Market Guide for Cloud Web Application and API Protection

Published 13 November 2023 - ID G00788949 - 25 min read

By Analyst(s): Dale Koeppen, Aaron McQuaid, Adam Hils, Rajpreet Kaur

Initiatives: Infrastructure Security; Build and Optimize Cybersecurity Programs; Security of Applications and Data

Cloud web application and API protection platforms provide protection from a broad range of sophisticated runtime attacks. Security and risk management leaders can use this Market Guide to analyze the cloud WAAP market and select solutions that meet their organization's needs.

Additional Perspectives

- Invest Implications: Market Guide for Cloud Web Application and API Protection (15 November 2023)

Overview

Key Findings

- API protection and security is now a primary interest and driver in the process of selecting cloud web application and API protection (cloud WAAP) solutions.
- Cloud WAAP provided as a service is now the dominant form factor to consider when selecting and acquiring WAAP services.
- The cloud WAAP market continues to suffer from excessive false positives and is driving a trend toward the adoption of artificial intelligence/machine learning (AI/ML) support to correlate and reduce alert fatigue and produce actionable events.
- Bot maturity and success rates are outpacing the capabilities of cloud WAAP bot management and protection. Advancement in bot technology shows that a sophisticated bot is now better at bypassing CAPTCHAs than humans.

Recommendations

- **If API security is the key factor for selecting WAAP services:** Prioritize vendors with strong API discovery capabilities and security beyond basic payload parsing and signature-based protections.
- **When selecting a cloud WAAP provider:** Prioritize requirements such as data sovereignty, cloud WAAP points of presence (POPs) availability, routing optimization and failover capabilities.
- **When selecting a cloud WAAP solution:** Prioritize cloud WAAP solutions that:
  - Leverage AI/ML and large language models (LLMs) to reduce alert fatigue, provide common language interpretation of events and identify advanced threats.
  - Gather multiple signals to validate real users and introduce advanced capabilities such as proof-of-work challenges to combat modern threats, such as CAPTCHA bypass by bots.

Strategic Planning Assumptions

By 2026, 40% of organizations will select a WAAP provider on the basis of its advanced API protection and web application security features, up from less than 15% in 2022.

By 2026, more than 40% of organizations with consumer-facing applications that initially relied only on a WAAP for bot mitigation will seek additional anomaly detection technology from specialized providers, up from less than 10% in 2022.

Market Definition

This document was revised on 16 November, 2023. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Gartner defines cloud WAAP as a category of security solutions designed to protect web applications irrespective of their hosted locations. Typically delivered as a service, cloud WAAP is offered as a series of security modules that provide protection from a broad range of runtime attacks. It offers protection from the Top 10 web application security risks defined by the Open Web Application Security Project (OWASP) and automated threats, provides API security, and can detect and protect against multiple sophisticated Layer 7 attacks targeted at web applications. Cloud WAAP's core features include web application firewall (WAF), bot management, distributed denial of service (DDoS) mitigation and API protection.

Market Description

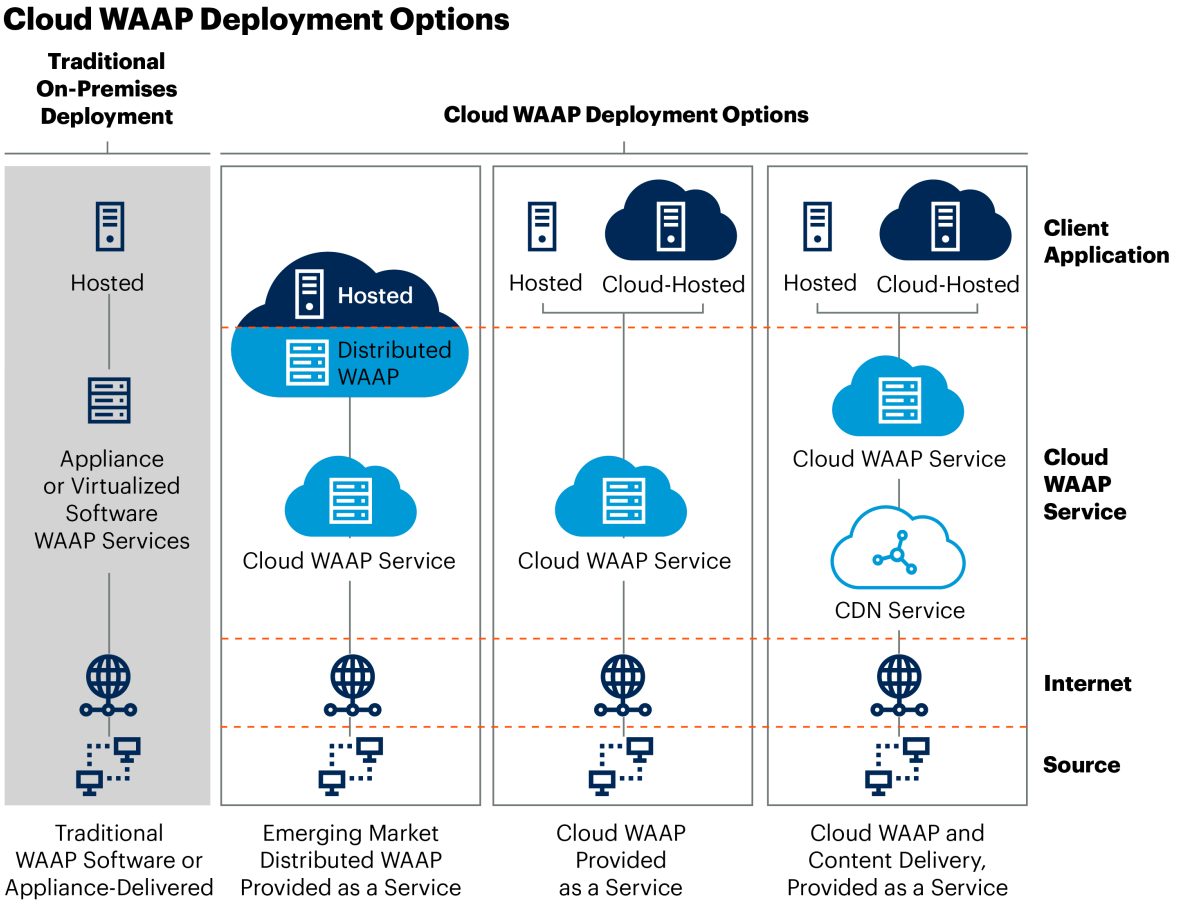
Cloud WAAP offerings are typically sold and delivered by technology providers as a service from the cloud. Based on end-user requirements, cloud WAAP solutions are provided through a deployment provided, managed and delivered by the cloud service. Physical WAAP appliance sales have declined to low single-digit growth, but they remain relevant to certain use cases. Most cloud WAAP vendors have prioritized a roadmap for a cloud-delivered approach.

The major drivers in the cloud WAAP market are the evolution of cloud hosting and the changing landscape of hybrid environments for enterprise applications. Now, a new kind of need for cloud infrastructure has emerged with consumers favoring on-premises cloud infrastructure environments because clouds are easy to consume and manage. The architectural synergies that exist between a cloud WAAP solution and the associated content delivery network (CDN) simplify the deployment of cloud applications.

Cloud WAAP solutions are typically provided via two distinct offerings (Figure 1):

- Stand-alone cloud WAAP — cloud-delivered services without a CDN. This kind of service is provided as a SaaS offering delivered by the cloud without directing the traffic through a private CDN.
- Cloud WAAP paired with CDN — cloud-delivered services with a CDN. This kind of service is provided through a group of geographically distributed points of presence that speed up the delivery of web content by bringing it closer to where users are located.

Figure 1: Cloud WAAP Deployment Options



Source: Gartner
788949_C

Gartner

Some cloud WAAP solutions provide WAAP services combined with CDNs, which enables high availability and performance by distributing the services in areas where end users are located. These CDNs act as an intermediary between source users and destination applications which direct traffic through core cloud WAAP and scrubbing services. It should be noted that organizations that choose not to utilize a cloud WAAP vendor's CDN may inadvertently limit their access to critical security features.

Cloud WAAP solutions become a logical choice for organizations that aim to protect natively built cloud applications because cloud WAAP solutions are easier to deploy and scale from an infrastructural perspective than their traditional appliance-based counterparts. However, cloud WAAP solutions still face the same operational challenges as traditional WAAP solutions with a higher-than-average operational touchpoint because they are prone to a high level of false positives. Cloud WAAP solutions delivered by vendors through private cloud offerings (such as CDNs) are highly scalable and provide centralized management and visibility with tight integrations with cloud hyperscalers.

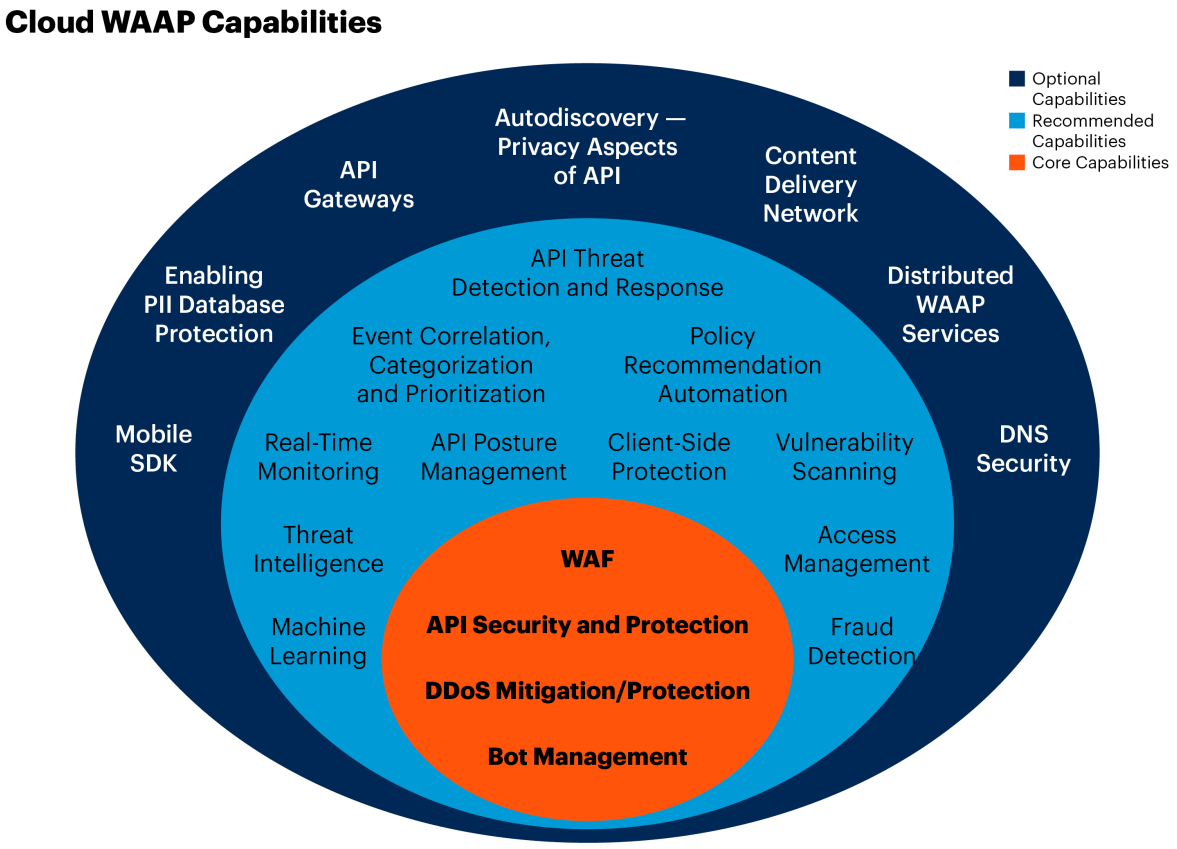
Cloud WAAP offers a series of core and required features through a traffic-processing engine, including:

- **Web application firewall (WAF).** It is mainly focused on exploit mitigations, such as injection attacks (cross-site scripting [XSS] attacks and SQL injection attacks) and application-level denial of service (DoS).
- **Distributed denial of service (DDoS) protection.** This provides protection against volumetric attacks (traffic flooding) and application-level attacks (which could include protocol, programmatic and computational attacks) or a combination of both that prevents services and application operations. These attacks leverage multiple points of presence and adopt large bandwidth provisioning techniques. (Some vendors also offer dedicated scrubbing centers and Layer 7 application DoS prevention to divert traffic away from targets.)
- **Bot mitigation.** This involves detection and mitigation, if necessary, of automated connections. It also includes user credential abuse attacks which are frequently automated, such as brute forcing, account takeovers and credential stuffing.
- **API protection.** In the past, this was often limited to JSON and XML payload processing as well as GraphQL parsing. Today, there is more focus on API posture management and API usage thresholds. Automated API traffic pattern learning (an emerging capability among WAAP offerings), or integration with API definitions such as the OpenAPI Specification (OAS) previously known as the Swagger Specification, may help provide a positive security model (default deny) for APIs.

Gartner's definition of cloud WAAP states that all four core capabilities must be provided within a single platform or offering. This is also applicable to vendors that provide distributed cloud WAAP services. All four capabilities described in the above list must be provided as a service from the cloud.

The following figure lists the core, recommended and optional capabilities end users should seek when selecting a cloud WAAP solution.

Figure 2: Cloud WAAP Capabilities



API = application programming interface; DDoS = distributed denial of service; DNS = Domain Name System; PII = personally identifiable information; SDK = software development kit; WAAP = web application and API protection; WAF = web application firewall

Source: Gartner

788949_C

Gartner

Market Direction

Gartner has seen a stagnation in the volume of calls from end users about WAAP and cloud WAAP solutions, with less than a 5% increase in calls from July 2022 through July 2023, while overall security calls have increased. [1] This would indicate that the WAAP market is not dynamic, end users and consumers have a better understanding of the market, and the WAAP technology is well adopted.

The current WAAP market has seen a consolidation of point solutions into broader platforms and continues to see larger vendors buying point solutions to round out their platform offerings. The cloud has brought new entrants into the market as cloud services can be hosted anywhere and protect applications hosted anywhere. Therefore, traditional appliance vendors are increasingly challenged by vendors that offer edge computing and CDN services as well as regional vendors expanding their services beyond their geographical regions.

Gartner has seen very little research and development (R&D) conducted to grow the traditional WAAP market. The traditional WAAP technology has stagnated for three to four years, and traditional WAAP services face the challenge in adopting a cloud-native delivery model. As a result, the market for cloud-delivered WAAP is seeing some further development and growth as end consumers require more mature and advanced protections for modern cloud-delivered applications. This is especially notable with cloud WAAP vendors providing more advanced capabilities for API threat detection and response.

Gartner still sees interest across all verticals and geographics in cloud WAAP, and most Gartner clients leverage a cloud WAAP solution to protect their web and API applications, irrespective of where their applications reside.

The following are some scenarios for nonspecific use cases:

- Clients wish to protect web and API applications or systems hosted within an infrastructure as a service (IaaS) or platform as a service (PaaS) architecture.
- Vendors or service providers that provide cloud-based SaaS services require their SaaS services to be protected.
- Clients wish to protect their web and API applications hosted in a private or on-premises environment, yet require cloud WAAP and CDN services to protect their applications and systems.

Many of today's modern applications are designed to operate in cloud environments. They leverage native-cloud infrastructure and services which make use of serverless computing, containers and microservices to achieve scalability, flexibility and high availability (see How to Modernize Your Application to Use Cloud-Native Architecture).

Modern software development has moved away from monolithic application designs and toward modern cloud-based applications that are developed and built with microservices architectures and APIs which allow these applications to communicate with each other and with public-facing services. These public web applications and the associated APIs become high-risk systems for businesses and priority targets for threat actors to search for possible vulnerabilities to exploit.

API protection has become a primary interest in the process of selecting a cloud WAAP solution. A WAF focuses on protecting the web-based front end of an application, whereas API protection puts emphasis on securing the API hooks that often power these web applications. Modern web applications heavily rely on APIs to communicate with back-end services, databases or other systems. Security and risk management leaders will require these APIs to be secured due to their considerate significance to the business by establishing a stronger security posture for selected web applications.

APIs exposed on public-facing assets increase the attack surface, and are priority targets for malicious actors. These exposed APIs often lead to sensitive data exfiltration, business logic flaws such as unauthorized access and possibly API DoS attacks, all of which can disrupt service availability.

Protecting APIs from various types of attacks is a top priority and a critical consideration when selecting a cloud WAAP solution, and is essential for maintaining the integrity, availability and confidentiality of web applications. The characteristics of modern applications and the significant growth in the number of cloud-native web applications and APIs have organically expanded attack surfaces. This is driving enterprises to defend against the associated threats and is influencing their need to adopt cloud WAAP solutions.

The following are some of the advantages that cloud WAAP services have over traditional appliance-based WAAP services:

- Integration as part of the continuous integration/continuous deployment (CI/CD) pipeline and development life cycle of applications, such as information sharing between real-time stand-alone tools like cloud-native application protection platforms (CNAPPs) and cloud WAAP solutions.
- API protection with automated API discovery, specific API threat protection and behavioral API anomaly detection.

- CDN and private cloud scrubbing services which are needed to mitigate DDoS threats that can't be dealt with by on-premises appliance solutions alone.
- Ease of consumption through a centralized cloud-based management console, tremendously simplifying the administration of various geographically dispersed appliances.
- Colocation of controls and services in either the cloud security infrastructure or the CDN infrastructure.
- The ability of cloud-based offerings to easily protect on-premises and cloud-based workloads, which CDN-based offerings excel at. Appliance-based offerings often struggle to protect cloud-based workloads due to the difficulties of managing and deploying appliances in public IaaS and PaaS environments.
- Autoscaling that cloud-delivered solutions provide, but many appliance-based solutions do not.
- Global scalability and geographic availability that cloud-delivered solutions support. Appliance-based solutions require manual scaling by adding more appliances.

Market Analysis

Based on Gartner client inquiries and end-user feedback, cloud adoption is now generally mainstream with most organizations having adopted some type of cloud service or delivering their services from the cloud. Many organizations have shifted their once publicly exposed applications from on-premises environments to cloud-provided environments, which offer greater scalability, elasticity and manageability while mitigating risks associated with technical debt.

As a result, consumers have placed more demand on traditional WAAP providers to provide comparable capabilities within a native cloud environment, so the WAAP market has seen a general trend or shift toward cloud-native integration and puts much less emphasis on appliances. What's more, the majority of vendors offering capabilities in the market have adjusted their service offerings to meet consumer demand while maintaining support for hybrid environments to accommodate applications irrespective of their hosted locations.

Product and solution offerings in the cloud WAAP market kept suffering from the same issues over the past several years, for example, generating an excessive number of alerts for consumers. Such a problem can happen even if a cloud WAAP solution is provided as part of a managed service.

Excessive false positive rates, the complexity of policy generation and the inability of cloud WAAP products to address more advanced threats that still plague modern web applications are just some of the concerns of the end-user community.

End users desire better methods of prioritizing discovered threats and vulnerabilities with automated, correlated and actionable recommendations for threat detection, policy generation and risk mitigations through the use of AI/ML behavioral monitoring and AI assistance or copilots.

As a result, many vendors are currently investing a great deal in R&D of ML models to meet these challenges. This won't completely solve the problem, though; even with more advanced ML techniques, false positive rates are still an issue. Whether or not technological breakthroughs such as LLMs, AI copilots and generative AI techniques will impact WAAP solutions, it is too difficult to predict and too early to tell.

Cloud WAAP Within DevSecOps

Cloud WAAP is generally managed and operated by the security operations side of the business, and sometimes there is a disconnect between security operations teams and development teams. Solutions like CNAPPs are designed to bridge the gap between development and security operations by providing both proactive and reactive sets of controls and visibility throughout the development life cycle and up to application runtime (see Market Guide for Cloud-Native Application Protection Platforms). Gartner considers the CNAPP market complementary to the cloud WAAP market.

A CNAPP provides insights into the whole process stretching from code development to the real-time, runtime behavior of a workload and the related applications. Because of their proximity to running applications, some CNAPP vendors with offerings providing network inspection capabilities have added basic WAAP capabilities to deal with the OWASP Top 10 web application security risks to their offerings.

Information security is constantly referring to the term “shift left” which describes a proactive approach to identifying and remediating vulnerabilities including web application and API vulnerabilities at an early stage of the development life cycle. This approach increases the accountability of code developers and emphasizes the hygiene of developed code in a CI/CD pipeline during an application development life cycle. However, if a solid development workflow is not put in place to proactively check and validate code, some code that may contain vulnerabilities can enter production environments.

Cloud WAAP’s primary purpose is to provide in-line protection for inbound traffic to running applications. Cloud WAAP is not designed to provide a correlated view of traffic security analytics with workload runtime visibility. Today, there is still a lack of correlation between anomalous traffic patterns and behavioral runtime analytics. Most cloud WAAP and CNAPP solutions do not share vulnerabilities and anomalous behaviors discovered by behavioral analytics, let alone compare, correlate and transform this information into actionable events. The lack of integration forces end users to funnel security logs from cloud WAAP and CNAPP environments into security information and event management (SIEM), security operations center (SOC) and security orchestration, analytics and reporting (SOAR) services in an attempt to correlate corresponding log information. This approach may require heavy log and report customization specific to an organization’s environment. Some vendors have identified this gap and are shifting to address it by combining WAAP with runtime visibility. [2]

After web application vulnerabilities are discovered by cloud WAAP or CNAPP runtime services, security operations teams are not generally responsible for rectifying these issues. It is developers’ responsibility to code and patch the discovered issues. The resolution process takes time, and the delta time between vulnerability discovery and patching puts vulnerable applications at risk if they are publicly exposed. During the delta time, the security operations team is expected to protect the application by implementing policies that affect the runtime operation of a workload within either cloud WAAP or CNAPP services to temporarily protect vulnerable applications until developers employ remediation measures. Essentially, cloud WAAP functionality can act as a virtual patching process until a permanent resolution is achieved.

A few cloud WAAP and CNAPP vendors have included distributed cloud WAAP capabilities in the CI/CD pipeline and started building distributed cloud WAAP services into application development processes. [3] A growing number of cloud WAAP vendors are adding deployment options to more automated cloud applications such as Kubernetes sidecars, containerized WAAPs and WAAP agents. This is an area where CNAPP offerings and cloud WAAP microenforcers will overlap in capabilities.

Cloud WAAP capabilities can be directly integrated at the host layer by:

- Pairing with the workloads within containers. This introduces containerized hosts or endpoint kernels or controller components within containers. This is a preferred method of adoption and can minimize the impact on the CI/CD pipeline.
- Adding ModSecurity plugins directly to web applications, which can be a popular open-source option.

Distributed cloud WAAP built into the CI/CD pipeline places capabilities such as WAF services at the host layer or at the container level could provide DevSecOps staff with guided help from capabilities such as dynamic application security testing (DAST) services when applications are pushed to production.

This approach can potentially bridge a significant operational and communication gap between the expectations of DevSecOps teams and application development teams by building security directly around published applications. It can provide visibility into preencryption runtime traffic, runtime WAF services and automation for the DevSecOps teams while minimizing the disruption of the CI/CD pipeline. However, this method can only support a subset of cloud WAAP capabilities and still lacks the feature set of a fully deployed cloud WAAP solution. The current recommendation is to keep CNAPP and cloud WAAP solutions separate until mature joint offerings are available.

Convergence of API Protection Products and Cloud WAAP

The capabilities of dedicated API protection products are overlapping with those of cloud WAAP platforms. This is caused by the fact that consumers want more aggressive API discovery, and threat detection and response capabilities to combine with traditional cloud WAAP capabilities.

Stand-alone API protection products protect web APIs from exploits, abuse and access violations. However, they generally lack the capabilities to protect against DoS attacks, which cloud WAAP solutions are able to do. Although all kinds of APIs can be protected, most organizations will initially focus on homegrown, public-facing APIs that provide connectivity to critical applications, especially aging APIs.

In some situations, an organization may prefer a point solution over a full cloud WAAP offering. Such a point solution can directly address specific use cases to mitigate risks. For example, an organization that takes an API-first approach to application security may need a specialized API runtime security solution for applications in a state of active development and containing critical API services. In such an instance, the organization is recommended to select a best-of-breed point solution on a short-term contract. It can sign a one-year deal with lock-in terms for second and third years instead of adopting a full cloud WAAP offering because the complexity of the combined cloud WAAP feature sets may generate heavy operational overheads.

Dedicated API protection services are mainly provided by emerging API security vendors that offer a more comprehensive and mature set of capabilities. However, API security functionality can be obtained as part of the expanded portfolio of offerings from vendors that provide API gateways, WAAP and application security testing (AST) services. It is possible that these markets will merge to provide better protection for running applications. Some vendor acquisitions and mergers have already happened. [4]

Evolving Threats to CAPTCHAs

"CAPTCHA" stands for completely automated public Turing test to tell computers and humans apart and is a security function that is mostly used on publicly exposed websites and for online services to distinguish between human users and automated bots. CAPTCHA services provide a defense mechanism whose objective is to prevent automated bots from interacting with websites. With such services, application owners can identify real user sessions from nonuser sessions and prevent nonuser sessions from interacting with their websites or applications. The CAPTCHA is a mitigation feature and a small subset component within the overall core bot management capability found in most mainstream cloud WAAP and CDN solutions and has been a staple capability for almost two decades. It should be noted that bot management extends beyond CAPTCHAs to provide additional and necessary features such as behavioral and traffic analysis, categorization, real-time monitoring, API protection and threat intelligence.

Bots that successfully access websites or applications are often programmed to scrape content, create accounts, post misleading information or perform other nefarious actions at scale. This consumes compute resources and poses a major risk to organizations. Bot management is designed to mitigate these threats, of which the CAPTCHA is a notable component.

However, CAPTCHA services need to evolve over time because advances in computer infrastructure, cloud infrastructure and ML have given threat actors the resources needed to create bots capable of beating CAPTCHAs at scale.

A recent study conducted by researchers from various institutes shows that humans take 3.6 to 42.7 seconds on average to solve a CAPTCHA with an average of 50% to 85% accuracy. The CAPTCHA's difficulty setting, the participant's age and the device that they use are also taken into account. Trained bots, however, take less than one second to 17.5 seconds on average to solve a CAPTCHA with an accuracy ranging from 85% to 100%, exceeding humans' accuracy range. What's more, they achieve an accuracy of 96% or above in most experiments. [5]

A number of assumptions can be made based on this research:

- Trained bots are vastly superior to humans when it comes to solving CAPTCHAs, and can effectively imitate real humans.
- CAPTCHAs have fallen behind modern bots in sophistication and are no longer truly effective in protecting against the most sophisticated bot attacks.
- Cloud WAAP vendors need to mature their own bot management services and introduce more advanced algorithms. They need to include AI/ML behavioral mechanics and analytics in a layered approach to meet the evolving challenge of telling humans from machines.
- Cloud WAAP vendors need more advanced endpoint validation methods which require identifying the source endpoint requesting web content and can determine if the session request is a genuine end-user device or an unsolicited machine impersonating a user endpoint (see Innovation Insight: Bot Management for the IAM Leader).

The study questions CAPTCHAs' value and prospects in the cloud WAAP market because CAPTCHAs can be beaten either by advanced bots or human-run CAPTCHA farms. Vendors should not rely on CAPTCHAs alone, and should offer broad and deep bot management capabilities that look at a range of signals such as Internet Protocol addresses, geographical locations, device profiles, user agents, traffic volume, and behavioral signals like navigation, mouse clicks and button presses. In this way, they can make risk-based decisions about displaying CAPTCHAs.

Consumers should understand that CAPTCHAs are not perfect. However, they should continue to leverage the CAPTCHA capabilities of bot management services in a way suitable to their organization's risk appetite as a defense-in-depth approach to protecting their web applications.

Consumers should select cloud WAAP providers that keep investing in R&D to make CAPTCHAs as resilient as possible. Cloud WAAP providers should gather signals during CAPTCHA-solving processes and solve discovered issues with advanced and mature capabilities such as proof-of-work challenges. In this way, they can augment their CAPTCHA services and punish identified bots with increased compute burdens.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

For the representative vendors listed here, Gartner uses client interactions, vendor briefings and analyst research to verify that their offerings represent examples of this market.

Vendor Selection

Table 1: Representative Vendors in the Cloud WAAP Market

(Enlarged table in Appendix)

Vendor Name	Product Name
Akamai Technologies	App & API Protector
Alibaba Cloud	Alibaba Web Application Firewall (WAF)
Amazon Web Services (AWS)	■ AWS WAF ■ AWS Shield
Barracuda Networks	Web Application Protection
Citrix	Citrix Web Application and API Protection Service
Cloudflare	Cloudflare Application Security and Performance Services
Edgio	Edgio Web Application and API Protection (WAAP)
F5	F5 Web App and API Protection (WAAP)
Fastly	■ Fastly Next-Gen WAF ■ Bot Protection ■ DDoS Mitigation
Fortinet	FortiWeb Cloud WAF-as-a-Service
Google	Google Cloud Armor
Imperva	Application Security
Indusface	AppTrana Cloud WAAP (WAF)
Microsoft	Azure Web Application Firewall
NSFOCUS	NSFOCUS Cloud WAAP
Penta Security	Cloudbric WAF+
Polaris	Polaris Web Application & API Protection
Radware	Cloud Application Protection Services
Reblaze	Cloud Native Web Application & API Protection (WAAP) Platform
Sucuri	Sucuri Website Security Platform
Tencent Cloud	■ Tencent Cloud EdgeOne ■ Tencent Cloud WAF
ThreatX	Cloud WAF
UBIKA	Ubika WAAP Gateway/Cloud Edition

Source: Gartner (November 2023)

Market Recommendations

Security and risk management leaders responsible for application and workload security must:

- Align the choice of cloud web application protection platforms with their security program mandates, risk mitigation requirements and architectural initiatives.
- For critical applications, establish the security requirements and priorities for each of their core, recommended and optional capabilities and features. Set desired evaluation criteria and develop measurable metrics to compare vendor offerings.

- Select the tool that provides the most granular visibility and reporting per application or workload and assists in the prioritization of remediation efforts.
- Prefer WAAP solutions that provide the ability to get inside an application, such as a container-based WAF that can leverage extended Berkeley Packet Filter (eBPF) to provide kernel- and network-level security visibility.
- Prioritize and test a cloud WAAP solution's core features that go beyond basic security testing runtime protection, including its ability to enable:
  - Automatic API discovery.
  - API threat protection and behavioral API anomaly detection.
  - Integration with your existing security monitoring and incident response processes.
  - Automatic suggested policy protection based on discovered vulnerabilities, such as AI copilots.
- Test and validate cloud WAAP solutions that offer generative AI and ML engines with established datasets to:
  - Correlate multiple events into actionable cases that improve detection rates, reduce the number of false alerts and prioritize remediation efforts based on attack path analysis.
  - Provide common language translations of both events and actionable cases.
  - Provide recommendations for policy rule generation based on discovery analysis or behavioral monitoring.
- For general security teams, prefer cloud WAAP offerings that can accommodate an on-premises strategy, even if the organization has only adopted a single cloud strategy. This should include options like the ability to load balance applications between cloud environments and support failover of applications on different cloud platforms.
- For DevSecOps teams, prefer cloud WAAP offerings that seamlessly integrate with existing security tools and have the capabilities to integrate with an application development life cycle where the cloud WAAP services become an integral step within a CI/CD pipeline.

- Ensure the vendor that you choose has a strong roadmap for integrating new security capabilities and features for protecting a native-cloud environment, and test these functions to validate that they meet your organization's expectations. WAF, DDoS, bot management and API protection are the core features of a WAAP solution today. But they may prove insufficient in protecting modern cloud-native applications from attacks.
- Prefer a point solution over a full cloud WAAP offering under certain circumstances. A point solution can directly address the niche challenges and specific use cases that your organization may have. For example, you may need to choose a point solution if your organization takes an API-first approach to application security.

Acronym Key and Glossary Terms

AI	artificial intelligence
API	application programming interface
AST	application security testing
bot	A software application programmed to do certain tasks
CAPTCHA	completely automated public Turing test to tell computers and humans apart
CDN	content delivery network
CI/CD	continuous integration/continuous deployment
CNAPP	cloud-native application protection platform
CWPP	cloud workload protection platform
DAST	dynamic application security testing
DDoS	distributed denial of service
DoS	denial of service
eBPF	extended Berkeley Packet Filter
IaaS	infrastructure as a service
JSON	JavaScript Object Notation
LLM	large language model
ML	machine learning
OAS	OpenAPI Specification
OWASP	Open Web Application Security Project
PaaS	platform as a service
POP	point of presence
R&D	research and development
SaaS	software as a service
SIEM	security information and event management

SOAR	security orchestration, analytics and reporting
SOC	security operations center
SQL	Structured Query Language
WAAP	web application and API protection
WAF	web application firewall
XML	Extensible Markup Language
XSS	cross-site scripting

Evidence

[1] Hundreds of inquiries that Gartner received about WAAP and cloud WAAP from end-user organizations were analyzed over the past 12 months between 2022 and 2023. The number of such inquiries increased by 5% year over year.

[2] A Cloud-Native Solution for Runtime API & App Protection, ThreatX.

[3] Web Application and API Security, Palo Alto Networks.

F5 Distributed Cloud WAF, F5.

[4] Akamai Technologies to Acquire API Security Company Neosec (a press release), Akamai Technologies.

[5] An Empirical Study & Evaluation of Modern CAPTCHAs, arXiv, Cornell University.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Hype Cycle for Workload and Network Security, 2023

Hype Cycle for Application Security, 2023

Market Guide for Cloud-Native Application Protection Platforms

Market Guide for API Gateways

How to Protect Your Cloud-Native Applications in Production

Table 1: Representative Vendors in the Cloud WAAP Market

Vendor Name	Product Name
Akamai Technologies	App & API Protector
Alibaba Cloud	Alibaba Web Application Firewall (WAF)
Amazon Web Services (AWS)	■ AWS WAF ■ AWS Shield
Barracuda Networks	Web Application Protection
Citrix	Citrix Web Application and API Protection Service
Cloudflare	Cloudflare Application Security and Performance Services
Edgio	Edgio Web Application and API Protection (WAAP)
F5	F5 Web App and API Protection (WAAP)
Fastly	■ Fastly Next-Gen WAF ■ Bot Protection ■ DDoS Mitigation
Fortinet	FortiWeb Cloud WAF-as-a-Service

Google	Google Cloud Armor
Imperva	Application Security
Indusface	AppTrana Cloud WAAP (WAF)
Microsoft	Azure Web Application Firewall
NSFOCUS	NSFOCUS Cloud WAAP
Penta Security	Cloudbric WAF+
Polaris	Polaris Web Application & API Protection
Radware	Cloud Application Protection Services
Reblaze	Cloud Native Web Application & API Protection (WAAP) Platform
Sucuri	Sucuri Website Security Platform
Tencent Cloud	■ Tencent Cloud EdgeOne ■ Tencent Cloud WAF
ThreatX	Cloud WAF
UBIKA	Ubika WAAP Gateway/Cloud Edition

Source: Gartner (November 2023)