, especially when bundling multiple options, such as Bot Manager subscriptions.”
- “Akamai lacks a positive security model.”
- “Customers using WAP cannot use Bot Manager.”
- “Clients frustrated by a dated policy and no useful way to test the updated rules.”
- “The less-expensive WAP solution has not yet fixed” Akamai’s pricing issue.

Contrast this with Imperva’s strengths cited above, plus:

- Gartner cited “flexible licensing for organizations with a mix of on-premises and cloud-hosted applications.”
- Imperva total cost of ownership is less expensive.
- Imperva WAFs use both positive and signature based security models. Dynamic application profiling provides the ability to automatically learn application behavior.
- Imperva cloud WAF includes bot management and Gartner cited “customers noted improvements in Incapsula bot mitigation.”
- Imperva WAF is available as an on-premises appliance, cloud WAF service, and also offered in AWS and Azure.

F5 Networks
F5 has managed to move out of the leaders quadrant. It was in the Leaders quadrant for only one year. This was mostly due to lack of progress made in the cloud WAF segment.

Gartner believes F5’s completeness of vision significantly decreased for the following reasons:

- F5 does not yet provide a fully-featured, and easy-to-manage self-service WAF.
- Gartner analysts see cloud WAF market share as a missed opportunity for F5’s product strategy and note it is a current portfolio gap.
- With their Advanced WAF, customers fail to get the best security features, even when purchasing the “best” bundle, needing an additional security license upgrade.
- Silverline’s infrastructure significantly lags behind its direct competitors.
- Many customers mention the need for a UI refresh, because it can be complex.
- Gartner analysts observe limited adoption of Silverline products, and low visibility in cloud WAF shortlists.

Contrast this with what Gartner says about Imperva:

- Imperva cloud WAF is a full-featured and easy to manage WAF. Imperva offers managed security services as well.
● Imperva cloud WAF is significantly growing and Imperva is continuing to invest heavily in its cloud based offering.
● Imperva offers flexible licensing with a mix of on-premises and cloud-hosted applications.
● Imperva recently announced a 10 second SLA for DDoS mitigation.
● While F5 customers have been complaining about UI for the last two years, Imperva has recently released Attack Analytics to get unified and improved monitoring for SecureSphere and Incapsula. It also made available a first version of role-based administration for Incapsula.
● Imperva cloud WAF has 6,500+ enterprise customers.

Cloudflare
Still in the Challengers quadrant, Cloudflare has actually seen their ability to execute decrease in Gartner rankings. Gartner points out several flaws in Cloudflare’s WAF:
● “Cloudflare can’t address use cases that require on premises physical or virtual appliances.”
● “Many customers, especially the larger organizations, rated Cloudflare alert and reporting low.”
● “Cloudflare lacks an automated aggregation of alerts for faster incident triage.”
● “Some customers complain of a higher-than expected frequency of local performance degradation.”
● “Cloudflare’s management console presents restrictions on offering more-granular configuration capabilities, such as building custom-made rules.”
● “Captcha remains the most frequent technique Cloudflare uses to block bots. This hurts the user experience.”
● “Cloudflare’s security roadmap appears to aim at good-enough security, with a focus on pervasive, commercial off-the-shelf (COTS) web applications (e.g., WordPress and Magento).”
● “When it comes to using new protection techniques based on in-house threat research, the vendor is less proactive than its leading competitors.”
● “The WAF also lacks an automated positive security model.”

Imperva strengths cited by Gartner to use against CloudFlare include:
● “Imperva 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.”
● “Imperva has recently released Attack Analytics to get unified and improved monitoring.”
● “Incapsula and SecureSphere benefit from the shared threat intelligence from ThreatRadar.”
Managing Gartner “Cautions” for Imperva

Guidance for handling customer questions on Imperva “cautions” are as follows:

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.

- The new leadership put in place a well-defined three-year strategy that addresses our customers on-premises, cloud-based and hybrid security needs. This includes the SecureSphere product line to protect on-premises environments.
- Imperva released Attack Analytics in May 2018. It combines security events from both SecureSphere and Incapsula to present distinct narratives.

Customers wish that Incapsula supported SSO features, such as SAML 2.0. They also would like better and more-flexible canned reports.

- Imperva consistently takes customer feedback into account to add new features.
- SSO features, such as SAML 2.0 and ADFS are in the roadmap for 4Q18 or 1Q19.

Customers considering Incapsula to replace SecureSphere often notice the lack of feature parity. The cloud WAF service cannot match yet the depth and breadth of security function covered by the appliance product line.

- Incapsula and SecureSphere security features are evolving based on customer needs.
- Customer needs for cloud-based and on-premises WAF are not exactly the same.
- The added value and feature parity comes from Attack Analytics (unified event management).

Several Gartner clients cited higher-than-competition prices for Imperva SecureSphere WAF, and to a lesser extent for Incapsula.

- Imperva SecureSphere WAF appliances are designed for high-end enterprise data centers.
- SecureSphere WAF is available as virtual appliances and in public cloud (AWS and Azure) at lower price points.
- Compared to Akamai, the only other leader in the MQ, Imperva total cost of ownership is lower.

Customers would like to see integration between Attack Analytics and the WAF management consoles, and more-unified management capabilities between SecureSphere and Incapsula.

- Attack Analytics is integrated within unified management console. Attack Analytics can also be launched directly from WAF management consoles.
• Unified Management: Cloud-based portal that will provide visibility into all WAF instances
  – SecureSphere, Incapsula, AWS, Azure and ThreatRadar. Imperva is committed to add
    several new unified management capabilities in the coming quarters based on customer
    feedback.
  – Some of the unified management console (UMC) highlights:
    o Customer interfaces with the UMC; by UI (desktop/mobile) or by API (unified
      gateway).
    o UMC lets customers visualize and configure all Imperva products and service on-
      premises, public-cloud-hosted or consumed as a service including edge services.
    o With unified management logs, security events and other telemetry are
      consolidated to one unified set of data-centric services.

Surveyed customers and resellers indicated that they did not get the same quality of support for
Incapsula compared to what they are used to with Securesphere.

• In 2018, Imperva successfully completed the migration from a shift-based support centered
  in Rehovot, to a full time “follow-the-sun” model with locations based in Dallas, Redwood
  Shores, Singapore, Israel and (soon to be) Belfast. Additional full time support engineers
  with advanced degrees in Networking have been the focus of this hiring and are showing
  great success/Improvement across all areas of the Cloud WAF and DDoS space.

Other Frequently Asked Questions

Q. Should I share this report with customers and prospects?
   A. Absolutely. Imperva continues to lead in the Magic Quadrant.

Q. How should I position this report with customers and prospects?
   A. Organizations are under tremendous pressure because:
      • Web app attacks are the #1 cause of data breaches
      • Changing trends – cloud migration and DevSecOps
      • Event overload – False positives and many events

Position Imperva strengths:
• Imperva frequently wins on the basis of security features and innovation
• 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
• Better manage the transition from WAF appliance to cloud WAF service
- Imperva offers flexible licensing for organizations with a mix of on-premises and cloud-hosted applications
- Imperva has recently released Attack Analytics to get unified and improved monitoring for SecureSphere and Incapsula

Q. How can I make the report available to customers or prospects?
A. Simply and only provide this link to anyone who wants to view the 2018 Gartner MQ Report.

Q. Will Imperva promote the MQ via other marketing channels?
A. Absolutely. Imperva is promoting the MQ on our own website, through our blog, via email and social media, via partners, and a variety of media channels.

Q. How can I use my social media accounts to promote this report?
A. We encourage you to post the following Gartner approved text using #GartnerMQ or #LeadersQuadrant hashtags from your personal Twitter account.

Suggested Social Media Posts [LINK] = https://www.imperva.com/resources/resource-library/reports/magic-quadrant-for-web-application-firewalls/

Twitter

Is a 5x MQ Leader for WAF securing your apps? @Gartner_inc named #Imperva a Leader for Web App Firewalls. Again.

Your apps are safer in our corner. #Imperva named WAF #MagicQuadrant Leader for 5 straight years

LinkedIn

We’ve secured leadership in the Magic Quadrant for 5 years running. Improving our best-in-class app security never gets old. Read the 2018 Gartner MQ WAF report. In case 4 years of WAF Leadership wasn’t enough. Trust a 5x Gartner Magic Quadrant Leader. Read the 2018 Gartner MQ WAF report.

Facebook

The 2018 Gartner Magic Quadrant for WAF report is out. Say Imperva five times fast. Read the Gartner report.

The Gartner WAF Magic Quadrant has a five-time leader. That’s #AppSecurity
Q. Can I create my own marketing collateral using the MQ?
   A. No. Gartner has very strict restrictions on use/promotion of the MQ. Violating these restrictions can result in Gartner revoking Imperva’s right to use the MQ entirely.