EXECUTIVE SUMMARY

Buyers Confront Stark Choices as Web Application and API Security Market Grows, Evolves

Gartner Names Akamai a Leader in Its 2022 Gartner® Magic Quadrant™ for Cloud Web Application and API Protection

Cybersecurity professionals are under intense pressure as web application and distributed denial-of-service (DDoS) attacks surge and ransomware proliferates. Web application and API security, in particular, have taken on greater importance in recent years with a rise in targeted attacks. As this is happening, security teams are being stretched thin and are confronting an increasingly complex application ecosystem as web applications rely on a multicloud environment.

The financial services sector offers a useful proof point for just how pernicious web application and API attacks have become. In November 2022, Akamai research found that web and API attacks against financial services companies had increased 257% over the previous 12 months as attackers continued to leverage zero-day vulnerabilities.

This surge in attacks can be attributed to several attack vectors, including local file inclusion and cross-site scripting, which attackers use to gain a foothold in the network. This makes securing web apps and APIs more important than ever, since once attackers have leveraged these vulnerabilities, they can then be used as an entry point to breach target organizations. In response, cybersecurity professionals are increasingly turning to vendors that provide a single offering to meet all of their web application and API security requirements. We think the 2022 Gartner® Magic Quadrant™ for Cloud Web Application and API Protection report is a valuable resource in helping these security professionals make purchasing decisions.

When it comes to evaluating the market for web application and API protection (WAAP) technology, companies now have more comprehensive and more complex WAAP needs. Buyers now need to consider vendors that, at a minimum, offer four core capabilities: web application firewall, DDoS protection, bot management, and API protection.

However, that is just a starting point. Most organizations should expand their requirements to include a much broader set of features as well. In its report, Gartner recommends buyers also consider the following capabilities:

- Client-side protection
- Vulnerability scanning
- Mobile app security
- DNS services and DNS security
- Content delivery network (CDN), load balancing, access management, and other features
- Protection against web defacement

The market evolves

While WAAP purchases historically tended to focus on appliances — and even now some organizations are buying appliances as replacement purchases — cloud WAAP deployments have come to predominate. According to Gartner, that's only going to continue.

"By 2024, 70% of organizations implementing multicloud strategies for web applications in production environments will favor cloud web application and API protection platform (WAAP) services over WAAP appliances and IaaS-native WAAP," Gartner predicts in the report.

Gartner® Peer Insights™ review. Submitted Apr 7, 2022:

> "Akamai AAP is a fully-featured WAF, including web attack detection, ddos protection, bot management and api protection. In addition to the outstanding production, the service team is quite professional and quick in response."
>
> — IT security and risk management professional in IT services industry

Gartner® names Akamai a Leader in its WAAP Magic Quadrant™ report

In the Gartner® Magic Quadrant™ for Cloud Web Application and API Protection, Gartner evaluated 11 different vendors across 15 different criteria and placed Akamai in its Leaders Quadrant™. In previous years, Gartner has published a similar report — the Magic Quadrant™ for Web Application Firewalls. Between the two reports, Akamai has now been named a Leader six consecutive times.

Within the 2022 Gartner report, Akamai was positioned highest for its "ability to execute" and furthest for its "completeness of vision."

> "With Akamai, we get access to the latest and greatest technologies sooner, at less cost and with less risk than if we invested to develop them internally."
>
> — Russ Soper, CIO of Customer Technology and Operations, Finastra

Akamai's take on the WAAP market

Akamai App & API Protector delivers a full suite of WAAP products — including web application firewall, bot mitigation, API security, and DDoS protection — that work closely together, providing customers with a holistic view of their security posture. And it has for years. Akamai's proven track record in the market is reflected in Akamai's Leadership positions in reports by other analyst firms.

For example, security teams need to remain vigilant against DDoS attacks and, within the Akamai suite, DDoS protection remains a core competency. In How to Respond to the 2022 Cyberthreat Landscape, Gartner cautions that organizations should expect attackers to "combine ransomware with other techniques, such as distributed denial of service (DDoS) attacks, to force public-facing services offline until organizations pay a ransom."

Similarly, we think Akamai simplifies the maintenance of APIs with advanced API capabilities that automatically discover a full range of known, unknown, and changing APIs across web traffic, including their endpoints, definitions, and traffic profiles.

Akamai's strengths go beyond its core WAAP products, however. Akamai's scale and long history in the market, with scores of enterprise customers, gives it an advantage over niche competitors, allowing the company to respond rapidly to emerging threats, both with product releases and internal expertise. In particular, the Akamai Intelligent Edge Platform is the world's largest content delivery network. Its thousands of edge servers in 134 countries give Akamai enormous visibility into emerging global threats. With these resources, Akamai is able to analyze 300 TB of attack data daily. The company also boasts more than 330 data security experts working to protect customers. This allows Akamai to provide services in more places and deflect threats closer to their point of origin.

Meanwhile, the Akamai Adaptive Security Engine that powers Akamai's WAF products automatically analyzes changes to the environment, internet traffic patterns, and the global threat landscape. Adaptive Security Engine then calculates a threat score to make or recommend modifications to an organization's tuning parameters. Customers can then customize rulesets to suit their business needs.

Download the full report, compliments of Akamai

The market for WAAP continues to evolve as enterprises add applications and APIs to support their ongoing cybersecurity needs.

For this report, Gartner evaluated 11 vendors that met their criteria for inclusion. If you're a security professional, you'll want to know more about those criteria and see the evaluations of these 11 vendors. We think it can be an important starting point in your search for a WAAP vendor to meet your needs.

> "By 2026, 40% of organizations will select a WAAP provider on the basis of its advanced API protections and web application security features — up from less than 15% in 2022."
>
> — 2022 Gartner® Magic Quadrant™ for Cloud Web Application and API Protection

Get the report

Visit akamai.com

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. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, MAGIC QUADRANT and PEER INSIGHTS are registered trademarks of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.