Intelligent Security
Starts at the Edge

Akamai Recognized in the
Gartner 2019 Magic Quadrant
for Web Application Firewalls
The Gartner 2019 Magic Quadrant for Web Application Firewalls is the latest release of Gartner’s annual unbiased assessment of major web application firewall (WAF) vendors. This year, Gartner analysts evaluated 12 vendors based on their completeness of vision and ability to execute.

For the third year in a row, Gartner has named Akamai a Magic Quadrant WAF Leader.

“The Leaders quadrant contains vendors that can shape the market by introducing additional capabilities in their offerings, raising awareness of the importance of those features and being the first to do so. They also meet the enterprise requirements for the different use cases of web application security.

“We expect Leaders to have strong market share and steady growth, but these alone are not sufficient. Key capabilities for Leaders in the WAF market are ensuring higher security and smooth integration in the web application environment. They also include advanced web application behavior learning; a superior ability to block common threats (such as SQLi, XSS and CSRF), protect custom web applications and avoid evasion techniques; and strong deployment, management, real-time monitoring and extensive reporting. They should also provide and regularly improve DDoS and bot mitigation capabilities. In addition to providing technology that is a good match with customer requirements, Leaders exhibit superior vision and execution for anticipated requirements and evolution in web applications that require paradigm changes.”

Why WAFs Are So Important

To stay competitive in today’s interconnected world, enterprises are deploying an ever-increasing number of public-facing applications — web applications, APIs, API-driven mobile apps, and IoT devices, to name a few.

This leads to greater complexity, more risk, and a broader attack surface. Sure enough, malicious actors have noticed.

In Akamai’s July 2019 State of the Internet / Security report, we reported observing nearly 4.5 billion web attacks during the 18-month period from November 2017 through April 2019.

That figure actually belies the rise in the number of average daily attacks during that period. Between November 2018 and April 2019, the daily average rose to more than 10 million. Three days had more than 30 million attacks — and on one day there were about 40 million attacks.

Unlike a regular firewall, which only serves as a safety gate between servers, a WAF is an application security measure that is located between a web client and a web server. It inspects HTTP traffic before it reaches your application, and protects your server by filtering out threats that could damage your site functionality or compromise data. This WAF functionality is crucial to protect against rapidly emerging web security threats.

Akamai Recognized in the Gartner 2019 Magic Quadrant for Web Application Firewalls
Akamai Recognized in the Gartner 2019 Magic Quadrant for Web Application Firewalls

A WAF protects against malicious attacks, such as SQL injection, malicious file execution, and cross-site scripting. These threats can penetrate and cripple a website, diminishing performance and exposing your enterprise to data breaches. They target multiple types of functionality within your site, attacking the site itself or forwarding logic to a database where the information stored inside it can be compromised.

The need for this protection is driving an ever-greater demand for WAF products as security leaders look to reduce the threat profile of their apps and APIs.

WAF Becoming a Cloud Service

Gartner expects that “by 2022, web application firewall (WAF) hardware appliances will represent fewer than 10% of new WAF deployments, which is a decrease from today’s 30%.”

On the other hand, Gartner expects growth in cloud WAF deployments. “By 2023, more than 30% of public-facing web applications and APIs will be protected by cloud web application and API protection (WAAP) services, which combine distributed denial of service (DDoS) protection, bot mitigation, API protection and WAFs. This is an increase from fewer than 10% today.”

Akamai’s Approach to WAF Services

At Akamai, we see these trends as further validation of our belief that cloud solutions have the scale and flexibility that enterprises need to thwart today’s ever-evolving threat landscape – qualities that are limited in on-premises WAFs.

Enterprises should note that using a cloud WAF provides a scalable platform that can be accessed globally, helping to protect against multiple threats for large web applications around the world.

Cloud solutions have Internet-wide visibility, so they can achieve more complete threat awareness. In fact, Akamai built its WAF products, Web Application Protector and Kona Site Defender, on the world’s largest cloud delivery platform: the Akamai Intelligent Edge, with more than 250,000 servers in 2,300 points of presence around the globe.

This gives Akamai an unparalleled combination of enormous scale and visibility into the ever-changing threat landscape. As a result, our WAF products are designed to help customers:

• Reduce the risk of downtime, data theft, and security breaches
• Scale to protect against the largest DoS and DDoS attacks
• Ensure high performance even during attacks
• Defend against new and emerging threats
Conclusions

The Gartner 2019 Magic Quadrant for Web Application Firewalls presents information to assist organizations in evaluating how WAFs can provide improved security that is easy to consume and manage, while respecting data privacy requirements.

SOURCES

1) Gartner, Magic Quadrant for Web Application Firewalls, Jeremy O’Hoinne, Adam Hils, Claudio Neiva, Rajpreet Kaur, 17 September 2019

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Akamai is currently offering complimentary access to the full report.

Read It Now